Ovum
TMT intelligence | informa

Enterprise Case Study: Integrating Management of GRC across a Large Enterprise

How HCL helped a major US energy company to implement a comprehensive GRC solution

Publication Date: 30 Nov 2016 | Product code: IT0018-001509

Alan Rodger

Summary

Catalyst

The considerable increase in compliance-related burden across all industries is very real and has led to a well-recognized and sizable rise in related spending to deal with the greater scale of work required. Consequently, there are significant pressures for greater efficiencies in operational areas that deal with GRC, often conflicting with the growing scale of challenges. Implementing a GRC solution can achieve cost savings while improving practices, but is a substantial undertaking and requires a combination of technical, solution-related expertise and a vision of the realities of what can be achieved at a business level, and insight into how to get there.

Ovum view

Services partners, via a heritage of working with a range of customers' GRC-related requirements, can provide a highly valuable advisory role in successfully guiding major GRC programs. Leadership and commitment from within the client organization, to a shared vision and set of benefits, also represent a make-or-break factor in reaching this success. The proof of this assertion is explored in this case study, which has been supported and validated by a senior representative from the client team involved in such an implementation.

Key messages

- Outdated and fragmented risk practices are not fit to support most organizations' compliance needs.
- Piecemeal efforts are unlikely to reach the potential that is achievable via a visionary program.
- Consider strongly the value of establishing a GRC program approach supported by partner domain expertise.
- The potential risks from a misconceived or ill-founded change program must be mitigated as much as possible via well-advised planning and collaborative implementation support.

Recommendations for GRC industry participants

Recommendations for enterprises

Ovum advises enterprises to develop a vision of the benefits that broad organizational adoption of an integrated approach to risk management and compliance practices could deliver. Use this to decide on what GRC functions to implement, looking ahead as far as practicably possible in the context of strategy, current capabilities, and forthcoming change that is known. These requirements should be mapped against GRC solution coverage, taking into account the value of existing technology usage and its sustainability.

Recommendations for vendors

GRC solution vendors and providers of services resources should grow their collaborative partnerships toward extending best practices relating to GRC, pooling the knowledge gained from client experience to refine the ways in which major client objectives can be served most effectively.

Using a GRC solution to solve fragmented risk and compliance management

Setting the business context

Client requirements

Like many enterprises, the subject of this case study faces the challenge of complying with a number of demanding, intersecting regulatory requirements. Specifically, in its case, the national infrastructure program, North American Electric Reliability Corporation (NERC), as well as state-level regulation of utility operations, and state rules on energy market operations all require substantial corporate capabilities to deal with industry-related compliance, plus numerous other standards-related and legal obligations.

The corporate leadership team made an undertaking to improve and refine the GRC practices across the organization, to assure the company's corporate customers and industry regulators of the integrity of its compliance framework, and its adherence to industry standards. In order to best serve stakeholder interests, and rather than looking solely to gain per-regulation efficiencies in the compliance and risk management operations undertaken, the company needed to maximize opportunities for achieving synergy across risk and compliance-related operational practices that could be optimized and standardized.

Existing processes involved inefficiency and risk and were not adaptive to change

The business units in the corporate hierarchy were independent and isolated, using their own processes and practices around the management of corporate policies, compliance, and enterprise risk. The processes in use were overwhelmingly manual, with automation limited to a tool based on Microsoft SharePoint. Tasks involved in operating the manual process of reporting metrics and status were considered tedious for the individuals involved, and also involved laborious manual operations to collect the necessary approvals from other users in authority positions. Problems were known to arise from human error risk in this process, and from the very limited automation, as well as duplicate controls across different areas of the organization that entailed multiple assessments of the same criteria, and therefore repeatedly incurred unnecessary cost.

The role of ICT/services in solving the problem

Existing landscape and solution selection

A solution evaluation and procurement program started in September 2013, and was completed in January 2014. The scope of the solution evaluation was to meet requirements for IT-related GRC, although the selection process incorporated due diligence on whether the solution could feasibly support broader GRC requirements. RSA Archer was selected, and progress toward an initial

implementation began in June 2014, with a senior employee from a business unit in the company appointed to a senior IT role overseeing corporate applications. This person supported the potential of a GRC program to address a broader range of requirements, spanning the business problems with its compliance operations. While the early stages of implementation progressed, the new appointee attended a user summit for RSA Archer customers and gained useful insight from other customers, particularly “lessons learned” from broader implementations of RSA Archer involving multiple modules.

Support was gained from business stakeholders for an extended plan that would address a broad set of GRC-related requirements from across many areas of the corporate structure, using more of the capabilities of RSA Archer, and building on the initial IT GRC implementation, of which the first phase went live in October 2014. The program of work toward developing a new plan for the broader GRC program was started, with a vital stage recognized as being the establishment of a services partnership that would provide both technical expertise relevant to the RSA Archer solution, and understanding of the risk management and governance practices relevant to the energy sector and local regulatory environment.

The important high-level requirements for a services partner were established, and included the ability to analyze and recommend reforms to the current GRC processes, and to detail technical possibilities of automation using the RSA Archer solution. A formal request for proposals (RFP) was rolled out, and multiple vendors were asked to respond to its detailed requirements, including core audit firms (“Big 4” companies) and InfoTech service providers. A proper process of bid assessments was rigorously followed.

HCL was already established as a key service provider resource to the client, within an infrastructure-level partnership, and as part of the partner selection process for the broader program, references were provided by its customers for the capabilities of HCL’s GRC practice. These detailed the company’s expertise and work experience in GRC-related business unit areas, as well as in exploiting RSA Archer as an automation tool. Multiple demos were provided by HCL to prove these capabilities, and every individual that would potentially be assigned to the project was interviewed in detail to understand their technical and functional skills.

HCL demonstrated capabilities that appealed most on a number of levels, including:

- The availability of senior members from HCL’s GRC Center of Excellence holding key GRC process knowledge.
- The availability of senior technical members with inside-out product awareness of RSA Archer.
- Readiness to accept technical challenges to implement the solution.
- The value of domain intelligence that would help to perfect target processes and set future automation expectations.

The client organization committed to strong participation in deciding (often via multiple interviews of individual candidates from HCL’s resource pool) the team that would undertake its implementation program. Business users (usually from the “process owner” level within the organization) were assigned to the project, and they became involved in every phase of solution development. With client agreement, HCL adopted agile methodology, enabling end users to visually approve the build as part of a collaborative development process.

Bringing the strategy to life

Over time, the progressive implementation of requirements relating to different risk practices (see Figure 1) proceeded in a number of business entities within the client's corporate structure, supported by a growing number of RSA Archer modules. An initial exercise was performed to understand maturity in risk and compliance practices across multiple business units, and this informed the early establishment of a governance structure that properly reflected the enterprise hierarchy. The eventual result was a three-year GRC roadmap with executable project components that was presented to the GRC steering committee. The scoping and planning involved a broadening range of teams from multiple business units that needed to collaborate with HCL, including:

- For compliance management requirements: internal audit team, IT compliance team, and operational compliance team.
- For vendor risk management requirements: vendor management team.
- For IT risk management requirements: corporate IT risk team.
- For policy management requirements: teams representing corporate policy management, ethics and compliance, HR, accounting, retail, and supply chain management disciplines.

Figure 1: Implementation timeline showing graduation of RSA Archer capabilities used

Source: Ovum

Many businesses have been using RSA Archer, with the solution achieving integration of practices, standardized terms, and a common view of information. There is also good satisfaction with the benefits of automating processes, including the reduced timescales and complexity of reporting and approval procedures. The value of the multiple processes implemented by HCL using RSA Archer and the service provider's related GRC business-related capabilities has led to a view of the client having access to a "one-stop shop" for all GRC processes. Across almost the whole organization, compliance practices are now using industry-leading RSA Archer processes for their day-to-day activities, replacing the multiple legacy applications that entailed cumbersome processes to achieve the equivalent tasks.

The client has identified to Ovum that all benefits and requirements agreed have been delivered over the duration of the program.

Outcome assessment

The decision to base extensive risk-related capabilities on the RSA Archer solution was taken advisedly, and has been validated by the ability to extend the implementation within the client organization at a good pace, without any stumbling blocks.

This organization believes that HCL's capabilities have provided excellent support and guidance throughout extensive business change. In particular, HCL was able to "look ahead" before the client embarked on each major step of the implementation program, providing evaluation of ways in which any potential challenges could be met in advance. The client attributes much credit for a 50% saving

(compared to the original forecast) on the cost of the program to the capabilities that HCL has contributed throughout the multi-phase implementation.

Having seen delivery of all the major requirements planned to date, the client categorizes the major "soft" benefits achieved as follows:

- A "single version of the truth" of all risk and compliance-related information across multiple business entities and functional areas.
- Integration of risk-related information across risk types.
- The implementation of best practices, supported by application functionality, across a broad range of functional areas and across business entities in the corporate structure.
- A program approach enabled visibility of which foundational elements needed to be established to support onboarding multiple risk and compliance practices across different business entities.
- An enterprise view of risk and the related management capability (critically underpinned by a common taxonomy that enables standardization, as well as accurate collaboration and communication).
- Automation, delivering reduced inefficiencies.
- Greatly improved reporting capabilities and processes.

More than 1,000 users in different risk practices across a number of business entities now use RSA Archer.

Lessons learned

Collaboration must be supported by strong decision-making

With a large number of stakeholders across a range of practice areas and business entities, contention between priorities and different requirements can arise. While two experienced stakeholder representatives managed these issues operationally, the client instituted a strong governance structure for the program, headed by an executive steering committee and including HCL GRC advisory representation. Investment in a strong project management office (PMO) capability, allowing measurement and management of implementation of program-related decisions, is also seen as a success factor.

Technical and business expertise are both required for success

This client committed strongly to a vision of how the RSA Archer solution could enable a growth in maturity and scope of its risk and compliance management capabilities, and invested strategically in a services partnership with HCL to support the extensive organizational changes required. These key decisions were both based on extensive due diligence of how each could contribute to refining and delivering a vision of GRC transformation across this client's corporate structure.

Appendix

Methodology

Ovum Enterprise Case Studies leverage in-depth interviews with key enterprise stakeholders as well as a review of any available documentation such as strategic planning, RFP, implementation, and program evaluation documents.

Further reading

Assessing the Requirements for Enterprise Governance, Risk, and Compliance (GRC) Solutions, IT0018-001468 (April 2015)

Author

Alan Rodger, Senior Analyst, Infrastructure Solutions, Ovum IT

alan.rodger@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo