CASE STUDY

Barclays information risk management programme

Barclays is a major global financial services provider engaged in retail banking, credit cards, corporate banking, investment banking, wealth management and investment management services with an extensive international presence in Europe, the Americas, Africa and Asia. With 145,000 employees in over 50 countries, Barclays moves, lends, invests and protects money for more than 49 million customers and clients worldwide.

The risk management challenge

Barclays has a highly devolved risk management organisation, comprising a Group Information Risk Management function, a General Retail Banking central Information Management team and local risk management and information security teams in each business area.

Barclays has also built a new Information Management (IM) function to drive information risk management principles across the Global Retail Banking (GRB) businesses. The role of this function is to provide strategic direction and oversight support from the centre for the individual business units across the organisation.

John Theobald, Head of Information Risk Management at Barclays GRB, explains the challenge of managing risk,

> *"A key priority for the IM team was to measure and report on the status of information risk in a consistent and meaningful way across our diverse business. We therefore needed a solution to capture key risk indicators from multiple sources and provide business-oriented risk information for individual business units and an aggregated view of risk for central functions."*

The chosen solution needed to support a large scale risk and compliance management initiative across a very large and diverse organisation and a number of specific key objectives including:

- The collection of risk and compliance data objectively and consistently without expending an unreasonable amount of effort or cost.
- An ability to integrate with Barclays' internal policy and standards requirements (e.g. PCI DSS, ISO27001) and operational risk reporting processes (e.g. conformance testing, incident reporting and risk assessment); and to handle additional control requirements when needed.
- A simple approach to the capture of risk indicators and compliance statistics in a standard format in business units with different levels of maturity.
- Sufficient objectivity in the data collection process to empower business units to conduct self-assessment rather than requiring central audit-based assessment
- A structured reporting capability that could depict trends and performance statistics to encourage and record an ever-improving control environment.

The fundamental business driver behind these objectives was Barclays' desire to drive down the business costs associated with the aggregate effect of minor 'information incidents' and to significantly reduce the likelihood of significant incidents.

The Solution

Barclays selected **Citicus ONE**, a leading web-based risk and compliance management software product that uniquely bases its methodology for managing risk on 20 years of rigorous research, including detailed analysis of the most comprehensive data available on what drives key areas of risk up or down. Work began in 2008 to build a risk management process, based on the roll out of **Citicus ONE** risk management software to meet Barclays' objectives.

John Theobald said,

> *"Making compliance reporting 'business as usual' via **Citicus ONE** was the key to our success; we complimented the operational risk reporting framework and adapted the new initiative to integrate with the existing process. The embedded organisational hierarchy supported by **Citicus ONE** allowed us to model our existing IRM organisation, enabling us to report at different levels and assess risk holistically."*

Barclays' business units were engaged early and immediately gained the benefits of replacing an archaic Excel-based process with a web-based data capture tool. Outside of the UK, **Citicus ONE** was deployed by conducting a series of conference calls, walking through the completion of the risk scorecard and raising awareness of the product set – this typically took an hour to complete. The ability to do this without extensive site visits greatly reduced the cost of implementation.

Citicus ONE's multi-level reporting, from high-level executive summaries - to a detailed technical level, ensures that all Barclays' management are kept informed of the status of risk and compliance in their areas of responsibility.

An improvement in the risk posture of the organisation was realised in a short period of time, as the identified gaps could be rapidly tracked to closure. The risk indicators captured in **Citicus ONE** can be represented in different ways and shared with additional Operation Risk processes and product sets.

An important factor in the success of the project was that implementing **Citicus ONE** did not change the existing Operational Risk process but complimented it; sharing data reduced the amount of effort required to collect the information, improved quality and consistency through correlation. Where duplication or over-compensating controls were identified they were retired, allowing cost reduction and best of breed controls sets were shared with the rest of the IRM organisation.

The capture of risk and compliance information at Barclays is now streamlined and the process remains consistent month on month. It is no longer an arduous task for staff to collect the statistics and evidence every quarter, just a case of refreshing the data from the previous assessment.

The Benefits

As a result of this initiative, key risk indicators are now, for the first time, centrally held, enabling GRCB to map the overall risk landscape and allow the Executive to make informed decisions about their risk appetite and where to apportion investment. It is now possible to use a consistent approach to identify risk pressure points and conduct risk and compliance trend analysis, making the best use of resource and investment for any proposed remediation work.

John Theobald said,

> *"We have moved from a position where it was difficult and time-consuming to identify significant risks across the enterprise to a state where we can set strategic plans making optimum use of resources and budget which is very important in the current financial climate.* ***Citicus ONE*** *has helped to define our strategy for the next year and prove that we are serious about the protection of our Information Assets which is important for stakeholders, customers and regulators alike. Our approach has allowed us to assess compliance against the policies and standards and drive remediation activity in a way that has been largely seamless to the business community."*

Barclays business units appreciated a common approach to the capture of risk indicators and were excited about the prospects of sharing this data for different purposes, adding value to their business by increasing control. The audit and operational risk community gained comfort from the clear evidence that the business units were managing and treating risk efficiently.

John Theobald added,

> *"Where businesses do not have information risk management representation we have empowered nominated business managers to collect this information, improving awareness of the company's policies and standards. All areas within IRM have matured and discussions about risk management are now at a different level – no longer are the business units afraid to report weaknesses in their control set as there is now more openness and transparency.* ***Citicus ONE*** *is integrated in the overall operational risk framework and recognised as de-facto standard for capturing and risk and compliance statistics."*

Looking forward

Now all risk assessment activity in Barclays GRB is moving to the process based on **Citicus ONE** as it has provided us with a scalable, consistent and proven method to capture, measure and report risk. This has resulted in the elimination of many archaic and cumbersome methods of capturing risk indicators.

Barclays are also extending this approach to areas beyond information risk and the flexibility of the approach has lent itself for specific control risk assessments such as mergers and acquisitions activity. The strategic direction will now expand to employ **Citicus ONE** to other risk entities such as Compliance, Business Continuity and Physical security.

For more information, contact:

Simon Oxley, Marco Kapp or Sian Alcock, Citicus Ltd, Tel: +44 (0)20 7203 8405 email: info@citicus.com.