



Royal Bank of Scotland – Taking data security to a new level

Executive Summary

In common with most global organisations, The Royal Bank of Scotland Group (RBS) depends on a large and extended network of business partners, third parties and customers. This extended enterprise environment presents a number of risks for such organisations.

RBS were aware of an ever increasing number of emerging risks and concentrated regulatory focus on data security. Given the changing environment and increased threat of data loss, RBS were determined to remain at the forefront of the financial services industry's response to data security and engaged KPMG to help them demonstrate their approach externally across the industry.

KPMG did this by mobilising a global team of over 400 individuals in just a few days, setting up operational hubs in four regions and creating a dedicated call centre in South Africa.

In the space of five weeks, KPMG carried out comprehensive reviews into the data security of 360 of RBS's third parties. As a result of this programme, RBS were able to demonstrate their continued focus and robust approach to data security.

How we made a difference

KPMG engaged its global network of technical specialists and programme management experts to ensure that the programme was mobilised within hours of initial contact with RBS. KPMG adopted a rigorous approach from the outset, including clearly defined screening to meet RBS requirements and review processes which are now becoming recognised as the industry standard.

Problem/opportunity faced by the client

In August 2008, RBS initiated a programme of work to gain a better understanding of the risk position relating to third parties and to gain comfort that robust data security controls were in place across their third party organisations to reduce the risk of data security breaches.

This programme was given the highest level of priority by the RBS Senior Executive. With thousands of third parties around the world, RBS would initially have to identify all high-risk third parties and then carry out a comprehensive data security review of them.

Project background

In mid September 2008, KPMG was asked to advise RBS how we might carry out data security reviews. All RBS third parties had to comply with a number of policies and procedures relating to data security. Ensuring adherence to these policies and procedures was proving to be very difficult

and RBS were therefore looking to implement a methodology which would manage and monitor this more effectively.

The initial objective was to identify and thoroughly assess 360 high-risk third parties within a six month timeframe and then produce reports that would satisfy the Bank's Senior Executive of their third parties' adherence to the Group's information security policy.

Shortly after the programme started, timescales were reduced to five weeks to complete the 360 data security reviews. This change reflected the priority which the RBS Senior Executive had placed on this programme of work.

As part of our brief, we were also asked to work with RBS to implement a standard process across the Group for ongoing data security reviews and assessments of any new and existing third parties.

The third parties encompassed a wide range of organisations located around the world, from sole traders to multinationals, including bank statement printers, computer hardware providers, publishers, payroll processors, cash logistics firms, security companies and lawyers. All of these had access in some way to confidential RBS customer data and their level of adherence to RBS policies had to be reviewed.

Consulting activity

The logistics of the programme meant we had to set up operational hubs in four locations: UK, Europe, US and Asia, quickly mobilising security, IT audit and risk management specialists from across the globe. We also created a dedicated call centre operation in the KPMG South Africa office, to carry out telephone interviews and to schedule appointments. Every team member had to undergo training on the programme procedures, as well as pass rigorous security screening to qualify them for work on a RBS engagement.

KPMG worked with RBS to resolve issues such as access to third parties, but we took full responsibility for the scheduling and performing of the data security reviews. On starting the programme, it became apparent that we would also have to focus on implementing a robust process which would ensure that up-to-date, detailed information could be recorded for each third party. RBS would then integrate this approach into its business as usual operations environment.

Due to the size and complexity of RBS as an organisation, there is always a risk that third parties and associated relationship managers will change and the risk classification of the data being handled by third parties may vary. Given the number and geographical spread of third parties, the list of third party organisations was understandably complex and our first task was to therefore create a third party list which would be manageable for years to come.

Stage 1: telephone interviews

Calling upon our industry knowledge of data security processes and using existing RBS documentation and policy requirements, RBS and KPMG implemented a strict list of criteria that the client's third parties were expected to satisfy. We then called each third party to schedule a telephone interview. The data complexity made this a lengthy process involving several thousand calls. In some cases the third party was unwilling to speak with us, so we had to present a strong case for how such a review would benefit them.

Even those third parties who no longer had a relationship with RBS had to provide assurance that they had fulfilled any contractual requirements on termination, and had disposed of any data satisfactorily.

The telephone questionnaire assessed the overall level of data security risk posed by a third party, uncovering the role they performed and the type of data they held. It was hoped that these calls would help screen out a large number of organisations as low-risk, and therefore not worthy of a site visit. However it quickly became clear that the information gained from these interviews was not sufficient to make such a judgment, which meant that every single third party on the list had to be visited by KPMG.

Stage 2: site reviews

These involved a detailed one-day assessment of a third party's information security controls and practices. We had to organise and carry out visits to third parties in over 50 countries around the world, including Argentina, Colombia, the Dutch Antilles, Tunisia, Indonesia, Chile, Pakistan, Liechtenstein, China, Uruguay, Venezuela and Kazakhstan.

The programme entailed making full use of the entire network of KPMG member firms, with over 400 individuals being mobilised at incredibly short notice, all arranged through the four regional operational hubs, as well as employing a dedicated South African Call Centre which would prove invaluable to this 24/7 operation.

When on site with the third parties, the KPMG assessor requested hard evidence of their security controls and procedures to note whether RBS policies were being adhered to. The effectiveness of the high level controls was also assessed. On completion of a review, we delivered a detailed report to RBS covering all our findings, including suggested remediation activity where appropriate. We then worked with RBS to complete a robust and detailed quality review of the reports, before submitting to RBS Senior Executive for sign-off.

The final reviews naturally showed gaps in some third parties' controls and procedures. We supported RBS's own security consultants to co-ordinate remediation activity, recommending how to improve data security controls and to ensure a third party's adherence to RBS policy.

Success factors and challenges

- RBS's determination to be the leaders in data security and management. It is setting the standards across financial services and is at the forefront of industry thinking and innovation around this subject.
- KPMG's market leading position which contributed to thought leadership and emerging industry standards.
- KPMG's established global network of technical specialists and programme management experts which enabled a quick mobilisation onto the engagement.
- A 24/7 delivery capability was implemented through the use of KPMG regional operational hubs and a dedicated call centre, to ensure that the programme's deliverables were achieved on time and within budget.
- A global programme management team which has the knowledge and experience of how to deal in this environment, through their globally distributed team.
- A 'can-do' attitude was demonstrated from the outset by the global KPMG team – examples included the speed of mobilisation, the amount of time invested by all team members on the programme, the integrated communication channels which were established between KPMG and RBS and the positive feedback obtained throughout the engagement from key client stakeholders.

- KPMG understood the need to develop a clearly defined and robust process which had to be integrated easily into the bank's business as usual operations for all future third party supplier data security reviews.
- KPMG's recognition that a clear and simple reporting process was required, in order to provide RBS with the necessary metrics to monitor progress throughout the programme and to ensure escalations/ issues were highlighted and resolved as early as possible. The reporting tools also needed to be integrated with RBS systems at the end of the engagement for business as usual supplier reviews.
- KPMG's risk based approach which allowed RBS to obtain a detailed understanding of the risk position associated with third party suppliers. This has subsequently led to the Security and Risk division leading the way in determining the requirements for a future-state operational risk framework and enabling a process of *continuous improvement* across the division.
- The output of the programme has now been embedded across the RBS Group and has resulted in a more robust understanding of third parties' criticality and risk.

Client/consultant relationship

The RBS Security and Risk Division had little history of working with KPMG. They were initially impressed by our swift mobilisation and the strength of our global team which was pulled together in a matter of days.

Our ability to meet the tight deadline of five weeks to complete 360 data security reviews was actually achieved with 24 hours to spare. This was an incredible team effort and an excellent example of the strong relationship which was forged between the RBS and KPMG programme teams.

KPMG's robust approach and proven methodology was sufficient for RBS to award us the second phase of work – a further 500 data security reviews over an eight week period. The timely delivery of the reviews and the integrated approach adopted by the global programme team has resulted in further work between RBS and KPMG in the data security area following on from this programme.

“We have moved from a blank sheet of paper to being recognised as industry leading in third party security in the space of five weeks.”

Emma Smith, Head of Group Information Security, Royal Bank of Scotland

Jason Davey, Director of Security and Payments, Policy and Assurance, Royal Bank of Scotland