PCI DSS and Gambling Commission RTS Case Study

Woods Group

BACKGROUND

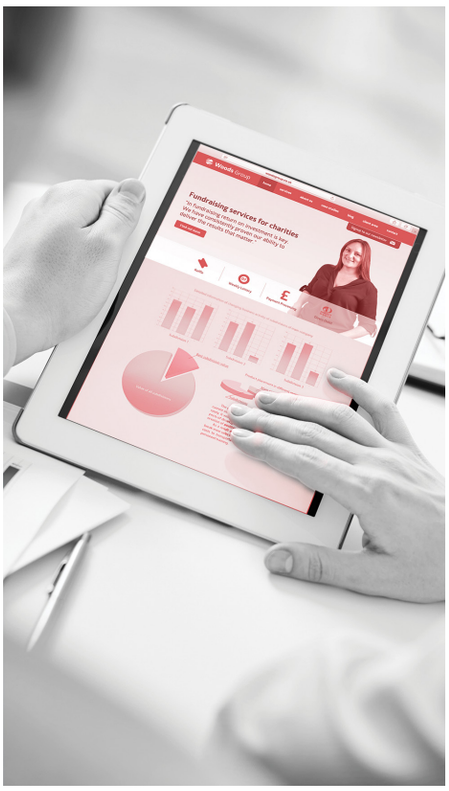
Founded in 1998, The Woods Group Limited (Referred to as both WGL and Woods) has established itself as a market-leading specialist in providing fundraising services for charities. Working with over 50 charities to help raise over £100 million in fundraising, Woods' services include raffles, weekly lotteries, payment processing and direct debit management. Woods 90-strong team of specialists is totally focused on the charity sector and has built excellent long term relationships with its clients, boasting a 95% retention rate.

Trust is at the core of client relationships and Woods has developed a reputation for its market leading approach in terms of strong governance and compliance with different standards. As it processes a number of payment card transactions, a key standard which Woods needs to comply with is the Payment Card Industry Data Security Standard (PCI DSS). In addition to this and as a remote operating licence holder (External Lottery Manager), Woods is required to comply with the Gambling Commission's Remote Gambling and Software Technical Standards (GC RTS). The security requirements for the GC RTS are based on a subset of ISO/IEC 27001:2013, the International Standard of Information Security Management.

This case study addresses how Woods, having identified a programme of process and internal system changes, not only achieved compliance with both Standards, including being externally assessed, but managed to do it in a very short and challenging timescale. The process not only brought about significant business change and benefit, but also established a strong platform for future growth. Starting in December 2014, Woods managed to achieve compliance (verified by an external assessment) by May 2015.

Business Drivers

Woods has always set itself the highest internal standards in terms of governance and compliance and has developed a reputation as market leader and standard bearer in the charity fundraising sector. In 2014, Woods planned a number of internal process and system improvements and conducted a review of its current information security and compliance status. It also set itself the challenge of going one step further than was required from a compliance perspective. Not only did it want to lead the market, but also wanted to provide its clients with the ultimate in reassurance around the protection of their data and their supporters' data.



PCI DSS

In terms of the number of payment card transactions, Woods was only required to complete a self-assessment questionnaire in order to comply with the PCI DSS. However, in order to be able to demonstrate its level of compliance in a more robust and transparent manner, it made a conscious and proactive decision to seek a Level 1 assessment by a PCI qualified security assessor (QSA) organisation. With its planned future growth and an anticipated increase in the number of payment card transactions, Woods also wanted to reassure itself and its clients that it was following best practice both in terms of technical and policy/process controls.

Gambling Commission RTS

Following changes in industry regulation, Woods was now required, by the Gambling Commission, to achieve compliance to GC RTS within a specific timeframe.

KEY STAGES

Selecting Partner

In order to achieve compliance with both PCI DSS and GC RTS, Woods decided to seek the support of a third party specialist and went through a selection process that involved short listing and meeting three potential suppliers, one of which Woods had engaged with previously. As Ian Scarr, Woods' Managing Director explains "Ultima Risk Management (URM) was selected for a number of reasons. Firstly, it was felt that URM demonstrated the greatest understanding of Woods and the day-to-day pressures that existed, and exhibited a similar mind set and values to Woods, instilling confidence from the outset. The second key factor was that URM was prepared to spend a day on site providing a high level data flow analysis conducted by one of its senior consultant QSAs. In the process, URM was able to demonstrate a commitment to the project and its compatibility and fit in terms of project approach and personnel. With hindsight, I can unequivocally say that we definitely picked the right partner!"

PCI Data Flow Analysis

A key aspect of any PCI DSS compliance project is to identify the flow of payment card data through the organisation and to determine which parts of the organisation's network, infrastructure and systems are involved in processing, transmitting or storing cardholder data. URM's QSA consultant was able to support Woods by mapping the payment card data flow, both within the existing operational environment and clearly setting out how, by making changes to the Woods environment and modifying the data flow, additional security benefits could be derived. Ian Scarr also adds "URM's QSA was also mindful of our strategic growth plans and presented a number of considered options which addressed not only the current environment, but also accommodated our anticipated growth."

Gap Analysis and Scope Setting

A gap analysis was conducted and URM helped Woods to formulate an ambitious but realistic and achievable plan to fulfil the corporate objectives and implement the requirements of both Standards in parallel and, in doing so, manage aspects involving considerable cultural change. Whilst it was feasible to run both compliance requirements as separate project streams, URM pointed out the considerable overlap and suggested that both streams could be integrated as one single, coherent process. As Barry Dix, Woods Finance Director, explains "This is an area where URM undoubtedly added value. Understanding the impact it would have on us, URM suggested that we approach both Standards as a single compliance project, ensuring all staff understood the reasons for change and linking it to a central compliance and framework improvement message."
A key aspect of PCI DSS was reducing the scope of the technical controls to only those systems that store, process or transmit cardholder data. URM provided practical advice and guidance on the ways to achieve this segmentation, without restricting future growth plans.

Technical Remediation Workshop

In order to address gaps identified, a workshop was organised with a representative from Woods (IT Manager), URM (QSA Consultant) and Wood's IT Solutions Provider. This three way collaborative workshop proved highly effective in producing a project and requirements specification.

Project Management

Woods benefitted from access to URM's specialist project management resources and skills to break down a sizeable project plan into four sub projects and consolidating work packages. URM implemented a practical level of project governance and baseline documentation to enable speedy progress and manage associated risks and issues. As Ian Scarr describes "Recruiting the URM Project Manager was without doubt, the best money spent. Her unwavering commitment, energy and enthusiasm carried us through and we are both grateful and indebted."

In order to meet the aggressive project deadlines, weekly meetings were held and attended by Woods senior management team members, including Managing Director, Finance Director and department heads. Within the weekly meetings and with the primary aim of addressing project governance, it was possible to discuss and tailor proposed policies and processes, along with managing ongoing staff communications.

Policy and Process Development

A key stage of the project was the development of policies and processes which met the requirements of PCI DSS and GC RTS, whilst at the same time being appropriate to an organisation of the size of Woods. As Ian Scarr explains "The policies and processes formed the umbrella framework over the organisation. They provided the catalyst for change, as well as providing the structure for growth. The processes brought a greater degree of formalisation to all operations and in particular IT."

PCI DSS Assessment and Report on Compliance

In order to prepare Woods for its formal PCI DSS Report on Compliance (RoC), URM conducted a pre assessment review, a 'dummy run' which Ian Scarr describes as "Very helpful and comforting, and provided a robust view of what had been done and what was left to do. As a result of all the preparation, the actual RoC was very straightforward."

KEY SUCCESS CRITERIA

Quite simply, URM's Project Manager made the project happen. As well as bringing subject matter expertise, her drive and energy were invaluable

Ian Scarr
Managing Director, The Woods Group Limited

URM's Support

When selecting URM as the partner for the project, Woods was able to benefit from the strength and depth of the team it could call upon, including QSAs, technical specialists to work with the IT Department and, not least, a project manager. Woods identified that with the amount of change they wanted to achieve in the timescales identified, it was essential to assign a project manager. Ian Scarr believes that URM's Project Manager played a pivotal role in the success of the project explaining "From day one, she adopted a hands-on approach and led from the front and quickly gained the respect of all staff with her unwavering commitment and work ethic. Such was her involvement by the end of the project, she was well known by all members of staff and was considered a member of the Woods team rather than an external resource. Quite simply, URM's Project Manager made the project happen. As well as bringing subject matter expertise, her drive and energy were invaluable."

Leadership and Resource Commitment

Leadership commitment was most clearly evidenced by the weekly senior management team (SMT) meetings, the detailed review of proposed changes and documents and regular communications. Despite day-to-day 'business as usual' pressures, the SMT always allocated time and made a member of the Team accessible as required.

One of the most critical success factors was Woods' ability to appropriately prioritise project activities within the constraints and demands of day-to-day business, recognising the benefit of short term effort investment required to achieve long term gains.

Deadlines

Working to such a tight deadline helped to maintain the focus and momentum of the project and ensure improvements were implemented without delay.

Alignment to Business Objectives

A key success criteria was the close alignment of the project, with strategic business goals and their clear communication. All staff could understand and identify with the purpose of the project and the benefits it would deliver to Woods and its clients.

Staff Attitude

Despite the operational challenges presented by the project, both in terms of deadlines and change, with the strong sense of purpose established by the SMT, Woods staff across the business engaged in the project with a high level of commitment, support and understanding. Consequently, Woods staff quickly embraced and achieved both cultural and operational change.

BENEFITS DERIVED

Enhanced Governance Framework

Ian Scarr believes that the overall framework established was one of the major benefits and legacies from the project, as he explains "Not only did it help us meet the requirements of GC and PCI DSS but provided us with a more formal structure to manage the business more effectively on an ongoing basis and provide a platform for growth. Since its implementation, the framework has been proactively used by the Management Team to manage and steer the Company on both a day-to-day and strategic basis."

Embedded Policies and Processes

Woods was successful in making pragmatic and practical policy decisions and embedding policies to make them a living and breathing reality; with documented processes serving as functional tools to baseline and manage performance.

Strengthened Network Infrastructure

The investments involved in achieving the compliance requirements delivered improvements across Woods' network infrastructure, beyond card processing and gaming infrastructure and helped build overall resilience.

Greater Maturity of Security Controls

The impacts of the project were broad reaching and improvements in security controls were realised across multiple domains, including human resource security, asset management, access control, physical and environmental security, supplier management and business continuity. The risk based process shone a light in all areas for Woods and provided a basis to identify where effort, resource and investment was best deployed.

Reassuring Clients and other Interested Parties

By going the extra mile and achieving PCI DSS Level 1 compliance alongside GC RTS, Ian Scarr believes that "Woods has been able to provide evidence of adopting internationally recognised best practice and substantiate its long standing commitment to protecting both its clients' and their supporters' information and to deliver continual improvement." Ian goes on to say "Our investments resonate extremely well with our clients, demonstrating that we understand that we have responsibilities for protecting their donors and supporter's information and that compliance is at the heart of our business."

Staff Development

In adopting a formal information security management system approach to manage both PCI DSS and GC RTS compliance, Woods consciously devolved responsibilities across the business to manage and maintain the management system. In doing so, Woods created opportunities to extend and develop a number of employees' skills in information security management and enhance their existing roles.

Winning New Business/New Clients

As Ian Scarr confirms "The work we have put into strengthening our information security and achieving compliance with key standards has been not just well received by existing clients but also by prospective clients. Without question, our commitment to achieving compliance above and beyond the requirements of an organisation of Woods' size has benefited us in responding to bids and in winning new clients."

> *"Without question, our commitment to achieving compliance above and beyond the requirements of an organisation of Woods' size has benefited us in responding to bids and in winning new clients."*

Ian Scarr
Managing Director, The Woods Group Limited

Woods Group

For more information on Woods' services:
T: 01249 653444 **E:** enquiries@woodsgroup.co.uk
W: woodsgroup.co.uk

URM
ULTIMA RISK MANAGEMENT

For more information on URM's consultancy services:
T: 0118 9027 450 **E:** info@ultimariskmanagement.com
W: ultimariskmanagement.com