JAMES HAY
PARTNERSHIP

BACKGROUND

James Hay Insurance Company Limited (trading as James Hay Partnership and herein after referred to as JHP) has evolved into a leading platform provider in the retirement and wealth planning market, supporting clients and their financial advisers with specialist services and flexible, competitive products, including its Modular iPlan. JHP forms part of the IFG Group plc which is a focused financial services company with full market listings in London and Dublin.

The vast majority of JHP's 600 strong workforce are based at its Head Office in Salisbury and office in Bristol, with other support staff based at Milton Keynes, Swavesey (Cambridgeshire), London and Glasgow.

In March 2015, JHP achieved certification to ISO 27001, the International Standard for Information Security Management. This case study examines the reasons why the Company sought certification, as well as some of the key stages of its journey to certification and the benefits that have been derived.

Business Drivers

For many organisations, the business drivers behind achieving ISO 27001 certification are externally based e.g. mandated by customers. This was not the case with JHP, where the motivation was driven from a desire to build on its existing strong controls and to continuously improve its information security practices through more centralised management. As an organisation within the financial sector, JHP is heavily audited by its larger clients and the Financial Conduct Authority (FCA), as well as undertaking internal audits overseen by IFG. As information security processes were being constantly audited, JHP made a conscious decision to adopt a more proactive 'front foot' approach. The initiative stemmed initially from the IFG IT Director, who appointed Jonathan Shehan as Information Security Manager and tasked him to oversee the certification project.

> *JHP made a conscious decision to adopt a more proactive 'front foot' approach.*

KEY STAGES

Setting Certification Scope

Following a high level health check from Ultima Risk Management (URM) in December 2013, which helped set out a roadmap and clarify the key steps required to gain ISO 27001 certification, the first key decision was to determine the scope of JHP's information security management system (ISMS). Whilst various subsets of the organisation were considered, it was decided to certify the whole organisation in order maximise the value from the process and avoid having to set potentially tricky internal boundaries.

Risk Assessment

With guidance from URM on the risk assessment methodology to be adopted, Jonathan Shehan conducted risk assessments across all JHP's major business processes in February and March 2014. In developing the information security risk management system, Jonathan was careful to integrate the Company's existing risk approaches such as established impact scales. Utilising URM's risk assessment tool, Abriska, JHP accounted for threats, controls, impacts and likelihoods and used the outputs to create a risk register and develop a risk treatment plan (RTP). This plan is reviewed every quarter to drive the remediation activities.

Policy and Process Development

A key activity in the journey to ISO 27001 registration was the rationalisation and prioritisation of information security related policies. As Jonathan Shehan explains "Over a period of time JHP had acquired a significant number of policy documents, many of which were inconsistent and had been developed in response to client or audit requirements.
A major task for the Company was to rationalise the number of policies and get them approved internally. In terms of embedding new and updated policies, this was achieved by department managers cascading key messages to their staff and reinforced by me doing walkabout audits and checking on the adoption of policies such as Clear Desk and Clear Screen. The Clear Screen Policy was further consolidated by the introduction of 10 minute auto lockouts. Within the IT Department, a comprehensive strengthening exercise was also undertaken to ensure all processes performed were underpinned and governed by security policies."

JHP adopted a similarly robust approach when reviewing the maturity of information security related processes. A goal was to ensure all key processes, such as asset management and starters and leavers processes, achieved a maturity level of at least 3 or 4 out of 5. Jonathan Shehan prioritised those processes supporting the most critical business functions to ensure completion in a timely fashion. As Jonathan explains "Our goal was to raise the bar and try to achieve greater consistency and repeatability across all security related processes."

ISMS Development

An important requirement of ISO 27001 is for the organisation to continuously review and develop its information security practices and information security management system (ISMS). Within JHP, a dedicated Information Security and Cyber Crime Committee (ISCCC) was established to fulfil exactly that role. As Jonathan Shehan explains "Prior to ISO 27001 being implemented, information security had been an agenda item on Group Committee meetings but now it has a formal committee in its own right". The ISCCC with its cross-function representation meets, and is chaired by JHP's CIO. Amongst other items, this Committee discusses annual objectives, reviews internal and outsourced audit reports, reviews incident reports, approves policies, considers resourcing (e.g. local security champions) and awareness programmes." Information security is also discussed at the IT Ops Committee, which meets quarterly. This Committee also has representation from all major functions areas of the business such as Sales, Finance, Risk and Administration. Jonathan Shehan adds "Between the 2 committees, we are able to ensure that the profile and awareness of information security remains high throughout the whole company."

The focus of JHP's ISMS is not just inward looking. Aside from setting internal information security objectives, JHP also formally reviews and monitors its key suppliers. Suppliers were initially assessed and prioritised from an access to sensitive information perspective e.g. outsourced service providers carry more risk. Following this prioritisation and in recognition of the benefit and value of certifying one's ISMS, suppliers are now checked for ISO 27001 registration. Where suppliers were not registered, a programme of formal risk assessments was started.

Stages 1 and 2 Assessments

JHP selected Certification Europe as its certification body due to the fact it provided the clearest instructions on what was expected at both Stage 1 and 2 assessments. In terms of preparing different parts of the business for the Stage 1 assessment, Jonathan Shehan produced a 15/20 item checklist for the various heads of department to check that all staff were fully complying with key policies and processes.

SUCCESS CRITERIA

Management Buy in

A major factor in JHP's successful ISO 27001 implementation was the support and commitment demonstrated by senior management within both JHP and at group level from IFG. Having Board representation on the ISCCC for example, ensured that information security was given the highest profile and that the ISO 27001 implementation project was fully resourced. With such strong leadership commitment, none of the staff were or are in any doubt that protecting business information was a key business priority and that everyone needed to adhere to identified policies and processes e.g. Clear Desk and Screen Policy.

Information Security Champion

Appointing an information security manager and champion was undoubtedly a pivotal decision by JHP in ensuring the ISMS was fully embedded and policed. Whilst having senior management support was key, JHP also acknowledged the importance of having one individual who was accountable for establishing the ISMS framework, encouraging and monitoring the various departments to ensure universal adoption of working practices and generally maintaining the momentum of the project. Other key roles included writing policies and representing information security on the ISCCC and IT Ops committees. Jonathan Shehan describes his role as being "the glue keeping everything together."

Setting Deadlines

Setting a deadline of achieving ISO 27001 certification within JHP's financial year was seen as beneficial in ensuring that the project momentum was never lost, as well as keeping everyone focussed on achieving a widely recognised key business objective.

URM

URM provided a 'light touch' advisory service throughout the project. With its extensive track record assisting organisations to achieve certification and understanding of the expectations of certification bodies, URM was able to provide clear direction and guidance.

> *I was most impressed by URM's flexibility, understanding of our organisation and ability to provide insight and support appropriate to JHP.*
>
> Jonathon Shehan - Information Security Manager

Early in the implementation, URM was able to help define the risk assessment methodology and use its risk assessment tool Abriska to produce the outputs which formed the basis of the ongoing RTP. As JHP moved into the risk treatment phase, URM visited periodically to review outputs and deliverables and ensure the Company was 'on the right track' and assess whether the requirements of the Standard were being fully met. As Jonathan Shehan explains "Having a vastly experienced organisation to provide advice and guidance was invaluable to us in achieving certification. I was most impressed by URM's flexibility, understanding of our organisation and ability to provide insight and support appropriate to JHP."

BENEFITS DERIVED

Strengthening of Information Security Practices

Whilst JHP has always been an information security aware organisation, it benefitted from more centralised management as well as a greater degree of formalisation and documentation of key policies and processes e.g. Clear Desk and Screen Policy, where all staff now adhere to the Policy and understand why it is there. Improvements have also been noted in physical security, where access to certain areas have been further tightened. HR processes have also been strengthened where the new starters induction programme now includes a substantial information security component and where there are greater controls over contractors e.g. requiring them to sign the Company's Acceptable Use Policy.

Enhanced Information Security Culture

In addition to the new starters induction programme, staff now receive regular on-line training covering topics such as data protection, incident reporting and the importance of IT security policies, ensuring that electronic data across the organisation has mandatory security controls and processes. With the increased training has come a heightened awareness culture and greater transparency. Jonathan Shehan comments "Where in the past many incidents would have gone unreported, the Company now has far greater visibility of events, incidents and emerging trends. I am now regularly asked questions such 'Is this a security issue?' or 'What needs to be done from a security perspective?' Another indicator of the developing culture is the fact that information security now has its own and dedicated Committee."

Reassuring External Interested Parties

As soon as registration had been achieved, a copy of the ISO 27001 certificate was sent to fund managers, independent financial advisers (IFAs) and the Financial Conduct Authority (FCA), providing them with tangible evidence of not just JHP's commitment to protecting information but to the process of continual improvement. As well as providing reassurance to existing interested third parties, it has also made due diligence activity and the preparation for external audits a lot easier.

Gaining Competitive Advantage

Having secured certification to ISO 27001, JHP now has a significant market differentiator when dealing with prospective clients. New clients can be reassured that any sensitive information is likely to be protected with more effective controls, following JHP's robust and audited risk assessment process.

Identifying Emerging Threats

The ISMS framework and dedicated IS roles have created a central focus point for the review and assessment of emerging threats (e.g. cyber fraud) on a continual basis. Given the ever changing landscape and nature of cyber crime, having a dedicated and centralised function reviewing all risks instils confidence that such threats will be addressed appropriately and not 'lost in the ether'.

NEXT STEPS

In line with the central ethos of ISO 27001, JHP's focus is totally committed to the continual improvement and refinement of the ISMS. A significant contributor to continual improvements is the annual information security risk assessment and resulting risk treatment plans with quarterly activity lists. The status of control maturity is continually reviewed by the ISCCC. Jonathan Shehan comments "Following certification, JHP set about a programme of activities to further raise information security awareness, including the appointment of local IS champions, particularly in remote locations. Intranet sites are also being developed to facilitate easier incident reporting in line with the Company's open and transparent culture. There is also an ongoing trend for JHP to embrace information security as 'business as usual' and for JHP to stay on the front foot."

JAMES HAY
PARTNERSHIP

T: 03455 212 414
E: JamesHay.Sales@Jameshay.co.uk
W: www.jameshay.co.uk

URM

For more information on URM's consultancy services:
T: 0118 2065 410 **E:** info@urmconsulting.com **W:** www.urmconsulting.com