Supply Chain Due Diligence – a Case Study

How INONI improved governance and reduced cost

The Company

Our client sponsor is CISO (Chief Information Security Officer) for a well-known specialist insurance and financial services provider. His role covers all aspects of business and technology security, resilience and continuity. The organisation has been in existence for over 100 years and now provides award-winning ethical services to a range of different client groups, including insurance brokers, independent financial advisers, organisations and individuals. Annual turnover is in excess of £0.5 Billion with operations in Europe, the Americas and Asia-Pacific region. In this study we respect our sponsor's request not to disclose the Company's identity.

The Challenge

Many insurance underwriters and commercial carriers of risk maintain a portfolio of retained and trusted suppliers to carry out preventive and remedial work on behalf of their clients. They select suppliers carefully to obtain the best return on their investment, inheriting as little risk as possible from each. This means that when a repairer is called in to respond to a claim, the work is done to a pre-agreed standard in every respect, including management and delivery, extending to include information security and continuity. We faced four main challenges or drivers:

- **Supplier risk profile** Our client would directly inherit the effects of any major issue affecting a supplier and the risk of this must be systematically minimised and controlled. The geographical distribution and diversity of clients inevitably means that the supplier portfolio is large, with a core of over 1000 that require due diligence checks to be performed.

- **Governance obligation** The organisation is mature and operates to high standards, delivering obligations to stakeholders as a matter of course, driving due diligence activity. Regulation by the FCA and PRA reinforces the fact that compliance is mandatory, requiring executives to carry out audits on suppliers both at procurement and periodically thereafter. Supplier Due Diligence needs to be up-to-date, complete and auditable.

- **Continuous activity** There is a steady workload as suppliers are cycled in and out of the list and best practice standards develop and improve. All are expected to stay aligned with international standards ISO 22301 and ISO 27001 for business continuity and information security.

- **Manual operation** Before INONI was engaged, our client's approach was labour-, spreadsheet- and communications –intensive. It was prone to error and oversight, and time-consuming, diverting senior staff from other vital activities. Furthermore, following a reduction in headcount, it was proving difficult for the team to meet its governance objectives and there was a recognised need to automate.

Our Approach

INONI projects work best when both provider and customer share the same detailed expectation of outcome and we achieved this particularly well in this case. We met with the project sponsor over a short period and fully co- designed the Supplier Due Diligence Portal using existing INONI's platform capability. We used the client's pre-existing question sets and processes and transferred them directly into INONI. Our aim was a smooth transition for all concerned, capitalising on the opportunity to improve whilst preserving any compatible aspects that worked. Key stages were:

- Map the requirement, creating secure self-assessment web-tools and a management interface.
- Populate the tools with controls, suppliers, FAQs, responses, message texts and configurable elements.
- Deliver the portal and pilot it with a selection of appropriate suppliers.

Our Solution

We deliver the Portal via a secure web interface allowing access by the insurer and its permitted suppliers. Any authorized party can log on and complete activities, submitting data when complete. We built this capability in two stages.

- First, we provided an interface for our client to upload its due diligence controls from spreadsheets into a pair of online interviews for completion by suppliers. These scored individually as the supplier completes them. The scores are filtered to give Key Performance Indicator (KPI) metrics and aggregated so they give an individual supplier analysis. They are then grouped with those of other suppliers, allowing comparison, statistical analysis, charting and so on.

- Second, we provided easy access for suppliers. They receive an email containing a URL and a few lines of instruction. A password is then provided, allowing them to sign on and complete the questionnaires. On submission, the software flags the supplier as 'Ready for Review' on the INONI console, alerting the manager. They then enter a due diligence workflow, providing acceptance or rejection of individual controls, or of the submission as a whole with confirmation and feedback. If they pass, they need not access the system again until reminded after say a year by email. The collected data is warehoused and becomes available for reporting and analysis, on and offline.

The portal also includes a powerful supplier support system linked to a database of FAQs and a description of the due diligence methodology. It all works well, and since commissioning in 2012, we have experienced just one client support query. We also provide a powerful administrator console, providing all the necessary secure elements such as content change, audit trails, version control and much more.

Valuable outcomes

We believe the project has been successful for the following reasons:

- **Efficient**, sharing the load between suppliers and client. This has halved the time spent chasing unfulfilled requests for information. The workload decreases year-on-year as clients converge on a stable acceptable state. Once a supplier has completed the initial pass, they need only notify our client when things change.

- **Continuous**, supporting procurement but periodically updated, picking up changes in supplier risk profile.

- **Practical** plain **language**, using questions based on ISO standards and current best practice.

- **Certainty**; evidential text means that supplier self-assessments can be validated.

- **Automated**, leaving less room for error or oversight.

- **Scalable**, allowing question variation and unlimited suppliers.

- **Bespoke reporting** and **management information**, supporting comparison and correlation.

- **Rich functionality** is already present and can be activated when required, without code change

Conclusion

We called the client prior to writing this to check he was happy with its content. He said

> *"We estimate we more than halved the time we used to spend on Supplier Due Diligence and we now complete twice as many each month. Instead of repeated calls and visits, they have to answer the questions, there's no chasing, and we can focus them on problems easily.   It's been highly effective for us."*

We also see the project as highly worthwhile and perhaps a foretaste of things to come for many regulated and publicly-owned organisations. We think it exemplifies transition from conventional procurement as one-time gatekeeper (once you're in, you're safe) and full-time gamekeeper, patrolling the supply chain, continuously searching out risks as they emerge. We think it's practical, commonsense governance and that all firms should consider this.

Please call us to find out more