

## Client seeks assistance to build a prioritised, costed plan for improving information security

### Problem statement

In an ever-evolving threat landscape, organisations can struggle to ensure they have effective cyber security controls in place, to both mitigate the risks they face, and protect key information assets from compromise.

It was on this basis that a major pensions and insurance client asked i-confidential to conduct a review of its security position. It wanted to use the results to establish a programme to address the most significant gaps.

### Our approach

Our Security Assessment product was used to conduct a review of the client organisation's information security controls. Security Assessment employs our proprietary Control Framework, a comprehensive library of standards-based security requirements, aligned to the latest threats. Each review is, however, tailored to the client, prioritising control areas based on their operating environment.

In this case, the review encompassed the entire organisation, including the application and infrastructure estates. The client's risk and investment appetite was also considered.

With the control review complete, our product provided a detailed analysis of costs and benefits for a series of recommended activities to address the critical highlighted gaps. This was then structured into a three-year security improvement programme (SIP). A constituent part of this analysis was identifying the logical first activities that would most readily address the organisation's key cyber security risks.

“The approach gave confidence to the risk committee and auditors...”

A further output from the review was a current risk position statement which detailed the significant gaps discovered. Security Assessment provides an easily understood management summary for executives. It shows results using a traffic-light system to highlight control states.

In addition, we provided a summary view of the required improvements and costs to move from the current state to an acceptable risk position.



*Management information is made easy to understand*

### The outcome

82 required controls were reviewed, and 10 risk areas identified, including 40 notable weaknesses. The SIP provided a straightforward cost-versus-risk view of the required improvements, showing the progressive risk



*Agreement on cyber risk investments was a key outcome*

The client's Head of IT Security was able to recommend to the executive the right level of targeted investments to make, based on their appetite for the various cyber risks. The approach gave confidence to the risk committee and auditors that the investment proposal was built on a sound and logical foundation.