

## Enhanced cyber risk measurement a real game-changer for confidence and credibility

### Problem statement

A major UK bank, reviewing its approach to security metrics and reporting, asked i-confidential to deliver a set of improvements. This was to include selection of an appropriate security metrics reporting solution. A key objective was enabling aggregation of individual control metrics to the organisation's material inherent cyber risks. This was required to measure cyber risk based on actual, monthly control metrics.



*Our client needed the right tool for metrics reporting*

### Our approach

i-confidential specified an initial set of reporting requirements to enable the selection of a suitable tool. We then participated in the client's selection panel to compare several reporting solutions. This process determined the incumbent GRC tool was the best choice for the organisation.

Next, we defined metric-to-risk aggregation algorithms, automated metric collection, and dashboard requirements for the solution. i-confidential led the technical

“Our approach enabled the client to move from a manual, control-based dashboard, to an automated solution.”

management of the client's integration partner, who configured the GRC tool to meet our specification.

The operating model for the new cyber metrics was also specified, in order to embed it into the monthly cyber reporting cycle. It was also integrated into operational risk governance and reporting processes.

### The outcome

Our approach enabled the client to move from a manual, control-based dashboard, to an automated solution. This let cyber teams manage and maintain operational control effectiveness based on timely and accurate security metrics data.



*We improved cyber risk measurement capabilities*

Previously, the cyber risk function had to manually gather metrics for controls and assign them to each material risk. This was subjective and inconsistent. We ensured monthly metrics results were assigned to the appropriate risk, and combined to show measurable elements of cyber risk.

With activities reported within the risk tool, the solution was aligned and embedded into the client's operational risk governance and reporting processes. This enhanced confidence in cyber measurement, and improved credibility within executive risk governance.