Case Study

ABC Services Limited

ABC Services Limited ("ABC") is a successful provider of IT & BPO Services to UK, and UK-registered multi-national, organisations.

ABC has maintained a focus upon risk, security and privacy, as a natural dimension of its services provision to clients. ABC holds formal certifications to international standards (such as ISO 22301 – Business Continuity, ISO 27001 – Information Security and ISO 9001 – Quality Management) these areas are also subject to on-going, multi-year, improvement programmes. This is most especially true of ABC's Enterprise Risk Management approach which is designed to enhance overall maturity and strengthen ABC's alignment with ISO 31000.

The ABC Board none-the-less recognise that, whilst its own activities and all these areas overlap and contribute to organisational / cyber resilience, the degree of focus previously placed on resilience is unlikely to be sufficient. An FY 2018-19 strategic objective is thus to improve ABC's organisational and cyber resilience. This is in response to a number of recent events & information received, including:

- Major incidents that have affected two direct competitors of ABC,
- ABC's own two recent (fortunately minor) incidents from which ABC may not yet have learnt all relevant lessons,
- A number of 'near misses' also experienced,
- Resilience concerns raised by the Services Regulator,
- Work on Resilience mooted by the IT Services Club in response to the above,

- Increasing client expectations both implicitly (through 'Meet the Client' exchanges) and explicitly (through increasingly demanding contractual requirements).

However, the ABC Board also recognises that Resilience is not, and never should be, an 'absolute' solution but is a key aspect of good organisational governance. As such it has commissioned a review to be managed by the ABCX Strategy Team which is facilitated through the use of SOLUXR's evaluation software.

Nature of the Respondent

As a Senior Manager, this individual has a long career behind him, but one spent almost entirely within the present organisation and all of it in the same services sector. He is generally recognised to be something of a cynic about new disciplines. Whilst recognising the company's importance, he tends to the view that they should be (largely) delivered implicitly rather than explicitly i.e. 'as part of the day job'. That said, he has been burned in the past for doing what he thought was the right thing, and in lieu of Executive Management / Board direction to do so. Perhaps as a defence mechanism, he often refers to 'many hands making light work' and for the organisation to 'only do as much as the competition' so as to not be commercially disadvantaged and/or suffer margin erosion.

Strategic Imperatives

The representative data entered to the SOLUXR tool for testing and re-use as demo material represents a 'true and fair' representation of a known / real organisation that is also considered 'typical'.

With a position of 66% of responses 'unable to demonstrate' or 'limited ability to demonstrate', it follows that there will be more, rather than less, Strategic Imperatives derived.

The below 'Top 10' are appropriate to act as broad categories into which significant numbers of recommended actions, can be grouped and are broadly equal in terms of importance.

1. Resilience as a regular Board Agenda Item & Focus
2. Resilience Policy & Framework incl. External Input
3. Resilience Outreach, Engagement & Benchmarking
4. Appointment of a Chief Resilience Officer (CRO)
5. Resilience Communications & Awareness Training
6. Resilience to be added as a 'Dimension' of Enterprise Risk Management
7. Crisis Management Plans to be Produced & Tested
8. Resilience Budget
9. Identify Cyber / Information Assets & Their Values
10. Processes for Periodic Review & Maturity Assessment