

4sl Consulting Service - Security & Information Assurance (IA)

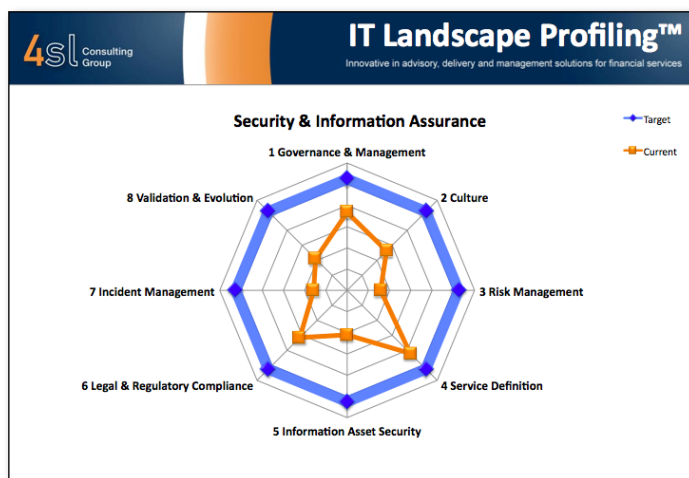
Client agenda: 4sl recognise that many clients prefer to appoint a service provider that can cover all of their security and information assurance requirements even if in some cases the supplier will only act as a single point of contact for multiple vendors involved in a more complex delivery arrangement. In response to this, 4sl has developed a comprehensive and holistic security & IA consulting service that can be delivered through a number of concise and self-contained work packages. The objectives of the service being to:

- Assess and measure organisational capability and maturity,
- Review corporate policy and standards, identify risks/gaps/constraints and implement remediation initiatives,
- Establish an effective governance framework, and
- Promote awareness and cultural understanding across the organisation.

The first activity will typically include a high level assessment, using 4sl's Landscape Profiling method, to understand the client's current environment and establish the level of capability and maturity of the organisation across a range of disciplines and behaviours. However, each work package can be delivered in stand-alone discrete phases.

1. Security & IA Assessment (measure the capability, maturity and identify gaps)

- A 4sl Landscape Profiling assessment against ISO27001 using the Capability and Maturity Model (CMM) of CobIT.
- This provides a metric measure that is mapped on the 8 lever Landscape Profile as follows:
 - Governance and Management (organisation & mandate)
 - Culture (awareness & sponsorship)
 - Risk Management (record of information assets and management of their risks)
 - Information Asset Security (Physical, Technical & Human Factor Security)
 - Legal & Regulatory Compliance
 - Compliance verification (monitoring and reporting on compliance levels)
 - Incident Management
 - Validation and Evolution



- These levers as shown in the profiler output above, can be changed to reflect different client priorities as appropriate. Each of the 8 levers is expanded into their sub-components through a set of comprehensive questions.
 - For smaller entities or SMBs, this package can be expanded to offer an internal audit if the client does not have audit capability in-house.
2. Governance framework
- A stand-alone service offering to establish an Information Security Management System (ISMS) based on ISO27001, either in a 'green field' manner where none exists or specific components that are found to be missing as a result of an assessment;
 - The ISMS provides the Security & IA governance within an entity. It comprises a number of descriptive policies and prescriptive standards and work instructions (control sets). The number and depth required varies dependent on the ISMS scope, risk profile and business. The time required varies from 1 – 8 days per document and the time to implement a full ISMS can range from 6 – 24 months; and
 - There is probably much more potential in offering this as a way of filling gaps for entities that have gone through an assessment and found they have gaps in their governance.
3. Security & IA solutions
- The design and/or implementation of third party solutions to mitigate operational risks and/or enable compliance verification
 - This offering ranges from the development of a core security architecture to meet policy/standards, mitigate specific risks (whether physical, technical or human factor) to the implementation of a global operational infrastructure.
4. Awareness programs (Integrate Security & IA into the business culture)
- Project/program support to help establish and promote internal campaigns, training sessions or simply collateral (publications, newsletters, advisory notes etc.).
 - Supplementary support for smaller entities or SMBs that do not have a dedicated team or enterprises that need a specific focus of awareness that is not available or addressed in-house.

From Corporate Policy to Operational Verification: The diagram below represents a typical albeit simplistic Security & Risk policy hierarchy we would expect to see adopted or promoted within an organisation when first engaging for the high level assessment. It demonstrates the need for policy and standards to be established at corporate level, with control points defined against them for implementation across IT, which would typically manifest their offerings as a set of products and services. Verification of those control points say through an internal audit, will often expose gaps that need to be remediated through a formal compliance or risk mitigation programme.

