ISF Case Study

Security Controls, Polices and Standards updates

Client: A global provider of customer-specific packaging headquartered and listed in London

Project outcome requirements: Guidance in creating a control library, which will support its new Information Security and Acceptable Use Policies, and imported into a Governance, Risk Management & Compliance (GRC) tool in the future

Challenges

- Organisation required a control library to assist in the implementation of their Information Security Policy & Acceptable Use Policy (AUP)
- The client was clear in their requirements for the control library content to:
  - support directly the key statements in their new Information Security Policy & AUP
  - be informed directly by the ***Standard of Good Practice (SOGP)***
  - be mapped to ISO27002:2013
  - refer to industry-recognised technical standards which can be used to inform the creation of implementation procedures
  - be created in a form capable of being imported into a GRC tool in the future

Solutions/Process followed by ISF

- Agreed on the approach for using the ***Standard of Good Practice (SOGP)*** at the beginning of the project with key stakeholders
- Gained an understanding of the key technologies in customer's environment, to determine which should be addressed by technical standard references in the control library
- Review of ISF Security Healthcheck framework to help write control statements which abstract away from the lower-level detail of SOGP
- Wrote control statements, driven by SOGP & Security Healthcheck and mapped to ISO 27002:2013, NIST CSF and CIS frameworks and standards to indicate minimal technical and governance controls required/recommended
- Shared deliverables with key stakeholders weekly to obtain continuous review and feedback.

SOGP

Project timeline

4 to 6 weeks, from scoping to reporting.

Benefits

- Facilitates presentation of clear, distinct, control statements to internal users
- Efficiencies gained (time and cost), through establishment of control library with minimal key critical controls, aligned with recognised industry frameworks and standards
- The control framework was structured and formatted to facilitate straightforward:
  - continuous updates over time
  - import to a GRC tool in the future.

"With the SOGP already mapped to ISO 27001:2013, NIST CSF and CIS frameworks and standards, and the expertise of the ISF team, we were agile and efficient in meeting our goals". – ISF Client

What is the ISF *SOGP*?

Need help with controls, policies and industry standards? Contact your regional director