How would Security Assessment evaluate your security risk?

Why Security Assessment?

It is challenging for businesses to determine their security risk position in an independent, systematic way.

i-confidential's **Security Assessment** product offers a structured method to review and rate the security control status of an organisation. Security Assessment has been used successfully by a number of major companies to identify security gaps and plan remediation activities.

Using our proprietary **Control Framework**, we target what our clients need to make their organisations secure. The Control Framework defines and prioritises the controls required to protect a business against the latest threats. It constitutes essential practice in cyber security, based on broad experience and industry standards, including:

- ISO 27000
- Critical Security Controls for Effective Cyber Defence (SANS)
- US National Institute of Standards and Technology (NIST)

Key features

Flexible – controls can be prioritised using an importance ranking – Required, Good Practice, and Generic. Reviews can target selected areas only, or a more comprehensive assessment can be done.

Comprehensive – we assess different aspects of control maturity – scope, ownership, capability, consistency, and measurement. This provides a richer picture of control status. We can provide the option of delving deeper using a, "Tell me, show me, prove it." approach to each control.

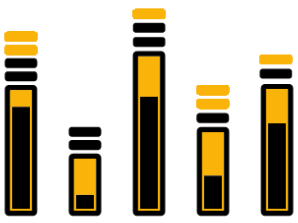
Accessible – Security Assessment generates management information using a simple traffic-light system to highlight the overall status of a risk area. It also conveys a current overall security position, including key summary information for stakeholders.

Informative – a final report provides ratings on each required control area's level of compliance based on key feature attributes, and illustrates any identified gaps. The report's risk statements and ratings are calibrated against the target organisation's risk appetite.

Moving forward

Armed with the findings from Security Assessment, clients commonly want a customised, costed, and phased security remediation plan.

Our product is designed with those next steps in mind. Its output is based on a detailed understanding of the organisational priorities established during the assessment engagement.



Security Assessment provides a number of deliverables:

- A security improvement plan describing the remediation projects required, spanning multiple years.
- Summarised costs per risk area.
- Activities scoped to address any organisational security gaps.
- A simple 'graphic equaliser' view of the improvement journey — executives can set desired risk levels.

For more information about how we can help your business, please contact us

i-confidential
Cyber Security & Information Risk Specialists ®

www.i-confidential.com
info@i-confidential.com
0131 445 1458