FINAL UK version – Security Maturity Assessment One-pager/PDF handout

Security Maturity Assessment:

Identifying Maturity Risks in Security Controls

Strengthening an organisation's security environment becomes critical as cyberattacks continue to increase in volume, complexity, and severity. Internal security monitoring may indicate that an organisation isn't currently compromised, but that doesn't mean that it won't be compromised at some point. Even the most mature security programme should constantly evolve, reassess, and improve to shift from being purely reactive to being proactive in its approach as IT components in use by the business change and the threat landscape also evolves.

DEFINING SECURITY MATURITY

Security compromise often happens when organisations don't have a complete grasp of the vulnerabilities facing them or adequate controls in place to manage them. The term "security maturity" refers to an organisation's security position relative to its risk environment and tolerances. Risk scenarios vary greatly according to the organisational environment, as each has its own security risk culture. Thus, the level of maturity is determined by how efficiently and consistently it implements security policy, controls, reporting and processes.

Ensono's Security Maturity Assessment helps clients minimize the possibility of a security breach by pinpointing current risks so they can make impactful changes to their security controls. Our team of expert security consultants, including former CISOs, can assess an organisation's security maturity and make actionable recommendations to enhance security controls, processes, automation, reporting and help to ensure a solid compliance stance as well.

Taking a holistic approach, Ensono security experts use the leading security framework from the Center for Internet Security (CIS) to review and rate the Top 18 security controls that span a client's security landscape. This framework can be mapped to others such as National Institute of Standard Technology (NIST) if that is the standard your organization uses. By reviewing security controls across all platforms and processes, the assessment provides a maturity score for each control; presents a gap analysis; and makes recommendations that can be prioritised based on the maturity scores.

18

Summary maturity assessment across the 18 key security controls

Gap analysis across security controls

Potential risks and business context

Actionable reccomendations

Proposed priorities based on the maturity scores

ensono

WHEN IS THE "RIGHT TIME" FOR A SECURITY MATURITY ASSESSMENT?

While an assessment can be done at any time, several common scenarios make the timing right for conducting a Security Maturity Assessment. For instance:

- Assessing the current state of an existing security programme, looking for ways to improve security and lower risks
- Before an audit, an assessment can identify areas for strengthening controls or show validation to a compliance auditor
- When embarking on large projects (such as infrastructure migration or application transformation) to assess the planned security control end state, identifying any gaps, and implementing necessary cybersecurity enhancements
- After a merger or acquisition, assess the entities being integrated to identify any differences in maturity and plan for implementing standards the highest shared security controls environment across both organisations

EXAMPLE OF A SUCCESSFUL SECURITY MATURITY ASSESSMENT

Ensono recently completed a successful security maturity assessment for a state government. In its effort to keep up with current technology, the state faced these challenges: a complex and dated environment that posed security risks and a retiring staff.

Ensono provided a Virtual CISO to augment the state's security team and to help develop the security function. The first activity by the Virtual CISO was to perform a security maturity assessment to provide a baseline for an improvement program. The assessment resulted in:

- Recommendations to strengthen the state's IT security controls and focus efforts to prevent future breaches
- A detailed plan that could be shared with the legislature for budget approval
- Comprehensive analysis to implement new controls and processes and address the security team's skill gaps
- An evaluation to help the state choose a cybersecurity solution to address each control gap

SECURING IT ENVIRONMENTS

Ensono keeps clients' critical business applications and infrastructure up and running—maintaining secure IT environments is a critical part of that mission. To learn more about Ensono's security services, visit https://www.ensono.com/services/security/