Cyber Smart – Stages of an assessment

At a high-level, assessments are comprised of four stages:

- **Stage 1:** Cyber Smart plans and prepares for the assessment.
- **Stage 2:** Cyber Smart determines the scope (i.e. assessment boundary) and approach for the assessment.
- **Stage 3:** Cyber Smart assesses the controls associated with each of the mitigation strategies.
- **Stage 4:** Cyber Smart develops the security assessment report.

The activities and considerations for each stage of an assessment are discussed in further detail below.

Stage 1: Assessment planning and preparation

Assessment planning

Prior to commencing an assessment, Cyber Smart will conduct assessment planning activities. These activities require us to discuss with the system owner:

- assessment scope (i.e. assessment boundary) and assessment approach (see further detail below)
- access to unprivileged and privileged user accounts, devices, documentation, personnel, and facilities
- any approvals required to run scripts and tools on the system (see further detail below)
- evidence collection and protection, including any requirements following the conclusion of the assessment
- where the security assessment report will be developed (e.g. on an assessor’s device or on an alternative device)
- approach to stakeholder engagement and consultation (including key points of contact)
- whether any service providers manage aspects of the system (including appropriate points of contact)
- access to any relevant prior security assessment reports for the system
- appropriate use, retention and marketing of the security assessment report by both parties.

Cyber Smart will develop an assessment test plan and share it with the system owner.

Stage 2: Determination of assessment scope and approach

Determine assessment scope

In determining the assessment scope (i.e. assessment boundary), Cyber Smart will first clarify the target maturity level with the system owner, noting that the Essential Eight is required to be implemented and assessed as a package. For example, if a system owner has not previously had an assessment demonstrating that they have implemented Maturity Level One, they should not begin an assessment against Maturity Level Two until they have done so, and likewise for Maturity Level Two before being assessed against Maturity Level Three.

Having identified a suitable target maturity level, the assessor should familiarise themselves with the requirements for that maturity level as it will impact the components or aspects of the system within scope of the assessment.

Once the scope of the assessment has been identified, and agreed upon with the system owner, a more accurate determination of the assessment's duration and any milestones will likely be possible.

The scope of the assessment should be documented within the security assessment report. Any components or aspects of a system deemed out of scope should also be documented and accompanied by a justification for their exclusion.

Determine assessment approach

In determining a suitable assessment approach, both qualitative and quantitative testing techniques should be considered. For example, qualitative testing techniques include documentation reviews and interviews with personnel administering or managing system security, while quantitative testing techniques include system configuration reviews and the use of scripts and tools. Sample sizes for testing should also be determined in consultation with the system owner, with the aim of assessing a reasonable representative sample of workstations (including laptops), servers and network devices.

Conducting assessments using interviews, reports and screenshots will always be inferior to conducting assessments using scripts and tools. Particularly as scripts and tools often assess many workstations and servers on a network, rather than a single sample workstation or server, and often identify issues that may be missed in interviews or overlooked by human analysis of reports and configuration settings. If adequate assessment scripts and tools are not already present on a system, assessors may seek to use their own scripts and tools following approval by the system owner.

Any assessment limitations, including sample sizes and constraints on technical testing, should be documented within the security assessment report.

Stage 3: Assessment of controls

The assessment of each mitigation strategy is performed by reviewing and testing the effectiveness of controls. This section provides guidance on the approach to assessing each mitigation strategy at a given maturity level, along with relevant assessment considerations. Guidance on determining the effectiveness of controls within each mitigation strategy is also provided within this section.

Assessment guidance for maturity levels in this section is cumulative. For example, the guidance provided in the Maturity Level Two section is focused on unique requirements above those of Maturity Level One. Likewise, the guidance provided in the Maturity Level Three section is focused on unique requirements above those of Maturity Level Two. This aligns with the manner in which assessments should be conducted against target maturity levels.