



# Penetration Testing Programme

Maturity Assessment Tools

## A. Overview

Many organisations are extremely concerned about potential and actual cyber security attacks, both on their own organisations and in ones similar to them. Many of these attacks exploit weaknesses in an organisations' applications and underlying infrastructure. To help identify as many of these vulnerabilities as possible within a critical timescale - and address them effectively - many organisations carry out penetration testing. However, establishing and managing a suitable penetration testing programme can be a very difficult task, even for the most advanced organisations.

The main drivers for penetration testing include a high degree of concern about:

- A growing requirement for compliance
- The impact of serious (often cyber related) security attacks on similar organisations
- Use of a greater number and variety of outsourced services
- Significant changes to business processes
- Raising awareness about possible Cyber security attacks.

When performing penetration tests, some organisations adopt an ad hoc or piecemeal approach, often depending on the needs of a particular region, business unit – or the IT department. Whilst this approach can meet some specific requirements, it is unlikely to provide real assurance about the security condition of your systems enterprise-wide.

Consequently, it is often more effective to adopt a more systematic, structured approach to penetration testing as part of an overall testing programme, ensuring that:

- Business requirements are met
- Major system vulnerabilities are identified and addressed quickly and effectively
- Risks are kept within acceptable business parameters.

All aspects of a penetration testing programme (which includes determining requirements; performing the actual tests; and carrying out follow up activities) need to be well managed, for example by:

- Establishing an assurance process to oversee the testing
- Monitoring performance against requirements
- Ensuring appropriate actions are being taken.

The effectiveness of your penetration testing programme should be evaluated regularly against approved criteria to help determine if objectives were met and that value for money has been obtained from your supplier(s).

CREST has developed a suite of maturity assessment tools to help you assess the status of your penetration testing programme on the industry standard scale of 1 (least effective) to 5 (most effective). The suite consists of three spreadsheet-based maturity assessment tools enabling an assessment to be made at a summary, intermediate or detailed level. The consolidated tool (which is macro-driven) will enable a selection of approaches to be adopted using just one tool.

**Warning:** The maturity assessment tools have only been designed to work on Windows-based computers.



## B. Maturity model

To carry out penetration testing effectively you will need to build an appropriate penetration testing programme the maturity of which can be assessed against a suitable maturity model by using the CREST penetration testing maturity assessment tools.

The maturity model used in the CREST suite of penetration testing assessment tools is based on a traditional, proven model shown below. This model can be used to determine the level of maturity of your penetration testing programme, ranging from 1 (least effective) to 5 (most effective).

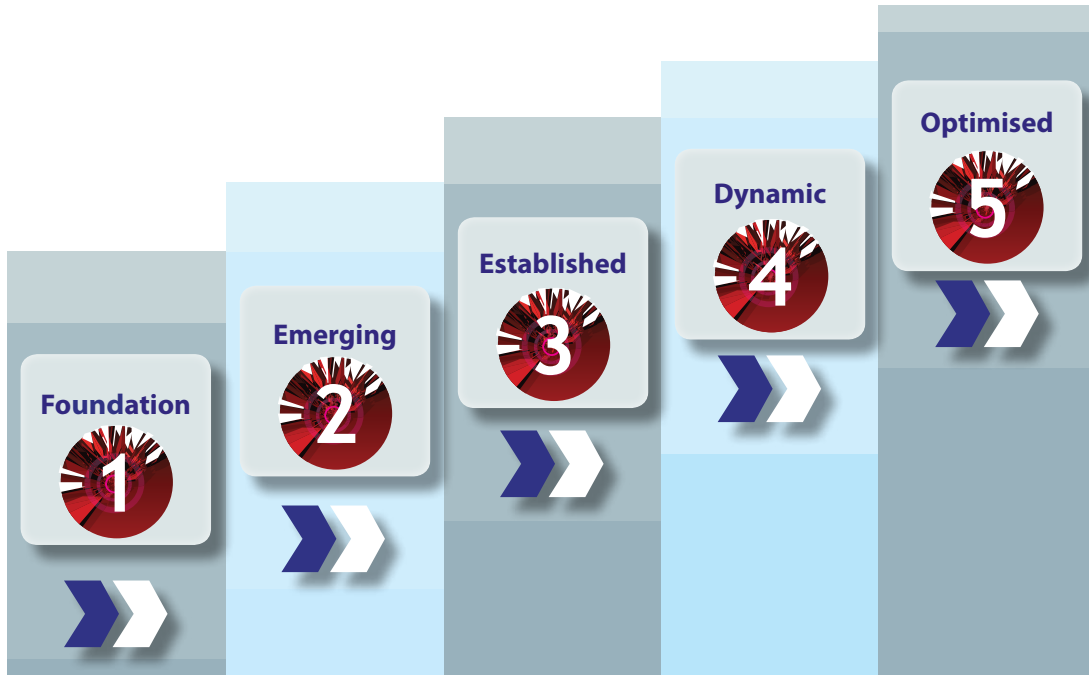


Figure 1: Maturity assessment model

Different types of organisation will require different levels of maturity for their penetration testing programme. For example, a small company operating in the retail business will not have the same requirement – or ability – to carry out penetration tests in the same way as a major corporate organisation in the finance sector – or a government department.

Consequently, the level of maturity your organisation has for your penetration testing programme should be reviewed in context and compared to your actual requirements for such a programme. The maturity of your organisation can then be compared with other similar organisation to help determine if the level of maturity is appropriate.

**Note:** The maturity of your penetration testing programme can play a significant role in determining the level of third-party involvement required to conduct independent penetration testing. Organisations with a mature penetration testing programme may manage most of their operations in-house, while those who are less mature may depend entirely on third parties.



## C. Penetration Testing Programme

Each organisation should develop an appropriate penetration testing programme that will enable them to adopt a systematic, structured approach to undertaking penetration testing enterprise-wide. This programme should cover all key activities required to prepare for penetration testing, undertake an appropriate set of tests in a consistent, well-managed way and ensure that these tests are followed up effectively.

Your penetration testing programme should consist of appropriately skilled people guided by well-designed, repeatable processes and effective use of relevant technologies that will enable you to conduct thorough penetration tests, successfully identifying and addressing vulnerabilities - and to prevent new ones from occurring.

However, many organisations do not know how effective their penetration testing programme is in practice. One of the best ways to help determine the effectiveness of your programme is to measure the level of maturity of your penetration testing programme in terms of:

- People, process, technology and information
- Requirements, testing and follow up.

The CREST suite of spreadsheet-based maturity assessment tools has been developed to help you assess the status of your penetration testing programme at three different levels, using two tools that do not require macros to be enabled, plus a more comprehensive and function-rich tool (recommended) that does require macros to work. You can select one or more combinations from the:

- **Summary assessment tool** (no macros), which allows an assessment to be made to determine the level of maturity of your penetration testing programme at a high level
- **Intermediate assessment tool** (no macros), which allows an assessment to be made at an intermediate, more detailed level
- **Consolidated assessment tool** (requires macros to be enabled), which allows more sophisticated assessments to be made to determine the level of maturity of your penetration testing programme at summary, intermediate or detailed levels - or a combination of all three.

**Note:** The penetration testing maturity assessment tools form part of a series of assessment tools developed by CREST, including high level and detailed Cyber Security Incident Response Assessment Tools.

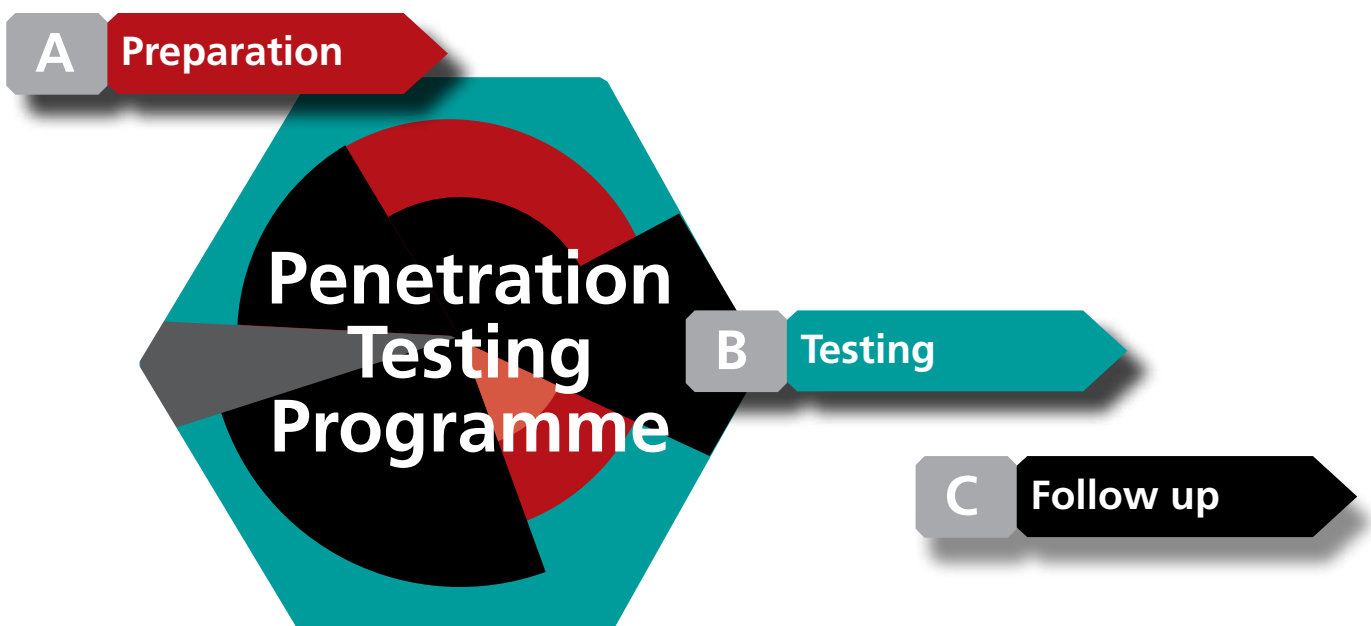


Figure 2: The Penetration Testing Programme

The CREST penetration testing maturity assessment tools have been developed in conjunction with representatives from a broad range of organisations, including industry bodies, consumer organisations, the UK government and suppliers of expert technical security

services. They provide you with an assessment against a maturity model that is based on the 22 steps within the 3 phase penetration testing management process presented in the CREST Penetration Testing Management Guide, as shown in the diagram below.

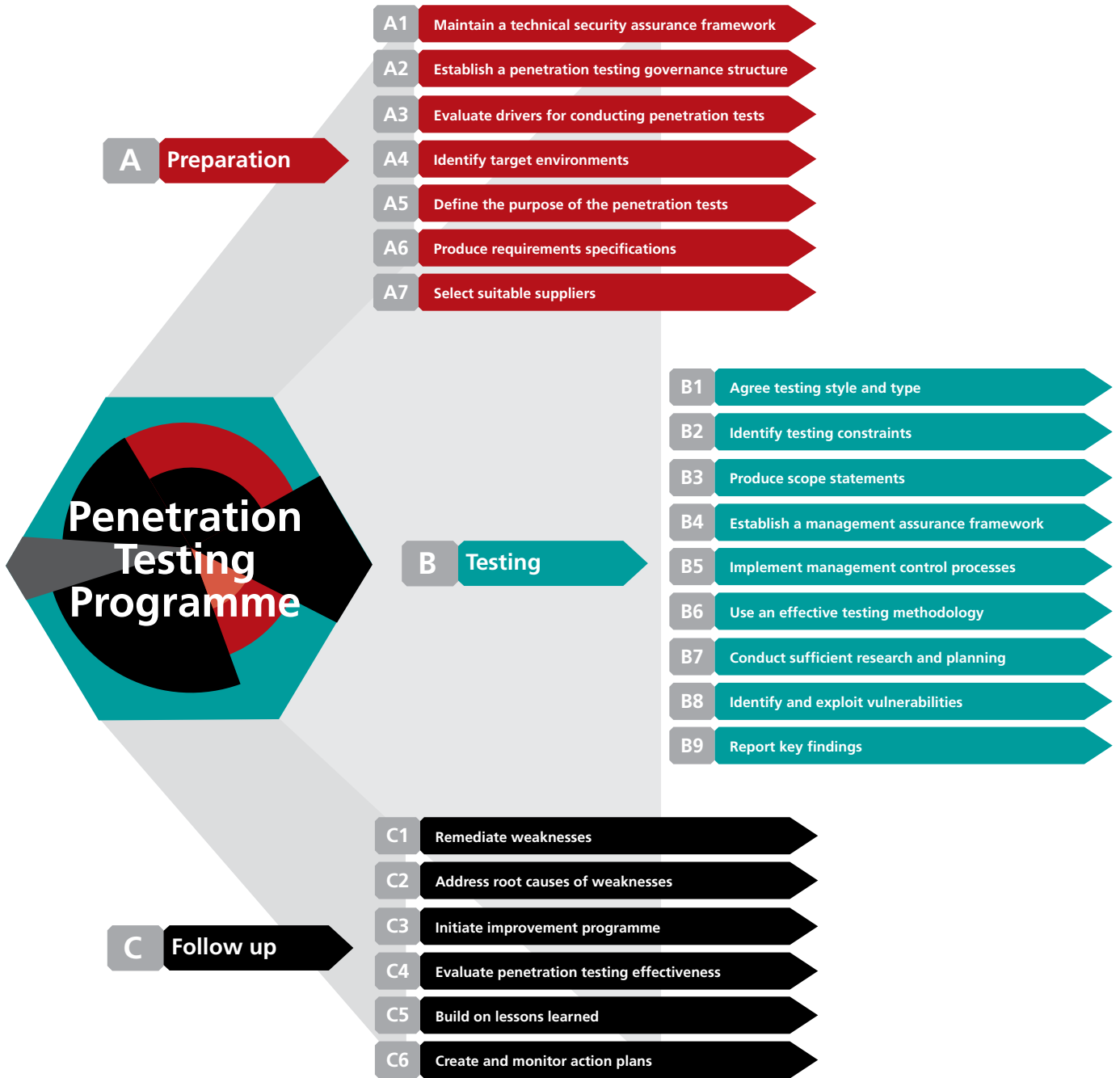


Figure 3: Key steps in the penetration testing management process





## D. Assessment tool functionality

The penetration testing assessment tools have been designed in a standard format and built to be used in a flexible, pragmatic, user-friendly manner. The Project Team has:

- Developed a maturity assessment capability that allows an organisation to determine the maturity of their penetration testing programme, ranging from 1 (least effective) to 5 (most effective), supplemented by 'don't know' and 'not selected' options
- Provided an easy-to-use question response mechanism, such as drop-down menus or radar selection buttons, allowing additional material to be attached as evidence of responses given
- Addressed the need to measure the status of current arrangements and target arrangements; and perform a gap analysis between the two
- Built-in a set of rich functionality
- Included an automatically calculated reporting capability, showing results at different levels against target and benchmarking ratings.

The tools are driven by responses to a set of carefully designed questions, validated by industry experts, which can be answered at three levels:

- Summary (S) - 28 questions
- Interim (I) - around 150 questions
- Detailed (D) - approximately 600 questions.

The Penetration testing maturity assessment tool also:

- Provides navigation through a range of mechanisms, such as worksheet tabs and hot buttons
- Enables weighting factors (eg x 2) to be applied to specific questions, which will influence the scoring mechanism
- Automatically saves responses after a certain period of time and shows progress made in answering questions.

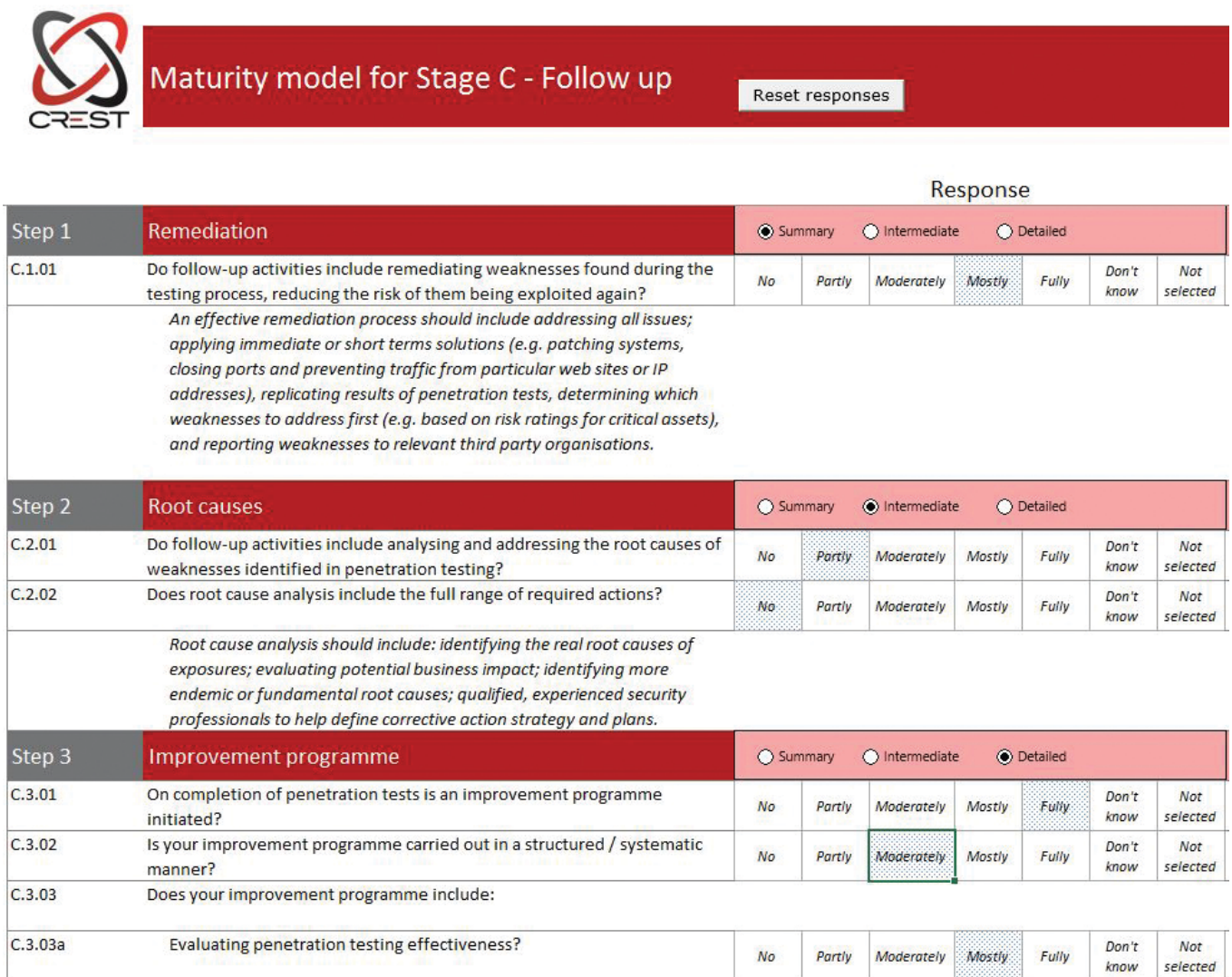
**Note:** In all the tools, there is helpful step-by-step assistance available in the **Guidance** worksheet, with background being provided in the **Introduction** worksheet.

## E. Assessment process

Each of the three assessment tools consists of a similar set of worksheets, enabling assessments of an organisation’s penetration testing programme to be made in a consistent manner at either a summary, intermediate or detailed level. The summary version allows a quick, high level overview to be obtained, whereas the detailed tools enable a more precise assessment to be made about the real maturity level of your penetration testing programme.

The results presented in all the tools are based on the responses given to a series of well-researched questions that have been validated by industry experts. You can select relevant responses to each question in the **Assessment** worksheets.

Using the macro-based tool, questions can be answered by just clicking on relevant radio buttons at summary, intermediate or detailed level – or a combination of all three. An example of a questionnaire screen in the **consolidated** assessment tool is shown below.



		Response						
<b>Step 1</b>	<b>Remediation</b>	<input checked="" type="radio"/> Summary <input type="radio"/> Intermediate <input type="radio"/> Detailed						
C.1.01	Do follow-up activities include remediating weaknesses found during the testing process, reducing the risk of them being exploited again?	No	Partly	Moderately	Mostly	Fully	Don't know	Not selected
<i>An effective remediation process should include addressing all issues; applying immediate or short terms solutions (e.g. patching systems, closing ports and preventing traffic from particular web sites or IP addresses), replicating results of penetration tests, determining which weaknesses to address first (e.g. based on risk ratings for critical assets), and reporting weaknesses to relevant third party organisations.</i>								
<b>Step 2</b>	<b>Root causes</b>	<input type="radio"/> Summary <input checked="" type="radio"/> Intermediate <input type="radio"/> Detailed						
C.2.01	Do follow-up activities include analysing and addressing the root causes of weaknesses identified in penetration testing?	No	Partly	Moderately	Mostly	Fully	Don't know	Not selected
C.2.02	Does root cause analysis include the full range of required actions?	No	Partly	Moderately	Mostly	Fully	Don't know	Not selected
<i>Root cause analysis should include: identifying the real root causes of exposures; evaluating potential business impact; identifying more endemic or fundamental root causes; qualified, experienced security professionals to help define corrective action strategy and plans.</i>								
<b>Step 3</b>	<b>Improvement programme</b>	<input type="radio"/> Summary <input type="radio"/> Intermediate <input checked="" type="radio"/> Detailed						
C.3.01	On completion of penetration tests is an improvement programme initiated?	No	Partly	Moderately	Mostly	Fully	Don't know	Not selected
C.3.02	Is your improvement programme carried out in a structured / systematic manner?	No	Partly	Moderately	Mostly	Fully	Don't know	Not selected
C.3.03	Does your improvement programme include:							
C.3.03a	Evaluating penetration testing effectiveness?	No	Partly	Moderately	Mostly	Fully	Don't know	Not selected

Figure 4: Questionnaire worksheet in the consolidated assessment tool

**Note:** For the **Summary** and **Intermediate** assessment tools (neither of which use macros), questions can be answered using drop-down menus at either summary or intermediate level, as required.

Three different target profiles have been created, which apply to **Basic**, **Important** or **Critical** business functions. These profiles can be applied by selecting the relevant tick box in the **Target** worksheet (see example below). Each of these profiles can be refined by changing the values in the corresponding cells to the right - or to a different set altogether by selecting the **Custom** tick box.

A weighting factor can be set in the **Weighting** worksheet to give the results to particular questions more importance than others. Furthermore, if you only wish to assess particulate elements of your penetration testing programme, then you simply click on the relevant **Not selected** tick box and the chosen question(s) will be greyed out in the question and results worksheets.

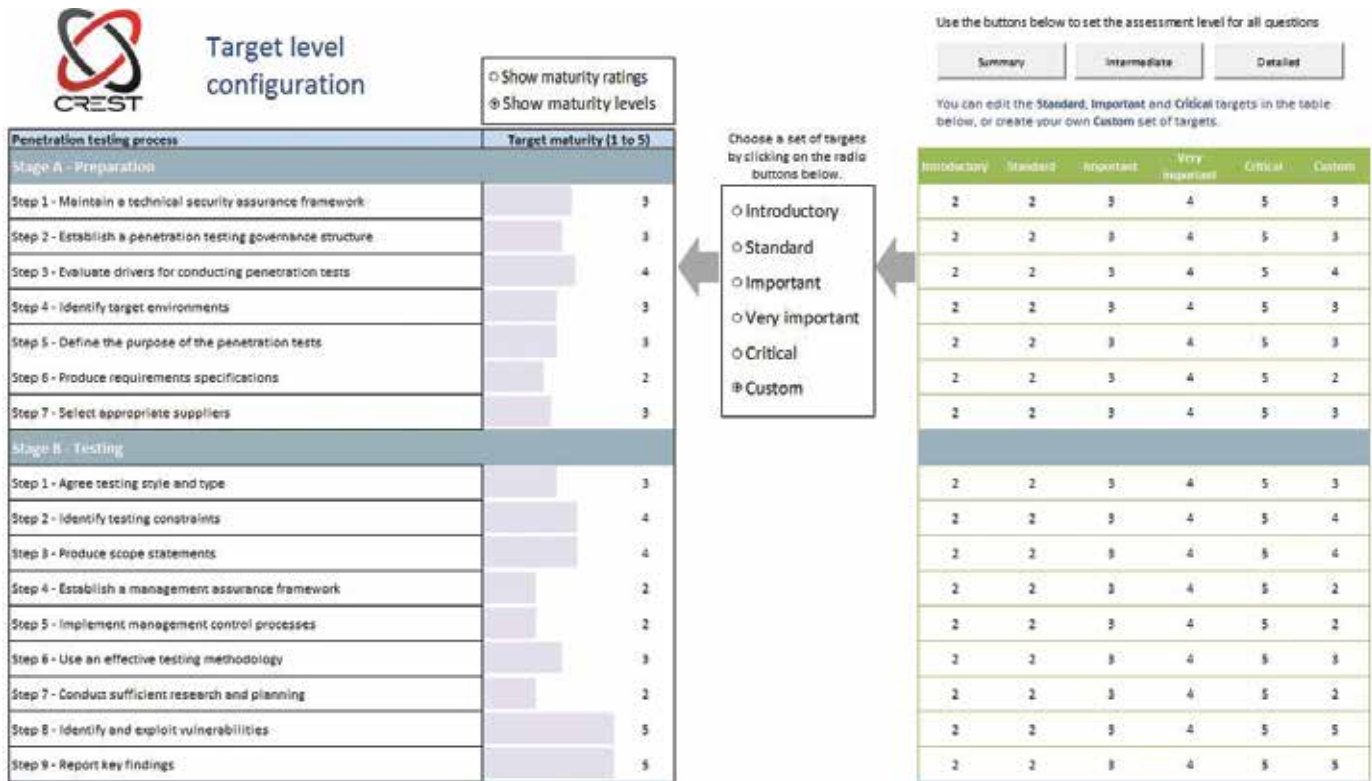


Figure 5: Weighting worksheet in the consolidated assessment tool



## F. Assessment results

Based on your responses to the questions in the **Assessment** worksheets your level of maturity for each of the 22 steps is calculated using a carefully designed algorithm that takes account of both the level of response to each question and the associated weighting factor.

The results derived from the completion of the questions in each tool are automatically:

- Shown as ratings for individual questions and aggregated up to action level, area level or for the entire penetration testing capability
- Presented in graphical format against the organisation's target profile, either as a bar chart or radar diagram
- Highlighted in a heat map using traffic lighting to highlight results as red, amber or green against user defined ranges.



A useful summary of your results is presented both as a bar chart and radar diagram (see below) in the Results worksheet. These **results** show the level of maturity for your penetration testing programme on the scale of 1 to 5 previously described, comparing this to the target and benchmark maturity ratings, based on your chosen target profile and benchmark ratings.

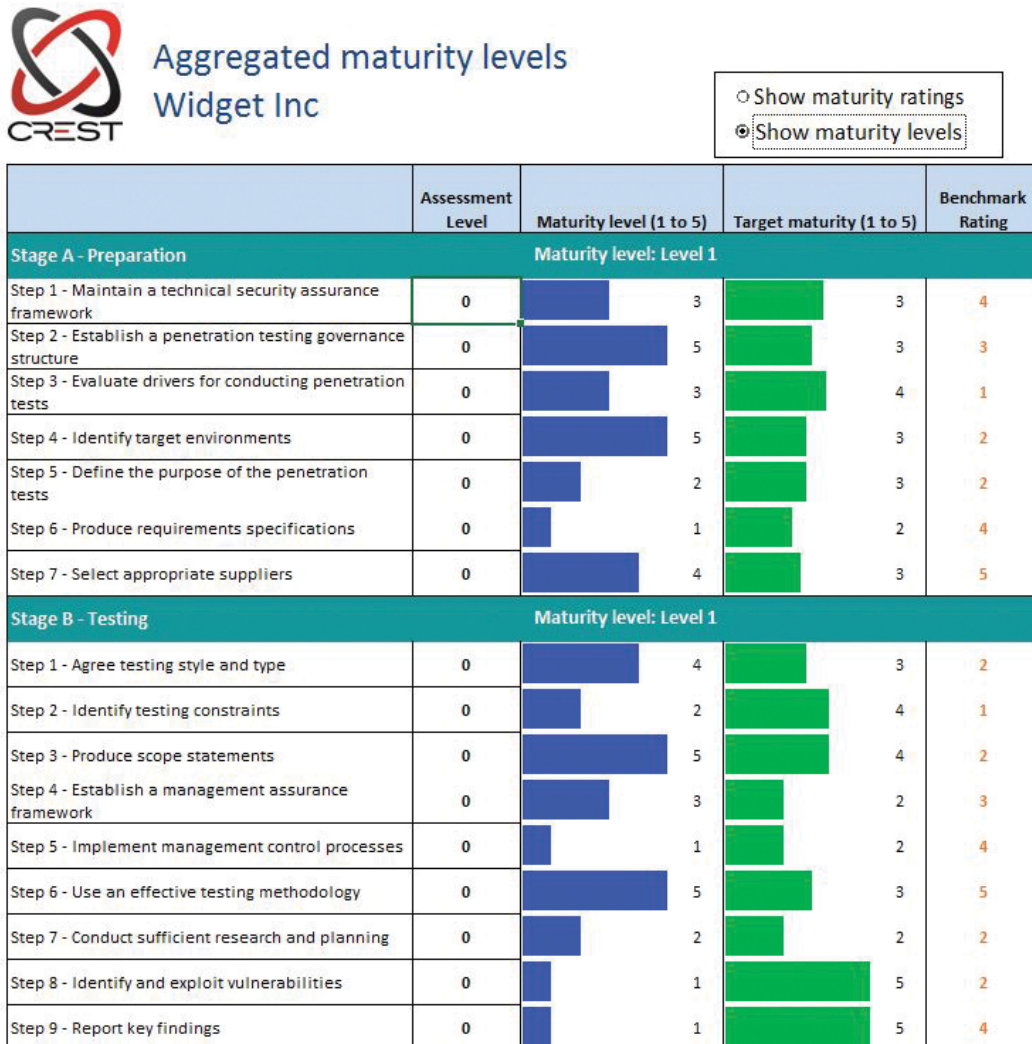


Figure 6: Bar chart presentation in Results worksheet

**Note:** You can assign a benchmark rating by simply overwriting the relevant orange figure in the right hand **Benchmarking Rating** column. This is not automatically calculated or imported, so will need to be based on benchmark analysis performed independently either by your own organisation or an external service provider.

Results are also shown as a radar diagram presenting details to be analysed using a graphical representation of your actual maturity ratings (the blue, green and orange lines) and target values (the light purple lines).

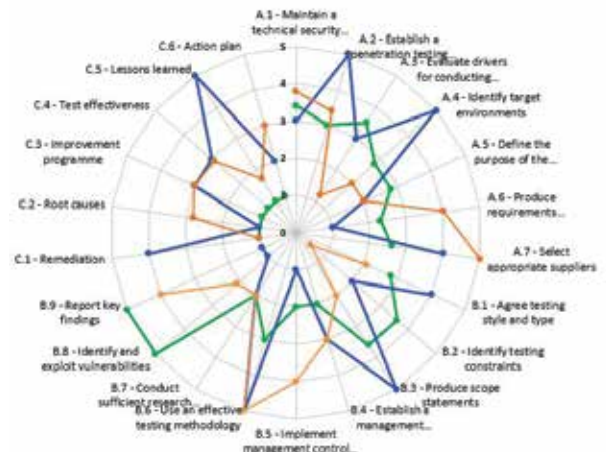


Figure 7: Radar diagram presentation in Results worksheet



## Notes





### **Company Membership**

Demonstrable level of assurance of processes and procedures of member organisations

### **Knowledge Sharing**

Production of guidance and standards. Opportunity to share and enhance knowledge

### **Professional Qualifications**

Validate the knowledge, skill and competence of information security professionals

### **Professional Development**

Encourage talent into the market. Provision of on-going personal development

For further information contact CREST at  
<http://www.crest-approved.org>

#### **Warning**

This Guide has been produced with care and to the best of our ability. However, CREST accepts no responsibility for any problems or incidents arising from its use.