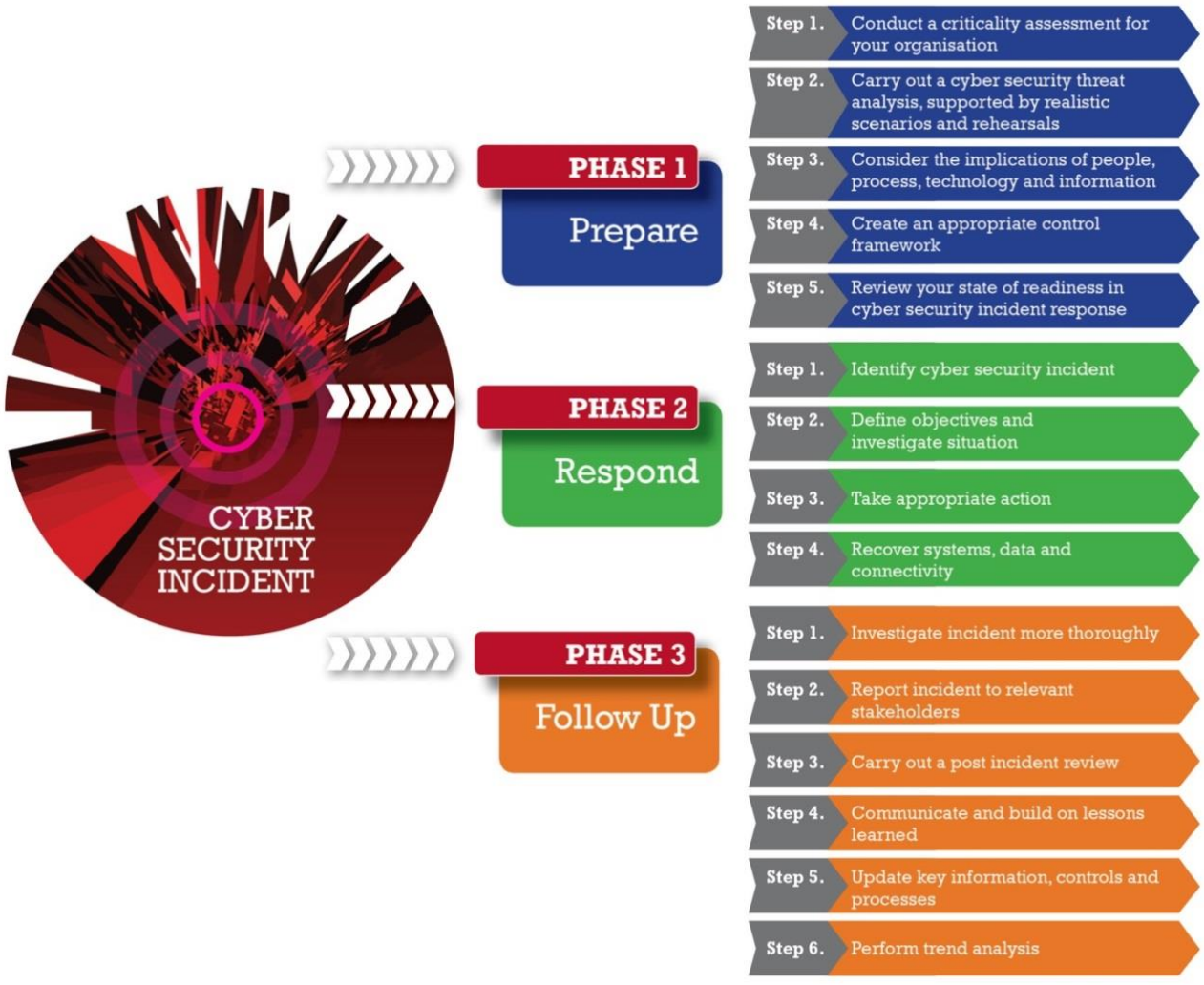
THE CREST CYBER SECURITY INCIDENT RESPONSE MATURITY ASSESSMENT TOOL

A. Overview

CREST has developed a maturity model to help you assess the status of your cyber security incident response capability. This model has been supplemented by *Release 1* of a spreadsheet-based maturity assessment tool, which helps you to measure the maturity of your cyber security incident response capability on a scale of 1 (least effective) to 5 (most effective). The powerful, yet easy-to-use tool consists of two different spreadsheets, enabling assessments to be made at either a summary or detailed level.

The assessment tool has 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. It provides you with an assessment against a maturity model that is based on the 15 steps within the 3 phase *Cyber Security Incident response process* presented in the ***CREST Cyber Security Incident Response Guide***, as shown in the diagram below.



The maturity assessment tool is available free of charge to all organisations. It can be downloaded from the CREST website at *www.crest-approved.com*.

B. Background

Many organisations are extremely concerned about potential and actual cyber security attacks, both on their own organisations and in ones similar to them. Dealing with cyber security incidents – particularly sophisticated cyber security attacks – can be a very difficult task, even for the most advanced organisations.

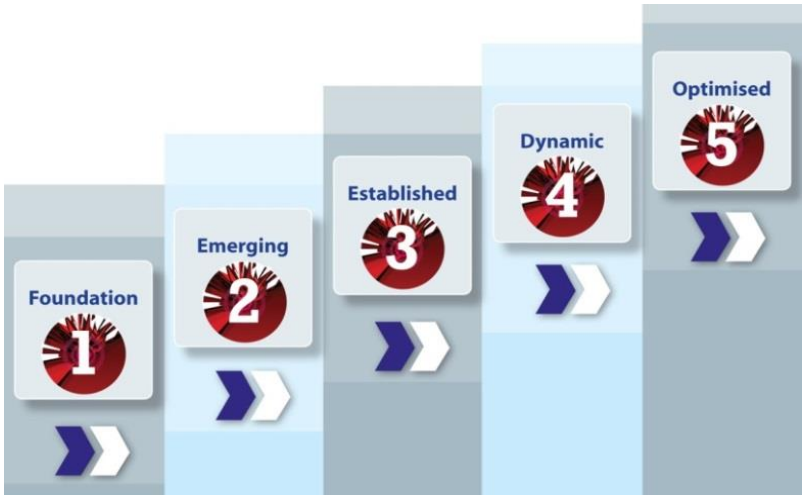
Your organisation should therefore develop a *Cyber security incident response capability*, tailored to meet the specific requirements of your organisation. Having the right capability can help you to conduct a thorough investigation and successfully eradicate adversaries who are deeply embedded in your systems.

Your cyber security incident response capability should consist of appropriately skilled people guided by well-designed, repeatable processes that enable the effective use of relevant technologies. It should enable all types of cyber security incidents - from basic malware infections to sophisticated cyber attacks - to be detected quickly, relevant investigation to be undertaken properly (often involving third party experts) and the spread of any damage to be contained. From this solid base, the source of the incident can be eradicated; appropriate remediation undertaken (and validated); and relevant information and systems recovered.

However, many organisations do not know their state of readiness to be able to respond to a cyber security incident in an appropriate manner. One of the best ways to help determine this state of readiness is to measure the level of maturity of your cyber security incident response capability, addressing:

- People, process, technology and information
- Preparedness, response and follow up activities.

The CREST maturity assessment tool has therefore been developed to help you assess the status of ***your*** cyber security incident response capability. The maturity model used in this tool is based on a traditional, proven model, as shown below.

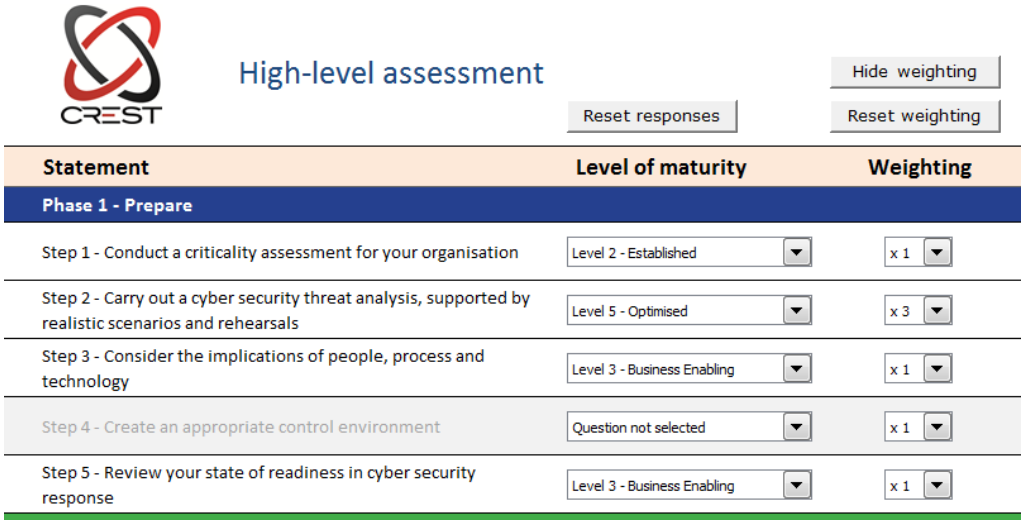


Different types of organisation will require different levels of maturity in cyber security incident response. Consequently, the level of maturity your organisation has in cyber security incident response should be reviewed in context and compared to your actual requirements for such a capability. The maturity of your organisation can then be compared with other similar organisation to help determine if your level of maturity is appropriate.

C. Carrying out an assessment

The assessment tool consists of two separate, but related spreadsheets, enabling assessments of an organisation's cyber security incident response capability to be made at either a summary or detailed level.

The high level version allows a quick overview to be obtained, whereas the detailed tool enables a more precise assessment to be made about the real maturity level of your cyber security incident response capability. The detailed tool is based on the responses given to a series of well-researched questions associated with each of the 15 steps. You can select relevant responses to each question by using the drop-down menus provided in the ***Assessment*** worksheet (see example below).

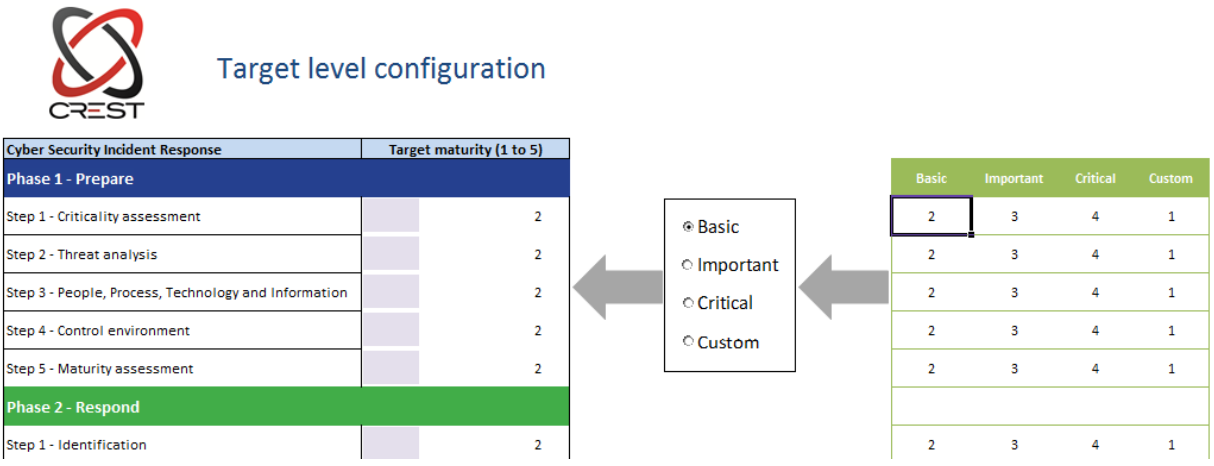


High-level assessment

Hide weighting | Reset responses | Reset weighting

Statement	Level of maturity	Weighting
Phase 1 - Prepare		
Step 1 - Conduct a criticality assessment for your organisation	Level 2 - Established	x 1
Step 2 - Carry out a cyber security threat analysis, supported by realistic scenarios and rehearsals	Level 5 - Optimised	x 3
Step 3 - Consider the implications of people, process and technology	Level 3 - Business Enabling	x 1
Step 4 - Create an appropriate control environment	Question not selected	x 1
Step 5 - Review your state of readiness in cyber security response	Level 3 - Business Enabling	x 1

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.



Target level configuration

Cyber Security Incident Response	Target maturity (1 to 5)
Phase 1 - Prepare	
Step 1 - Criticality assessment	2
Step 2 - Threat analysis	2
Step 3 - People, Process, Technology and Information	2
Step 4 - Control environment	2
Step 5 - Maturity assessment	2
Phase 2 - Respond	
Step 1 - Identification	2

Basic
Important
Critical
Custom

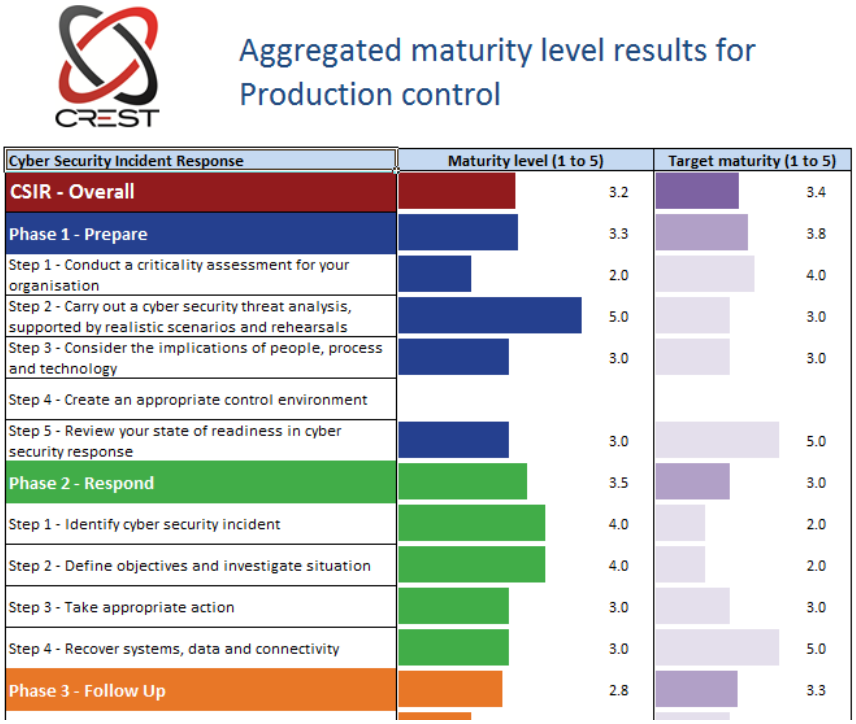
Basic	Important	Critical	Custom
2	3	4	1
2	3	4	1
2	3	4	1
2	3	4	1
2	3	4	1
2	3	4	1

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 cyber security capability, 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.

D. Analysing assessment results

Based on your responses to the questions in the ***Assessment*** worksheets your level of maturity for each of the 15 steps is calculated by the tool using a carefully designed algorithm that takes account of both the level of response to each question and the associated weighting factor.

A useful summary of your results is produced automatically and presented both as a bar chart and radar diagram (see below) in the ***Results*** worksheet, which show the level of maturity for your cyber security incident response capability on the scale of 1 to 5 previously described, comparing this to the target maturity rating, based on the target profile chosen.



Results shown as a radar diagram (see below) allow 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).