

Handling and Assessing NCRA responses

**Summary of activities to do when receiving the NCRA responses**

1. Collate data as soon as it becomes available, as this helps to see the patterns and gaps in the collective data.

1. Look for very similar / identical answers across responses from the same organisation e.g. vulnerabilities all the same.

1. Be willing to go back to the response-sending organisation(s) and check whether it was one or many people doing the responses. There should be noticeable differences in answers if multiple people were involved.

1. Look for common systems in the same sector; they should be there. A missing system can be an indicator that not all systems have been identified, or maybe there is a ‘trust’ issue that needs to be fixed.

1. Check that the systems are at a business functional level, and not something like a small networking component, unless this part is genuinely critical.

1. Compare NCRA responses with any security audit information you may have. There should be a correlation. If not, this may be a hint to ask for more information.

1. Put real energy and time into building the relationships with the organisations. The effort will be rewarded in terms of finding the right cyber security responses at a national level and continuing to have support from the organisations. ☺

**Checklist for assessing the quality of NCRA responses**

* Is the form complete?

We would expect to see all the major questions answered, or ‘placeholders’ included for information that is to follow. The optional information may be provided but it is not essential.

* Does it look as though what is completed look to be done accurately?

We would expect there to be a good level accuracy e.g. word use, spelling, and punctuation, for system names, explanations, and descriptions.

* Has each organisation identified the range of systems expected?

There are a variety of standard systems that could be viewed as critical, covering business, mission and safety; though some straddle more than one area.

* Is there a sensible range of answers per system?

It is unlikely that all responses in each section will score in the same e.g.

vulnerabilities, threats, etc. Therefore, check whether there is a spread of results.

* Have conversations taken place with each organisation to help complete the forms?

Most organisations tend to benefit from a little help or clarification; or may already be seeking help to complete the questionnaires. In these discussions, additional confidence may have been gained from having:

o An appropriate level of seniority present o Access to people with knowledge and experience o Access to people in the right department who own the system o A decent amount of time for discussion o A sense of engagement and enthusiasm towards the NCRA o People involved who have an attention to detail & the ‘big picture’.

* How do the similar system responses from one organisation compare to another?

Given that some systems e.g. cash / accounting systems are found in many organisations, it can be useful to compare responses. This can help to get a sense for the level of risk appetite and basic levels of protection.

* Based on experience, do any of the answers seem odd or unexpected?

It is expected that the people reviewing the answers will have had some experience of the sectors, organisations and the systems within them. It should therefore be possible to make some ‘judgement calls’ on whether the answers seem sensible.

* Are there any unusual or interesting systems reported?

Many systems in an organisation could be classed as critical. It depends on the business, business model, organisational setup, risk posture, etc. However, if unusual systems are reported, it would be useful to check why included and possibly ask more about them. We usually expect just to see functional / service-based systems being classed as critical e.g. core network control system, accounting system, factory control system, generating control system, distribution system, software update system, etc. Note that some of these ‘systems’ will include roles that are done by people and people can be hacked too!

* Are any of the responses particularly high or low?

If answers are too high, it could be a cry for help, wanting attention, or suspecting that funds will be made available to help the organisation; or the organisation really has a genuinely high-risk system. While answers that all appear low could be indicative of an organisation in denial or wanting to cover up risks. Or the organisation really is on top of its cyber risks ☺.

* Have the responses been reported as validated in the organisation?

If the organisation can claim that their system owners, tech director or other responsible members have all helped to form the response it is generally a good sign.

* Has each organisation’s response been ‘signed-off’ at a senior level?

Having a senior responsible owner for the response, who can authorise the release of the response, and claim that the right people have contributed to it, is another good sign.

* Has the organisation reached out for clarification before submission?

If the organisation had any doubts about the meaning of the questions or what sensible responses should be and asked for clarification, then this is yet another good sign.

Ver