

Doing Workshop 2 justice

**Workshop 2 preparation and function**

This is one of the most important documents you will read in relation to the NCRA. The quality of the data that you receive is fundamental to the quality of the NCRA conclusions and recommendations that you will be able to make. Please remember that the lowest data quality you accept **IS** the data quality standard that you accept. Therefore, as a local NCRA team, if you fail to check, fail to challenge, or fail to meet the data quality level required, then you should expect unreliable findings, development of the wrong capabilities, and CNII organisations being more exposed to cyber-attacks. This approach will lead to increased risks to your way of life!

This guide is a supplement to the document named, “[Handling and Assessing NCRA responses](https://www.ncra.pro/_files/ugd/ec5ea3_0ccf84449c4c414e92e9266bbc6c5e75.docx?dn=br_Handling%20and%20Assessing%20NCRA%20responses)”. The UK team has written this guide because all observed local NCRA teams have needed more guidance in the preparation and delivery of Workshop 2.

The starting point for this guidance the completion of Workshop 1, where CNI organisation delegates understand their country’s version of the NCRA questionnaire, details on how to select a NCRA-level system, and guidance on how to use the vulnerabilities yardstick. For the purposes of this guide, the UK team has assumed that those completing the questionnaire were not in attendance at Workshop 1 and did not communicate their NCRA insights. Attendance of the wrong CNI organisations delegates often happens and therefore this guidance helps to fill the gap.

**Immediately after Workshop 1**

**Organise the place for responses.**

The local NCRA team members must organise a suitable place(s) for receiving, storing, and analysing the questionnaires. Please see the [video](https://youtu.be/tW4yCY1SB44) on data security from the [www.ncra.pro](http://www.ncra.pro) website. Given the sensitivity of this aggregated information, the ideal location is a standalone machine into which the NCRA local team can import raw questionnaire data into and export anonymised and pictorialized graphs and charts (sometimes in presentation form) from.

**Immediate questionnaire completion guidance**

If the CNI organisation delegates do not already have a NCRA questionnaire, please ensure you send it out ASAP. To maintain the NCRA momentum gained from doing Workshop 1, the questionnaire you should send it to the CNI organisation delegates with repeated thanks for attending, the rationale for the NCRA, and the following guidance:

* *Identify the NCRA-level systems that relate most closely to your primary business services e.g. production, logistics, and sales.*
* *Coral the right people who own the service and who understand the various IT components that define the system.*
* *Ensure the system boundary is understood, it is often useful to draw architectural pictures of the system, covering the IT stack (network, servers, applications, and common enterprise IT services) and the roles and processes associated with the it.*
* *Please do* ***NOT*** *just give the questionnaire to your IT team and expect them to complete it accurately. Those in the IT team are rarely the business owners for the business services and often misjudge answers.*
* *Ensure that you grade each system identified on its own merits. It is highly unlikely that any two systems within an organisation will have the same CIA ratings, impact, threats, or vulnerabilities. You will have built every system for its own purpose and usually with common but also different applications / components to other systems.*
* *Before answering the impact section, consider the scale of the service that your system relates to e.g. local-only suppliers, through to national monopoly.*
* *Before completing the vulnerabilities section, review the vulnerabilities yardstick built into the questionnaire as a worksheet / tab. Note that it takes constant vigilance, scaled resources, and significant security focus to maintain all vulnerabilities at a low level for any system. Review each lowest vulnerability option in the yardstick descriptions first, if your system does not achieve that, then look at the next highest. Select the level that most closely matches. Note that not all options are applicable to the system under review, if that is the case you should select the lowest.*
* *Ensure that a security-accountable board-level person reviews the answers to each system and asks pertinent challenging questions of the team that has provided the answers to ensure accuracy. This could be a CISO, CIO, COO, or an equivalent.*
* *And if you need to a re-run of any of the information presented in Workshop 1, or you need any help completing the questionnaire, please do contact your sector liaison in the NCRA team.*

**Facilitating the completion of a questionnaire.**

You may, as a member (liaison) of your country’s NCRA team an organisation may ask you to help complete their NCRA questionnaire. You could do this remotely if theirs is just a simple to answer query. Or you may need to sit with them if there are sections of the questionnaire that they need help with.

When to step-in and help an organisation complete their questionnaire is clearly a judgement call, based on their need, and the people you have available. However, as a guide, if the organisation’s system has a high impact (finance, people, reputation, other sectors.) then it is worth helping them earlier. Leaving it later, will mean they complete the questionnaire wrongly and you will call them into a W2 session to explain their answers. This does little for improving relations or gaining support for their continued involvement in the annual NCRA process. However you choose to help, you will need to be able to comment on every aspect of the questionnaire.

**As organisations return their questionnaires**

You should follow a process as each organisation returns their completed questionnaire. Clearly, you need to follow the guidance that is related to data security and the guidance previously mentioned in the document named, “[Handling and Assessing NCRA responses](https://www.ncra.pro/_files/ugd/ec5ea3_0ccf84449c4c414e92e9266bbc6c5e75.docx?dn=br_Handling%20and%20Assessing%20NCRA%20responses)”. However, there are additional checks that suitably skilled and experienced team members can do.

**You should check that the right systems are included.**

Within each organisation’s completed NCRA questionnaire, look at the systems listed in the organisation worksheet and at the top of each corresponding completed system worksheet. Does the organisation look to have identified systems corresponding to their critical services i.e. production, logistics, and sales. Or does it look as though the IT team have been tasked with completing the questionnaire, with systems like routers, switches, databases, servers, firewalls, etc. For reference, only a major telecoms organisation, central IT department, or internet services provider would have a legitimate business service strongly reliant on IT components like routers. Therefore, if an organisation has chosen the wrong level of system granularity it is best to contact the organisation immediately and begin a dialogue, which will result in you explaining to them that they will need to redo some or all of the questionnaire.

**Check whether the system responses are based on ‘as is’ or ‘to be’.**

As a guide, the value of the NCRA is in using the ‘as-is’ information i.e. how each organisation determines each of their systems right now. However, this can be a difficult aspect for the NCRA team to gauge. Many organisations do not want to admit that their systems are not as security performant as they should be and will provide information on what they think you want to see or that which reduces their embarrassment or need for intervention.

Therefore, it is worth doing reviews of specific sections and cross-checks between different sections of the questionnaire responses. For instance:

* Contrast the CIA ratings with the system name / definition.
* Cross check CIA ratings with the vulnerabilities.
* Make use of non-NCRA knowledge when reviewing the responses.
* Know who in each organisation completed their questionnaire.
* Assess whether the impacts make sense.

***Contrast the CIA ratings with the system name / definition.***

Cross-check the system definition against their identified CIA rating for that system. Note that anything that contains sensitive data or sensitive configurations will normally be rated as either “high” or “very high” for confidentiality and integrity. This ensures that their data and configurations remain away from unauthorised eyes and from inadvertent changes. And if the system needs to be near constantly accessible then availability should be “high” or “very high”. A “very high” rating would indicate the system can only be unavailable for seconds or minutes a day, high up to an hour, medium a day, and low anything over a day.

For reference, the higher the CIA ratings are, the more money that an organisation should be spending on their system. And achieving a “very high” rating across all confidentiality, integrity and availability aspects can be extremely expensive indeed.

***Cross check CIA ratings with the vulnerabilities.***

It is perfectly OK with an organisation indicating that they want high or “very high” ratings for the CIA aspects of their system, especially if those levels fit the needs of the system. However, the higher these CIA ratings are, the more focus is needed on cross-checking with their answers to the vulnerabilities. For instance, if confidentiality and integrity are rated high or above, the organisation should have few vulnerabilities related to secure configuration, data security, identity and access management, logging and monitoring, penetration testing, and vulnerability management. And if availability needs to be high or above, then make sure that vulnerabilities related to having a good asset inventory, secure configurations, and incident response are in place.

***Make use of non-NCRA knowledge when reviewing the responses.***

The members of the NCRA team should (ideally) have insights into the organisations’ systems and their configurations. That could be through previous engagements, having worked in those organisations, or previous reports e.g. incidents, info sharing, etc.

Do consider whether the services / systems represented include the systems that you would have identified. Sometimes, organisation overlook critical systems and do not report them. Other than your own specialist knowledge, develop lists of expected systems (see Appendix A for ideas), and look at the responses from other similar organisations for their system choices.

Looking at the vulnerabilities section you will know if they have a training program, a decent monitoring system, an incident response team, using vendor-supported and current software, etc. Where you see discrepancies, it is advisable to make a note for potential follow-up conversations.

***Know who in each organisation completed their questionnaire.***

It can be useful to know which people in each organisation completed the questionnaire. Ideally it should have been a team approach, with board members inc. the CISO, the system owner, the main system users, knowledgeable staff in the IT department, internal cybersecurity team, and anyone else who can usefully answer the questions, being involved. If the questionnaire has just been delegated to the IT department it is likely there will be signs that the answers are ‘off’. For instance, the systems will be IT components like routers, firewalls, servers, all of which are not business service systems. And the vulnerabilities can be minimal, as IT people often do not have the same level of cybersecurity understanding as a CISO, auditors, or other cybersecurity specialists. Therefore, it is a clever idea to ask the organisations, in advance of completing their questionnaire, to do it as a team.

***Assess whether the impacts make sense.***

Looking at the impacts section, you will hopefully have a clever idea of the scale of their operations and whether an outage of a system would have their declared impacts. However, sometimes an organisation does not realise the impact they could have; perhaps they have taken more market share in the last few years and have not had an outage. Or they do not realise that they have become a go-to service for an increased number of organisations and people, who are now dependent on that service / system.

Some impacts are also quite hard to gauge, for instance, financial cost to the nation. Much depends on the scale of usage of the service / system, whether the whole service / system is affected, whether the organisation has effective back-up and recovery approaches, how long the service could be out for (though this should be covered in the description of the reasonable worst-case scenario), and whether dependent organisations have alternatives that they can use e.g. freshwater tanks, portable electrical generators, radios, etc.

Therefore, the NCRA team will need to use their best judgement to determine whether the impacts are realistic. It is worthwhile trying to develop a ‘picture’ aka dependency map of the various dependencies across CNI systems at the information and physical levels. This can encapsulate various data e.g. entities, relationships, metadata (names, descriptions, types, frequency, etc.), criticality, quality indicators, security, etc. A good data graphing tool i.e. database with graphical frontend would be useful here. Note that this is not a feature that is built into the NCRA analytical spreadsheet but needs to be built from the information in the responses, and outside knowledge.

**Determining who comes to workshop 2**

Please remember that Workshop 2 is an opportunity for a full team review of the data that organisations have submitted. Before Workshop 2 you should have entered each organisations’ system related data from their respective questionnaire into the analytic spreadsheet.

**When to ask a CNI organisation in for special attention**

As you assess the data quality and data responses, you will be looking for those organisations that have data gaps and wrongly entered data. This is especially important for those organisations that have identified systems that have an impact level of three and above, as these have national level impacts (i.e. not just localised to the company or a small region). Where an organisation has these systems, and the data looks suspect, it is worth inviting them for a 1-2-1 review session. You should see this as a formal meeting and is especially necessary if an identified organisation has not responded well to friendly requests for data updates.

**Which CNI organisations to worry about (impact level and sector)**

There are CNI organisations that by default are more relevant than others. These tend to be any organisations that have a large market share (30%+) i.e. oligopoly, or higher broaching on monopoly status. These organisations tend to be in the finance, telecoms, utilities, and government sectors, where there may only be one or two suppliers in each category that is of note.

**How to invite the organisation in for a W2 conversation**

The request for attendance at a Workshop 2 meeting is by exception for those organisations that you need to be concerned about. You should make this request formally and with the full support of the NCRA champions e.g. NCRA lead, country premier, governor, etc. You should send it to a senior in-country representative of the organisation, with escalation to an international senior team, when necessary. The invite should detail the importance of the NCRA, the importance to the NCRA of having excellent data from the organisation, and the need for either improved engagement or better-quality data. It should make it clear that your country needs to have high cyber-security confidence in the organisation and its systems, as theirs are the most critical (highest impact).

**Helping the CNI organisations recognise there is no value in bravado.**

In this age of cyber-attacks there are various national and international cyber standards that must be complied with. And the range of cybersecurity standards under which senior members of companies can now be prosecuted for non-compliance is now increasing. So, when an organisation provides information that indicates their systems are more secure than they are, it may leave the organisation more exposed to cyber-attacks and will devalue the conclusions and recommendations from the NCRA. As a NCRA team member, it is your responsibility to make this clear to the representatives from each organisation being invited to attend Workshop 2.

If the organisation is willing, suggest it would be good if members of your local NCRA team help them to complete or revise their questionnaire responses. This will help ensure that they identify the right systems, sections are complete, and data is accurate.

**Approaches to take during Workshop 2 conversations**

The meetings in Workshop 2, with organisations that have critical systems, are to ask the organisation’s representatives various high-level AND detailed questions, which could be open, closed and probing. However, please remember that the NCRA is not an IT audit, and as such the questions should avoid discussing IT resources / components. Please note that a recommendation from the NCRA could be that a selection of systems are independently audited.

**Putting the organisation at ease**

Trust is a huge part of getting good NCRA questionnaire responses. For some organisations this could be the first time they have met you and the NCRA team. Please keep in mind that building strong relationships throughout the process is essential. Getting to a level of trust requires that you like each other and behave in a consistently agreeable manner. Part of that is putting the organisation’s representatives at ease by having warm and welcoming interactions, stating how information provided will be protected, and having the shared goals of keeping critical services operating.

**Opening questions to ask an organisation during W2**

The initial round of questions should focus on making sure the organisation’s representative knows why they are attending and gauging their general approach to cybersecurity. For instance:

* Do you know system ‘X’ would cause impact ‘Y’ if it went off-line?
* Do you realise that we have cyber standards for CNI organisations?
* Do you think that you have answered the questionnaire well?
* Can you tell us more about system ‘X’?
* What is your organisation’s approach to dealing cyber-attacks?
* How do you apply cybersecurity knowledge to protect your systems?
* Can you describe what cyber threat intelligence (CTI) your organisation uses?

Then move onto to ask questions about specific systems that are of interest. Here are some example open / probing questions that you could use / adapt as necessary:

* Can you describe the system configuration for system ‘X’?
* How did you reach that conclusion for the system configuration?
* How do you use evidence from cyber threat intelligence (CTI) and monitoring systems to know who is attacking / likely to attack system ‘X’ and the means they would use / are using?
* In what way(s) does the system have access to the internet?
* Please describe why you think system ‘X’ has a secure configuration?
* What is the fallback plan if system ‘X’ is out of action?
* How long could system ‘X’ be off-line for and is this represented in your reasonable worst-case scenario description?
* If you had another go at identifying all the various information dependencies associated with system ‘X’ what else would you include?
* How useful did you find the vulnerabilities yardstick for completing the vulnerabilities section for system ‘X’?

And finally, with all good questioning, there is value in asking closed (yes / no response) questions to finalise facts. Here are examples, that you could again use / adapt as you see fit:

* To confirm, are you saying you are basing the cyber threats on actual attacks that you have seen via your modern comprehensive monitoring system?
* So, the impact on other sectors is high for finance, government, and tourism, as that is system X’s customer base?
* Just to check, you have never performed a penetration test for system ‘X’ in the last 12 months?
* So, system ‘X’ did suffer a successful cyber-attack 2 months ago?

**Appendix A: Possible critical systems in each sector**

| **Sector** | **Service** | **Example Systems** |
| --- | --- | --- |
| **Communications** | Global internet | BGP routing |
|  | Domestic internet | Cable routing infrastructure |
|  | Mobile telephony | Cell towers infrastructure |
|  | Landline telephony | Exchange centres |
|  | Billing (usage) | Billing systems |
|  |  |  |
| **Finance** | Investment banking (stocks) | Stock exchange |
|  | Domestic banking | Mobile banking apps |
|  | Pensions | Pensions website |
|  | Insurance | Insurance website |
|  | Clearing | SWIFT network |
|  |  |  |
| **Food** | Farming | Industrial control systems |
|  | Processing | Industrial control systems |
|  | Distribution | Logistics systems |
|  | Storage | Warehouse system |
|  | Governance / regulation | Import / export processing |
|  |  |  |
| **Mining** | Welfare (air, water) | Water extraction |
|  | Mineral extraction | Industrial control systems |
|  | Distribution | Logistics systems |
|  | Business (sales / purchases) | Billing systems |
|  |  |  |
| **Energy** | Generation | Industrial control systems |
|  | Storage | Industrial control systems |
|  | Distribution | Industrial control systems |
|  | Billing (sales / purchases) | Billing systems |
|  | Demand management | Industrial control systems |
|  |  |  |
| **Water** | Water treatment (potable) | Industrial control systems |
|  | Water treatment (sewerage) | Industrial control systems |
|  | Distribution | Industrial control systems |
|  | Billing (sales / purchases) | Billing systems |
|  | Reservoir management | Industrial control systems |
|  |  |  |
| **Health** | Hospital services | Patient management systems |
|  | General Practitioner services | Patient management systems |
|  | Procurement | Supply chain management |
|  | Health info distribution | Websites |
|  | Medical record services | Records management systems |
|  | Epi / Pandemic response | Track and trace |
|  |  |  |
| **Transport** | Control centres | Radio / telephony systems |
|  | Billing | Billing systems |
|  | Depots | Logistics systems |
|  |  |  |
| **Public Safety** | Legal services | Records management systems |
|  | Court services | Records management systems |
|  | Policing services | Police national database |
|  |  |  |
| **Government** | Treasury services | Finance systems |
|  | Tax and revenue services | Money collection system |
|  | National security | Security databases |
|  | Welfare | Money distribution systems |

**Appendix B: Starting point architectural views of systems**

Enterprise architecture is a whole discipline, which organisations use it to build up a solid understanding of their IT enterprise. The technical aspects usually start with conceptual (high-level) diagrams, moving into logical (non-vendor specific descriptions) views and then physical (vendor / application specific) views. With each level of detail comes more metadata and a better understand of interfaces and linkages. If done well, organisations model their full enterprise architecture and the store the details in a suitable enterprise architecture modelling tool. But even views of the IT enterprise stored in PowerPoint have value.

The following simple views of an IT enterprise are at the conceptual level and are here to provide an appreciation of the sorts of diagrams that can help explain the system in context.





