

NCRA Cycle

# Introduction to the NCRA cycle

This short document provides a high-level overview of the National Cyber Risk Assessment (NCRA) and the role that it plays in the cyber security capacity building cycle.



The NCRA process has 4 key steps that form a cycle and for the process to be effective and have a measurable impact on the security of a nation’s Critical National Infrastructure (CNI) it is essential that all 4 steps are completed in each cycle and that the cycle is repeated on a regular basis. The following sections describe each of the 4 steps in the NCRA driven capacity building lifecycle.

## Measure the risk with a survey questionnaire

The first step is to identify the CNI sectors and systems and get an accurate national picture of the cybersecurity risks to each system. The measurement of the risk is done using a short survey questionnaire that is securely sent out to the owners of the CNI systems in each sector. The survey questionnaire gathers information about the cyber security approach of each organisation and the characteristics of each system in terms of threats, impacts, exposure and vulnerabilities.

The survey process is usually launched during an initial workshop with representatives from all the organisations that own or are responsible for CNI systems. This workshop provides the opportunity to gain trust and buy-in from the CNI community and explain how to complete the questionnaire.

This interactive survey approach has the additional benefit of assisting with the formation of a collaborative community and partnership between government and the private sector.

## Analyse the survey data

Once the results from the survey questionnaire are returned to the local NCRA team they will need to be checked for accuracy and consistency before being fed into the analysis process. During this analysis the survey data is copied into an analytic spreadsheet that will automatically generate national, sector and organisational views of the cyber security risks.

This analysis also gives insights into the nature of the cyber security threats and vulnerabilities for each system. Each system is given a score for the impact from and likelihood of a cyberattack and this allows systems to be assessed and prioritised according to risk.

## Prioritise investment in national cybersecurity capacity building

The next step in the process is to use the risk assessment information to identify the highest risk systems and any systemic cyber security vulnerabilities across sectors or the nation. It is typical at this stage to identify priority levels and group systems accordingly so that risk mitigation activities can be focussed on where they will have the greatest impact. National cyber security capacity building initiatives can also be prioritised to address the most common gaps and vulnerabilities. One of the deliverables from the NCRA is a summary report that presents the findings form the risk assessment at the national and sector level. The summary report also provides a set of recommended capacity building activities designed to mitigate the identified risks.

The prioritisation stage is particularly important as there will always be more risk mitigation work to do than any nation has the resources to complete and it is critical to focus the available effort where it will have the greatest national impact.

## Act to implement cybersecurity capacity building initiatives

The final step is in many ways the most important as this is where the insights into risk, threats and vulnerabilities are used to take action to mitigate the risk. This action will typically take the form of a number of projects that focus on building cyber security capacity to fill gaps highlighted in the risk analysis. These will be unique to each nation but could include improving cyber security skills, implementing security and resilience standards for CNI, incident management and building the capabilities to counter cybercrime.

## Repeat the cycle

Finally, it is important to regularly (e.g. annually) return to the measurement stage and repeat the NCRA process. In this way it will be possible to track changes to the national risk picture, measure the effectiveness of the actions taken and adapt national priorities to achieve the greatest impact on the security of key CNI systems.