*<Country Logo / NCRA project logo>*

*<Country>* NCRA

Project Management Plan

Version *<1.0>*

Date: *<dd/mm/yyyy>*

**Document control**

 **Document information**

|  |  |
| --- | --- |
|  | **Information** |
| Document Owner | *<Owner Name>* |
| File Name | *<Name>* |

**Document history**

|  |  |  |
| --- | --- | --- |
| **Version** | **Issue Date** | **Changes** |
| *<1.0>* | *<Date>* | *<Section, Page(s) and Text Revised>* |
|  |  |  |
|  |  |  |
|  |  |  |

**Document approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Name©** | **Signature** | **Date** |
| NCRA Sponsor |  |  |  |
| NCRA Lead |  |  |  |

**Contents**

[The Plan 5](#_Toc52252219)

[Background to the National Cyber Risk Assessments 5](#_Toc52252220)

[Purpose of National Cyber Risk Assessments 5](#_Toc52252221)

[Summary of this NCRA project 5](#_Toc52252222)

[NCRA project objectives and inferred outputs 5](#_Toc52252223)

[NCRA Approach 5](#_Toc52252224)

[NCRA scope – work packages 6](#_Toc52252225)

[NCRA Scope - CNI Organisations 6](#_Toc52252226)

[NCRA project organisation structure including roles and responsibilities 7](#_Toc52252227)

[NCRA schedule – high level 8](#_Toc52252228)

[Interfaces and dependencies 9](#_Toc52252229)

[Assumptions 10](#_Toc52252230)

[Monitoring and acceptance 10](#_Toc52252231)

[NCRA budgets / funding 11](#_Toc52252232)

[NCRA Project communications / stakeholder engagement approach 12](#_Toc52252233)

[Data quality approach 12](#_Toc52252234)

[Data security approach 13](#_Toc52252235)

[UK NCRA team support approach 14](#_Toc52252236)

[Initial NCRA risk and issues log 14](#_Toc52252237)

[Appendices for the plan 16](#_Toc52252238)

[App A: Full List of deliverables 16](#_Toc52252239)

[App B: List of all CNI Organisations to be invited 17](#_Toc52252240)

[App C: Completed RACI chart 18](#_Toc52252241)

[App D: Baseline resourced schedule 19](#_Toc52252242)

[App E: Full List of interfaces & dependencies 21](#_Toc52252243)

[App F: Full list of assumptions 22](#_Toc52252244)

[App G: Full communications and engagement approach 23](#_Toc52252245)

[App H: Full approach to achieving data quality 25](#_Toc52252246)

[App I: Full approach to achieving data security 26](#_Toc52252247)

[App J: Full list of risks and issues 27](#_Toc52252248)

***Template guide***

***How to use this template***

*This is a guide to competing a NCRA project management plan. The sections detailed here are the ones that you are advised to complete.*

***Text in blue italics*** *is designed to help you complete each section. This text should be removed before you issue the document*

***Examples in red italics*** *have been included. You should amend where appropriate with information relevant to your NCRA, and change the colour to black and remove italics when done.*

*.*

# **The Plan**

## **Background to the National Cyber Risk Assessments**

Since 2018, the UK Home Office, in partnership with the UK’s Foreign & Commonwealth Development Office (FCDO), has worked with a number of African Commonwealth countries to help them implement National Cyber Risk Assessment (NCRA) projects.

By providing guidance, tools, training and support, these projects have enabled the national local cybersecurity teams to conduct their first complete cyber risk assessment cycle.

However, with cyber risks to Critical National Infrastructure (CNI) increasing there is a need to scale the number of countries that can perform a NCRA independently. To achieve this, the UK’s Home Office cyber team has developed a web portal containing all the materials needed for countries to successfully deliver their own NCRAs.

## **Purpose of National Cyber Risk Assessments**

Experience shows that conducting national cyber risk assessments is an essential cybersecurity enabler that provides a repeatable ‘data-driven’ picture of national cyber risks. This picture can be used to: inform national strategies and policies; create a Critical National Infrastructure (CNI) asset register; and prioritise the investment of scarce resources on mitigating risk to the most critical national assets.

## **Summary of this NCRA project**

This NCRA project management plan provides an overview of the tasks, resources and approaches needed to deliver one cycle of *<* *Country’s >* NCRA in *<2020/21>.* *<Country’s> <team name / department>* will lead the delivery of the NCRA project, using the materials and insights available in the NCRA portal. If requested, the UK Home Office’s cyber team can be available to provide reviews at critical points in the NCRA process.

## **NCRA project objectives and inferred outputs**

1. To gain an ***understanding of the risks*** from cyber-attacks and vulnerabilities to <country’s> Critical National Infrastructure.
2. To use the NCRA conclusions to create ***actionable recommendations*** to minimise cyber risks to the Critical National Infrastructure.
3. To build a baseline ***asset register*** of the CNI organisations and the Critical National Infrastructure that each organisation owns.
4. To assist in the creation of a ***collaborative CNI / Cybersecurity environment***, where organisations can trust each other to share relevant cyber information.
5. To acquire the ***skills and national capability*** to deliver further NCRA cycles, completely independently of the UK team.

## **NCRA Approach**

The NCRA will be conducted in five sequential, but slightly overlapping stages. The main points of these stages are described here:

* Stage 1 – Preparation / scoping: Agree the scope and compete this plan for the NCRA; identify <*country*>’s CNI stakeholders; and ensure that all the required approvals and resources are in place.
* Stage 2 – Survey (inc. workshop 1): Explain the NCRA benefits to CNI organisation representatives. Gather data about cyber security risk to critical systems by sending a survey questionnaire to the public and private sector organisations that own CNI in <*country*>.
* Stage 3 – Analysis (inc. workshop 2): Ensure returned surveys contain good quality data. Analyse the data using spreadsheet tools that enable each aspect of cyber security risk to be visualised and analysed at a national, sector, organisation, and system level.
* Stage 4 – Conclusions (inc. workshop 3): Present and discuss the risk insights. Recommend actions resulting from the analysis. Document the final conclusions in a report.
* Stage 5 - Next steps: Use the NCRA recommendations to develop an action plan that addresses the highest priority CNI risks.

## **NCRA scope – work packages**

The successful delivery of a NCRA requires that it is scoped correctly. This high-level Work Breakdown Structure (WBS) graphically describes the main work streams and work packages that will be completed. The full list of associated project deliverables is included in the appendix.

*[It is recommended that you use this as the starting point for your own work breakdown structure, and then use it to create a detailed NCRA project schedule. Note that numbering (not shown in this version) is often used to denote a hierarchy e.g. 1 at the top, 1.1 for next tier down, and 1.1.1, 1.1.2. for peers. Note that this diagram was drawn in the free and easily downloadable graphing package ‘Draw.io’, which also has a MS Word plugin for inserting diagrams into documents.]*



*[It may also be useful to identify any exclusions that the NCRA project will not cover. These will be specific to your country but will help ensure there is no confusion over the scope and reduce chances of ‘scope creep’.]*

## **NCRA Scope - CNI Organisations**

For our first NCRA we have chosen the sectors and organisation types that we must get system risk information about. Based on our country’s needs we think these are the most important:

*[Here is an example list, it should be replaced with your list:*

* *Telecoms – Mobile Providers and Internet backbone provider*
* *Financial Services – Commercial banks, Retail banks, Clearance bank(s), Commercial Insurers*
* *Energy Services – Hydropower, Wind Power, Oil, Coal and Gas*
* *Government – All government departments inc. Foreign, Home, Treasury, Mining, etc.*
* *Tourism – Hotel operators,*
* *Health – Hospitals,*
* *Education – Universities*
* *Transport – Shipping, Rail, Airports*

*It should be your intention to get at least the top 3-5 organisations that make up 60-80% of the market share of each sector involved. This way you will have a reassuring amount of coverage. Note that some sectors, depending on how they are structured may only have 1 or 2 organisations. This is OK, get all of them on board.]*

A full list of the needed organisations, that contribute to these sectors, is shown in the appendix.

## **NCRA project organisation structure including roles and responsibilities**

*[You may wish to start with some positive text about the team, and team selection e.g.*

*“This NCRA project is opting to start with a strong, well-resourced team of knowledgeable, experienced and skilled people. There is expertise from all the sectors, together with expert Excel skills and cyber security systems knowledge.”*

*However, if this is not the case then you should rephrase this and identify resourcing gaps in the risks section; with actions to fix them.]*

The roles structure for this NCRA project, and interaction with CNI organisation representatives will be aligned as follows:

*[Below is an example structure, if this doesn’t work for you, please create your own:]*



]

We are aiming to fill these NCRA Team roles with the following people, from these organisations*:*

*[You need to update this list with the real information that you have available. To start, you may wish to include a number of people for each role; not everyone will be available and some may not accept the role].*

| **Job**  | **Name of NCRA team member** | **Position**  | **Organisation** |
| --- | --- | --- | --- |
| *Minister* | *Name of Person 1* | *e.g. head of Cyber Ministry* | *e.g. Cyber Ministry*  |
| *Department Head* | *Name of Person 2* | *e.g. head of CERT* | *e.g. Country's CERT* |
| *NCRA Team Lead* | *Name of Person 3* | *e.g. highly trusted senior staffer in CERT* | *e.g. Country's CERT* |
| *Liaison - Government* | *Name of Person 4* | *e.g. government director* | *e.g. Homeland security* |
| *Liaison - Financial Services* | *Name of Person 5* | *e.g. member of financial services regulator* | *e.g. Fin-Reg* |
| *Liaison - Energy* | *Name of Person 6* | *e.g. member of energy sector regulator* | *e.g. Energy-Reg* |
| *Liaison - Telecoms* | *Name of Person 7* | *e.g. member of telecoms regulator* | *e.g. OfTel* |
| *Liaison - Another sector* | *Name of Person 8* | *e.g. direct of financial services regulation* | *e.g. A.n.other* |
| *Events organiser(s)* | *Name of Person 9* | *e.g. Contractor who does events* | *e.g. Events 'r' us* |
| *Cyber Expert - Telecom systems* | *Name of Person 10* | *e.g. CERT staffer for telecoms* | *e.g. Country's CERT* |
| *Cyber Expert - Financial systems* | *Name of Person 11* |  | *etc* |
| *Cyber Expert - General* | *Name of Person 12* |  | *etc* |
| *Results presenter (often Team Lead)* | *Name of Person 13* | *e.g. highly trusted senior staffer in CERT* | *e.g. Country's CERT* |
| *Data Analyser(s)* | *Name of Person 14* | *e.g. manager for data science*  | *e.g. Data science unit* |

*[If there are gaps and risks associated with the team you may wish to include some words like*

*“Note that there are still some risks and decisions to be made to confirm this line-up. However, the essential roles have been filled and a critical mass has been achieved”]*

The full RACI mapping is shown in the appendix.

## **NCRA schedule – high level**

*[It is useful to include a summary graphic that highlights the main stages of the NCRA project and the major milestones. Note that this is effectively a cartoon, and it is not a substitute for a proper schedule. You may wish to include the proper resourced schedule in the appendix to provide a baseline. The schedule should be updated every week as progress information is received and processed.]*

Attached below is our summary graphic of the NCRA timeline. A full baseline version of the schedule, including the majority of activities, is included in the appendix.

*[Please edit the diagram with your expected months, e.g. Dec to May. And include any changes that reflect your detailed schedule e.g. names of stages, specific milestones. You may even wish to add actual dates against the milestones]*



## **Interfaces and dependencies**

This section identifies any other groups, projects and organisations that will be involved in the project or will be impacted by the project*.*

*[Please add or delete dependencies / interfaces based on your own knowledge. For example, if the project is dependent on an external product or an external decision.*

*To give some ideas, some examples are shown in the grid below. If there are more than 5, you may wish to include the most important here, and the full list in the appendices section.]*

| **Interface or dependency with:** | **Description** | **Management plan** |
| --- | --- | --- |
| *Organisation X recruitment team* | *Recruitment of team lead manager by x date* | *Role and responsibility documented in project plan & RACI chart. Exact skills profile and job description to be written.*  |
| *Organisation Y cyber security experts* | *Ad-hoc access to cyber security experts to review NCRA responses* | *Role and responsibility documented in project plan & RACI chart.* |
| *Government strategy and policy unit* | *The strategy unit needs to be prepared to receive the NCRA recommendations, if they are to be used.*  |  |
| *Minister X’s approval to engage organisations in Sector Y* | *Ministerial approval is required to engage organisations in Sector Y.*  |  |

## **Assumptions**

This section lists the assumptions that have been made in order to conceive this project and to plan it. Assumptions will be tested for validity on a weekly basis as part of the project review meetings.

*[Assumptions may have been made around legislation, other projects, availability of funds, market conditions, availability of specific people, access to organisational data, etc.*

*The most important should be listed and actions put in place to measure / test whether the assumption remains valid. If an assumption becomes invalid you may need to revisit your approach or accept a different result.*

*Some examples are listed in the grid below. Please add or delete assumptions based on your own knowledge. If there are more than 5 assumptions, you may wish to include the most important here, and put the full list in the appendices section.]*

| **Assumption:** | **Impact of invalidity:** | **Action to test:** |
| --- | --- | --- |
| *CNI organisations provide high quality data* | *Recommendations will be poor / inaccurate. NCRA & team suffers reputational harm.*  | *Review each response as it arrives. Activate remedial quality improvements* |
| *CNI organisations accept our secure environment*  | *CNI orgs do not provide their CNI system data* | *Ask them directly if they are comfortable / show they steps taken towards security* |
| *Covid19 does not cause economic downturn*  | *NCRA funding could be curtailed with loss of resources* | *Stay engaged with financial authority. Check if NCRA funding remains ringfenced.* |

## **Monitoring and acceptance**

The NCRA project needs to be monitored for progress, errors, and completion. The following checks will be used:

*[Please apply your favoured approach(es) for checking that a project is on track. This should cover:*

* *How feedback will be collected on the value of this project by the NCRA stakeholders.*
* *How the Project Sponsor will determine that the NCRA project has been delivered to specification and has achieved the intended impact.*
* *The timescales and milestone dates for collecting the above information.*
* *How, when and to whom the feedback will be reported.*

*Outlined below are just some examples.]*

* *CNI organisations will be asked, after workshop 1, if they have fully understood the purpose of the NCRA AND will deliver their completed questionnaires.*
* *CNI organisations will asked to discuss the NCRA results feedback during workshop 3; and identify whether risk views are expected or need adjusting.*
* *The project sponsor will accept that the NCRA project has delivered if:*
	+ *There is proof that the data collected was to a good standard.*
	+ *That at least 60% of the invited CNI sector organisations (especially the largest sector organisations) have completed and returned their questionnaires.*
	+ *There is acceptance from the CNI organisations and NCRA team that the findings are a true and accurate picture of <country’s> cyber risk.*
	+ *The NCRA project completes on time and within budget.*
* *The project will have delivered on time if:*
	+ *Workshop 1 happens by <dd/mm/yyyy>.*
	+ *Workshop 3 happens by <dd/mm/yyyy>.*
	+ *‘Next steps’ are happening by <dd/mm/yyyy>.*
* *The Team lead will hold a review meeting on <Tuesday mornings> each week, to check on:*
	+ *Number of questionnaires returned; from sectors / organisations.*
	+ *Quality of data in questionnaires; including remedial actions.*
	+ *Spend to date vs budget vs delivery.*
	+ *Changes to risks, assumptions, etc.*
	+ *Deviances from timescale / achieving major milestones.*
	+ *Resource availability for continued delivery.*
	+ *Any feedback from the CNI organisations that should be acted upon.*

## **NCRA budgets / funding**

*[In comparison to the costs of fixing a major CNI cyber event, a risk assessment is a trivially low-cost initiative! However, you will need to identify the costs of: what needs to be produced, people’s time, materials, venues, refreshments, security items, software licences, and logistics. We would also suggest holding a contingency fund just for the unexpected, and to cover mitigating risks. You should include in the plan what you think the total cost will be, and all costs should be in your preferred currency. Examples are shown here, but there maybe others that you need to include.]*

*Ensure someone is in charge of managing the finances and approving the spend on activities and products.*

In comparison to the costs of fixing a major CNI cyber event, a risk assessment is a trivially low-cost initiative! We have budgeted the cost of an NCRA at c.*£50000* This includes the costs for all expected activities and products, noting a 10% contingency / reserve budget is included for mitigating risks and dealing with the unexpected. These are shown below:

| **Activity / product:** | **Information**  | **Budget:** |
| --- | --- | --- |
| *Secure server / desktop* | *A Windows 10 Pro desktop* | *£800* |
| *Software licences* | *MS Excel / Project / Office 365* | *£500* |
| *Travel to visit CNI organisations* | *Costs of travel e.g. cars, accommodation, food, etc.* | *£5000* |
| *Venues and refreshments for workshops* | *3 workshops for up to 100 CNI representatives, held in major city conferencing rooms* | *£8000* |
| *A man-years’ worth of equivalent time* | *The combined salaried costs for all the members of the core team. This may already be factored into their job descriptions / roles.*  | *£30000* |
| *Contingency* | *Reserve funds for fixing risks.* | *£4500* |

## **NCRA Project communications / stakeholder engagement approach**

*[You will need to know how you are planning to engage with all your stakeholders; when this is going to happen; what you intend to say; and who is going to say it to whom. Here are some aspects to consider:*

* *You should expect that some CNI organisation representatives will be reluctant to be involved, so how will you convince them?*
* *You should expect some organisation’s representatives will not understand the process or aspects of the questionnaire, so how will you help them learn?*
* *You should expect some representatives to get their data returns wrong, so how will you help them to give better answers?*
* *You can expect some pointed questions about data security, so how will you reassure them?*

*Ensure someone is in charge of communications, and that stakeholders are being engaged, are satisfied with the interactions, and can see the results of their feedback!*

*The examples below go some way towards engagement planning but you will need to consider the NCRA and your stakeholders in your context.]*

We have a lot of stakeholders in our NCRA project, and we need to get the right level of engagement with all of them; with increased engagement at specific times. Here we outline the major parts of our intended communications approach, noting a fuller version is included in the appendix.

* *To reassure the minister that we have control of the NCRA: we will provide weekly 1-page highlight reports. These will explain what we have achieved, what is coming up, and any risks or issues that we need to escalate.*
* *To keep the CNI organisations engaged: we will hold an initial workshop aimed at all of them. We will use our sector liaisons to get feedback often, so we can act on it. We will provide them with access to the CNI owners section of the NCRA portal.*
* *To get the CNI organisations to return high quality data: We will thank those that have returned their data to a high standard on time. We will reach out and ask for meetings to discuss gaps and inconsistencies in the data. We will aim to meet on their premises to discuss.*
* *To keep the CNI organisations aware of our progress. We will hold 3 main workshops. We will provide fortnightly comms explaining where we have reached and what is happening next, including ‘save the date’ style information. We will be transparent about how we are really doing.*
* *To reveal the results of the NCRA analysis to the CNI Organisations: We will hold a special feedback session. We will augment the session with a fun cyber exercise to get them in the mindset of thinking about cybersecurity for the CNI. We will ensure that suitable refreshments are provided as we want them alert and willing to ask questions.*
* *To get the CNI organisations to discuss the findings in their sector. We will break each sector into a separate area. We will use our liaisons to facilitate discussions. We will write 2-page sector reports that convey findings specific to each sector. We will seed the discussions with questions for the liaisons to ask – some generic and some based on the findings.*

## **Data quality approach**

*[You must ensure that you can get the best quality data from the CNI organisations. This can be a difficult task. Some organisations will fail to deliver anything, some will not enter into the spirit fully, some will just make mistakes.* ***Data quality is probably the area in the NCRA where you will collectively need to put the most effort, and keep check of responses!*** *Therefore, you will need to have people who are trusted, liked and knowledgeable to talk to the CNI organisation representatives – possibly at many levels of seniority. There is a video on the portal that explains many of the steps you should take.*

*Ensure someone is in charge of data quality, and that you really are getting great quality data!*

*In this section of the plan, you should identify what you are specifically going to do to get great data quality. Some suggestions are provided but much more could be done. A fuller data quality plan could be better articulated in an appendix.]*

Great data quality is essential if our final results are to be accurate, believed and considered for inclusion in cyber strategies, policies and risk reduction initiatives. To ensure the data meets the necessary standard we will:

* *Provide guidance to the CNI organisations, including examples of what great quality responses look like.*
* *Sit with them and help them complete their questionnaires; asking questions to understand how they are reaching their conclusions.*
* *Use the MS Excel version of the questionnaire, and the analytic spreadsheet with their respective built-in ‘mechanistic’ data checkers to assess gaps and likely inconsistencies.*
* *Use our cyber systems experts to review the questionnaire responses, and highlight anything they find suspicious and worth a follow-up.*
* *Do multi-level engagements to help resolve any data clarity issues e.g. Sponsor or Minister to CEO, and Team-lead to director of system owner’s area.*

## **Data security approach**

*[CNI organisations will likely consider the data they are giving to you as sensitive. Therefore, one of your tasks is to protect it. There is a video on the portal that explains many of the steps you should take. And you can tell your CNI organisation reps that you have taken them.*

*Note that this goes beyond physical and cyber security: this is all about who is actually trusted to see the data!*

*Always consider, if the data got in the wrong hands, could it cause embarrassment? Or help cyber-attackers focus their efforts?*

*Ensure someone is in charge of data security, and spot checks are done to ensure it is functional and effective!*

*In this section of the plan, you should identify what you are specifically going to do to secure the data. Some suggestions are provided but much more could be done. A fuller data security plan could be articulated in the appendix.]*

Our CNI organisations are trusting us with data about their systems on which our country depends! Although this data is high-level, its loss or misuse could cause embarrassment and aid cyber-attackers. We are therefore taking steps to strongly safeguard the data. This covers the period from data being sent to us, through analysis and presentations, to disposal. These actions are best seen in the data security appendix. However, the top five are listed here:

* *Completed questionnaires will be sent encrypted over secure messaging services, with passkeys sent via other secure channels.*
* *The questionnaire responses will be held on an encrypted computer, in a locked room, in a military-guarded building.*
* *Only two security-vetted people will have access to the data analysis computer: the team lead and the data analyst. They will each have different non-admin usernames and passwords.*
* *The computer will be standalone; with all connectivity disabled, <via the bios/ wire removal>, except one USB socket.*

## **UK NCRA team support approach**

*[The UK Home Office’s cyber team is unable to devote full-time cyber specialists to this NCRA. However, we have identified a number of points in the process where you could ask for review-based help. Of course, you don’t have to take us up on the offer. It’s your data, your CNI organisations and your results. However, if you do want some help then you will need to share dates when you think you will be ready for us to help you. If you choose not to, you can delete this section.]*

For our first NCRA we have chosen to ask the UK Home Office’s cyber team for help. This will be to review the progress of our NCRA and offer suitable guidance. Specifically:

* *A review of this plan before it goes for approvals. We expect this to be between <dd/mm/yyyy> and <dd/mm/yyyy>.*
* *A review of the draft Probability Impact Grid, to help with our ‘tuning’ of the scoring mechanism in the analysis spreadsheet. We expect this to be between <dd/mm/yyyy> and <dd/mm/yyyy>.*
* *A review of the analytic pictorial outputs, to help us draw conclusions about the insights that we can feed into our NCRA presentation(s) and report(s). We expect this to be between <dd/mm/yyyy> and <dd/mm/yyyy>.*

## **Initial NCRA risk and issues log**

*[All projects have risks, and when they occur, they are classified as issues. Both risks and issues need actions to resolve them. Risks and issues should be reviewed at least weekly, with suitable effort assigned for review and mitigation.*

*Ensure someone is in charge of risk management, and there is total clarity about who is going to deal with resolving each one!*

*Not all the risks will be in your control to fix. Some will require that you work with your stakeholders to do so.*

*A set of common risks and mitigating actions have been set out as examples.]*

An analysis of the NCRA plan has shown that we have a range of risks that we need to mitigate. We have chosen to list the top five here, with a full list in the appendix. The team lead has a standing weekly task to review the risks. Should risks occur we are dedicated to getting them mitigated as best as possible, and as quickly as possible.

| **Risk** | **Impact** | **Likelihood** | **Owner** | **Mitigating action(s)** |
| --- | --- | --- | --- | --- |
| *Data quality is below standard* | *H* | *M* | *Team lead* | *Do the mitigation tasks identified in the data quality plan e.g. identify where data needs improvement; ask organisations to re-do; do together in a join team-org meeting; send in some additional help; remove from analysis.*  |
| *CNI organisations don’t engage* | *M* | *H* | *Team Lead* | *Do the mitigation tasks identified in the Engagement plan e.g. call & write; hold additional explanation meetings; get sponsor to engage with organisation’s board members; change cyber laws to make response compulsory (long term ambition!)*  |
| *Data is lost / stolen* | *H* | *L* | *Team lead* | *Do the mitigation tasks identified in the Security plan e.g. lockdown existing data, work out whose data is missing, alert them, carry out investigation.* |
| *Resources unavailable* | *M* | *L* | *Sponsor* | *E.g. Identify new people; refocus efforts of existing people.* |
| *Country disruption* | *M* | *?* | *Sponsor* | *Determine level of impact, identify workarounds; reschedule meetings and gatherings.*  |

# **Appendices for the plan**

## **App A: Full List of deliverables**

This section identifies all the major project deliverables*. [This section includes all the deliverables we would expect to be created / issued in an NCRA. You may wish to identify more]*

|  |  |  |
| --- | --- | --- |
| **Deliverable:** | **Related to Scope item:** | **Description:** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## **App B: List of all CNI Organisations to be invited**

This section identifies all the sectors, organisations and lead points of contact*.*

*[This section identifies all the sectors, organisations and lead points of contact. You may wish to identify more information e.g. phone numbers, position in company, main services, etc.]*

|  |  |  |
| --- | --- | --- |
| **Sector:** | **Organisation** | **Main point(s) of contact:** |
| *<e.g. Telecoms>* | *<e.g. Telco Max>* | *<name 1>* |
| *<e.g. Financial Services>* | *<e.g. Uber Bank>* | *<name 2>* |
| *<e.g. Energy>* | *<e.g. HydroPower>* | *<name 3>* |
| *<e.g. Government>* | *<e.g. Homeland Security>* | *<name 4>* |
|  |  |  |
|  |  |  |
|  |  |  |

## **App C: Completed RACI chart**

This section identifies the main people associated with the national local NCRA team, their roles, and their various responsibilities.

*[This section identifies all the names of people associated with the NCRA local team and delivery of the NCRA. The RACI chart in Excel form (not this picture) is downloadable from the NCRA portal. You should identify who is doing what role, and what their R, A, C or I action is in relation to each task.*

*Note that the responsibilities should align to the plan.*

*Further information is available about RACI charts in video and through internet searches. It is a great tool for providing clarity on who is doing what!]*



## **App D: Baseline resourced schedule**

*[It is advisable to create a schedule in a proper scheduling tool like MS Project. However, this is expensive software and cheaper options are available, including using MS Excel to lay out tasks, resources and timelines.*

*The list below gives you a good idea on the range of tasks that are required at each stage. However, there will be others that need to be factored in based on your country’s context, the plan, and what you want to achieve. You may also wish to include activities that you expect other projects / organisations to do – this could come from your dependencies list. Remember to add milestones, as these provide a focal point for delivery and acceptance.]*

| **Stage & Purpose** | **Team activities** |
| --- | --- |
| **Preparation**To ensure that everything is in place to successfully complete an NCRA project.  | * *Identify the senior sponsor for the project.*
* *Gain formal approval for the project.*
* *Identify the CNI-owning organisations who will participate in the project.*
* *Identify people for the local team roles.*
* *Scope and tailoring options.*
* *Produce the plan for the project.*
* *Tailor and use the ‘standard letter’ to request formal approval for the project.*
* *Tailor the survey questionnaire (word and / or excel versions)*
* *Ask UK team to review the plan.*
* *Approve the project proposal/plan, survey method and survey questionnaire.*
 |
| **Survey**To engage with the organisations who are responsible for CNI assets and conduct the risk assessment data gathering exercise using the survey questionnaire.  | * *Tailor standard letter to request CNI organisations participate in the NCRA project.*
* *Contact CNI owning organisations to request. participation in the survey*
* *Identify official Windows laptops or desktops that will be used to store the survey data.*
* *Host a launch event or workshop for the CNI stakeholders, if possible.*
* *Provide CNI stakeholders with access to the training material that has been specifically designed to help them complete the survey questionnaire.*
* *Send out the survey questionnaire to each participating organisation.*
* *Ensure that survey questionnaires are returned on time.*
* *Read the guidance on quality checking the survey returns.*
* *Check the quality of the survey returns.*
* *Tailor and use analytic spreadsheet that will hold the survey results.*
* *Ask UK team to review a few ‘anonymised’ responses where data is suspect.*
 |
| **Analysis**To combine the data from the survey questionnaires, analyse the resulting risk charts and conduct the assessment.  | * *Quality-check and import the data from the survey questionnaire spreadsheets into the analytic spreadsheet.*
* *Generate the risk assessment charts.*
* *Contact the CNI owning organisations to resolve any issues with their data.*
* *Ask UK team to help review graphs and charts produced from analysis.*
* *Use guidance to fine-tune the scoring algorithms.*
 |
| **Conclusions**To complete the risk assessment by drawing together the insights from the analysis tools and documenting the findings and recommendations in the final report and presentation for senior stakeholders, sector leads and the organisations who took part in the survey.  | * *Draft the final report and presentation, using templates.*
* *Brief the conclusions to senior stakeholders and feed back to CNI owners.*
* *Ask UK team to help draw out recommendations based on conclusions.*
 |
| **Next steps**To develop and implement an action plan to take forward the recommendations from the final report and address the highest priority CNI risks identified by the NCRA.  | * *Develop the action plan to implement the report recommendations.*
* *Identify and bid for required resources.*
* *Plan for next (annual) refresh of NCRA.*
* *Use additional post-NCRA capacity building packages on the e-learning portal.*
 |

## **App E: Full List of interfaces & dependencies**

This section identifies all the interfaces and dependencies that need to be managed to successfully deliver the NCRA*.*

*[This section identifies all the interfaces and dependencies that need to be managed to successfully deliver the NCRA. You should complete this and then ensure these are actually being managed. Good practice is to include the management of these in your detailed schedule.*

*The list shown is identical to that in the main body of the plan document.]*

| **Interface or dependency with:** | **Description** | **Management plan** |
| --- | --- | --- |
| *Organisation X recruitment team* | *Recruitment of team lead manager by x date* | *Role and responsibility documented in project plan & RACI chart. Exact skills profile and job description to be written.*  |
| *Organisation Y cyber security experts* | *Ad-hoc access to cyber security experts to review NCRA responses* | *Role and responsibility documented in project plan & RACI chart.* |
| *Government strategy and policy unit* | *The strategy unit needs to be prepared to receive the NCRA recommendations, if they are to be used.*  |  |
| *Minister X’s approval to engage organisations in Sector Y* | *Ministerial approval is required to engage organisations in Sector Y.*  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## **App F: Full list of assumptions**

This section identifies all the assumptions that we will be regularly testing, as changes could cause unwanted NCRA outcomes*.*

*[This section identifies all the assumptions that you need to be regularly testing. Changes to assumptions, usually if they prove false, can cause unwanted NCRA outcomes. You should complete this and then ensure these are actually being managed. Good practice is to include checks of assumptions in your detailed schedule and weekly meetings.*

*The list shown is identical to that in the main body of the plan document.]*

| **Assumption:** | **Impact of invalidity:** | **Action to test:** |
| --- | --- | --- |
| *CNI organisations provide high quality data* | *Recommendations will be poor / inaccurate. NCRA & team suffers reputational harm.*  | *Review each response as it arrives. Activate remedial quality improvements* |
| *CNI organisations accept our secure environment*  | *CNI orgs do not provide their CNI system data* | *Ask them directly if they are comfortable / show they steps taken towards security* |
| *Covid19 does not cause economic downturn*  | *NCRA funding could be curtailed with loss of resources* | *Stay engaged with financial authority. Check if NCRA funding remains ringfenced.* |
|  |  |  |
|  |  |  |
|  |  |  |

## **App G: Full communications and engagement approach**

This section identifies all the methods we will use to engage with our CNI organisations and other critical stakeholders. It also includes what we will do if we don’t get the engagement that we need.

*[This section should identify all the methods you will use to engage with our CNI organisations and other critical stakeholders.*

***It should also include table headings what you will do if you don’t get the engagement that you need. And it should relate to the RACI about who is ‘on point’ for doing the engagement.***

*You should complete this and then ensure these are actually being managed. Good practice is to include engagement checks in your detailed schedule and weekly meetings.*

*The list shown is identical to that in the main body of the plan document.]*

| **Stakeholder:** | **Method & frequency:** | **Purpose:** |
| --- | --- | --- |
| *Minister* | *We will provide weekly 1-page highlight reports. These will explain what we have achieved, what is coming up, and any risks or issues that we need to escalate.* | *To reassure the minister that we have control of the NCRA* |
| *CNI Organisations* | *We will hold an initial workshop aimed at all of them. We will use our sector liaisons to get feedback often, so we can act on it. We will provide them with access to the CNI owners section of the NCRA portal.* | *To keep the CNI organisations engaged* |
| *CNI Organisations* | *We will thank those that have returned their data to a high standard on time. We will reach out and ask for meetings to discuss gaps and inconsistencies in the data. We will aim to meet on their premises to discuss.* | *To get the CNI organisations to return high quality data* |
| *CNI Organisations* | *We will hold 3 main workshops. We will provide fortnightly comms explaining where we have reached and what is happening next, including ‘save the date’ style information. We will be transparent about how we are really doing.* | *To keep the CNI organisations aware of our progress* |
| *CNI Organisations* | *We will hold a special feedback session. We will augment the session with a fun cyber exercise to get them in the mindset of thinking about cybersecurity for the CNI. We will ensure that suitable refreshments are provided as we want them alert and willing to ask questions.*  | *To reveal the results of the NCRA analysis to the CNI Organisations* |
| *CNI Organisations* | *We will break each sector into a separate area. We will use our liaisons to facilitate discussions. We will write 2-page sector reports that convey findings specific to each sector. We will seed the discussions with questions for the liaisons to ask – some generic and some based on the findings.* | *To get the CNI organisations to discuss the findings in their sector.* |
|  |  |  |
|  |  |  |
|  |  |  |

## **App H: Full approach to achieving data quality**

*[This section is critical!*

***It should identify ALL the ways in which you are going to ensure that you get the data quality you need. Put REAL energy and focus in obtaining great data and the whole process will go much better.***

***Watch the NCRA portal video about data quality and extract additional ideas!***

*You should complete this and then ensure that data quality is actually being obtained. Good practice is to include engagement checks in your detailed schedule and weekly meetings.*

*The list shown is identical to that in the main body of the plan document.]*

Great data quality is essential if our final results are to be accurate, believed and considered for inclusion in cyber strategies, policies and risk reduction initiatives. To ensure the data meets the necessary standard we will:

* *Provide guidance to the CNI organisations, including examples of what great quality responses look like.*
* *Sit with them and help them complete their questionnaires; asking questions to understand how they are reaching their conclusions.*
* *Use the MS Excel version of the questionnaire, and the analytic spreadsheet with their respective built-in ‘mechanistic’ data checkers to assess gaps and likely inconsistencies.*
* *Use our cyber systems experts to review the questionnaire responses, and highlight anything they find suspicious and worth a follow-up.*
* *Do multi-level engagements to help resolve any data clarity issues e.g. Sponsor or Minister to CEO, and Team-lead to director of system owner’s area.*
* *Etc*
* *Etc.*

## **App I: Full approach to achieving data security**

*[This section is also critical!*

***A failure to protect your NCRA data will lead to reputational harm, and potentially additional attacks on your countries CNI!***

***Watch the NCRA portal video about data security and extract additional ideas!***

*You should complete this and then ensure that data security is actually being obtained. Good practice is to include ‘spot checks’ on your security setup.*

*The list shown is identical to that in the main body of the plan document.]*

Great data quality is essential if our final results are to be accurate, believed and considered for inclusion in cyber strategies, policies and risk reduction initiatives. To ensure the data meets the necessary standard we will:

* *Completed questionnaires will be sent encrypted over secure messaging services, with passkeys sent via other secure channels.*
* *The questionnaire responses will be held on an encrypted computer, in a locked room, in a military-guarded building.*
* *Only two security-vetted people will have access to the data analysis computer: the team lead and the data analyst. They will each have different non-admin usernames and passwords.*
* *The computer will be standalone; with all connectivity disabled, <via the bios/ wire removal>, except one USB socket.*
* *Etc*
* *Etc.*

## **App J: Full list of risks and issues**

*[Please complete this section after filling in most of the other sections, and engage various people to ensure you have a good 360 degree understanding of where your risks are.*

*A failure to identify the risks and to manage them will lead to surprises – most of which won’t be fun, creating stress and probably embarrassment. Remember, chance favours the prepared mind!!*

*As the risks are mitigated re-evaluate the impact and likelihood.*

*The example list is the same as the one in the main body of the plan document.]*

An analysis of the NCRA plan, and engagement with various people has given us a 360 degree view of the risks to our NCRA. Our full list of major risks is detailed here:

| **Risk** | **Impact** | **Likelihood** | **Owner** | **Mitigating action(s)** |
| --- | --- | --- | --- | --- |
| *Data quality is below standard* | *H* | *M* | *Team lead* | *Do the mitigation tasks identified in the data quality plan e.g. identify where data needs improvement; ask organisations to re-do; do together in a join team-org meeting; send in some additional help; remove from analysis.*  |
| *CNI organisations don’t engage* | *M* | *H* | *Team Lead* | *Do the mitigation tasks identified in the Engagement plan e.g. call & write; hold additional explanation meetings; get sponsor to engage with organisation’s board members; change cyber laws to make response compulsory (long term ambition!)*  |
| *Data is lost / stolen* | *H* | *L* | *Team lead* | *Do the mitigation tasks identified in the Security plan e.g. lockdown existing data, work out whose data is missing, alert them, carry out investigation.* |
| *Resources unavailable* | *M* | *L* | *Sponsor* | *E.g. Identify new people; refocus efforts of existing people.* |
| *Country disruption* | *M* | *?* | *Sponsor* | *Determine level of impact, identify workarounds; reschedule meetings and gatherings.*  |