

<Country name>: National Cyber Risk Assessment (NCRA) questionnaire

# <Country name>: national cyber risk assessment (NCRA) questionnaire

This form is designed to capture your assessment of the criticality, strengths and weaknesses of your cyber systems and the cyber threat environment. The guidance notes provided should be referred to when completing this questionnaire.

Questions marked with \* require a response.

## 1.Information about your organisation

In this section please provide some background information about your organisation and the services that it provides.

* 1. **Please provide the name of your organisation below \***

**1.2. Please briefly list the main services that your organisation provides \***

**1.3. Please show which of the following sectors your organisation belongs to \***

*Mark all that apply.*

* + - Communications and Internet Services
    - Defence
    - Energy
    - Emergency services
    - Finance and banking
    - Government
    - Health
    - Transport
    - Sport
    - Water

**1.4. Please list the critical cyber systems supporting the services that your organisation provides \***

* 1. **Prominence of cyber security within the organisation – please select one or more from the following options**

*Mark all that apply.*

* + - Cyber security is a recognised Board level priority
    - A cyber security risk management process is in-place and acted on
    - Cyber security is on the corporate risk register
    - A senior SIRO (senior information risk owner) or ITSO (IT senior owner) role is in place
    - Cyber security user awareness and training is provided
    - Other:

## 2.Critical system characteristics

This section captures the characteristics of critical cyber systems. See explanatory notes for each

**2.1. Which of the cyber systems at 1.4 does this questionnaire describe? Which department, organisation or business is responsible for this system? \***

**2.2. Please provide a brief description of the system including the functions it provides and the services that are supported.**

**2.3. Please indicate why this may be considered a critical system**

**2.4. System connectivity: please select the checkboxes below that are applicable to this system\***

*Mark all that apply.*

* + - The system is not connected to other systems or networks (stand-alone)
    - The system is connected to a common enterprise network
    - The system is connected to the Internet
    - The system is connected to physical control or measurement systems (e.g. SCADA (Supervisory Control and Data Acquisition) or Building Management)
    - Other:

**2.5. System hosting: please select the option below that best describe how the system is hosted. \***

*Mark only one*

* + - The system is hosted locally on IT that is owned and managed by the organisation
    - The system is wholly or partly hosted by a third-party service provider
    - The system is hosted on a commercially provided cloud service
    - Other:

**2.6. Is it clear who is responsible for the cyber security of the system?**

*Mark only one.*

* + - Yes
    - No

**2.7. If the answer to 2.6 above is 'no' then please explain how and to whom responsibility for cyber security is allocated**

**2.8. Internal business criticality: Please give an indication of the criticality of this system to the business of the organisation. \***

*Mark only one.*

* + - Low criticality (disruption to this system can be tolerated)
    - Medium criticality (disruption of this system can be tolerated for a short time)
    - High criticality (no disruption to this system can be tolerated/any disruption has immediate impact)
    - Very high criticality (immediate and major disruption of critical services)

**2.9. Outward dependencies: please list below any other cyber-systems that this system depends on. \***

**2.10. Inward dependencies: please list below any other cyber-systems that are directly depend on this system. \***

**2.11. [Optional - this question is for any additional comments you may have on the characteristics of your critical cyber system]**

## 3.Cyber risks

This section is to identify the cyber risk and to determine what would be a 'reasonable worst-case scenario' illustrating the risk posed to your system.

**3.1. Please rate the importance of the 3 aspects of Information Security for your system. \***

*Mark only one per row.*

|  | Low | Medium | High | Very high |
| --- | --- | --- | --- | --- |
| Availability |  |  |  |  |
| Integrity |  |  |  |  |
| Confidentiality |  |  |  |  |

**3.2. Please indicate how important cyber security threat intelligence is to your system security**

*Mark only one.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |  |
| Not relevant |  |  |  |  |  | Critical to remaining secure |

**3.3. Have you consulted other agencies/experts to assess the threats/hazards posed to your cyber systems in the last 12 months? \***

*Mark only one.*

* + - Yes, we have an internal threat analysis team
    - Yes, we have consulted with government authorities
    - Yes, we have consulted industry advisors
    - Not in the last 12 months
    - Never
    - Other:

**3.4. How would you rate your ability to access cyber security threat intelligence?**

*Mark only one.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |  |
| Threat intelligence is not available |  |  |  |  |  | Real-time threat intelligence |

**3.5. Which cyber security threat actors are you concerned about \***

*Mark only one per row.*

|  | Not concerned | low concern | Medium concern | High concern |
| --- | --- | --- | --- | --- |
| Cyber criminals |  |  |  |  |
| Cyber terrorists |  |  |  |  |
| Hacktivists |  |  |  |  |
| State or state-sponsored actors |  |  |  |  |
| Accidents |  |  |  |  |

Insiders

**3.6. Which cyber-attack vectors are you most concerned about? \***

*Mark only one per row.*

|  | Not concerned | Low concern | Medium concern | High concern |
| --- | --- | --- | --- | --- |
| Phishing |  |  |  |  |
| Malware |  |  |  |  |
| Insiders |  |  |  |  |
| Supply chain |  |  |  |  |
| Other (DDos, etc….) |  |  |  |  |

**3.7. Combine your answers to questions 3.1, 3.5, and 3.6 to create a reasonable worst-case scenario (see notes)**

**3.8. [Optional - this question is for any additional comments you may have on threats to your critical cyber system]**

## 4.Impact

This section asks you to estimate the scale of impact in the reasonable worst-case scenario.

**4.1. Please estimate what the impact would be on people who use your services \***

*Mark only one.*

* + - Low (disruption would affect fewer than 10,000 people)
    - Medium (disruption would affect 10,000-100,000 people)
    - High (disruption would affect 100,000-1 million people)
    - Very High (disruption would affect over 1 million people)

**4.2. Please estimate the impact on other essential services \***

*Mark only one per row.*

|  | No impact | Low impact (localised, short duration, low intensity) | Medium impact (not localised, medium duration and intensity) | High impact (widespread, lasting, and intense duration) |
| --- | --- | --- | --- | --- |
| Communications. and Internet Services |  |  |  |  |
| Energy |  |  |  |  |
| Government |  |  |  |  |
| Finance and Banking |  |  |  |  |
| Transport |  |  |  |  |

**4.3. Estimate the impact on industry and the economy \***

*Mark only one.*

* + - Low impact (less than 0.01% of GDP)
    - Medium impact (0.01-0.1% of GDP)
    - High impact (0.1-1% of GDP)
    - Very high (over 1% of GDP)

N.B: GDP of <Country Name> (<Last year with data>) = <XXXX> billion dollars

**4.4. Estimate the impact on the following \***

*Mark only one per row.*

|  | No | Low | Medium | High |
| --- | --- | --- | --- | --- |
| National Security |  |  |  |  |
| National Icons |  |  |  |  |
| National reputation |  |  |  |  |
| Popular confidence |  |  |  |  |
| Popular outrage |  |  |  |  |
| Other |  |  |  |  |

**4.5. (If the impact on specific events is to be assessed) What would be the scale of impact on [event] in the reasonable worst-case scenario?**

*Mark only one per row.*

|  | No/low | Medium | High | Very High |
| --- | --- | --- | --- | --- |
| Number of events affected |  |  |  |  |
| Intensity of disruption |  |  |  |  |
| Duration of disruption |  |  |  |  |

**4.6. [Optional - this question is for any additional comments you may have on the impacts of disruption to your critical cyber system]**

## 5.System vulnerabilities

This section captures a view of the potential vulnerabilities of the system against the UKs Ten Steps to Cyber Security.

**5.1. How would you rate the vulnerability of your system against each of the ten steps below:**

*Mark only one per row.*

|  | Low vulnerability | medium vulnerability | high vulnerability | Very high vulnerability |
| --- | --- | --- | --- | --- |
| Risk management |  |  |  |  |
| Secure configuration |  |  |  |  |
| Network security |  |  |  |  |
| Malware prevention |  |  |  |  |
| Removable media controls |  |  |  |  |
| User education |  |  |  |  |
| Manage user privileges |  |  |  |  |
| Access Control |  |  |  |  |
| Incident management |  |  |  |  |
| Continuous monitoring |  |  |  |  |
| Redundancy/System Availability |  |  |  |  |
| Home and mobile policy |  |  |  |  |

**5.2. [Optional - this question is for any additional comments you may have on the vulnerability of your critical cyber system]**

Version/Date