Defence Cyber
Protection Partnership

Guidance

Cyber Security Model:

Risk Assessment (RA) Workflow

October 2019

Contents

1. What is the Risk Assessment (RA)?

The Risk Assessment is the first stage in the Defence Cyber Protection Partnership (DCPP) Cyber Security Model. It is a questionnaire that assesses the Cyber Risk Profile of a contract and can be completed by The Authority[1].

There are five possible Cyber Risk Profiles: Not Applicable, Very Low, Low, Moderate and High.

Once completed, a Risk Assessment Reference (RAR) is generated, which should be issued to suppliers that have been invited to tender and are required to complete a related Supplier Assurance Questionnaire (SAQ).

An SAQ is not required for contracts assessed as Not Applicable, however suppliers are still recommended to achieve Cyber Essentials certification.

For more information about the Cyber Security Model and the Defence Cyber Protection Partnership, visit: https://www.gov.uk/government/collections/defence-cyber-protection-partnership.

2. How to use this guide

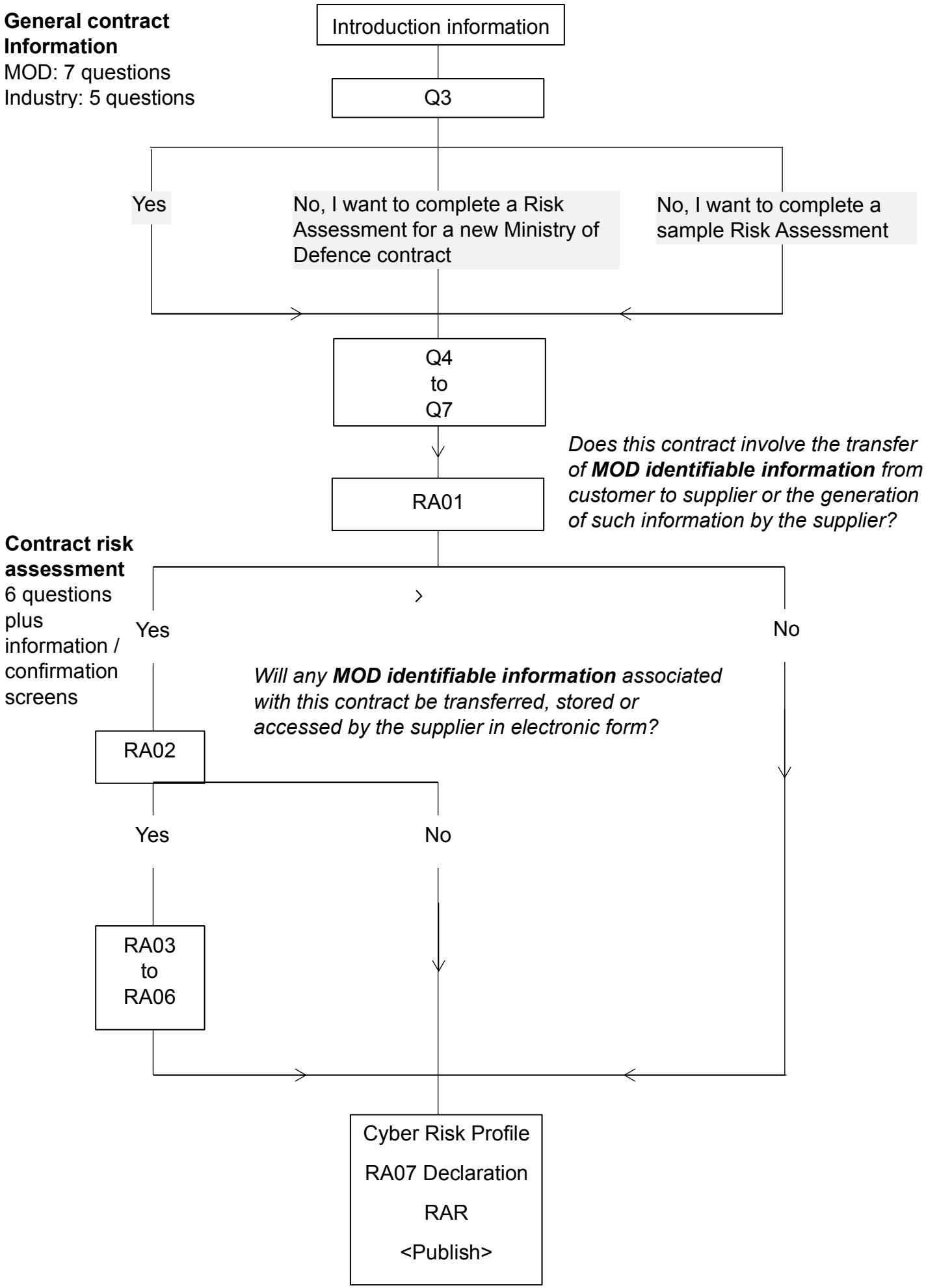
This guide includes a workflow diagram of the questions which must be completed by The Authority when responding to the RA. The answers provided by The Authority in each case, relating to a requirement, will determine which questions are asked.

The question references (e.g. RA01) in the workflow refer to the full question and answer options listed on page 4. Use both the workflow and the questions to understand what information will be required when responding to the RA.

To view associated question-level guidance, visit Supplier Cyber Protection, the online service at https://supplier-cyber-protection.service.gov.uk/ and complete a sample Risk Assessment.

[1] The Authority is the person accountable for determining the Cyber Risk Profile appropriate to a contract and, where the contractor has not already been notified of the Cyber Risk Profile prior to the date of this contract, shall provide notification of the relevant Cyber Risk Profile and cyber security instructions as soon as reasonably practicable; and notify the contractor as soon as reasonably practicable where The Authority reassesses the Cyber Risk Profile relating to a specific contract.

3. Risk Assessment workflow diagram



4. Risk Assessment questions

Q3 **Is this Risk Assessment for work that you are subcontracting as part of a larger contract that you are bidding for?**

Yes - provide SAQ reference

No, I want to complete a Risk Assessment for a new Ministry of Defence contract ***(MOD with correct DUNS only)***

No, I want to complete a sample Risk Assessment

Q4 **Provide a name and description for the contract.**

Q5 **Does the contract have start and end dates?**

(estimate indicator available)

Yes - provide dates

No, it is a rolling contract

Q6 - MOD **Provide the value of the contract**

(estimate indicator available)

Contract value Currency

Q7a - MOD **Which Ministry of Defence sub-organisation is the contracting authority?**

Air Command

Army Command

DBS (Defence Business Services)

DECA (Defence Electronics Components Agency)

DE&S (Defence Equipment and Support)

DIO (Defence Infrastructure Organisation)

DSG (Defence Support Group)

DSTL (Defence Science and Technology Laboratory)

HO&CS (Head Office and Corporate Services)

JFC (Joint Forces Command)

MDPGA (MOD Police & Guarding Agency)

Navy Command

UKHO (UK Hydrographic Office)

Other Contracting authority

Q7b - MOD **Which Domain is the contracting authority?**

(Domain specific, according to Q7a)

RA01 **Does this contract involve the transfer of MOD identifiable information from customer to supplier or the generation of such information by the supplier?**

No Yes

RA02 **Will any MOD identifiable information associated with this contract be transferred, stored or accessed by the supplier in electronic form?**

No Yes

RA03 – MOD **What is the highest level of classification of the information and handling requirements associated with the overall contract?**

OFFICIAL

OFFICIAL SENSITIVE

SECRET

TOP SECRET

RA03 – Industry **What is the highest level of classification of the information and handling requirements associated with the contract you received from your contracting authority?**

OFFICIAL

OFFICIAL SENSITIVE

SECRET

TOP SECRET

RA04 **What is the highest classification of the information and handling requirements for the information your supplier will process to fulfil this contract?**

OFFICIAL

OFFICIAL SENSITIVE

SECRET

TOP SECRET

RA05 **Will this contract require the processing of personal data?**

(Compliance with the Cyber Security Model does not infer that you meet any data processing requirements specified by The Data Protection Act 2018 and/or GDPR)

NOTE FOR THE PURPOSES OF THIS DISCRIMINATOR: Personal data does not include business contact information that relates to an identified or identifiable person within the project / commercial team and is transferred to the supplier for the purposes of forming or managing the contract.

None

Personal Data

Special Category Personal Data

RA06 **To fulfil this contract, will your supplier require access to your network/system(s)?**

No

User Access

Privileged user (e.g. Admin)

Cyber Risk Profile

User presented with Cyber Risk Profile

If you do not think that this reflects the cyber risk associated with this contract, then click “Save and View Answers” to review your responses and make any necessary corrections.

If you think this adequately represents the cyber risk, click "Next" and submit your declaration.

RA07 Declaration

I have authority to complete the Risk Assessment.

The answers provided have been verified with all appropriate personnel and are believed to be true and accurate in all respects.

All information which should reasonably have been shared has been included in the responses to the questions.

Should any of the information on which the responses to this Risk Assessment are based change, my company undertakes to notify the Ministry of Defence as soon as is reasonably practicable.

My company acknowledges that the Ministry of Defence reserves the right to audit the responses provided at any time.

For and on behalf of my company, I confirm the above statements.

Risk Assessment Reference (RAR)

User is provided with unique reference

Publish

Click **“Publish”** to allow Supplier Assurance Questionnaires to be submitted against this contract. Then issue this Risk Assessment Reference (starting RAR) to all suppliers who are bidding for this contract and ask them to complete a Supplier Assurance Questionnaire.