|  |  |
| --- | --- |
|  | 20 April 2020 |

Effective Practices for Cyber Incident Response and Recovery

Public Consultation - Optional Response Template

# Instructions:

The FSB invites comments on the consultative document on [Effective Practices for Cyber Incident Response and Recovery](https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document/) that includes a list of specific questions as a guide. To help respond to the public consultation, this optional response template is provided.

The template has been designed to be completed as a form in Microsoft Word. To assist with automated compilation of answers, respondents are only able to make changes in the spaces set aside for answers.

For the context of any question or for defined terms, please refer to the relevant parts of the consultative document.

Please save and submit the completed questionnaire as a Microsoft Word document, rather than converting it to a PDF. A password may be applied; in that case you should communicate the password by separate email or by telephone conversation arranged by email.

**The FSB invites stakeholders to provide their responses by Monday 20 July 2020 by e‑mail to** [**CIRR@fsb.org**](mailto:CIRR@fsb.org) **with “CIRR” in the e-mail subject line**. The feedback received will be taken into account in the FSB’s development of the final toolkit of effective practices, which will be published in October.

You may choose to leave answers blank – in that case it is acceptable to leave the answer reading “Click here to answer text”.

Should you wish to obtain an unlocked version of this template in order to facilitate sharing of draft answers in your organisation, please contact the FSB Secretariat on the e-mail address above. In that case, you would still be requested to copy your answers to the locked version on the template to ensure accurate processing of the data.

| Questions | Answers |
| --- | --- |
| **Information about the respondent** | |
| A. Name of respondent institution/firm | Click here to enter text. |
| B. Name of representative individual submitting response | Click here to enter text. |
| C. Email address of representative individual submitting response | Click here to enter text. |
| D. Do you request non-publication of any part(s) of this response? If so, which part(s)?  *Unless non-publication (in part or whole) is specifically requested, all consultation responses will be published in full on the FSB’s website. An automated e-mail confidentiality claim will not suffice for these purposes.* | Click here to enter text. |
| E. Would you like your response to be confidential (i.e. not posted on the FSB website)? | Choose an item. |
| **Consultation questions** | |
| **General questions** | |
| 1. Have you learnt any lessons from the COVID-19 pandemic and related cyber activity that will contribute to your cyber incident response and recovery practices? | Click here to enter text. |
| 1. To whom do you think this document should be addressed within your organisation? | Click here to enter text. |
| 1. How does your organisation link cyber incident response and recovery with the organisation’s business? Does your organisation follow international standards or common frameworks? If so, which international standards or common frameworks? | Click here to enter text. |
| 1. Does your organisation structure its cyber incident response and recovery activities along the seven components set out in the FSB toolkit? Please describe any additional components your organisation considers. | Click here to enter text. |
| 1. Based on your organisation’s experience, please provide any additional effective practice(s) for any of the tools. Please list the number of the tool (e.g. Tools 1 – 46) and describe the effective practice(s). | Click here to enter text. |
| 1. Based on your organisation’s experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6). | Click here to enter text. |
| 1. What role, if any, should authorities play in supporting an organisation’s cyber incident response and recovery activities? | Click here to enter text. |
| 1. Governance |  |
| * 1. To what extent does your organisation designate roles and responsibilities as described in Tool 3? Does your organisation identify these roles by business line, technology application or department? | Click here to enter text. |
| * 1. How does your organisation promote a non-punitive culture to avoid “too little too late” failures and accelerate information sharing and CIRR activities? | Click here to enter text. |
| 1. Preparation |  |
| * 1. What tools and processes does your organisation have to deploy during the first days of a cyber incident? | Click here to enter text. |
| * 1. Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months. | Click here to enter text. |
| * 1. How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)? | Click here to enter text. |
| 1. Analysis |  |
| * 1. Could you share your organisation’s cyber incident analysis taxonomy and severity framework? | Click here to enter text. |
| * 1. What are the inputs that would be required to facilitate the analysis of a cyber incident? | Click here to enter text. |
| * 1. What additional tools could be useful to analyse the effectiveness of cyber incident response and recovery activities and the severity, impact and root cause of cyber incidents? | Click here to enter text. |
| * 1. What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation? | Click here to enter text. |
| 1. Mitigation |  |
| * 1. Besides reducing impact to business and system security, what are other considerations that need to be taken into account during mitigation? | Click here to enter text. |
| * 1. What tools or effective practices does your organisation have related to mitigating the impact from: (i) data breaches (ii) loss of data integrity and (iii) ransomware events? | Click here to enter text. |
| * 1. What tools or practices are effective for integrating the mitigation efforts of third-party service providers with the mitigation efforts of the organisation? | Click here to enter text. |
| * 1. What additional tools could be useful for including in the component Mitigation? | Click here to enter text. |
| * 1. Are there situations in which effective practices for mitigation and restoration activities of the organisation are the same or overlap substantially? If yes, please provide examples. | Click here to enter text. |
| 1. Restoration |  |
| * 1. What tools and processes does your organisation have available for restoration? | Click here to enter text. |
| * 1. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities? | Click here to enter text. |
| * 1. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data? | Click here to enter text. |
| 1. Improvement |  |
| * 1. What are the most effective types of exercises, drills and tests? Why are they considered effective? | Click here to enter text. |
| * 1. What are the major impediments to establishing cross-sectoral and cross-border exercises? | Click here to enter text. |
| * 1. Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery? | Click here to enter text. |
| 1. Coordination and Communication |  |
| * 1. Does your organisation distinguish “coordination activities” from broader “communication” in general? If yes, please describe the distinct nature of each component. | Click here to enter text. |
| * 1. How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident? | Click here to enter text. |
| * 1. Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities? | Click here to enter text. |