NHS England

Cyber Assessment Framework–aligned Data Security and Protection Toolkit

Strengthening Assurance – Independent Assessment and Audit Framework

Creating a culture
of Improvement

Information and Technology
for better health and care

Final

17/12/24

Objective D – Minimising the impact of incidents

Description

Capabilities exist to minimise the adverse impact of an incident on the operation of essential functions, including the restoration of those functions where necessary, and to uphold the rights of impacted individuals.

Overview of the underlying Principles

Principle D1: Response and recovery planning

Principle D2: Lessons learned

Principle D1: Response and recovery planning

Description

There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential function(s) in the event of system or service failure and to uphold the rights of impacted individuals. Mitigation activities designed to contain or limit the impact of compromise are also in place.

Overview of the underlying Contributing outcomes

Contributing outcome D1.a – Response plan

Contributing outcome D1.b – Response and recovery capability

Contributing outcome D1.c – Testing and exercising

Contributing outcome D1.a – Response plan

Description

You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function(s) and covers a range of incident scenarios.

The expectation for this contributing outcome is **Partially Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved** All the following statements are true:	**Achieved** All the following statements are true:
NA#1. Your incident response plan is not documented. NA#2. Your incident response plan does not include your organisation's identified essential function(s). NA#3. Your incident response plan is not well understood by relevant staff. NA#4. Your incident response plan does not cover your obligations as a controller or processor.	PA#1. Your response plan covers your essential function(s). PA#2. Your response plan comprehensively covers scenarios that are focused on likely impacts of known and well-understood attacks and incidents only. PA#3. Your response plan is understood by all staff who are involved with your organisation's response function. PA#4. Your incident response plan is documented and shared with all relevant stakeholders. PA#5. Your response plan covers your obligations as a controller or processor. PA#6. Your response plan includes notifying impacted system partners.	A#1. Your incident response plan is based on a clear understanding of the security risks to information, systems and networks supporting your essential function(s). A#2. Your incident response plan is comprehensive (i.e. covers the complete lifecycle of an incident, roles and responsibilities, and reporting) and covers likely impacts of both known attack patterns and breaches of individuals' rights and of possible attacks and breaches, previously unseen. A#3. Your incident response plan is documented and integrated with wider organisational business plans and supply chain response plans, as well as dependencies on supporting infrastructure (such as power, cooling etc). A#4. Your incident response plan is communicated and understood by the business areas involved with the operation of your essential function(s). A#5. Your incident response plan covers your obligations as a controller or processor.

		A#6. Your response plan includes notifying impacted system partners.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework.

The approach and documentation list described below are a suggestion to the independent assessors, and do not have to be followed stringently.

Suggested approach to testing – Partially Achieved

1) **Incident Response plans** - Obtain and inspect the incident response plans, assessing whether:
   a) It shows that the organisation's essential functions have been considered, with specific business areas and key contacts named who hold responsibility for those functions in the event of an incident. (PA#1)
   b) Scenarios have been identified and documented for known attacks and incidents. (PA#2)
   c) The roles and responsibilities of staff within the response function have been clearly documented and assigned. (PA#3)
   d) It includes a section on the obligations of the organisation as controller or processor of personal data for the reporting of incidents. This section should show the organisation's awareness of relevant data protection obligations, and how they will comply with them during an incident. It should also identify the stakeholders to be informed, such as the Information Commissioner's Office (ICO), and the timelines and procedure for informing them, for example through the Data Security and Protection Toolkit (DSPT) reporting portal. (PA#5)
   e) The response plans include the requirement to notify impacted system partners (PA#6)
2) **Sharing with relevant stakeholders-** Obtain evidence that the incident response plan(s) has been approved by a relevant group and distributed to the response team. (PA#4).
3) **Personal data** – Review the latest report of an incident involving personal data and verify that procedures were followed appropriately. (PA#5)
4) **System partners** – A list of system partners exists, with key contacts for each to enable notification. (PA#6, A#6)

Additional approach to testing – Achieved

1) **Incident Response plan** - Obtain and inspect the incident response plan, assessing whether:
   a) It covers all stages of the incident response lifecycle, including preparation, detection, containment, eradication, recovery, and post-incident activities, for the most likely scenarios as dictated by risk assessments. (A#2)
   b) Dependencies on supporting infrastructure have been identified and documented. This also includes dependencies on suppliers and technology. (A#3)
   c) It is integrated with other relevant policies and processes, for example the incident review process and business continuity policy. (A#3)
   d) Its location is well-known and easily accessible to staff. (A#4)

2) **Risk assessments or risk management report**– Assess whether a risk assessment has been undertaken for each essential function, with the risks accounted for in the incident response plan(s). The risks identified should inform the response plan activities. (A#1)
3) **Staff knowledge** – Assess whether relevant staff have read and understood the document. This should also include third parties where relevant. Is there evidence of understanding, such as briefing sessions, emails, meeting minutes etc. (A#4)

Suggested documentation list – Partially Achieved

- Incident response plan(s)
- Evidence of incident response plan being approved and distributed to relevant staff members
- Report of the latest incident involving personal data
- Evidence of communication plans / channels with system partners to coordinate incident response

Additional documentation for Achieved level

- Image of policy repository (shared on screen)
- Risk assessment for each essential function
- Evidence of cross-organisational understanding of the incident response plan(s).

Contributing outcome D1.b – Response and recovery capability

Description

You have the capability to enact your incident response plan, including effective limitation of impact on the operation of your essential function(s). During an incident, you have access to timely information on which to base your response decisions.

The expectation for this contributing outcome is **Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following statements is true:	Partially Achieved	Achieved All the following statements are true:
NA#1. Inadequate arrangements have been made to make the right resources available to implement your response plan. NA#2. Your response team members are not equipped to make good response decisions and put them into effect. NA#3. Inadequate back-up mechanisms exist to allow the continued operation of your essential function(s) during an incident.	*Partial achievement is not possible for this contributing outcome*	A#1. You understand the resources that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available. A#2. You understand the types of information that will likely be needed to inform response decisions and arrangements are in place to make this information available. A#3. Your response team members have the skills and knowledge required to decide on the response actions necessary to limit harm, and the authority to carry them out. A#4. Key roles are duplicated, and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential function(s). A#5. Back-up mechanisms are available that can be readily activated to allow continued operation of your essential function (although possibly at a reduced level) if primary networks and information systems fail or are unavailable.

		A#6. Arrangements exist to augment your organisation's incident response capabilities with external support if necessary (such as specialist cyber incident responders).

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework.

The approach and documentation list described below are a suggestion to the independent assessors, and do not have to be followed stringently.

Suggested approach to testing

1. **Incident response plans** - Obtain and inspect the incident response plans, assessing whether:
    a) The resourcing requirements to respond to the most likely incidents have been identified and how the resources will be made available when needed. (A#1)
    b) Roles and responsibilities have been assigned for all key roles, and whether a backup member of staff has been identified to assume responsibility if required. (A#4)
2. **Scenario planning** - Obtain and inspect documentation relating to scenario planning and assess whether it contains:
    a) Clear identification of activities and a clear owner with authority to carry them out. (A#3)
    b) The type and source of information required to carry out the plan. (A#2)
3. **Scenario testing** - Enquire and obtain evidence of a sample of the tests undertaken, verifying that testing took place in the last 12 months. Verify that knowledge was captured and shared with all members, including those who could not attend. (A#3,A#4)
4. **Incident resourcing** –Obtain the testing and exercising documentation to ascertain whether the resourcing requirements documented in the scenario plan are realistic. (A#1)
5. **Staff resilience** - Enquire of the members of staff named as backups as to whether they are aware of their responsibilities, and whether they have received training for it. Inspect the evidence of training being undertaken. (A#4)
6. **Staff skills and knowledge** – Review evidence of a skills analysis, training needs analysis or similar which outlines the skills required and their presence within the team and any training required. (A#3)
7. **Clear roles and decision-making authority** - Assess whether a clear escalation process is in place, with a defined chain of command dictating the authority of each member of the response team. (A#3)
8. **Information availability for response decisions** –For a sample of each type of information identified, verify that the source of the information is recorded, and in cases where the information is confidential or private, verify that the activity owner either has access to it, or has a method of gaining access when required (for example, access to a specific system). (A#2)
9. **Information continuity** –Also verify that the latest plan takes into account the possibility of the system containing the information being unavailable and includes additional methods of obtaining the required information. (A#2)
10. **Backup plans and processes** - Obtain and inspect the latest business continuity plan to assess whether back-up mechanisms have been identified and documented to allow continued operation of essential functions. This includes roles and responsibilities of relevant staff to activate the back-up mechanisms. Assess whether the plans in place allow for ready activation of the back-up mechanisms, and whether any dependencies have been identified and planned for. (A#5)

11. **Minimum operational provision** - Obtain a sample of the organisations' essential functions and assess whether the acceptable level of operation of essential functions has been defined, approved and assess whether the plans in place allow for this level of operation. (A#5)
12. **External CIR support** - Test if the organisation is aware of the Cyber Incident Response (CIR) services provided by NHS England. (A#6)

Suggested documentation list

- Incident response plan(s)
- Evidence of scenario planning
- Latest tests of scenario plans
- Documentation of the latest training attended by the response team
- Skills analysis or training needs analysis
- Evidence of established chain of command during incidents
- Response team organisational chart
- Documentation of information sources and methods of gaining access to information required for incident response
- Evidence of back-up mechanisms being identified for continuation of services
- Assessment of acceptable levels of operation of essential functions for example recovery time objective (RTO), recovery point objective (RPO) etc.
- Agreement/contract with external support provider or process includes contacting NHS England for CIR services

Contributing outcome D1.c – Testing and exercising

Description

Your organisation carries out exercises to test response plans, using past incidents that affected your (and other) organisation, and scenarios that draw on threat intelligence and your risk assessment.

The expectation for this contributing outcome is **Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved**	**Achieved** All the following statements are true:
NA#1. Exercises test only a discrete part of the process (for example that backups are working), but do not consider all areas. NA#2. Incident response exercises are not routinely carried out or are carried out in an ad-hoc way. NA#3. Outputs from exercises are not fed into the organisation's lessons learned process. NA#4. Exercises do not test all parts of the response cycle.	*Partial achievement is not possible for this contributing outcome*	A#1. Exercise scenarios are based on incidents experienced by your and other organisations or are composed using experience or threat intelligence. A#2. Exercise scenarios are documented, regularly reviewed, and validated. A#3. Exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learned. A#4. Exercises test all parts of your response cycle relating to your essential function(s) (for example restoration of normal function levels).

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework.

The approach and documentation list described below are a suggestion to the independent assessors, and do not have to be followed stringently.

Suggested approach to testing

1) **Threat intelligence** - Enquire of the sources of information used to design the scenarios, which could include sources of threat intelligence, experience from past incidents, or product-specific sources of information. Assess whether the use of those sources is adequate and documented. (A#1)
2) **Exercise scenario documentation** - Obtain and inspect the exercise scenario documentation, and assess whether it contains:
    a) Details of exercises conducted. (A#2)
    b) Evidence of aligning to best practices. (A#1)
    c) A regular testing schedule or evidence of that exercise have been conducted at regular intervals or are scheduled. (A#3)
    d) How the entire lifecycle of the incident response has been covered, including preparation, detection, containment, eradication, recovery to normal function levels, and post-incident activities. (A#4)
3) **Exercise scenario** - Obtain and inspect a sample of exercise scenarios. Assess whether:
    a) They are the most likely scenarios for this organisation. (A#1)
    b) Their content allows the organisation to effectively test how they manage the impacts of the scenarios. (A#2)
4) **Exercise scenario testing** - Obtain and inspect the outputs of a sample of the exercises scenarios that were run in the last 12 months, and verify that:
    a) The outputs were discussed and approved by a relevant authority, with responsibility for updating policies and processes being assigned to named owners with clear timelines(A#2).
    b) A lessons learned exercise was carried out to identify improvements points and findings. The outputs of this exercise should be reviewed and approved by an appropriate authority (A#3).
    c) Their content tests processes outlined in the organisation’s incident response plan (A#1).
    d) The organisation has a process for ensuring their exercise scenarios are updated over time (A#2).
5) **Incident Response plan** - Obtain and inspect the incident response plans and verify that those improvements and findings were incorporated in the plans, which were then approved by a relevant authority (A#3).
6) **Staff communication** - Ensure that the updated incident response plan was communicated to all relevant stakeholders following its update (A#3).

Suggested documentation

- Threat intelligence sources
- Exercise scenario documentation
- Schedule for testing and exercising activities
- Evidence of lessons learned and actions taken following testing and exercising activities
- Procedures for updating testing and exercising activities over time
- Incident response plan(s)
- Evidence of updated incident response plan being communicated to all relevant stakeholders

Principle D2: Lessons learned

Description

When an incident or near miss occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.

Overview of the underlying Contributing outcomes

Outcome D2.a – Incident root cause analysis

Outcome D2.b – Using incidents and near misses to drive improvements

Outcome D2.a – Incident root cause analysis

Description

When an incident or near miss occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.

The expectation for this contributing outcome is **Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved**	**Achieved** All the following statements are true:
NA#1. You are not usually able to resolve incidents or near misses to a root cause. NA#2. You do not have a formal process for investigating causes.	*Partial achievement is not possible for this contributing outcome*	A#1. Root cause analysis is conducted routinely as a key part of your lessons learned activities following an incident or near miss. A#2. Your root cause analysis is comprehensive, covering organisational process issues, as well as vulnerabilities in your networks, systems or software. A#3. All relevant incident or near miss data is made available to the analysis team to perform root cause analysis.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework.

The approach and documentation list described below are a suggestion to the independent assessors, and do not have to be followed stringently.

Suggested approach to testing

1. **Incident Response lessons learned** – Obtain and inspect the incident response process or policy, and assess whether lessons learned exercises and root cause analysis are documented as a key step in the response process for both incidents and near misses, and responsibilities for those key steps have been clearly assigned (A#1)
2. **Incident sampling** - Obtain the list of incidents and near miss data that have taken place in the last 12 months. Confirm if all required data on incidents or near misses has been made available for analysis. From that list, choose a sample (see Introduction to CAF Independent Assessment Framework for more information) of incidents and request to see their lessons learned and root cause exercise. (A#1, A#3).
3. **Root cause analysis** - Assess the methodology in place at the organisation for undertaking root cause exercises, including the ownership and scope of the exercise and the routes to approval of the results. Determine whether the scope of the exercise includes vulnerabilities in the network, systems and software; organisational processes and people processes; and suppliers and suppliers processes. (A#2)
4. **Methodology** - Determine whether the methodology includes best practice examples of the type of data to be used during root cause analysis of common incidents and near misses and enquire of the process to get access to that data by a member of staff. Verify that the lessons learned activities for the incidents you have sampled were completed following the correct methodology, as assessed during step 3 (A#2)

Suggested documentation

- Evidence of lessons learned being documented as part of incident management processes
- List of incidents and near misses from the past 12 months or incident review logs
- Documented lessons learned and root cause analysis activities
- Evidence of methodology and considerations for undertaking root cause exercises

Outcome D2.b – Using incidents and near misses to drive improvements

Description

Your organisation uses lessons learned from incidents and near misses to improve your security measures.

The expectation for this contributing outcome is **Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	Partially Achieved	Achieved All the following statements are true:
NA#1. Following incidents and near misses, lessons learned are not captured or are limited in scope. NA#2. Improvements arising from lessons learned following an incident or near miss are not implemented or not given sufficient organisational priority.	*Partial achievement is not possible for this contributing outcome*	A#1. You have a documented incident review process/policy which ensures that lessons learned from each incident or near miss are identified, captured, and acted upon. A#2. Lessons learned cover issues with reporting, roles, governance, skills and organisational processes as well as technical aspects of networks and information systems. A#3. You use lessons learned to improve security measures, including updating and retesting response plans when necessary. A#4. Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed quickly. A#5. Analysis is fed to senior management and incorporated into risk management and continuous improvement.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework.

The approach and documentation list described below are a suggestion to the independent assessors, and do not have to be followed stringently.

Suggested approach to testing

1. **Incident review process/policy** - Obtain the incident review process/policy, and assess whether the document contains:
   a) A requirement for lessons learned to be undertaken for near misses as well as incidents. (A#1)
   b) Assigned responsibilities for capturing lessons learned, updating relevant processes and documentation, and disseminating the learning throughout the organisation. (A#1)
   c) A documented authority to review the outputs of lessons learned exercises and direct the improvements in security measures (A#3).
   d) A clearly defined prioritisation process for the identified security improvements, including ownership for implementing changes and the process for approval of changes. (A#4)
   e) The escalation process and reporting lines to senior management. (A#5)
2. **Lessons learned activities** - Assess whether the scope of the lessons learned activities include a review of reporting, roles, governance, skills and organisational processes as well as technical aspects of networks and information systems (A#2).
3. **Incident sampling** - Obtain the list of incidents that have taken place in the last 12 months. From that list, choose a sample (see Introduction to CAF Independent Assessment Framework for more information on sampling) and request to see the respective lessons learned exercise. Verify that:
   a) The scope of the samples matches the expected scope as per the incident review process/policy, as assessed during step 2 (A#2)
   b) The findings of the samples have been documented, with remediation actions designed and their implementation assigned to a named owner with adequate timelines. (A#3)
4. **Retesting** - Enquire of any plans to re-test the response plans with the updated security measures, where necessary and obtain evidence that this test is being designed (A#3).
5. **Mitigating actions** - Obtain and inspect documentation showing the progress that has been made on the implementation of mitigation actions. This may include updates to policies and process documentation, but also technical changes to security systems as required (A#4).
6. **Approval of mitigating actions** - Obtain and inspect the Terms of reference and minutes of the responsible group(s) to verify that outputs of the lessons learned exercises are being discussed, reviewed and approved by the responsible group(s). The remediation actions should be prioritised and approved by a relevant authority, with a named owner and adequate timelines put in place (A#1).

7. **Incorporating into risk management and continuous improvement –** Obtain examples of where lessons learned exercise and root cause analysis from incidents and near misses have been incorporated into risk management and continuous improvement. (A#5)

Suggested documentation

- Incident review process/policy
- Documented lessons learned and root cause analysis activities
- Evidence of methodology and considerations for undertaking root cause exercises
- List of incidents from the last 12 months
- Evidence of actions take following lessons learned activities
- Evidence of planning to re-test response plans or evidence that re-testing has occurred
- Evidence of policies, processes and systems being updated following lessons learned activities
- Terms of reference and minutes of relevant groups
- Evidence of risk management processes being updated following lessons learned activities.