Data Security and Protection Toolkit 2024-25

CAF aligned DSPT - Objective C – Detecting cyber security events

This session is being recorded and will be uploaded to the CAN workspace

NHS England
14 August 2024

Welcome and agenda for today

Housekeeping

- The session is being recorded and is a one-way broadcast, please use the Q&A function to ask any questions
- The slides and recording will be uploaded to the CAN workspace after there will be a link to the recordings for non-CAN members
- The first three webinars have been uploaded to YouTube (unlisted) and can be accessed via the DSPT News page:

  Webinar 1 Background and overview: https://www.youtube.com/watch?v=BG6YE1h4W40

  Webinar 2 Section A - Managing risk: https://www.youtube.com/watch?v=2aZ6TyEkUgc

  Webinar 3 Section B - Protecting against cyber attack and data breaches: https://youtu.be/IP0Fs1iX1WU

  Webinar 4 Section E - Using and sharing information appropriately https://youtu.be/JvJhxen6aEg

  Webinar 5 Section D - Minimising the impacts of incidents https://youtu.be/afLkL27_JEQ

- If you experience any technical issues, please leave and re-join the call

Webinar content

Session 2 – Objective A – managing risk

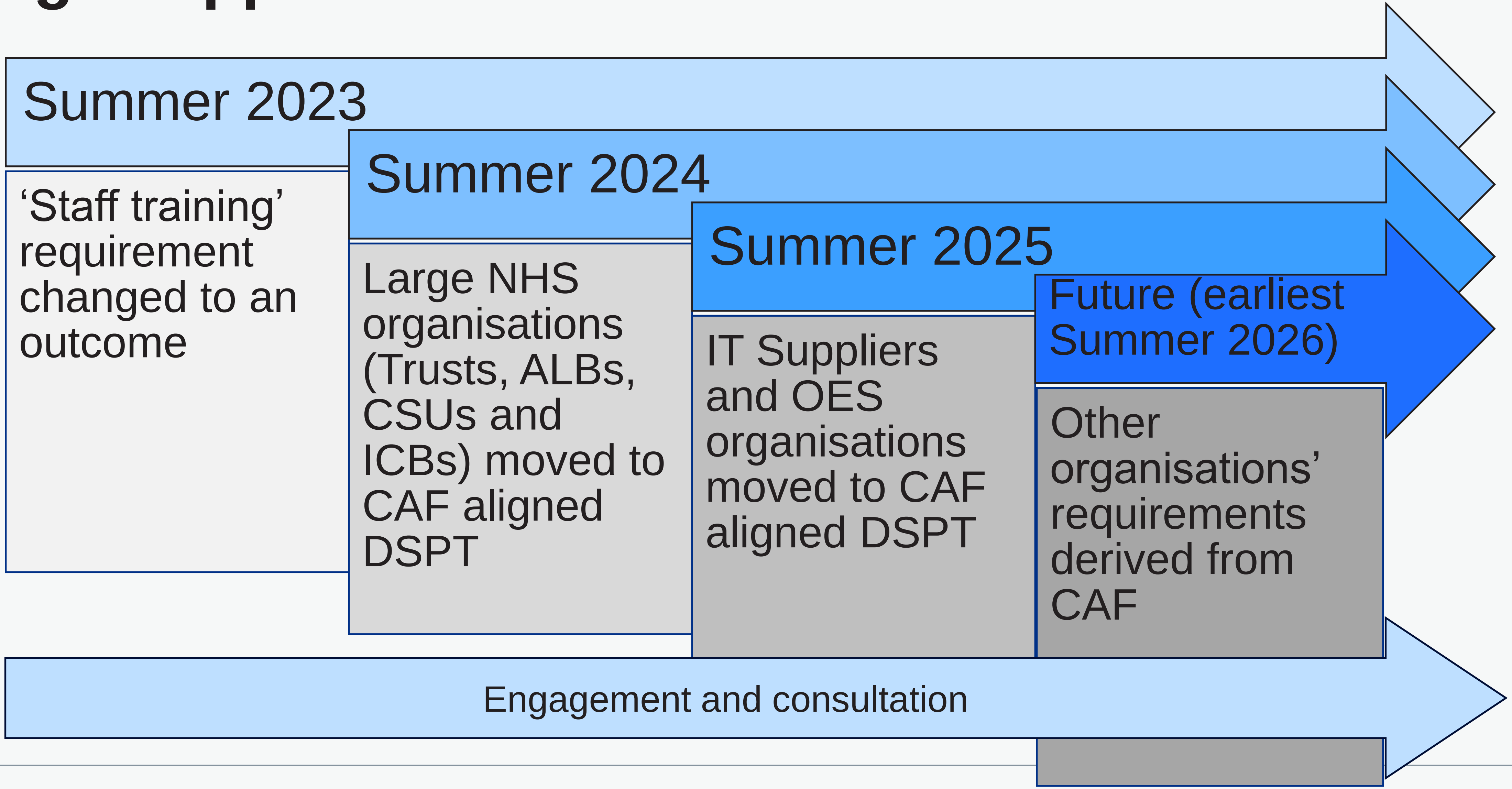
- Overview – what is in the Objective and which teams need to be involved in responding to it?
- Contributing outcomes – A step through C1a-d
- Half Time Quiz
- Contributing outcomes – A step through C1.e and C2
- Q&A session

What is happening and why?

What you need to know

- In September 2024 the DSPT will be changing to adopt the National Cyber Security Centre's Cyber Assessment Framework (CAF) as its basis for cyber security and IG assurance.
- This change will lead to NHS Trusts, CSUs, ALBs and ICBs seeing a different interface when they log in, which sets out CAF-aligned requirements in terms of Objectives, Principles and Outcomes.
- The goal of the CAF is to set out broad principles to drive good decision-making, rather than a "compliance checklist" of good practices.
- Expectations for cyber security and IG controls should remain at a reasonably comparable level to the current DSPT, tightening only in areas where NHSE and DHSC believe the higher standard to be a necessary obligation.
- Guidance will be produced and webinars have been stood up to help organisations understand the content, approach and expectations of the CAF-aligned DSPT.

Staged approach for DSPT



Summer 2023

‘Staff training’ requirement changed to an outcome

Summer 2024

Large NHS organisations (Trusts, ALBs, CSUs and ICBs) moved to CAF aligned DSPT

Summer 2025

IT Suppliers and OES organisations moved to CAF aligned DSPT

Future (earliest Summer 2026)

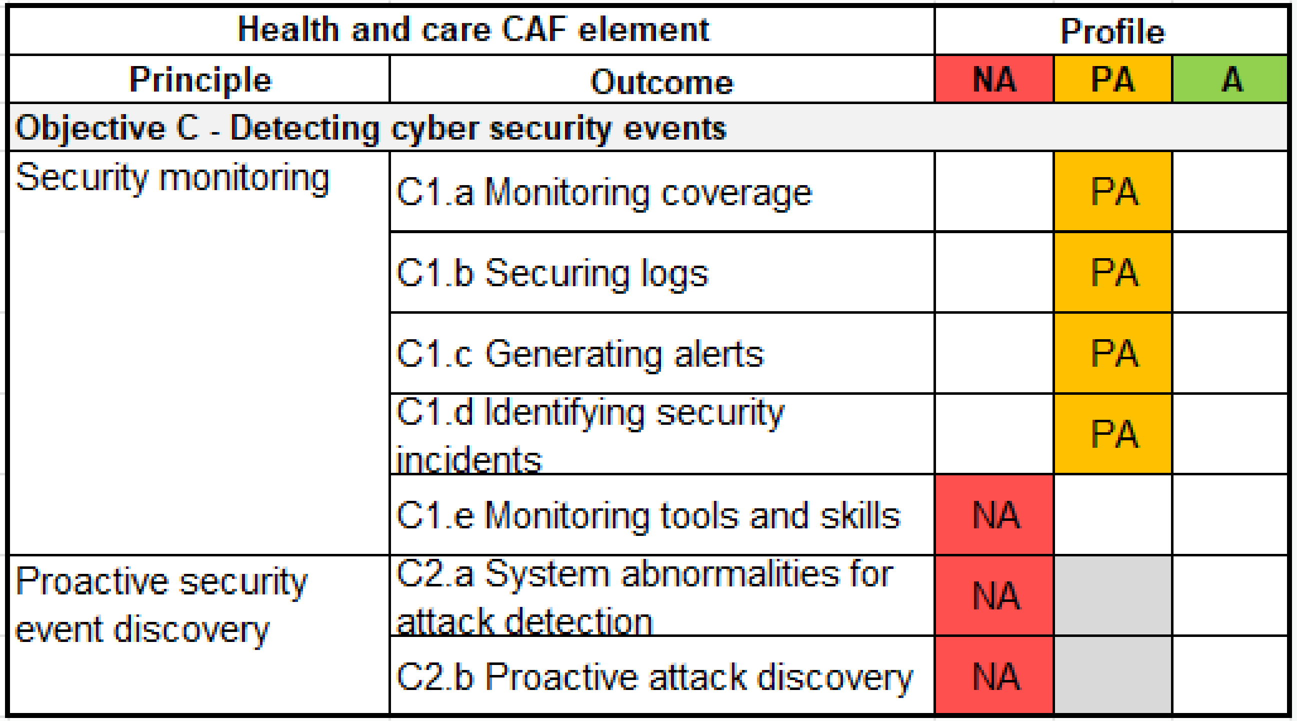
Other organisations’ requirements derived from CAF

Engagement and consultation

Objective C - Detecting cyber security events

Expectations for Standards met:

Objective C - Detecting cyber security events



Health and care CAF element		Profile		
Principle	Outcome	NA	PA	A
Objective C - Detecting cyber security events				
Security monitoring	C1.a Monitoring coverage		PA	
	C1.b Securing logs		PA	
	C1.c Generating alerts		PA	
	C1.d Identifying security incidents		PA	
	C1.e Monitoring tools and skills	NA		
Proactive security event discovery	C2.a System abnormalities for attack detection	NA		
	C2.b Proactive attack discovery	NA		

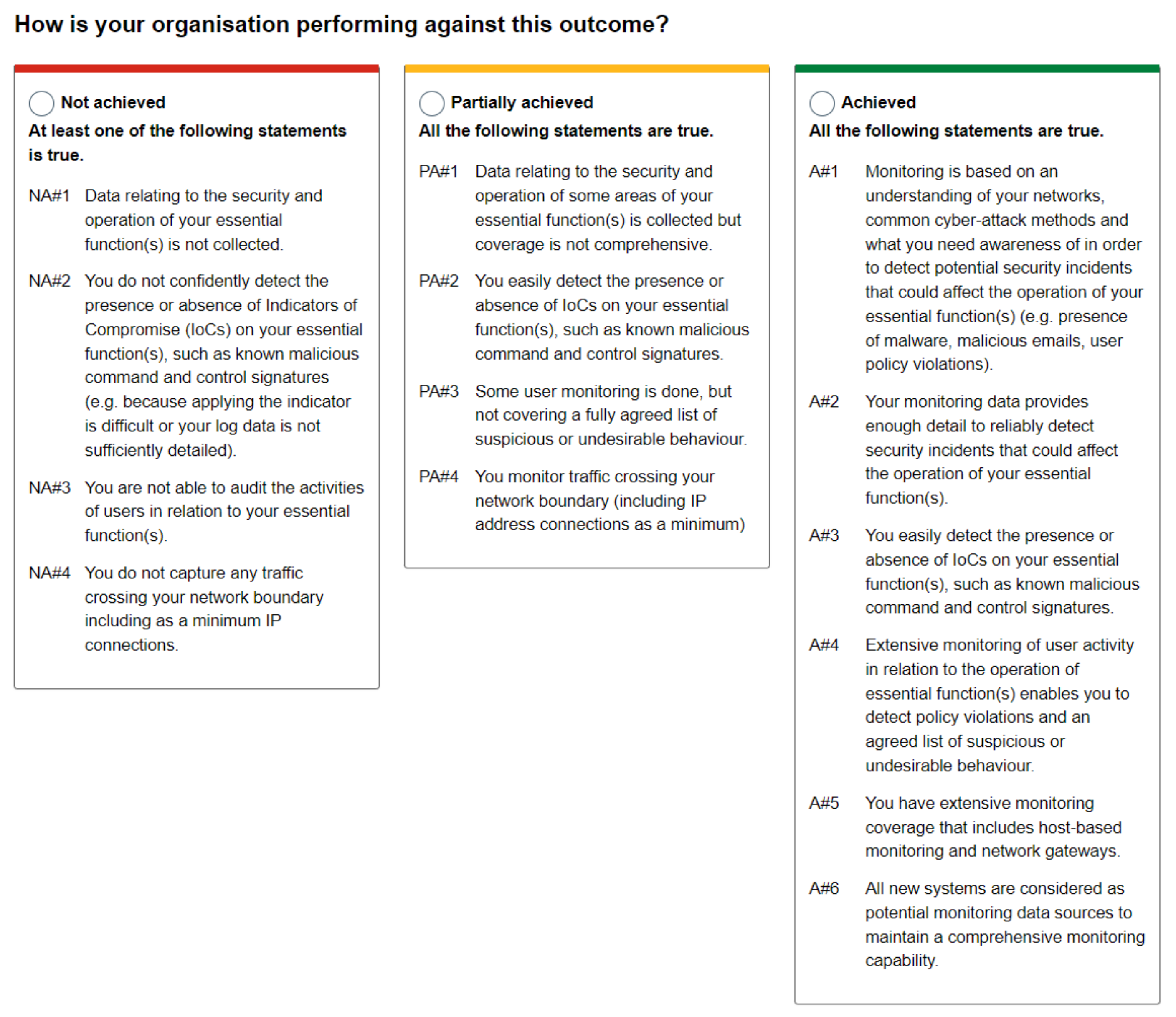
Principle:
C1 Security monitoring

Contributing outcome:
C1.a Monitoring coverage

The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s).

Expectation

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



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 Data relating to the security and operation of your essential function(s) is not collected.

NA#2 You do not confidently detect the presence or absence of Indicators of Compromise (IoCs) on your essential function(s), such as known malicious command and control signatures (e.g. because applying the indicator is difficult or your log data is not sufficiently detailed).

NA#3 You are not able to audit the activities of users in relation to your essential function(s).

NA#4 You do not capture any traffic crossing your network boundary including as a minimum IP connections.

○ **Partially achieved**

All the following statements are true.

PA#1 Data relating to the security and operation of some areas of your essential function(s) is collected but coverage is not comprehensive.

PA#2 You easily detect the presence or absence of IoCs on your essential function(s), such as known malicious command and control signatures.

PA#3 Some user monitoring is done, but not covering a fully agreed list of suspicious or undesirable behaviour.

PA#4 You monitor traffic crossing your network boundary (including IP address connections as a minimum)

○ **Achieved**

All the following statements are true.

A#1 Monitoring is based on an understanding of your networks, common cyber-attack methods and what you need awareness of in order to detect potential security incidents that could affect the operation of your essential function(s) (e.g. presence of malware, malicious emails, user policy violations).

A#2 Your monitoring data provides enough detail to reliably detect security incidents that could affect the operation of your essential function(s).

A#3 You easily detect the presence or absence of IoCs on your essential function(s), such as known malicious command and control signatures.

A#4 Extensive monitoring of user activity in relation to the operation of essential function(s) enables you to detect policy violations and an agreed list of suspicious or undesirable behaviour.

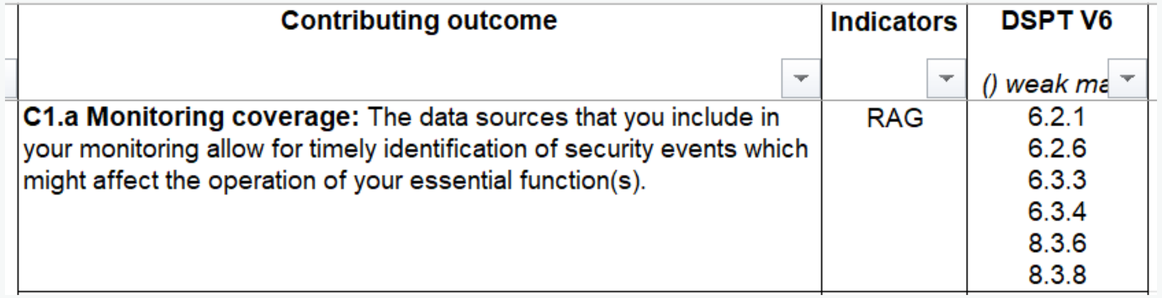
A#5 You have extensive monitoring coverage that includes host-based monitoring and network gateways.

A#6 All new systems are considered as potential monitoring data sources to maintain a comprehensive monitoring capability.

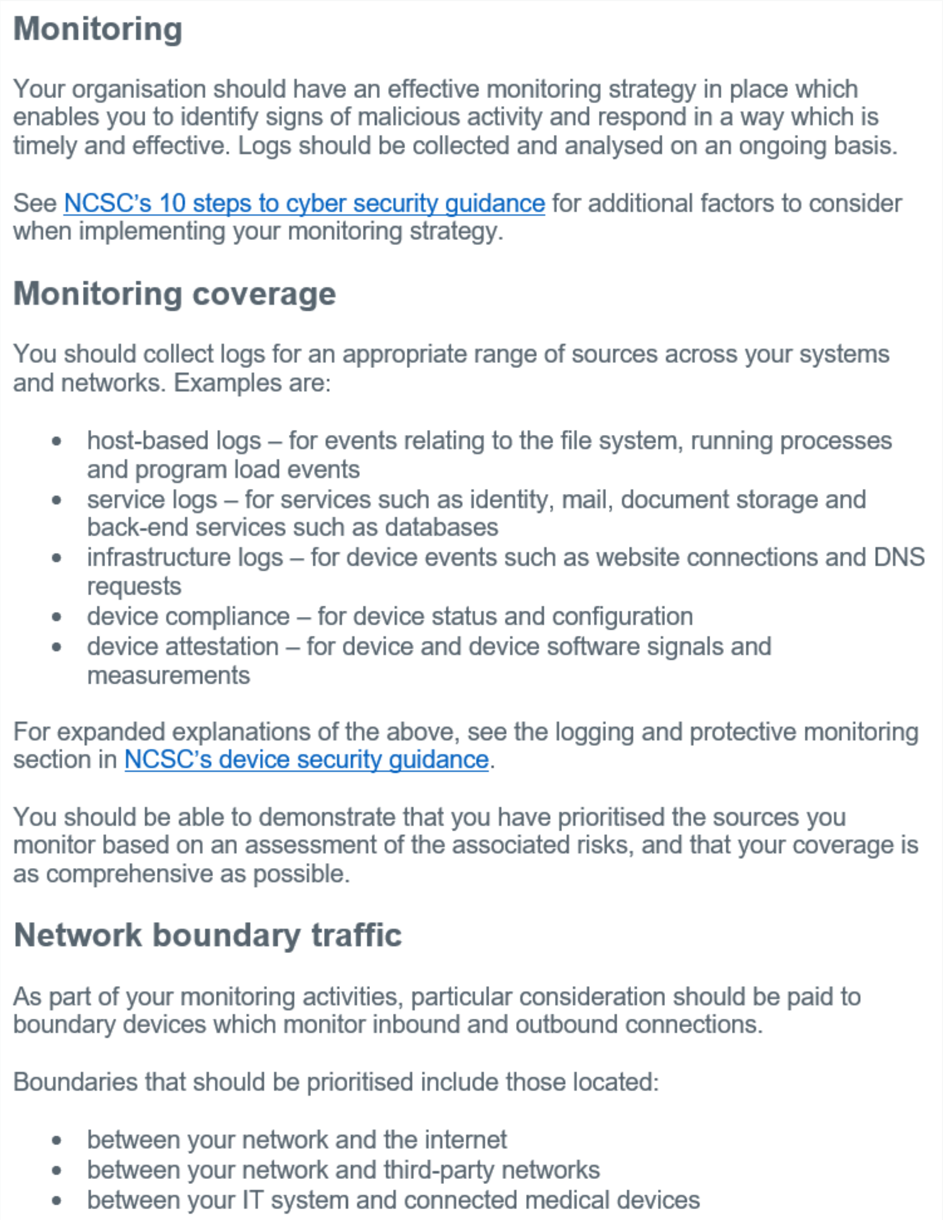
Principle:
C1 Security monitoring

Contributing outcome:
C1.a Monitoring coverage

Mapping, Guidance and Evidence to upload



Contributing outcome	Indicators	DSPT V6
		() weak ma
C1.a Monitoring coverage: The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s).	RAG	6.2.1 6.2.6 6.3.3 6.3.4 8.3.6 8.3.8



Monitoring

Your organisation should have an effective monitoring strategy in place which enables you to identify signs of malicious activity and respond in a way which is timely and effective. Logs should be collected and analysed on an ongoing basis.

See NCSC's 10 steps to cyber security guidance for additional factors to consider when implementing your monitoring strategy.

Monitoring coverage

You should collect logs for an appropriate range of sources across your systems and networks. Examples are:

- host-based logs – for events relating to the file system, running processes and program load events
- service logs – for services such as identity, mail, document storage and back-end services such as databases
- infrastructure logs – for device events such as website connections and DNS requests
- device compliance – for device status and configuration
- device attestation – for device and device software signals and measurements

For expanded explanations of the above, see the logging and protective monitoring section in NCSC's device security guidance.

You should be able to demonstrate that you have prioritised the sources you monitor based on an assessment of the associated risks, and that your coverage is as comprehensive as possible.

Network boundary traffic

As part of your monitoring activities, particular consideration should be paid to boundary devices which monitor inbound and outbound connections.

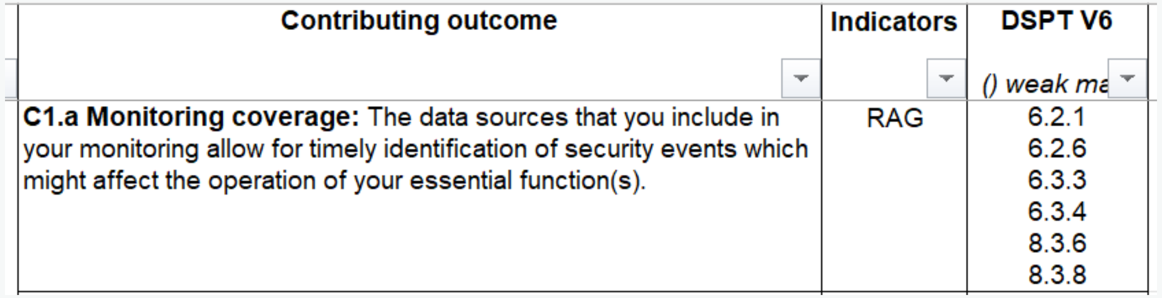
Boundaries that should be prioritised include those located:

- between your network and the internet
- between your network and third-party networks
- between your IT system and connected medical devices

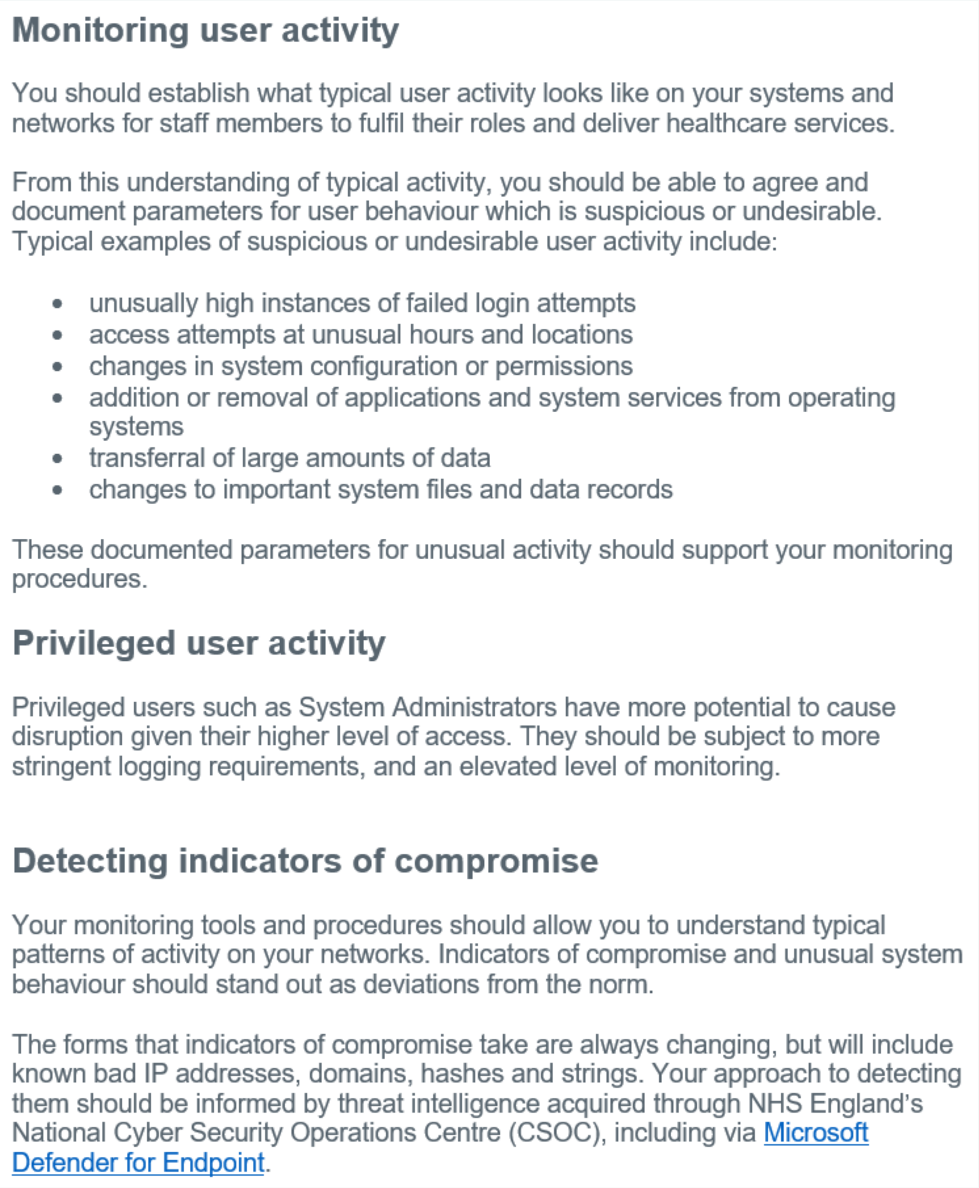
Principle:
C1 Security monitoring

Contributing outcome:
C1.a Monitoring coverage

Mapping, Guidance and Evidence to upload



Contributing outcome	Indicators	DSPT V6
		() weak ma
C1.a Monitoring coverage: The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s).	RAG	6.2.1 6.2.6 6.3.3 6.3.4 8.3.6 8.3.8



Monitoring user activity

You should establish what typical user activity looks like on your systems and networks for staff members to fulfil their roles and deliver healthcare services.

From this understanding of typical activity, you should be able to agree and document parameters for user behaviour which is suspicious or undesirable. Typical examples of suspicious or undesirable user activity include:

- unusually high instances of failed login attempts
- access attempts at unusual hours and locations
- changes in system configuration or permissions
- addition or removal of applications and system services from operating systems
- transferral of large amounts of data
- changes to important system files and data records

These documented parameters for unusual activity should support your monitoring procedures.

Privileged user activity

Privileged users such as System Administrators have more potential to cause disruption given their higher level of access. They should be subject to more stringent logging requirements, and an elevated level of monitoring.

Detecting indicators of compromise

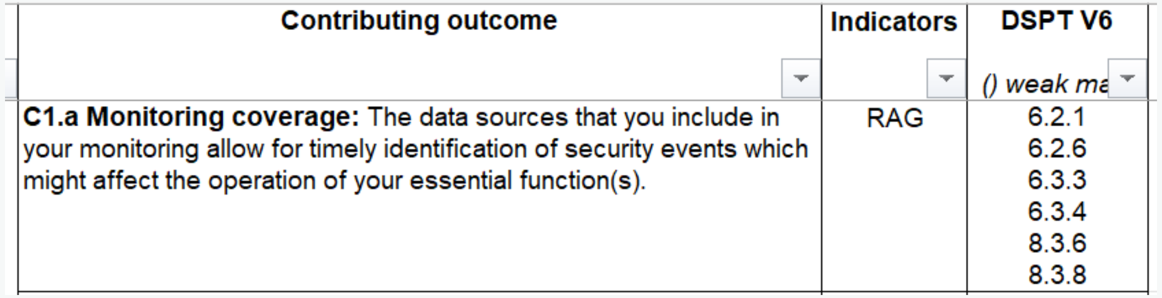
Your monitoring tools and procedures should allow you to understand typical patterns of activity on your networks. Indicators of compromise and unusual system behaviour should stand out as deviations from the norm.

The forms that indicators of compromise take are always changing, but will include known bad IP addresses, domains, hashes and strings. Your approach to detecting them should be informed by threat intelligence acquired through NHS England's National Cyber Security Operations Centre (CSOC), including via Microsoft Defender for Endpoint.

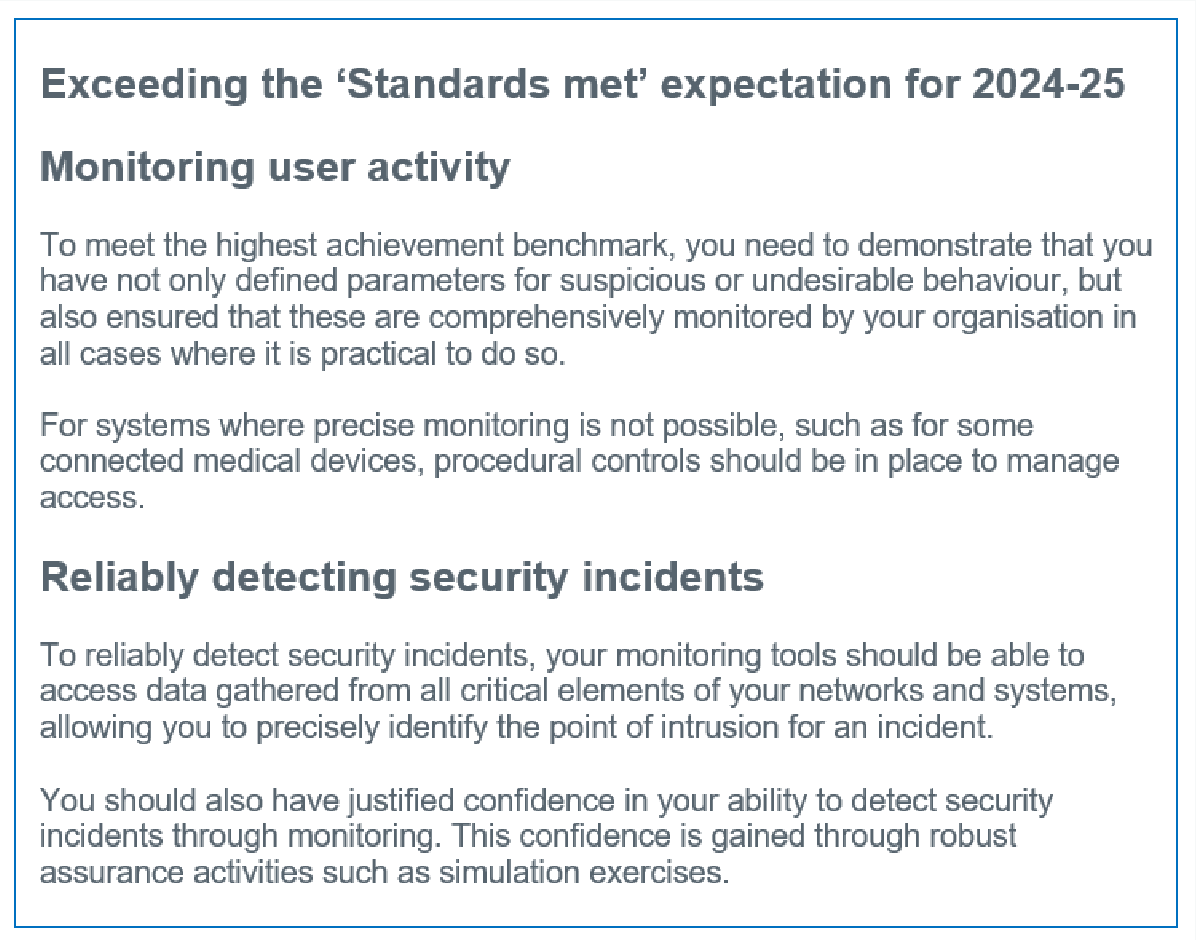
Principle:
C1 Security monitoring

Contributing outcome:
C1.a Monitoring coverage

Mapping, Guidance and Evidence to upload



Contributing outcome	Indicators	DSPT V6 () weak ma
C1.a Monitoring coverage: The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s).	RAG	6.2.1 6.2.6 6.3.3 6.3.4 8.3.6 8.3.8



Exceeding the ‘Standards met’ expectation for 2024-25

Monitoring user activity

To meet the highest achievement benchmark, you need to demonstrate that you have not only defined parameters for suspicious or undesirable behaviour, but also ensured that these are comprehensively monitored by your organisation in all cases where it is practical to do so.

For systems where precise monitoring is not possible, such as for some connected medical devices, procedural controls should be in place to manage access.

Reliably detecting security incidents

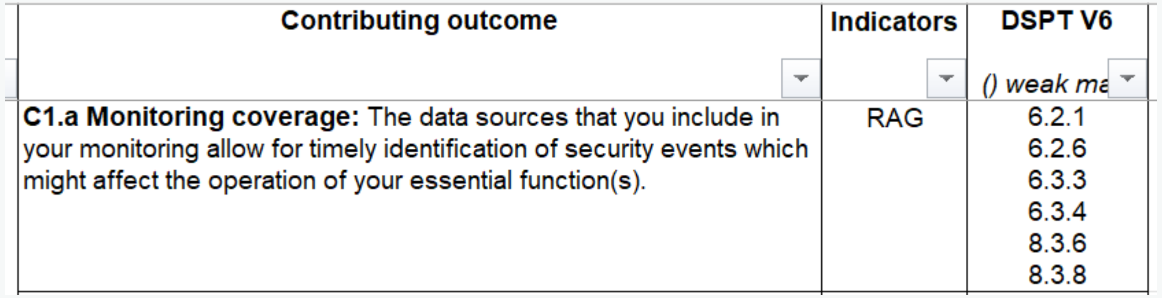
To reliably detect security incidents, your monitoring tools should be able to access data gathered from all critical elements of your networks and systems, allowing you to precisely identify the point of intrusion for an incident.

You should also have justified confidence in your ability to detect security incidents through monitoring. This confidence is gained through robust assurance activities such as simulation exercises.

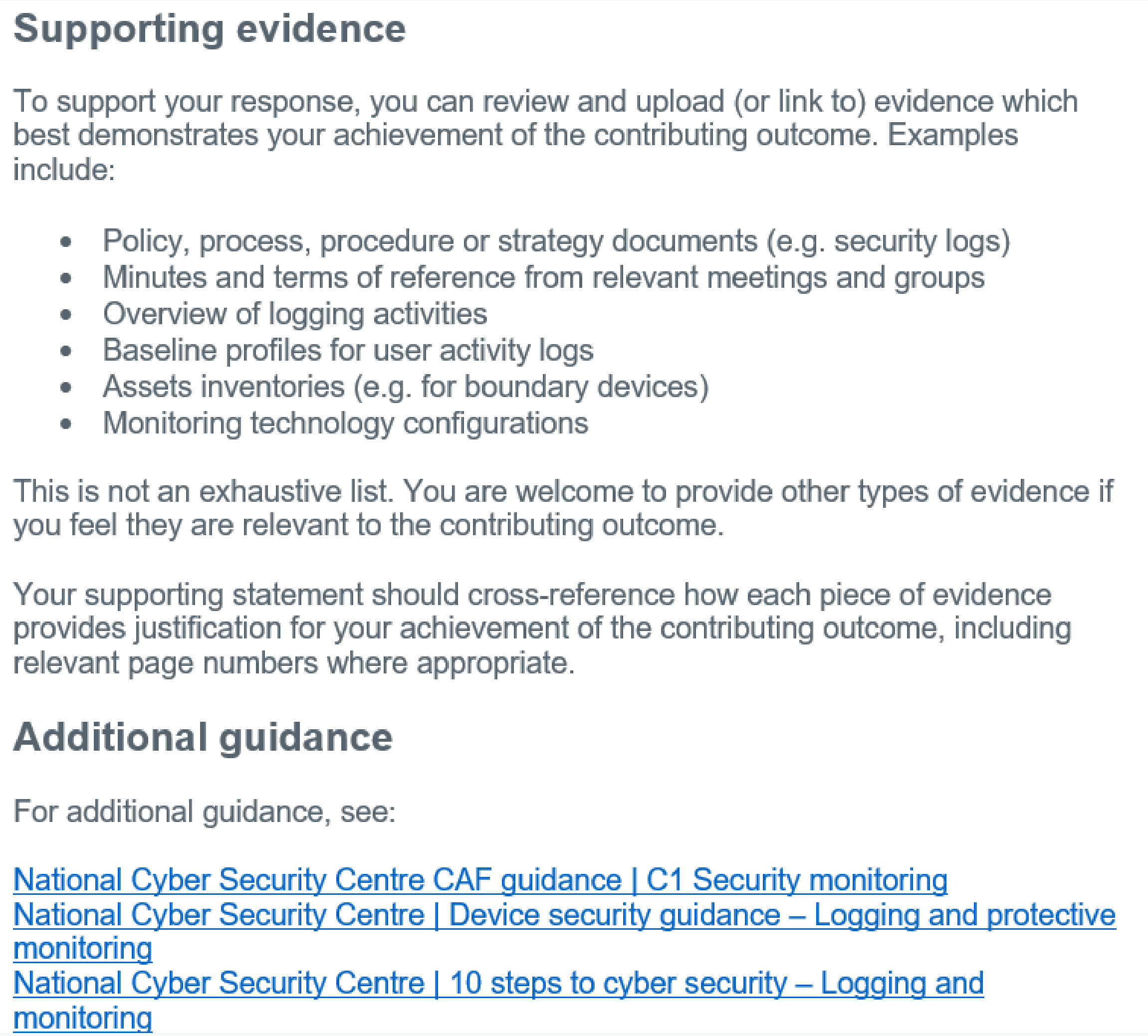
Principle:
C1 Security monitoring

Contributing outcome:
C1.a Monitoring coverage

Mapping, Guidance and Evidence to upload



Contributing outcome	Indicators	DSPT V6 () weak ma
C1.a Monitoring coverage: The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s).	RAG	6.2.1 6.2.6 6.3.3 6.3.4 8.3.6 8.3.8



Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- Policy, process, procedure or strategy documents (e.g. security logs)
- Minutes and terms of reference from relevant meetings and groups
- Overview of logging activities
- Baseline profiles for user activity logs
- Assets inventories (e.g. for boundary devices)
- Monitoring technology configurations

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | C1 Security monitoring
National Cyber Security Centre | Device security guidance – Logging and protective monitoring
National Cyber Security Centre | 10 steps to cyber security – Logging and monitoring

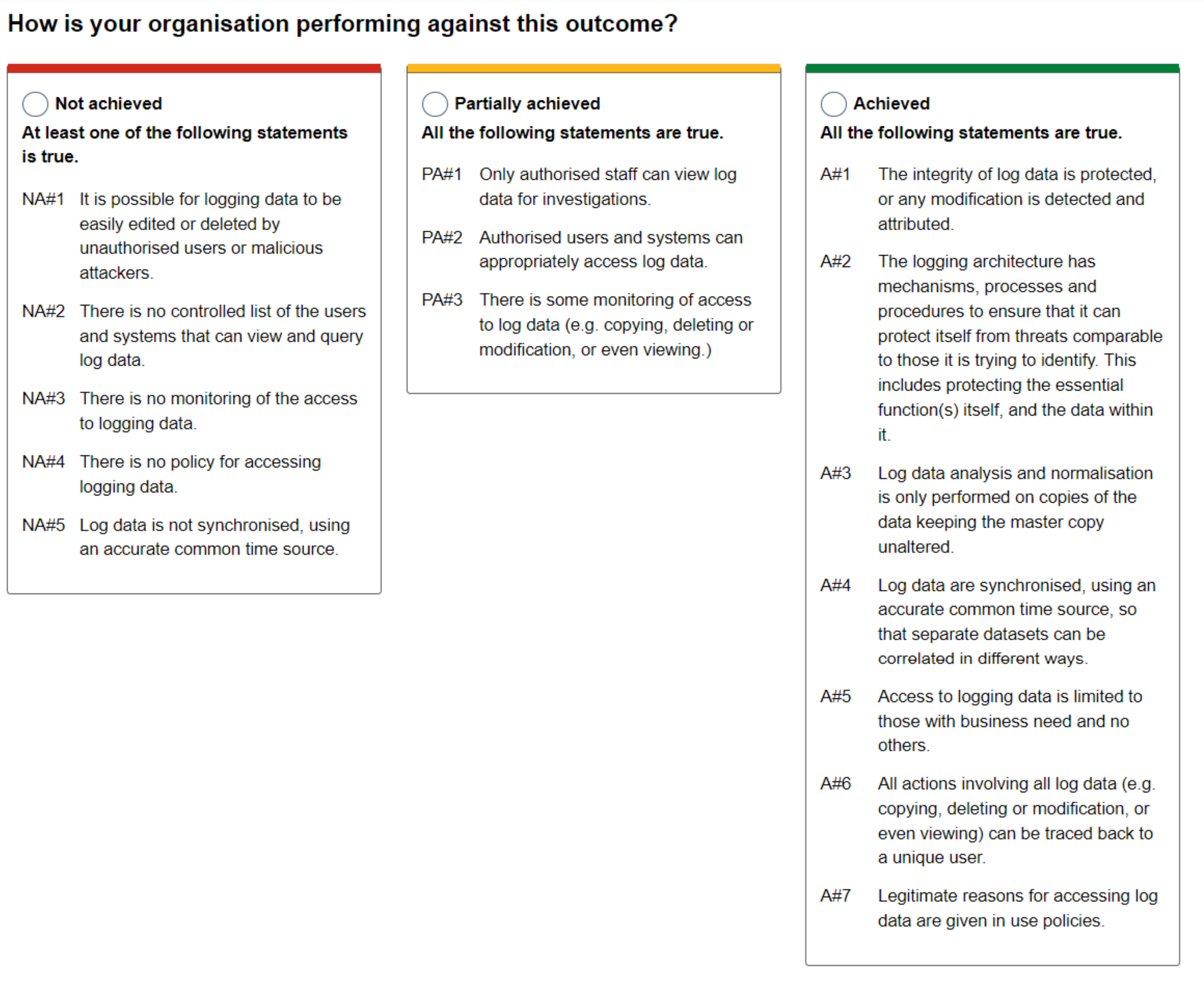
Principle:
C1 Security monitoring

Contributing outcome:
C1.b Securing logs

You hold log data securely and grant appropriate access only to accounts with business need. No system or user should ever need to modify or delete master copies of log data within an agreed retention period, after which it should be deleted.

Expectation

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



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 It is possible for logging data to be easily edited or deleted by unauthorised users or malicious attackers.

NA#2 There is no controlled list of the users and systems that can view and query log data.

NA#3 There is no monitoring of the access to logging data.

NA#4 There is no policy for accessing logging data.

NA#5 Log data is not synchronised, using an accurate common time source.

○ **Partially achieved**

All the following statements are true.

PA#1 Only authorised staff can view log data for investigations.

PA#2 Authorised users and systems can appropriately access log data.

PA#3 There is some monitoring of access to log data (e.g. copying, deleting or modification, or even viewing.)

○ **Achieved**

All the following statements are true.

A#1 The integrity of log data is protected, or any modification is detected and attributed.

A#2 The logging architecture has mechanisms, processes and procedures to ensure that it can protect itself from threats comparable to those it is trying to identify. This includes protecting the essential function(s) itself, and the data within it.

A#3 Log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered.

A#4 Log data are synchronised, using an accurate common time source, so that separate datasets can be correlated in different ways.

A#5 Access to logging data is limited to those with business need and no others.

A#6 All actions involving all log data (e.g. copying, deleting or modification, or even viewing) can be traced back to a unique user.

A#7 Legitimate reasons for accessing log data are given in use policies.

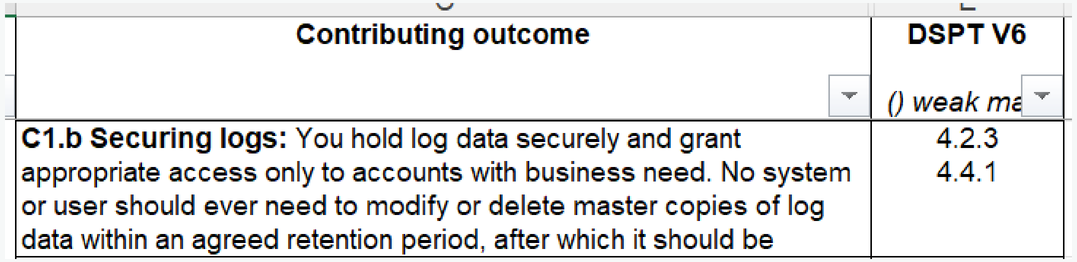
Principle:

C1 Security monitoring

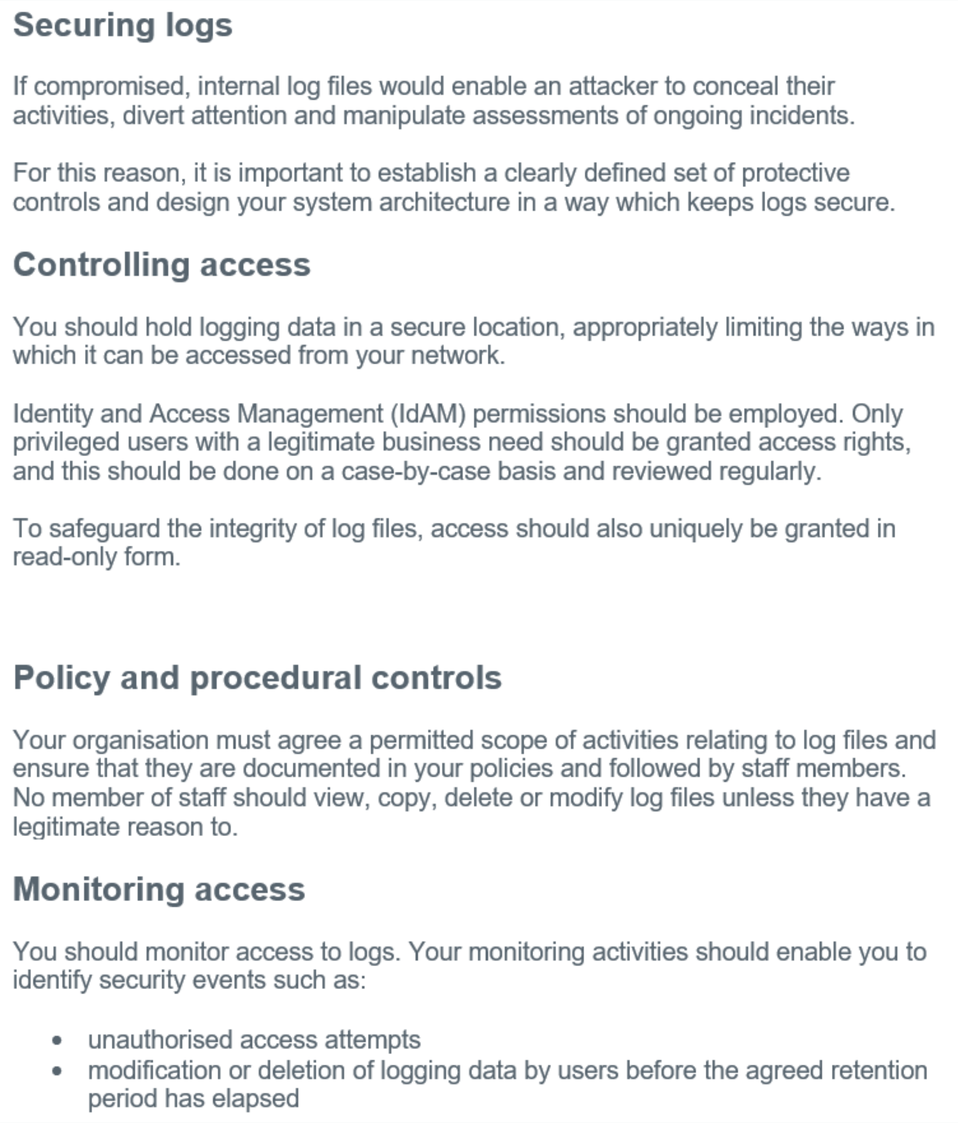
Contributing outcome:

C1.b Securing logs

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 *() weak ma*
C1.b Securing logs: You hold log data securely and grant appropriate access only to accounts with business need. No system or user should ever need to modify or delete master copies of log data within an agreed retention period, after which it should be	4.2.3 4.4.1



Securing logs

If compromised, internal log files would enable an attacker to conceal their activities, divert attention and manipulate assessments of ongoing incidents.

For this reason, it is important to establish a clearly defined set of protective controls and design your system architecture in a way which keeps logs secure.

Controlling access

You should hold logging data in a secure location, appropriately limiting the ways in which it can be accessed from your network.

Identity and Access Management (IdAM) permissions should be employed. Only privileged users with a legitimate business need should be granted access rights, and this should be done on a case-by-case basis and reviewed regularly.

To safeguard the integrity of log files, access should also uniquely be granted in read-only form.

Policy and procedural controls

Your organisation must agree a permitted scope of activities relating to log files and ensure that they are documented in your policies and followed by staff members. No member of staff should view, copy, delete or modify log files unless they have a legitimate reason to.

Monitoring access

You should monitor access to logs. Your monitoring activities should enable you to identify security events such as:

- unauthorised access attempts
- modification or deletion of logging data by users before the agreed retention period has elapsed

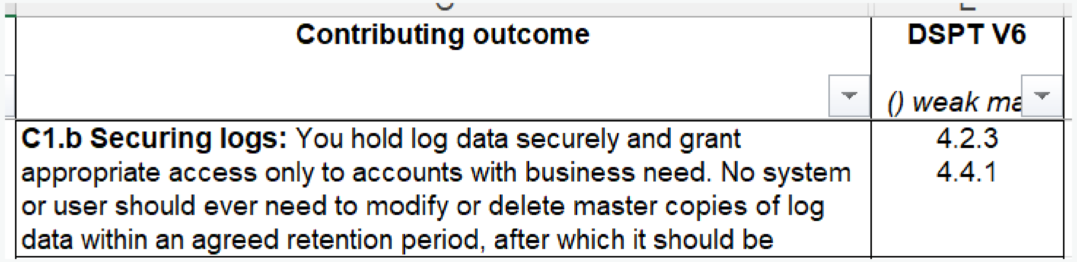
Principle:

C1 Security monitoring

Contributing outcome:

C1.b Securing logs

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 () weak ma
C1.b Securing logs: You hold log data securely and grant appropriate access only to accounts with business need. No system or user should ever need to modify or delete master copies of log data within an agreed retention period, after which it should be	4.2.3 4.4.1

Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- Policy, process, procedure or strategy documents (e.g. security logs)
- Minutes and terms of reference from relevant meetings and groups
- Details of security measures for logging

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | C1 Security monitoring

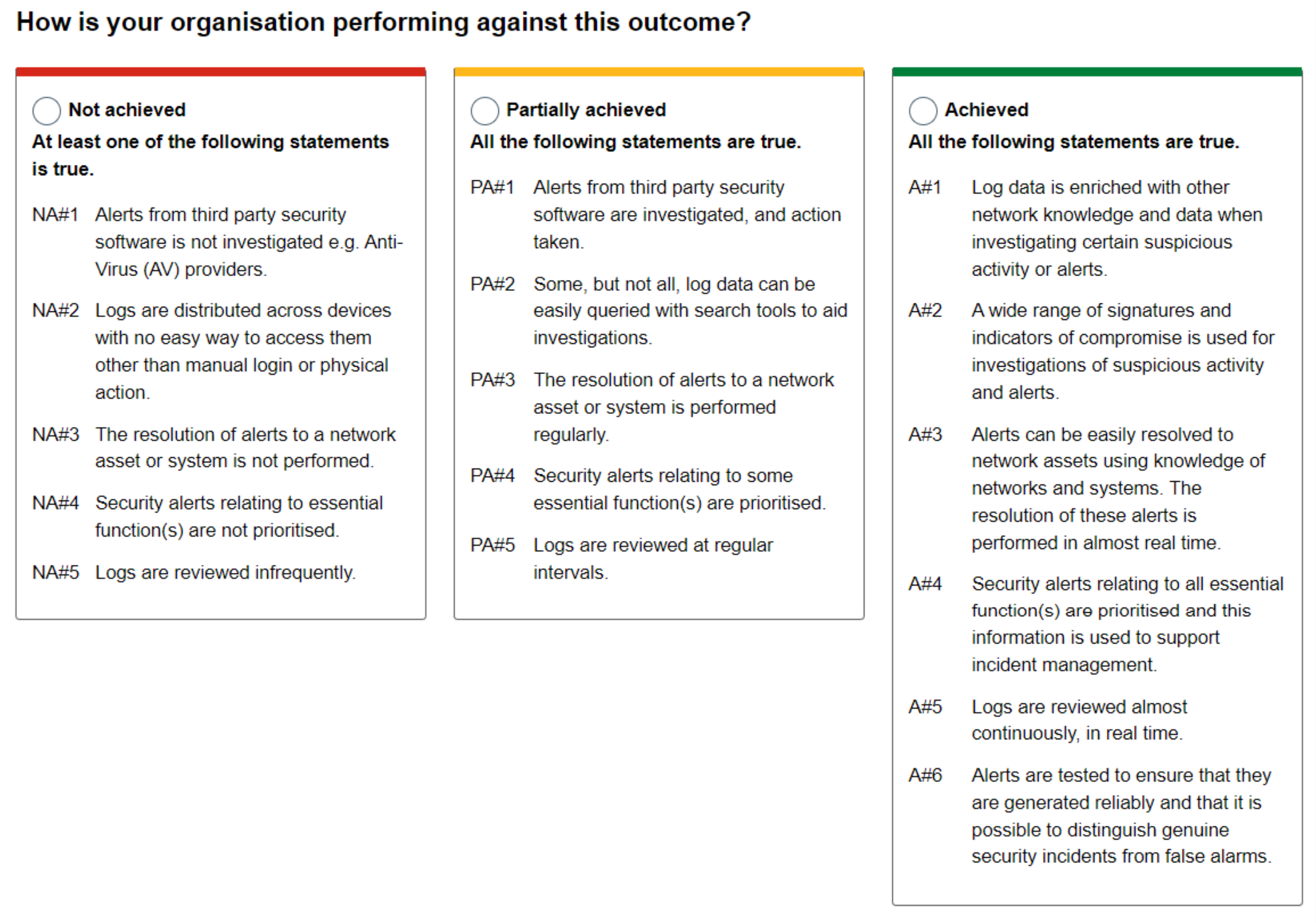
Principle:
C1 Security monitoring

Contributing outcome:
C1.c Generating alerts

Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts

Expectation

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



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 Alerts from third party security software is not investigated e.g. Anti-Virus (AV) providers.

NA#2 Logs are distributed across devices with no easy way to access them other than manual login or physical action.

NA#3 The resolution of alerts to a network asset or system is not performed.

NA#4 Security alerts relating to essential function(s) are not prioritised.

NA#5 Logs are reviewed infrequently.

○ **Partially achieved**

All the following statements are true.

PA#1 Alerts from third party security software are investigated, and action taken.

PA#2 Some, but not all, log data can be easily queried with search tools to aid investigations.

PA#3 The resolution of alerts to a network asset or system is performed regularly.

PA#4 Security alerts relating to some essential function(s) are prioritised.

PA#5 Logs are reviewed at regular intervals.

○ **Achieved**

All the following statements are true.

A#1 Log data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts.

A#2 A wide range of signatures and indicators of compromise is used for investigations of suspicious activity and alerts.

A#3 Alerts can be easily resolved to network assets using knowledge of networks and systems. The resolution of these alerts is performed in almost real time.

A#4 Security alerts relating to all essential function(s) are prioritised and this information is used to support incident management.

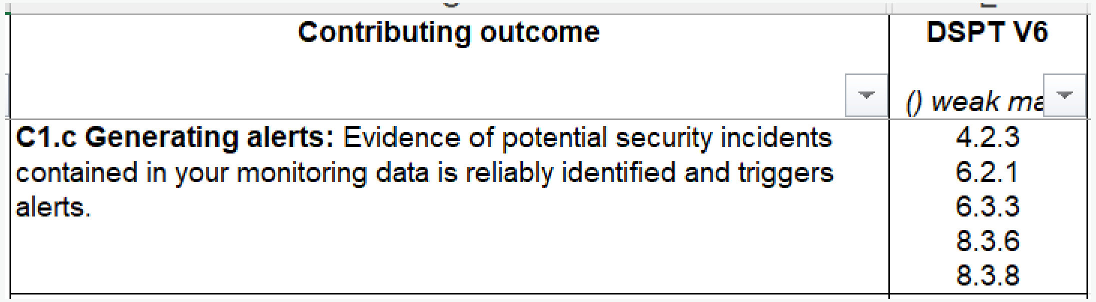
A#5 Logs are reviewed almost continuously, in real time.

A#6 Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.

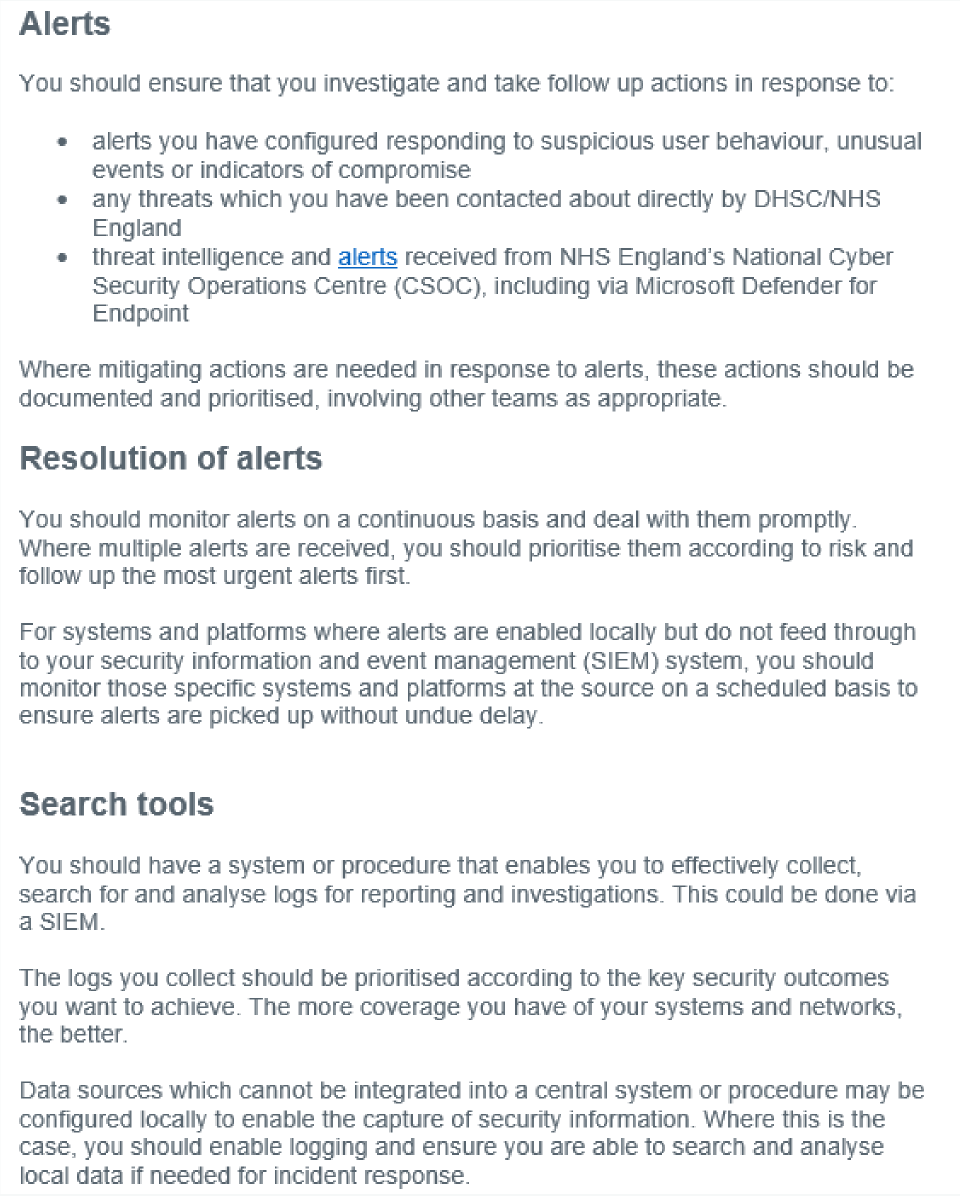
Principle:
C1 Security monitoring

Contributing outcome:
C1.c Generating alerts

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 () weak ma
C1.c Generating alerts: Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.	4.2.3 6.2.1 6.3.3 8.3.6 8.3.8



Alerts

You should ensure that you investigate and take follow up actions in response to:

- alerts you have configured responding to suspicious user behaviour, unusual events or indicators of compromise
- any threats which you have been contacted about directly by DHSC/NHS England
- threat intelligence and alerts received from NHS England's National Cyber Security Operations Centre (CSOC), including via Microsoft Defender for Endpoint

Where mitigating actions are needed in response to alerts, these actions should be documented and prioritised, involving other teams as appropriate.

Resolution of alerts

You should monitor alerts on a continuous basis and deal with them promptly. Where multiple alerts are received, you should prioritise them according to risk and follow up the most urgent alerts first.

For systems and platforms where alerts are enabled locally but do not feed through to your security information and event management (SIEM) system, you should monitor those specific systems and platforms at the source on a scheduled basis to ensure alerts are picked up without undue delay.

Search tools

You should have a system or procedure that enables you to effectively collect, search for and analyse logs for reporting and investigations. This could be done via a SIEM.

The logs you collect should be prioritised according to the key security outcomes you want to achieve. The more coverage you have of your systems and networks, the better.

Data sources which cannot be integrated into a central system or procedure may be configured locally to enable the capture of security information. Where this is the case, you should enable logging and ensure you are able to search and analyse local data if needed for incident response.

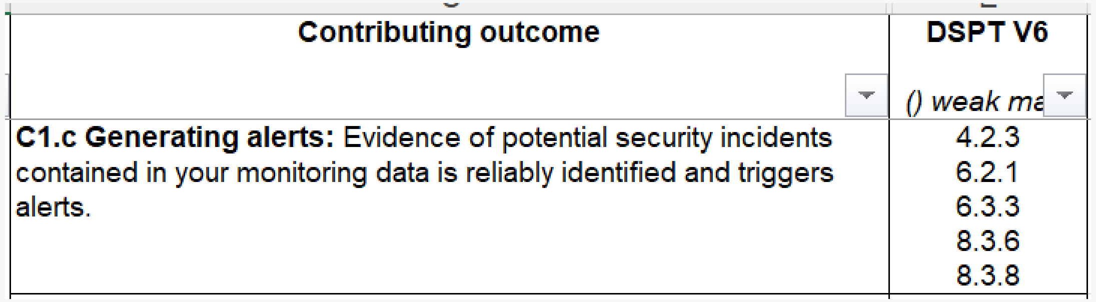
Principle:

C1 Security monitoring

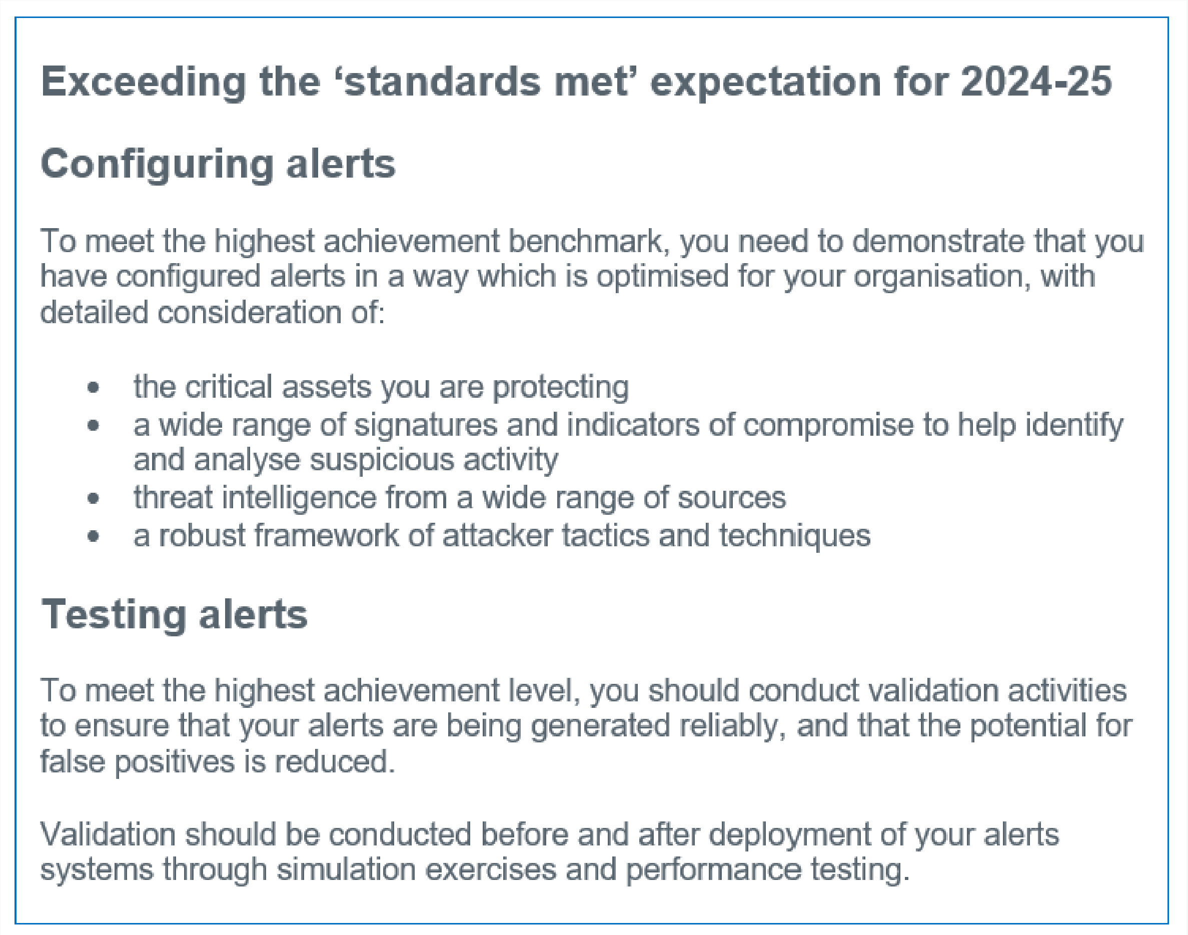
Contributing outcome:

C1.c Generating alerts

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 () weak ma
C1.c Generating alerts: Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.	4.2.3 6.2.1 6.3.3 8.3.6 8.3.8



Exceeding the ‘standards met’ expectation for 2024-25

Configuring alerts

To meet the highest achievement benchmark, you need to demonstrate that you have configured alerts in a way which is optimised for your organisation, with detailed consideration of:

- the critical assets you are protecting
- a wide range of signatures and indicators of compromise to help identify and analyse suspicious activity
- threat intelligence from a wide range of sources
- a robust framework of attacker tactics and techniques

Testing alerts

To meet the highest achievement level, you should conduct validation activities to ensure that your alerts are being generated reliably, and that the potential for false positives is reduced.

Validation should be conducted before and after deployment of your alerts systems through simulation exercises and performance testing.

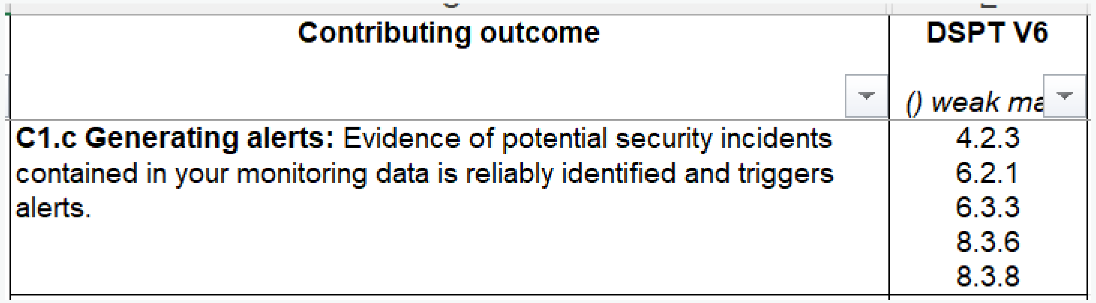
Principle:

C1 Security monitoring

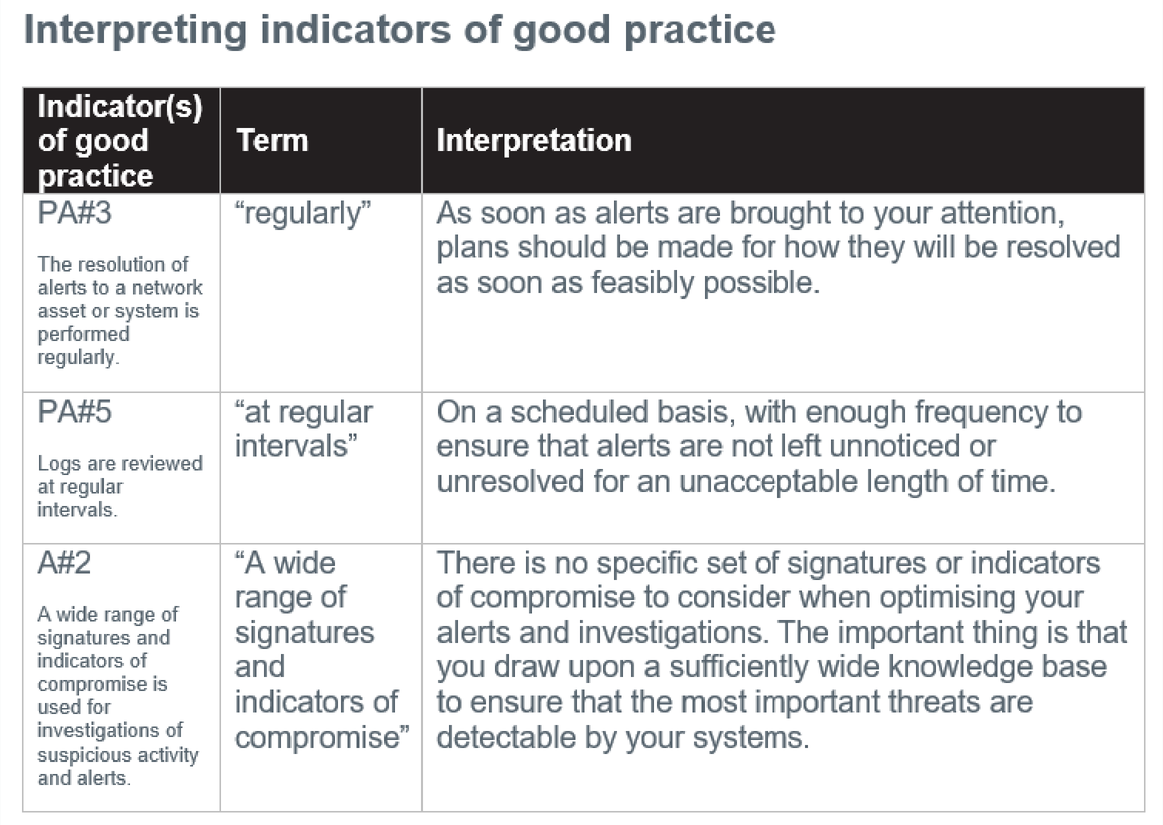
Contributing outcome:

C1.c Generating alerts

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 () weak ma
C1.c Generating alerts: Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.	4.2.3 6.2.1 6.3.3 8.3.6 8.3.8



Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#3 The resolution of alerts to a network asset or system is performed regularly.	"regularly"	As soon as alerts are brought to your attention, plans should be made for how they will be resolved as soon as feasibly possible.
PA#5 Logs are reviewed at regular intervals.	"at regular intervals"	On a scheduled basis, with enough frequency to ensure that alerts are not left unnoticed or unresolved for an unacceptable length of time.
A#2 A wide range of signatures and indicators of compromise is used for investigations of suspicious activity and alerts.	"A wide range of signatures and indicators of compromise"	There is no specific set of signatures or indicators of compromise to consider when optimising your alerts and investigations. The important thing is that you draw upon a sufficiently wide knowledge base to ensure that the most important threats are detectable by your systems.

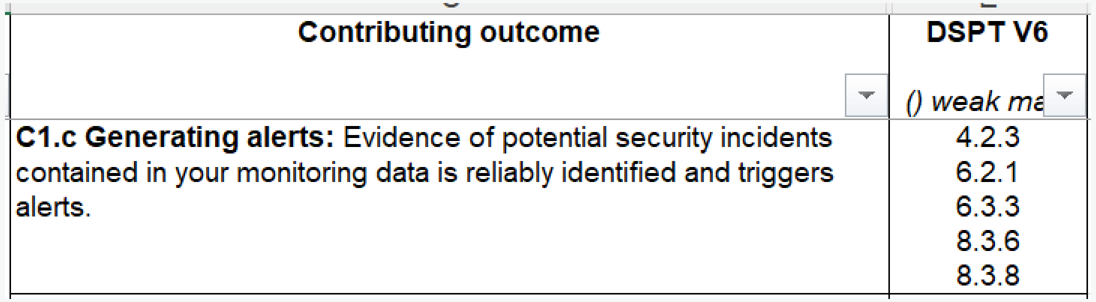
Principle:

C1 Security monitoring

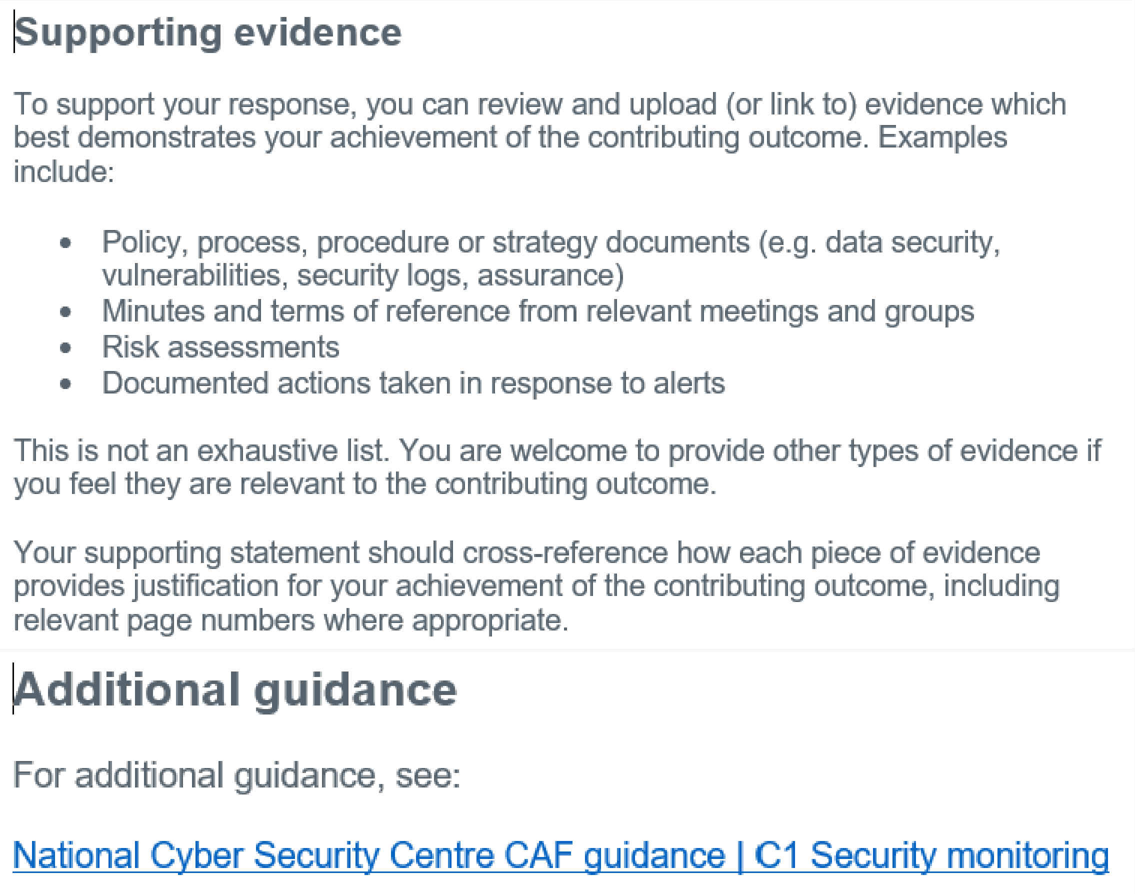
Contributing outcome:

C1.c Generating alerts

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 () weak ma
C1.c Generating alerts: Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.	4.2.3 6.2.1 6.3.3 8.3.6 8.3.8



Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- Policy, process, procedure or strategy documents (e.g. data security, vulnerabilities, security logs, assurance)
- Minutes and terms of reference from relevant meetings and groups
- Risk assessments
- Documented actions taken in response to alerts

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | C1 Security monitoring

Principle:

C1 Security monitoring

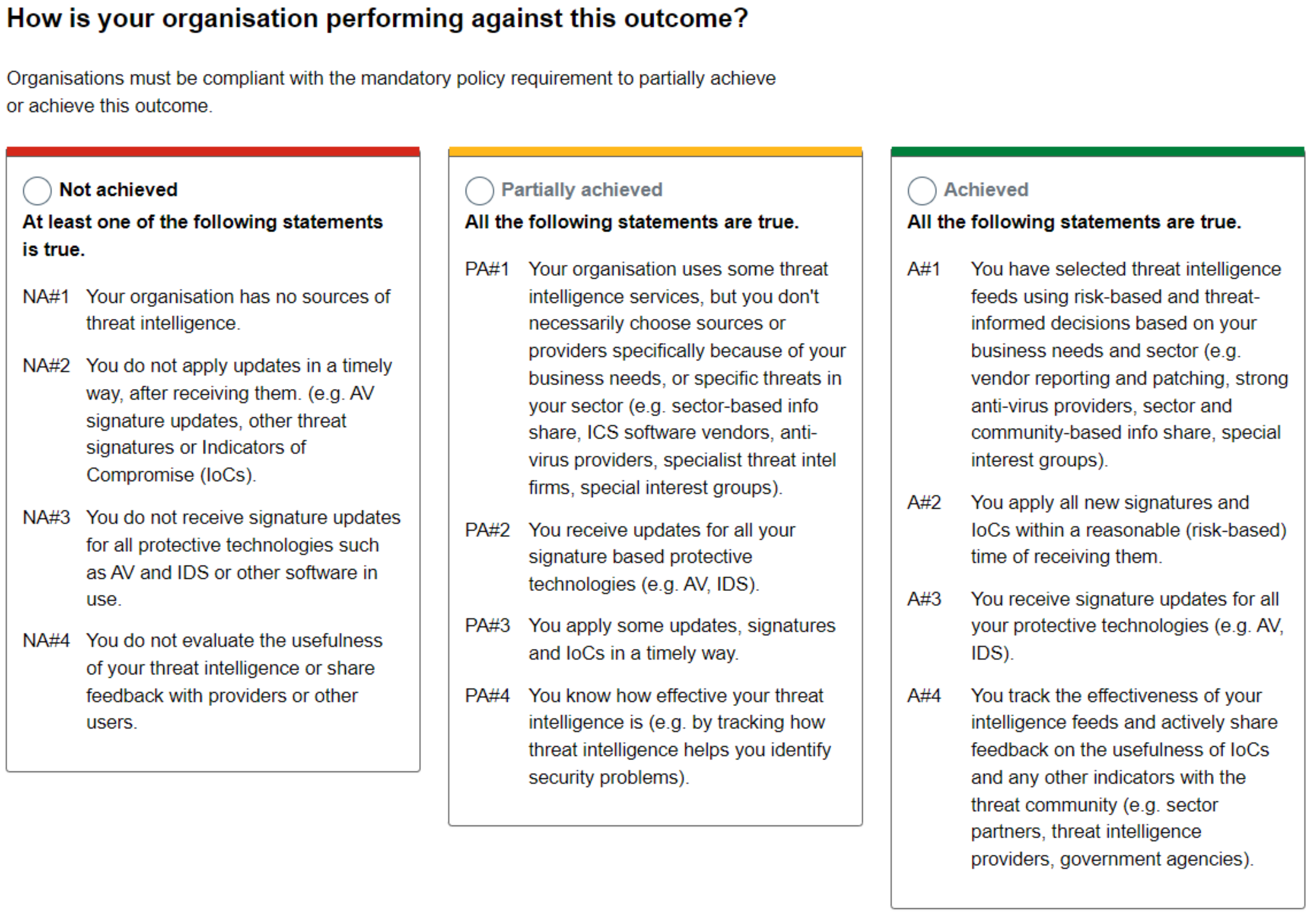
Contributing outcome:

C1.d Identifying security incidents

You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response

Expectation

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



How is your organisation performing against this outcome?

Organisations must be compliant with the mandatory policy requirement to partially achieve or achieve this outcome.

○ **Not achieved**

At least one of the following statements is true.

NA#1 Your organisation has no sources of threat intelligence.

NA#2 You do not apply updates in a timely way, after receiving them. (e.g. AV signature updates, other threat signatures or Indicators of Compromise (IoCs).

NA#3 You do not receive signature updates for all protective technologies such as AV and IDS or other software in use.

NA#4 You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.

○ **Partially achieved**

All the following statements are true.

PA#1 Your organisation uses some threat intelligence services, but you don't necessarily choose sources or providers specifically because of your business needs, or specific threats in your sector (e.g. sector-based info share, ICS software vendors, anti-virus providers, specialist threat intel firms, special interest groups).

PA#2 You receive updates for all your signature based protective technologies (e.g. AV, IDS).

PA#3 You apply some updates, signatures and IoCs in a timely way.

PA#4 You know how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security problems).

○ **Achieved**

All the following statements are true.

A#1 You have selected threat intelligence feeds using risk-based and threat-informed decisions based on your business needs and sector (e.g. vendor reporting and patching, strong anti-virus providers, sector and community-based info share, special interest groups).

A#2 You apply all new signatures and IoCs within a reasonable (risk-based) time of receiving them.

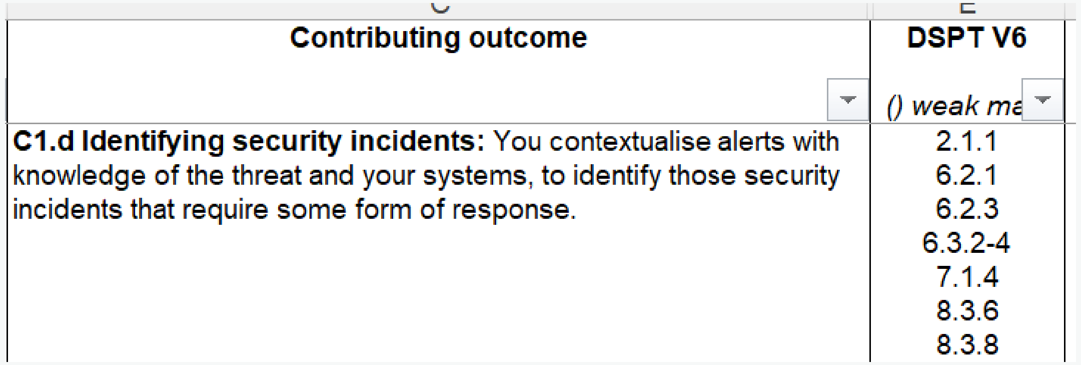
A#3 You receive signature updates for all your protective technologies (e.g. AV, IDS).

A#4 You track the effectiveness of your intelligence feeds and actively share feedback on the usefulness of IoCs and any other indicators with the threat community (e.g. sector partners, threat intelligence providers, government agencies).

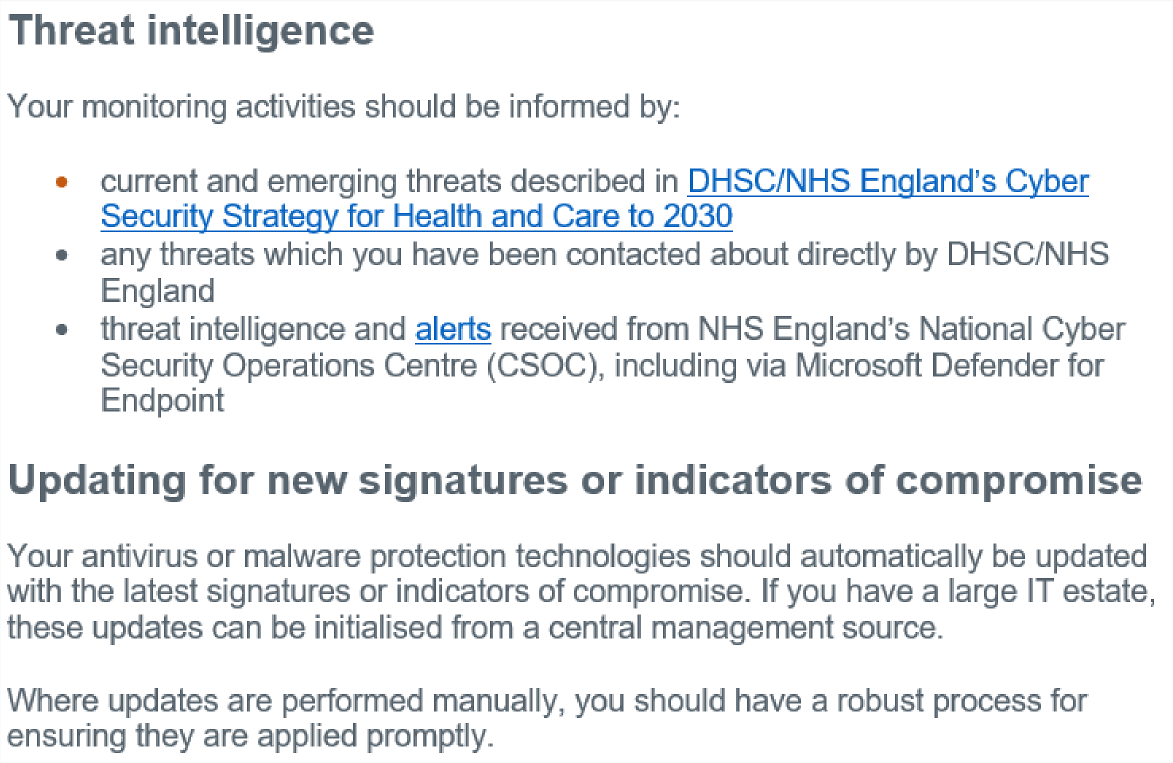
Principle:
C1 Security monitoring

Contributing outcome:
C1.d Identifying security incidents

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 () weak ma
C1.d Identifying security incidents: You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.	2.1.1 6.2.1 6.2.3 6.3.2-4 7.1.4 8.3.6 8.3.8



Threat intelligence

Your monitoring activities should be informed by:

- current and emerging threats described in DHSC/NHS England's Cyber Security Strategy for Health and Care to 2030
- any threats which you have been contacted about directly by DHSC/NHS England
- threat intelligence and alerts received from NHS England's National Cyber Security Operations Centre (CSOC), including via Microsoft Defender for Endpoint

Updating for new signatures or indicators of compromise

Your antivirus or malware protection technologies should automatically be updated with the latest signatures or indicators of compromise. If you have a large IT estate, these updates can be initialised from a central management source.

Where updates are performed manually, you should have a robust process for ensuring they are applied promptly.

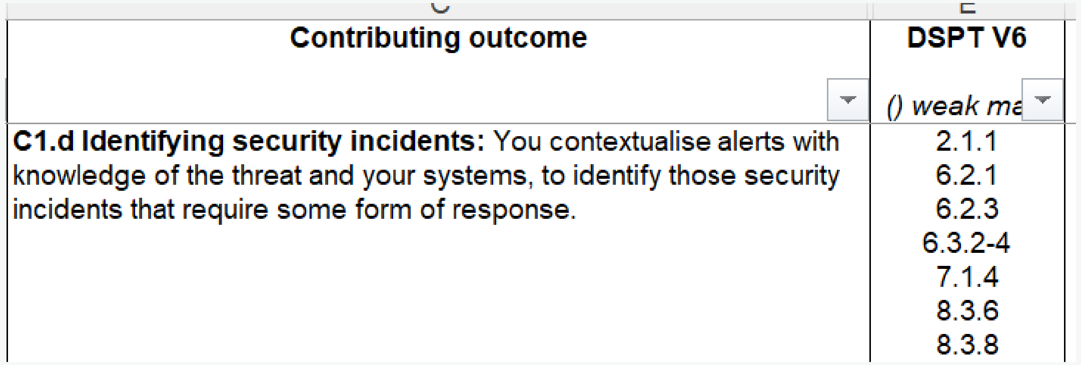
Principle:

C1 Security monitoring

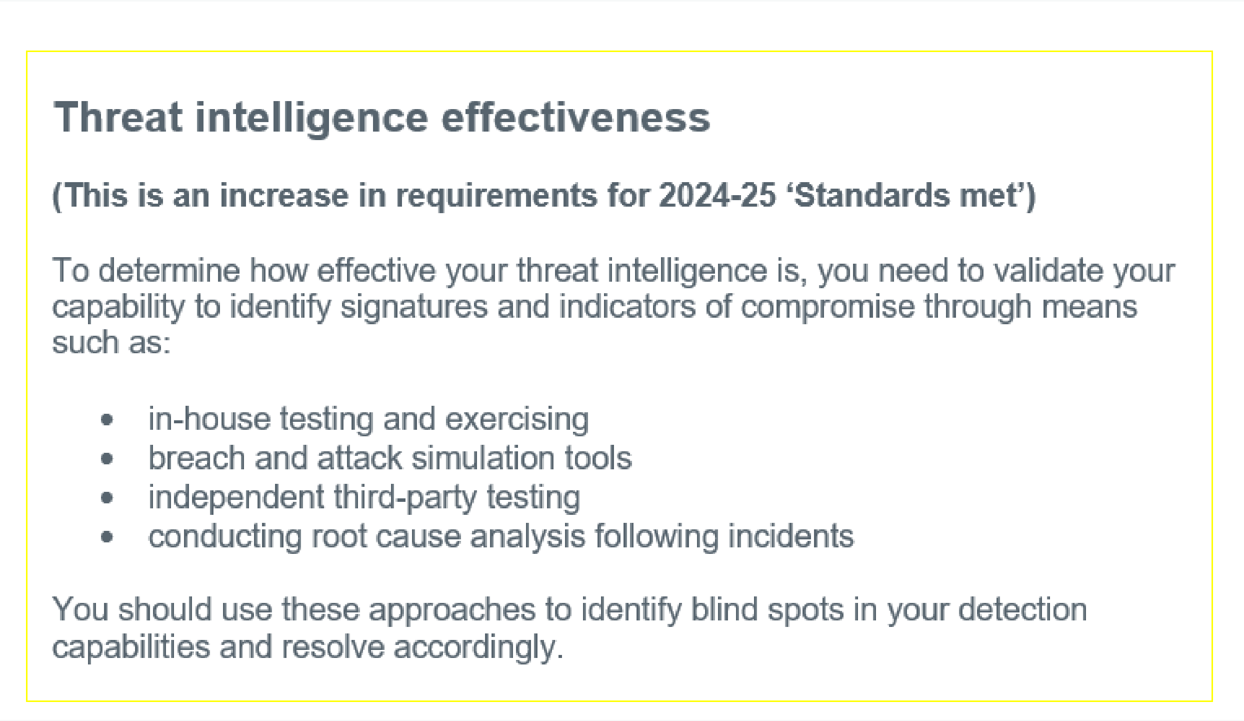
Contributing outcome:

C1.d Identifying security incidents

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 () weak ma
C1.d Identifying security incidents: You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.	2.1.1 6.2.1 6.2.3 6.3.2-4 7.1.4 8.3.6 8.3.8



Threat intelligence effectiveness

(This is an increase in requirements for 2024-25 ‘Standards met’)

To determine how effective your threat intelligence is, you need to validate your capability to identify signatures and indicators of compromise through means such as:

- in-house testing and exercising
- breach and attack simulation tools
- independent third-party testing
- conducting root cause analysis following incidents

You should use these approaches to identify blind spots in your detection capabilities and resolve accordingly.

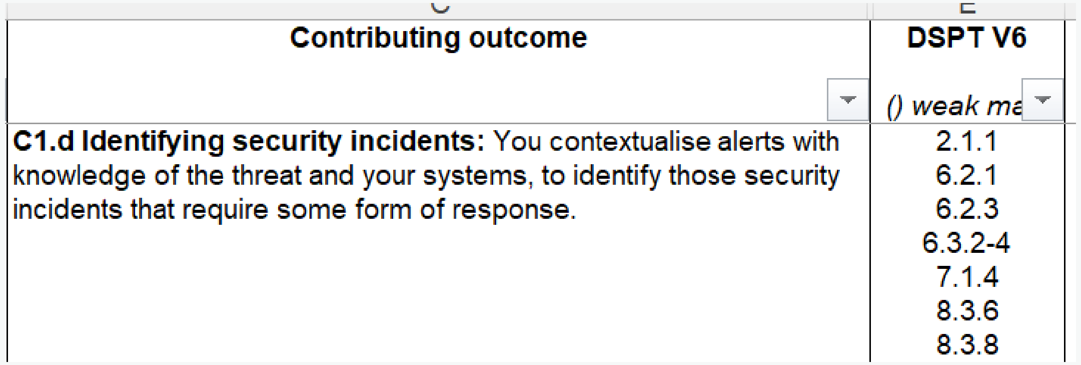
Principle:

C1 Security monitoring

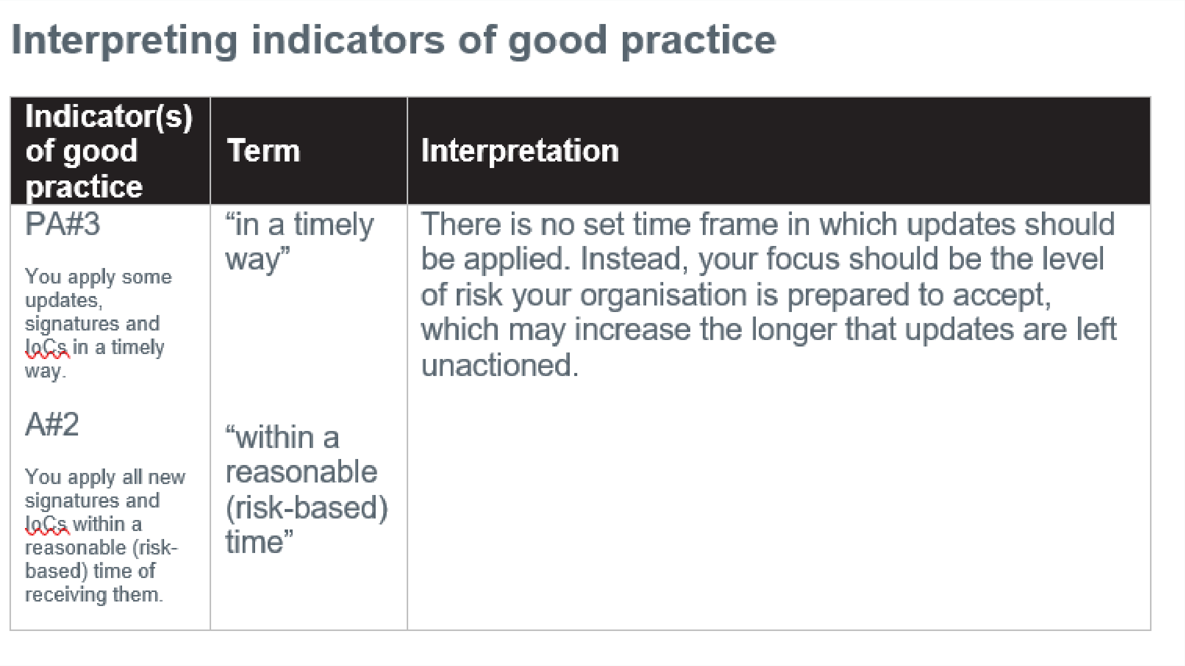
Contributing outcome:

C1.d Identifying security incidents

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 () weak ma
C1.d Identifying security incidents: You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.	2.1.1 6.2.1 6.2.3 6.3.2-4 7.1.4 8.3.6 8.3.8



Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#3 You apply some updates, signatures and IoCs in a timely way.	"in a timely way"	There is no set time frame in which updates should be applied. Instead, your focus should be the level of risk your organisation is prepared to accept, which may increase the longer that updates are left unactioned.
A#2 You apply all new signatures and IoCs within a reasonable (risk-based) time of receiving them.	"within a reasonable (risk-based) time"	

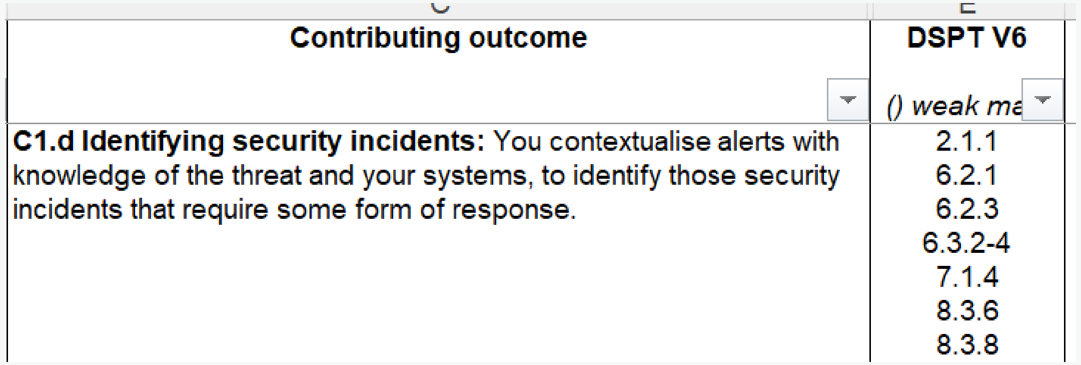
Principle:

C1 Security monitoring

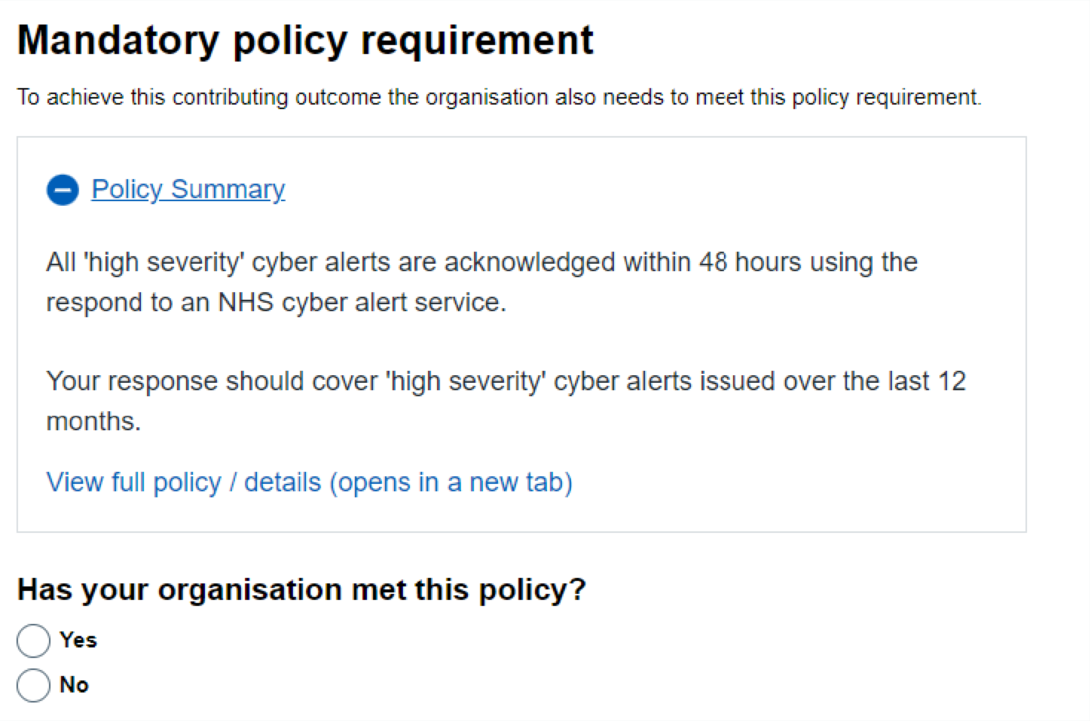
Contributing outcome:

C1.d Identifying security incidents

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 () weak ma
C1.d Identifying security incidents: You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.	2.1.1 6.2.1 6.2.3 6.3.2-4 7.1.4 8.3.6 8.3.8



Mandatory policy requirement

To achieve this contributing outcome the organisation also needs to meet this policy requirement.

All 'high severity' cyber alerts are acknowledged within 48 hours using the respond to an NHS cyber alert service.

Your response should cover 'high severity' cyber alerts issued over the last 12 months.

View full policy / details (opens in a new tab)

Has your organisation met this policy?

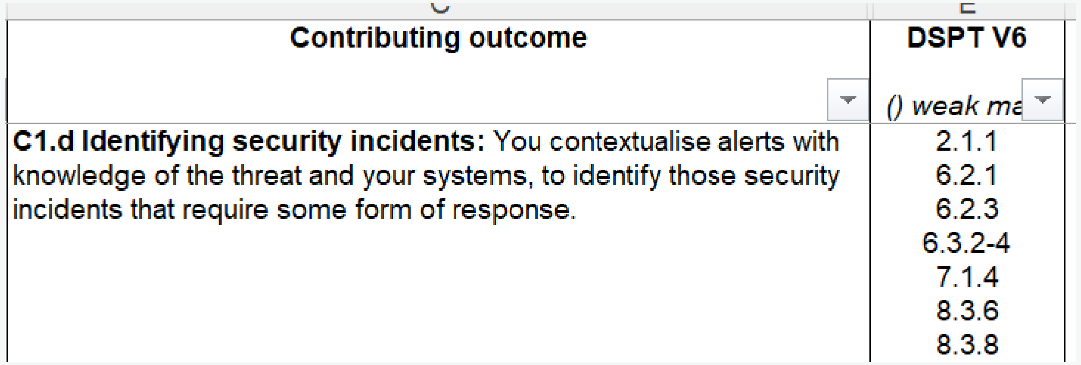
○ Yes

○ No

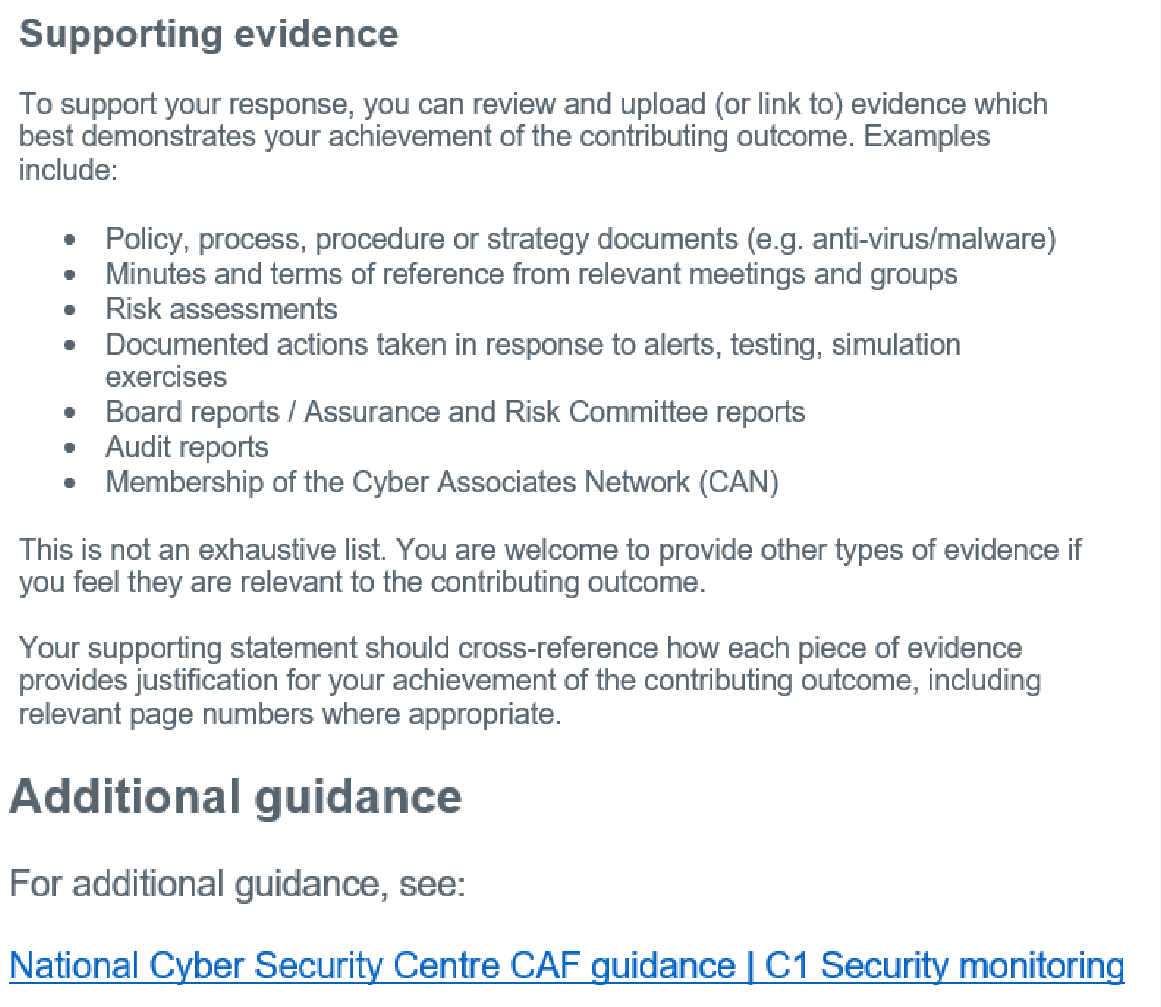
Principle:
C1 Security monitoring

Contributing outcome:
C1.d Identifying security incidents

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6
	() weak ma
C1.d Identifying security incidents: You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.	2.1.1 6.2.1 6.2.3 6.3.2-4 7.1.4 8.3.6 8.3.8



Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- Policy, process, procedure or strategy documents (e.g. anti-virus/malware)
- Minutes and terms of reference from relevant meetings and groups
- Risk assessments
- Documented actions taken in response to alerts, testing, simulation exercises
- Board reports / Assurance and Risk Committee reports
- Audit reports
- Membership of the Cyber Associates Network (CAN)

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

Additional guidance

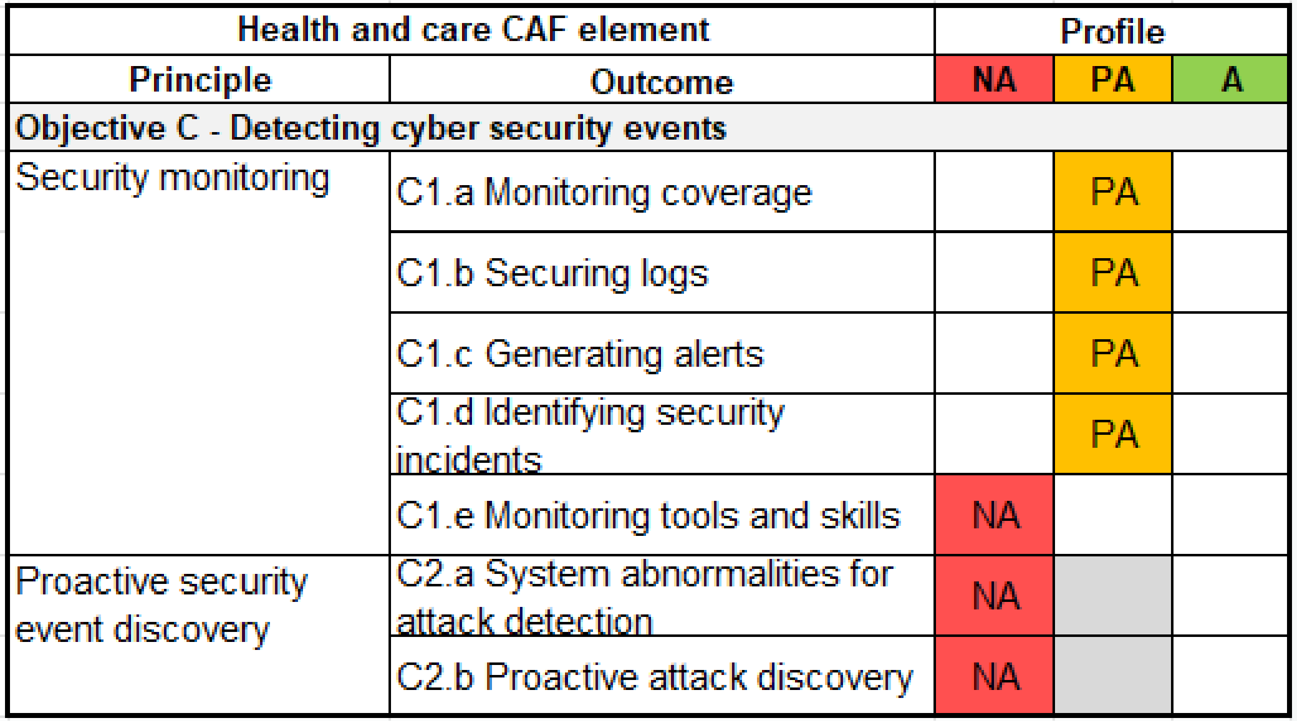
For additional guidance, see:

National Cyber Security Centre CAF guidance | C1 Security monitoring

Half time quiz
(‘not acheived’)

Expectations for Standards met:

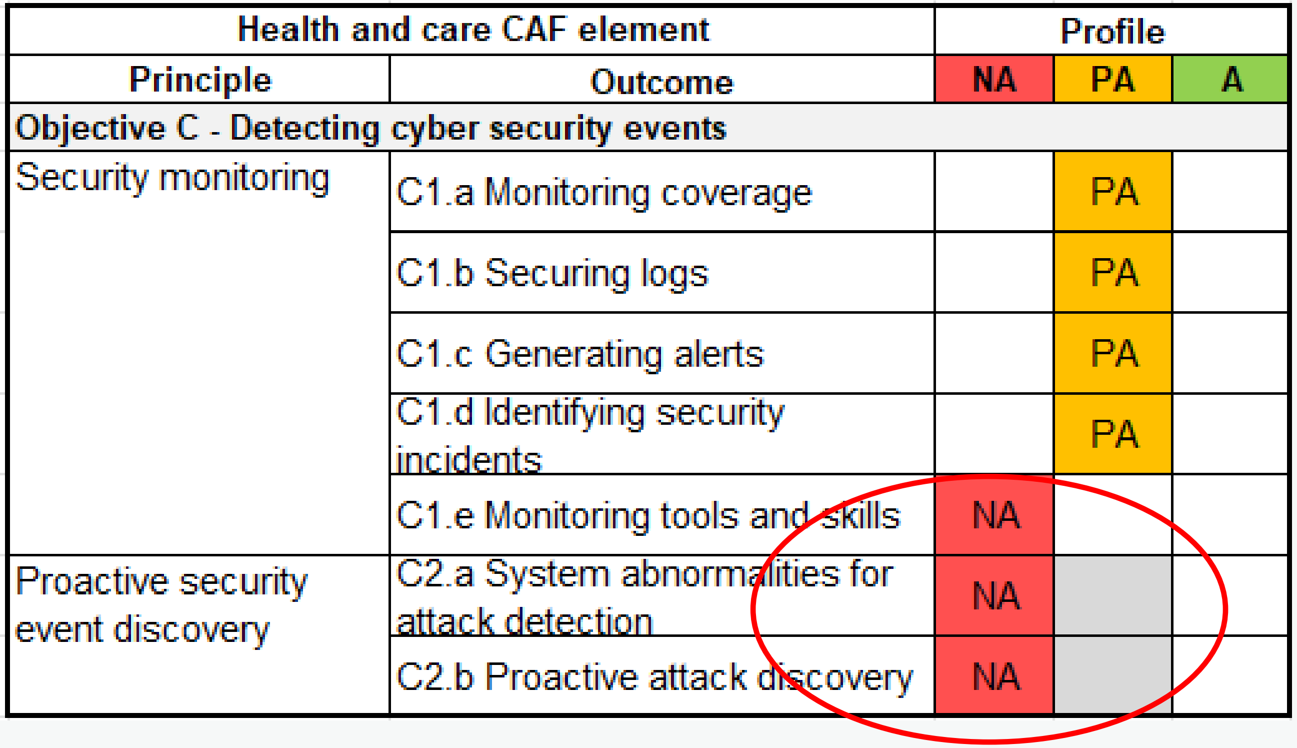
Objective C - Detecting cyber security events



Health and care CAF element		Profile		
Principle	Outcome	NA	PA	A
Objective C - Detecting cyber security events				
Security monitoring	C1.a Monitoring coverage		PA	
	C1.b Securing logs		PA	
	C1.c Generating alerts		PA	
	C1.d Identifying security incidents		PA	
	C1.e Monitoring tools and skills	NA		
Proactive security event discovery	C2.a System abnormalities for attack detection	NA		
	C2.b Proactive attack discovery	NA		

Expectations for Standards met:

Objective C - Detecting cyber security events



Health and care CAF element		Profile		
Principle	Outcome	NA	PA	A
Objective C - Detecting cyber security events				
Security monitoring	C1.a Monitoring coverage		PA	
	C1.b Securing logs		PA	
	C1.c Generating alerts		PA	
	C1.d Identifying security incidents		PA	
	C1.e Monitoring tools and skills	NA		
Proactive security event discovery	C2.a System abnormalities for attack detection	NA		
	C2.b Proactive attack discovery	NA		

Three outcomes the expected achievement level is Not achieved

Question 1: What should do for outcomes where the expectation is set at Not Achieved?

a) Ignore them

OR

b) provide a response, showing you have considered the implications of the contributing outcome for your organisation and documenting any of the work you are undertaking towards this outcome.

What should do for outcomes where the expectation is set at Not Achieved?

Correct Answer is:

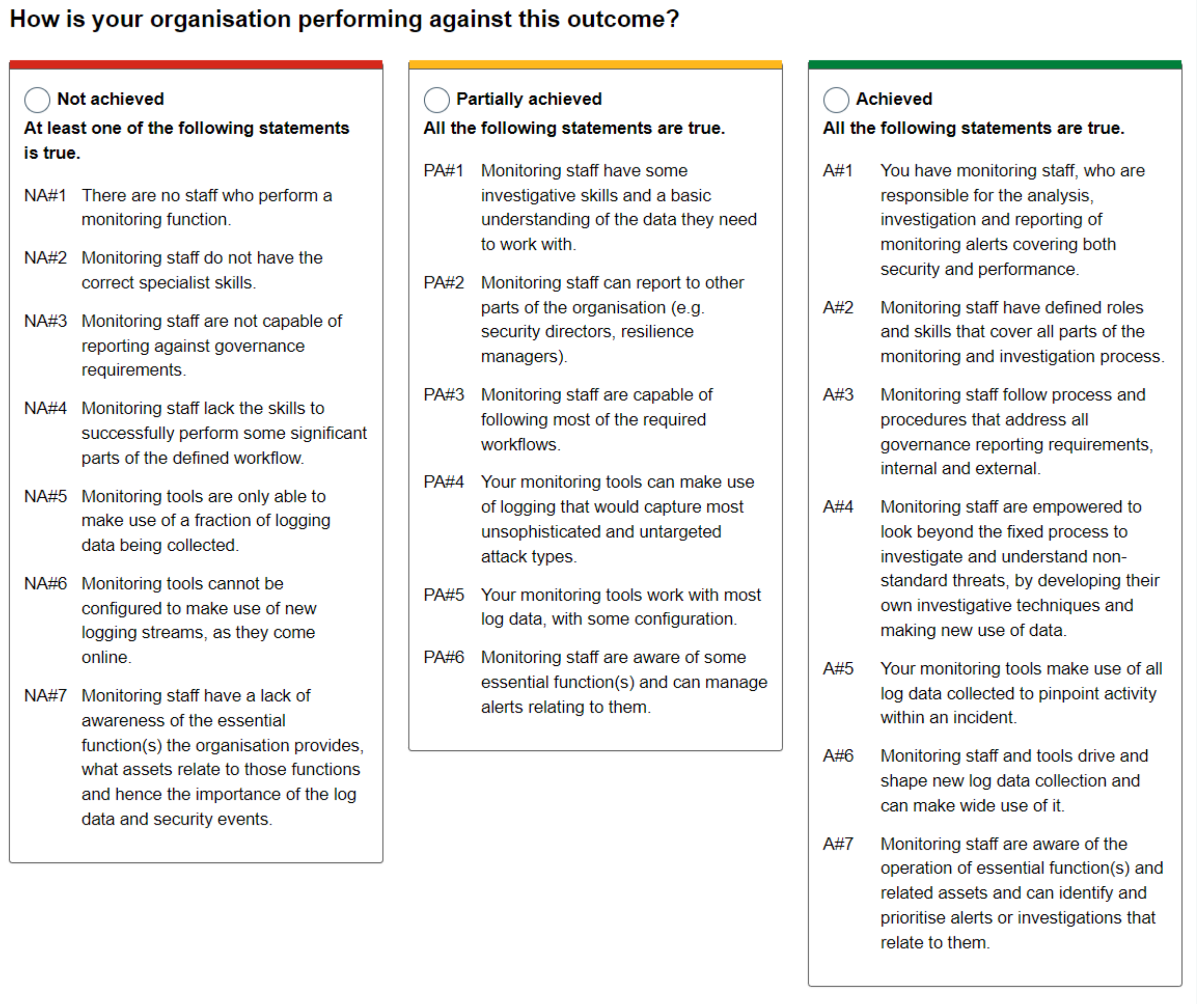
b) **provide a response, showing you have considered the implications of the contributing outcome for your organisation and documenting any of the work you are undertaking towards this outcome.**

The DSPT ‘Standards met’ expectation should be regarded as a minimum compliance level, not the end goal of your organisation’s cyber security and IG activities.

I have met some of the Partially Achieved Indicators of Good Practice, but the expectation is set at Not Achieved?

Expectation

The baseline expectation for this contributing outcome is ***Not achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 There are no staff who perform a monitoring function.

NA#2 Monitoring staff do not have the correct specialist skills.

NA#3 Monitoring staff are not capable of reporting against governance requirements.

NA#4 Monitoring staff lack the skills to successfully perform some significant parts of the defined workflow.

NA#5 Monitoring tools are only able to make use of a fraction of logging data being collected.

NA#6 Monitoring tools cannot be configured to make use of new logging streams, as they come online.

NA#7 Monitoring staff have a lack of awareness of the essential function(s) the organisation provides, what assets relate to those functions and hence the importance of the log data and security events.

○ **Partially achieved**

All the following statements are true.

PA#1 Monitoring staff have some investigative skills and a basic understanding of the data they need to work with.

PA#2 Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).

PA#3 Monitoring staff are capable of following most of the required workflows.

PA#4 Your monitoring tools can make use of logging that would capture most unsophisticated and untargeted attack types.

PA#5 Your monitoring tools work with most log data, with some configuration.

PA#6 Monitoring staff are aware of some essential function(s) and can manage alerts relating to them.

○ **Achieved**

All the following statements are true.

A#1 You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance.

A#2 Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process.

A#3 Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external.

A#4 Monitoring staff are empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.

A#5 Your monitoring tools make use of all log data collected to pinpoint activity within an incident.

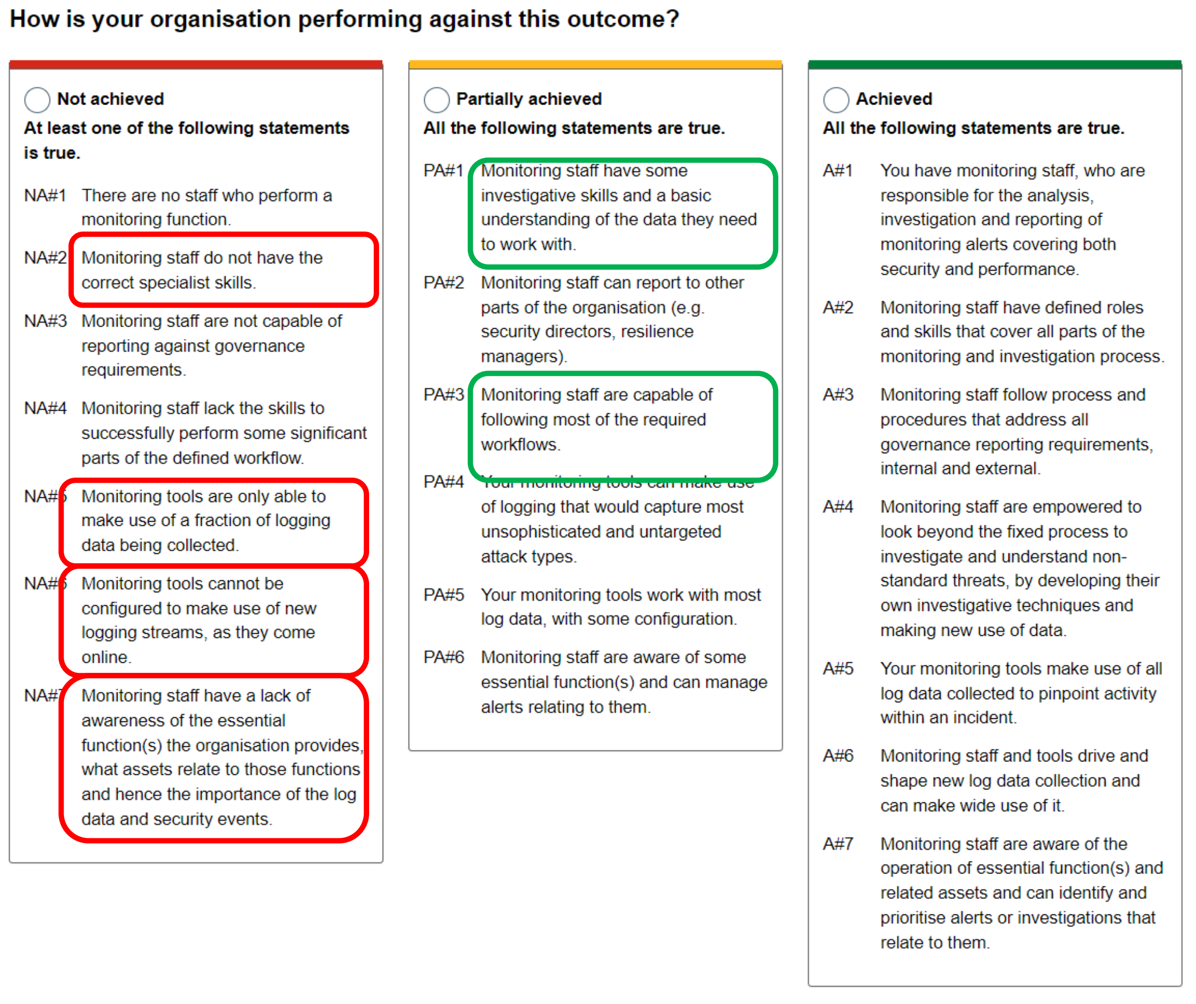
A#6 Monitoring staff and tools drive and shape new log data collection and can make wide use of it.

A#7 Monitoring staff are aware of the operation of essential function(s) and related assets and can identify and prioritise alerts or investigations that relate to them.

What Achievement level should I select?

Expectation

The baseline expectation for this contributing outcome is ***Not achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 There are no staff who perform a monitoring function.

NA#2 Monitoring staff do not have the correct specialist skills.

NA#3 Monitoring staff are not capable of reporting against governance requirements.

NA#4 Monitoring staff lack the skills to successfully perform some significant parts of the defined workflow.

NA#5 Monitoring tools are only able to make use of a fraction of logging data being collected.

NA#6 Monitoring tools cannot be configured to make use of new logging streams, as they come online.

NA#7 Monitoring staff have a lack of awareness of the essential function(s) the organisation provides, what assets relate to those functions and hence the importance of the log data and security events.

○ **Partially achieved**

All the following statements are true.

PA#1 Monitoring staff have some investigative skills and a basic understanding of the data they need to work with.

PA#2 Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).

PA#3 Monitoring staff are capable of following most of the required workflows.

PA#4 Your monitoring tools can make use of logging that would capture most unsophisticated and untargeted attack types.

PA#5 Your monitoring tools work with most log data, with some configuration.

PA#6 Monitoring staff are aware of some essential function(s) and can manage alerts relating to them.

○ **Achieved**

All the following statements are true.

A#1 You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance.

A#2 Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process.

A#3 Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external.

A#4 Monitoring staff are empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.

A#5 Your monitoring tools make use of all log data collected to pinpoint activity within an incident.

A#6 Monitoring staff and tools drive and shape new log data collection and can make wide use of it.

A#7 Monitoring staff are aware of the operation of essential function(s) and related assets and can identify and prioritise alerts or investigations that relate to them.

What Achievement level should I select?

Expectation

The baseline expectation for this contributing outcome is ***Not achieved***

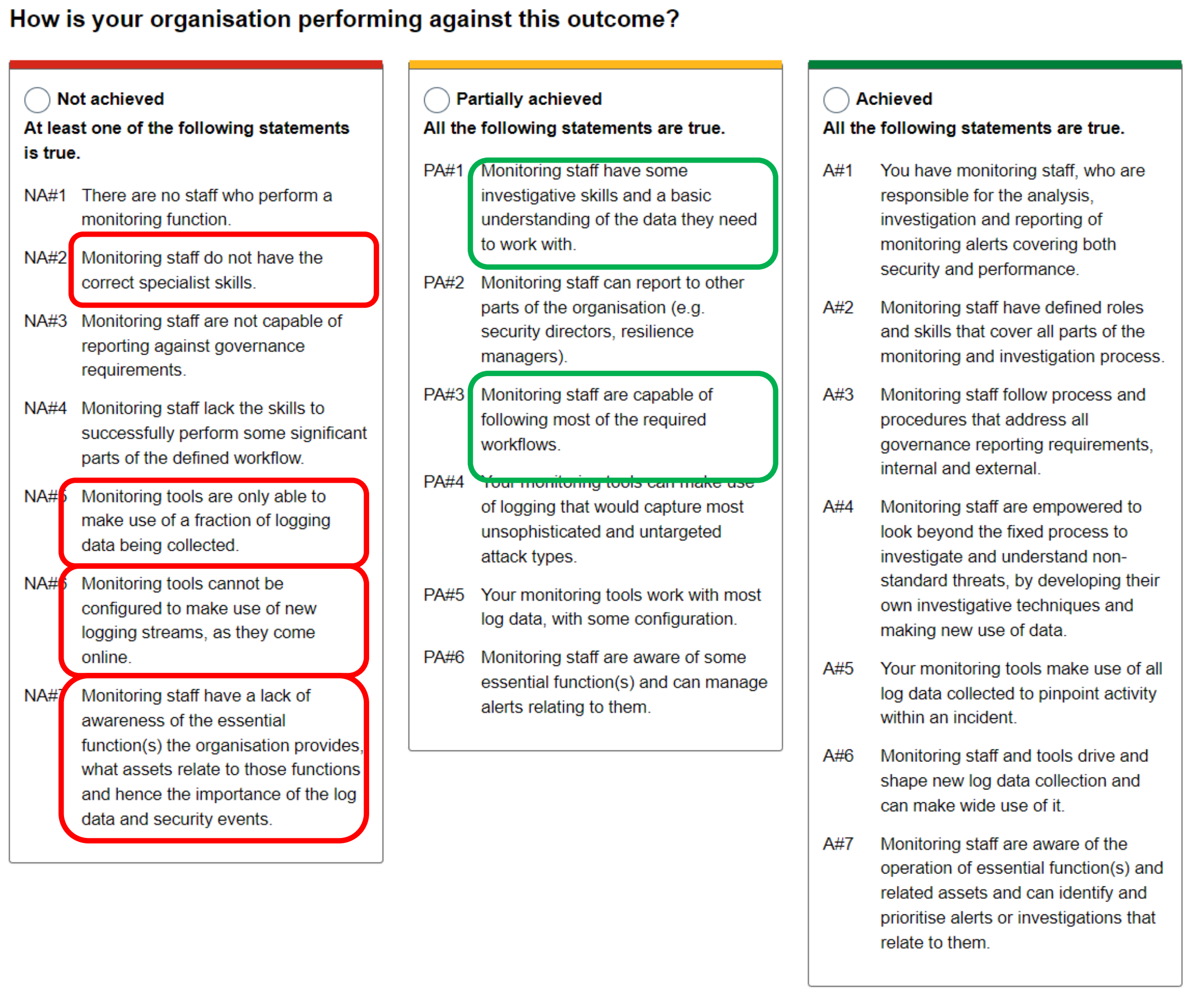
Answer

If any of the Indicators listed under Not achieved are true, you should mark yourselves **Not achieved**.

Rationale

The indicators listed under ‘Not achieved’ list statements which are incompatible with achieving or partially achieving the outcome.

Security chain is only as strong as the weakest link. The best security capabilities in the world aren’t much use if there’s a great big hole in the middle.



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 There are no staff who perform a monitoring function.

NA#2 Monitoring staff do not have the correct specialist skills.

NA#3 Monitoring staff are not capable of reporting against governance requirements.

NA#4 Monitoring staff lack the skills to successfully perform some significant parts of the defined workflow.

NA#5 Monitoring tools are only able to make use of a fraction of logging data being collected.

NA#6 Monitoring tools cannot be configured to make use of new logging streams, as they come online.

NA#7 Monitoring staff have a lack of awareness of the essential function(s) the organisation provides, what assets relate to those functions and hence the importance of the log data and security events.

○ **Partially achieved**

All the following statements are true.

PA#1 Monitoring staff have some investigative skills and a basic understanding of the data they need to work with.

PA#2 Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).

PA#3 Monitoring staff are capable of following most of the required workflows.

PA#4 Your monitoring tools can make use of logging that would capture most unsophisticated and untargeted attack types.

PA#5 Your monitoring tools work with most log data, with some configuration.

PA#6 Monitoring staff are aware of some essential function(s) and can manage alerts relating to them.

○ **Achieved**

All the following statements are true.

A#1 You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance.

A#2 Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process.

A#3 Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external.

A#4 Monitoring staff are empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.

A#5 Your monitoring tools make use of all log data collected to pinpoint activity within an incident.

A#6 Monitoring staff and tools drive and shape new log data collection and can make wide use of it.

A#7 Monitoring staff are aware of the operation of essential function(s) and related assets and can identify and prioritise alerts or investigations that relate to them.

Principle:

C1 Security monitoring

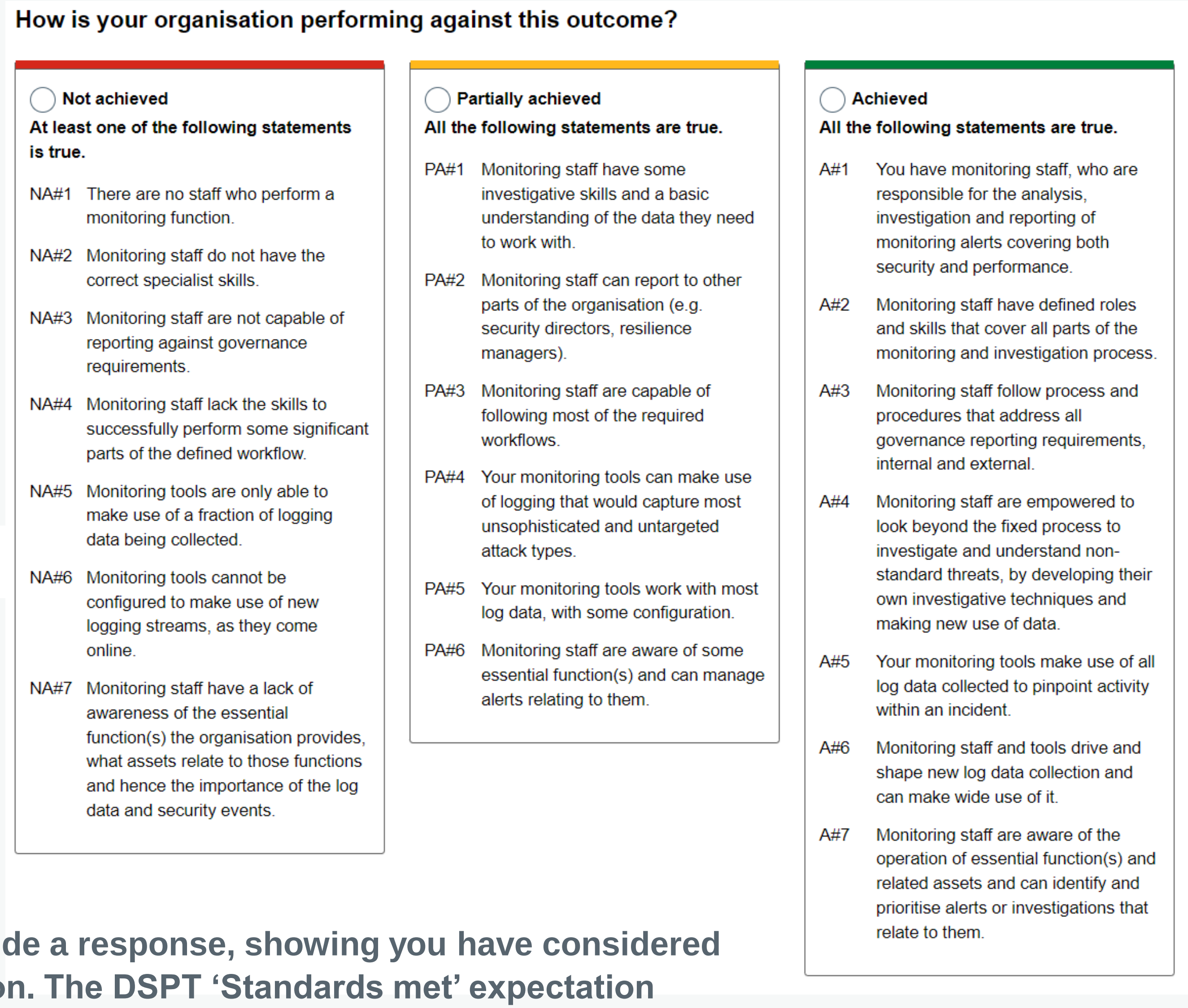
Contributing outcome:

C1.e Monitoring tools and skills

You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response

Expectation

The baseline expectation for this contributing outcome is ***Not achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 There are no staff who perform a monitoring function.

NA#2 Monitoring staff do not have the correct specialist skills.

NA#3 Monitoring staff are not capable of reporting against governance requirements.

NA#4 Monitoring staff lack the skills to successfully perform some significant parts of the defined workflow.

NA#5 Monitoring tools are only able to make use of a fraction of logging data being collected.

NA#6 Monitoring tools cannot be configured to make use of new logging streams, as they come online.

NA#7 Monitoring staff have a lack of awareness of the essential function(s) the organisation provides, what assets relate to those functions and hence the importance of the log data and security events.

○ **Partially achieved**

All the following statements are true.

PA#1 Monitoring staff have some investigative skills and a basic understanding of the data they need to work with.

PA#2 Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).

PA#3 Monitoring staff are capable of following most of the required workflows.

PA#4 Your monitoring tools can make use of logging that would capture most unsophisticated and untargeted attack types.

PA#5 Your monitoring tools work with most log data, with some configuration.

PA#6 Monitoring staff are aware of some essential function(s) and can manage alerts relating to them.

○ **Achieved**

All the following statements are true.

A#1 You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance.

A#2 Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process.

A#3 Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external.

A#4 Monitoring staff are empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.

A#5 Your monitoring tools make use of all log data collected to pinpoint activity within an incident.

A#6 Monitoring staff and tools drive and shape new log data collection and can make wide use of it.

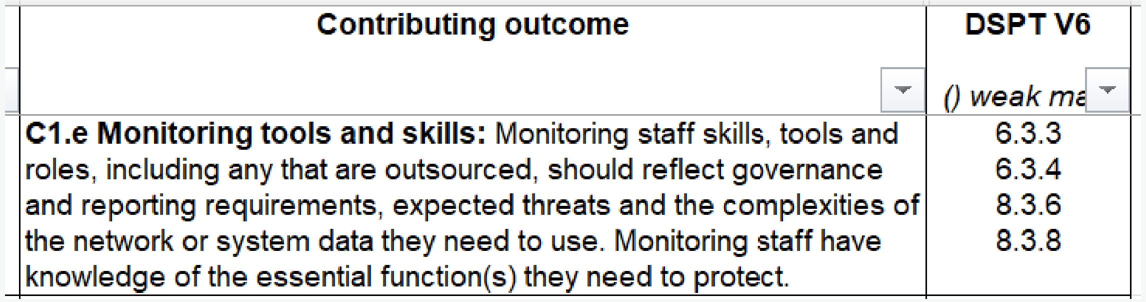
A#7 Monitoring staff are aware of the operation of essential function(s) and related assets and can identify and prioritise alerts or investigations that relate to them.

You are still required to assess your achievement level and provide a response, showing you have considered the implications of the contributing outcome for your organisation. The DSPT ‘Standards met’ expectation should be regarded as a minimum compliance level, not the end goal of your organisation’s cyber security and IG activities.

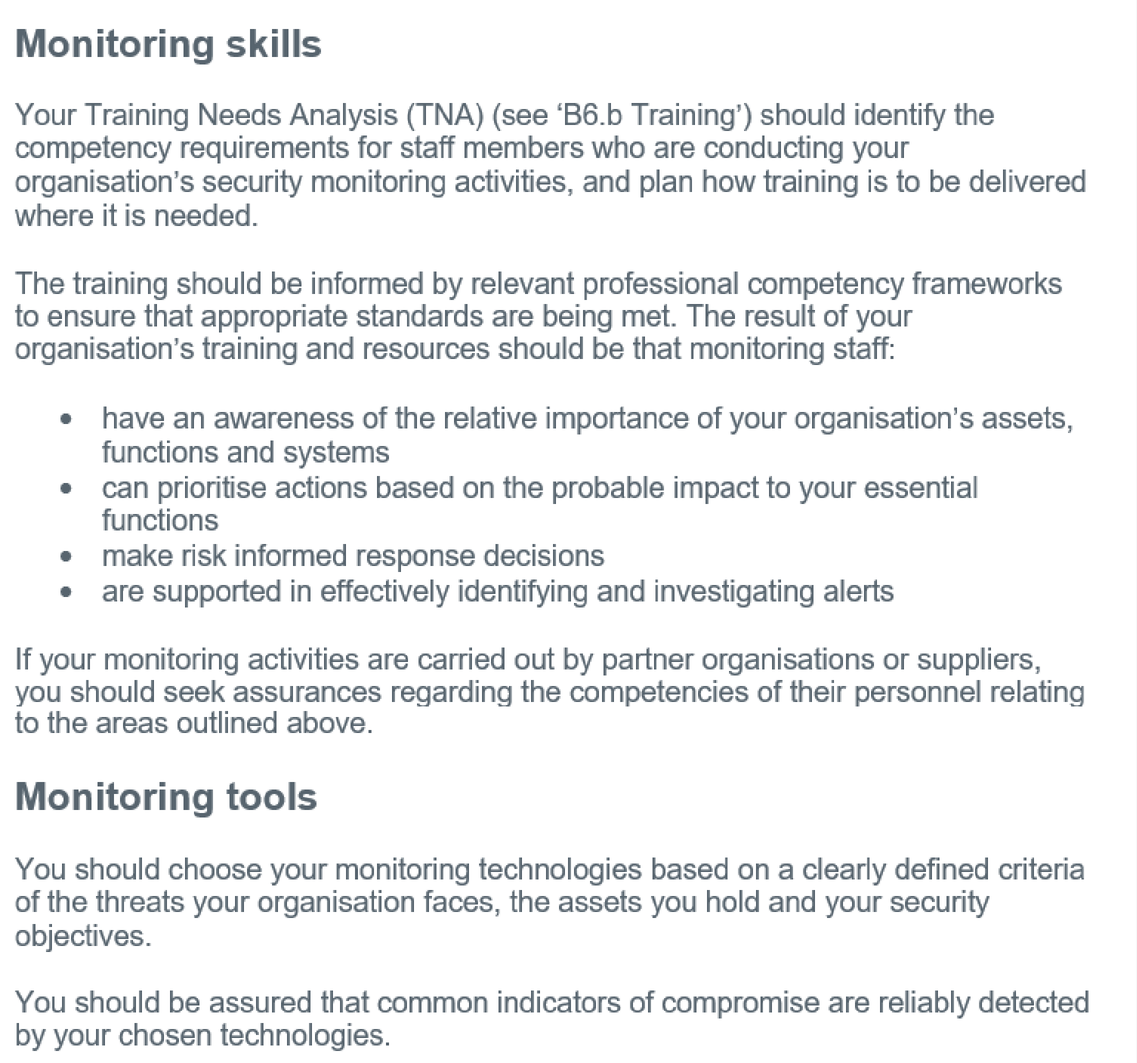
Principle:
C1 Security monitoring

Contributing outcome:
C1.e Monitoring tools and skills

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 *() weak ma*
C1.e Monitoring tools and skills: Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential function(s) they need to protect.	6.3.3 6.3.4 8.3.6 8.3.8



Monitoring skills

Your Training Needs Analysis (TNA) (see ‘B6.b Training’) should identify the competency requirements for staff members who are conducting your organisation’s security monitoring activities, and plan how training is to be delivered where it is needed.

The training should be informed by relevant professional competency frameworks to ensure that appropriate standards are being met. The result of your organisation’s training and resources should be that monitoring staff:

- have an awareness of the relative importance of your organisation’s assets, functions and systems
- can prioritise actions based on the probable impact to your essential functions
- make risk informed response decisions
- are supported in effectively identifying and investigating alerts

If your monitoring activities are carried out by partner organisations or suppliers, you should seek assurances regarding the competencies of their personnel relating to the areas outlined above.

Monitoring tools

You should choose your monitoring technologies based on a clearly defined criteria of the threats your organisation faces, the assets you hold and your security objectives.

You should be assured that common indicators of compromise are reliably detected by your chosen technologies.

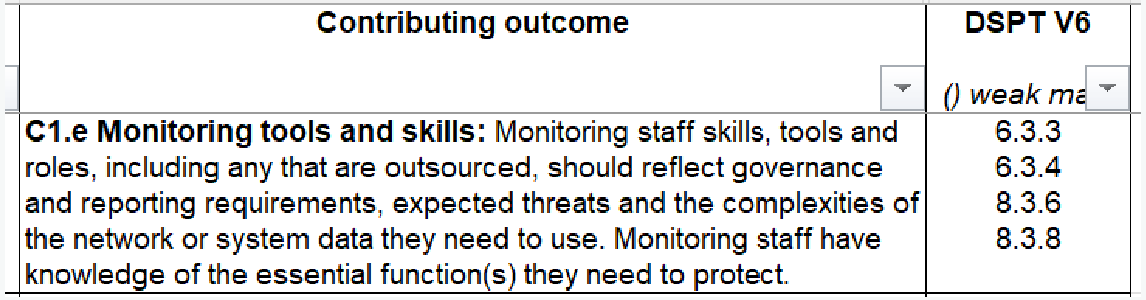
Principle:

C1 Security monitoring

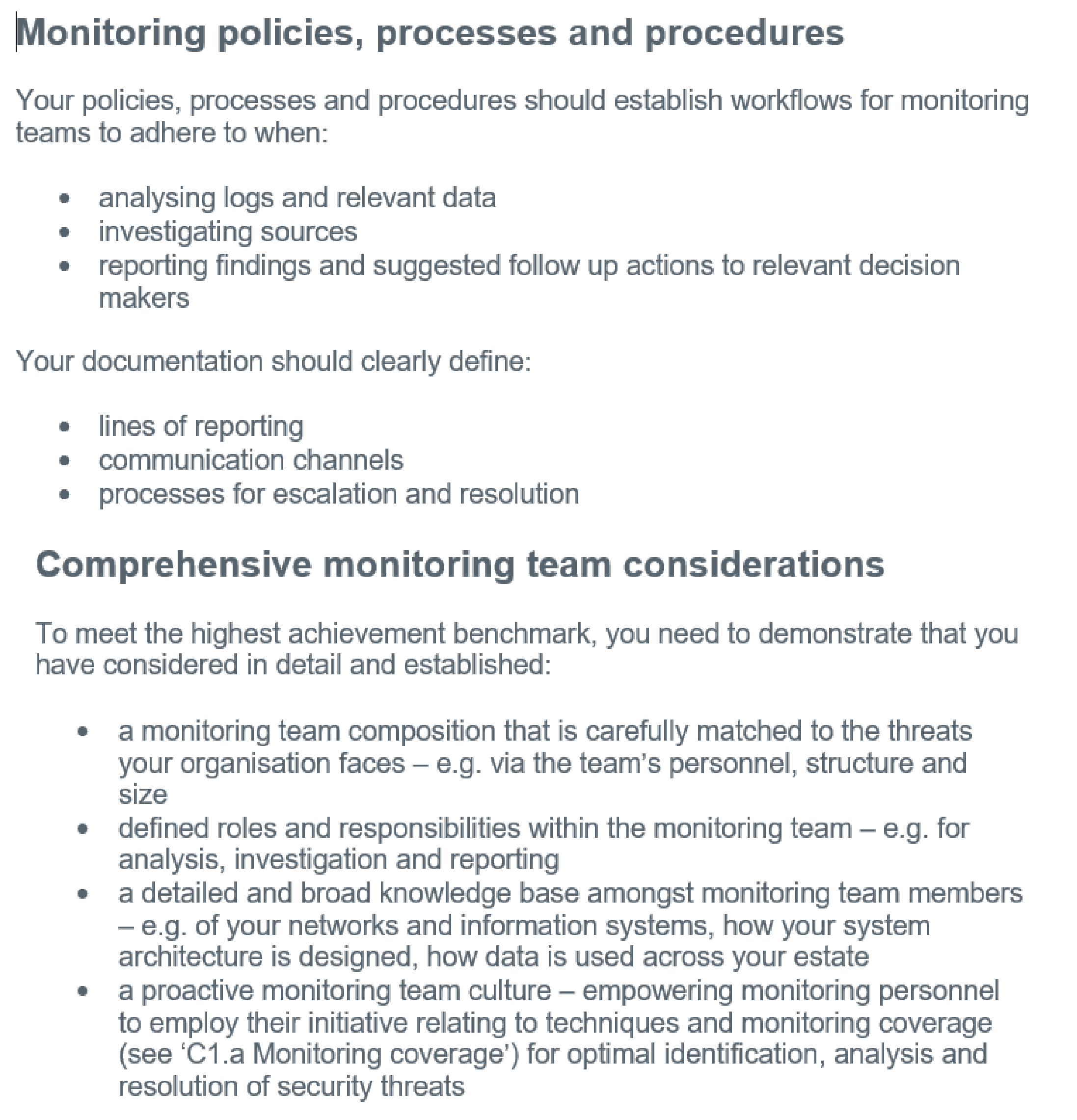
Contributing outcome:

C1.e Monitoring tools and skills

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 *() weak ma*
C1.e Monitoring tools and skills: Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential function(s) they need to protect.	6.3.3 6.3.4 8.3.6 8.3.8



Monitoring policies, processes and procedures

Your policies, processes and procedures should establish workflows for monitoring teams to adhere to when:

- analysing logs and relevant data
- investigating sources
- reporting findings and suggested follow up actions to relevant decision makers

Your documentation should clearly define:

- lines of reporting
- communication channels
- processes for escalation and resolution

Comprehensive monitoring team considerations

To meet the highest achievement benchmark, you need to demonstrate that you have considered in detail and established:

- a monitoring team composition that is carefully matched to the threats your organisation faces – e.g. via the team's personnel, structure and size
- defined roles and responsibilities within the monitoring team – e.g. for analysis, investigation and reporting
- a detailed and broad knowledge base amongst monitoring team members – e.g. of your networks and information systems, how your system architecture is designed, how data is used across your estate
- a proactive monitoring team culture – empowering monitoring personnel to employ their initiative relating to techniques and monitoring coverage (see 'C1.a Monitoring coverage') for optimal identification, analysis and resolution of security threats

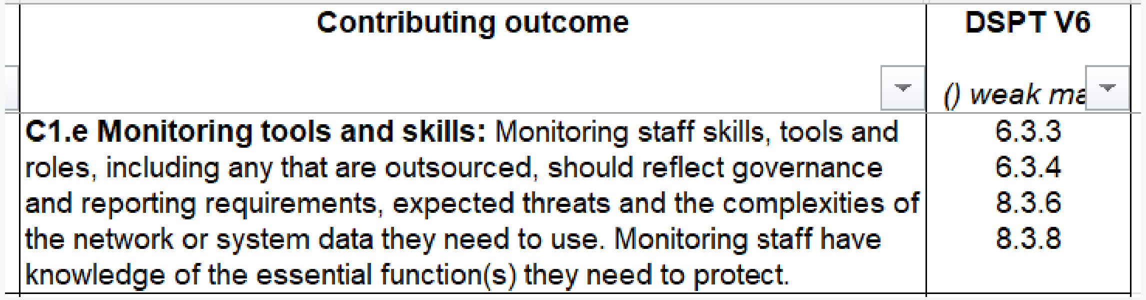
Principle:

C1 Security monitoring

Contributing outcome:

C1.e Monitoring tools and skills

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 *() weak ma*
C1.e Monitoring tools and skills: Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential function(s) they need to protect.	6.3.3 6.3.4 8.3.6 8.3.8

Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- Policy, process, procedure or strategy documents (e.g. security logs, events management)
- Training Needs Analysis (TNA)
- Training records
- Job specifications for specialised roles
- Supplier assurance documentation

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | C1 Security monitoring

Principle:

C2 Proactive security event discovery

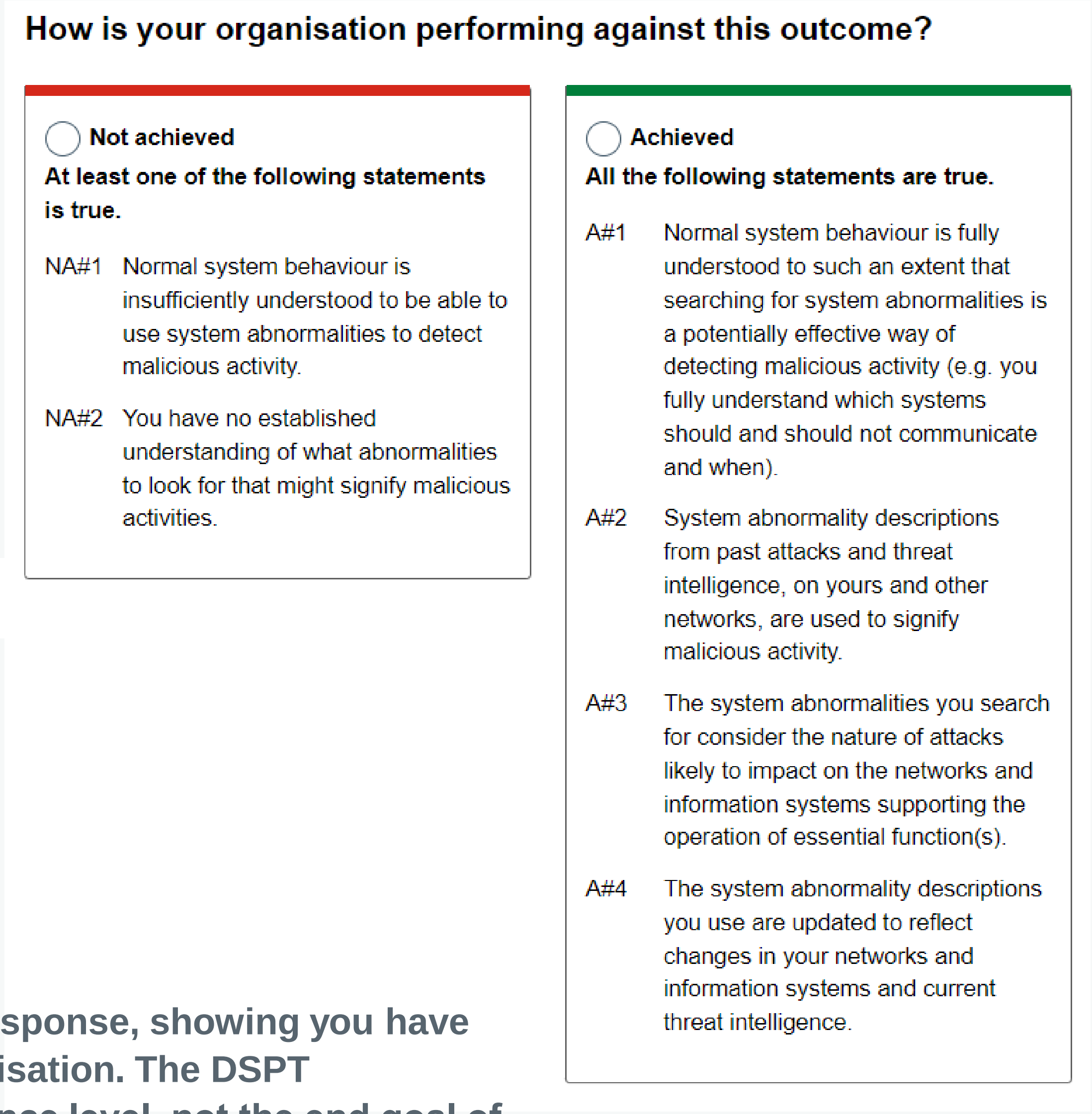
Contributing outcome:

C2.a System abnormalities for attack detection

You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify

Expectation

The baseline expectation for this contributing outcome is ***Not achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 Normal system behaviour is insufficiently understood to be able to use system abnormalities to detect malicious activity.

NA#2 You have no established understanding of what abnormalities to look for that might signify malicious activities.

○ **Achieved**

All the following statements are true.

A#1 Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity (e.g. you fully understand which systems should and should not communicate and when).

A#2 System abnormality descriptions from past attacks and threat intelligence, on yours and other networks, are used to signify malicious activity.

A#3 The system abnormalities you search for consider the nature of attacks likely to impact on the networks and information systems supporting the operation of essential function(s).

A#4 The system abnormality descriptions you use are updated to reflect changes in your networks and information systems and current threat intelligence.

You are still required to assess your achievement level and provide a response, showing you have considered the implications of the contributing outcome for your organisation. The DSPT 'Standards met' expectation should be regarded as a minimum compliance level, not the end goal of your organisation's cyber security and IG activities.

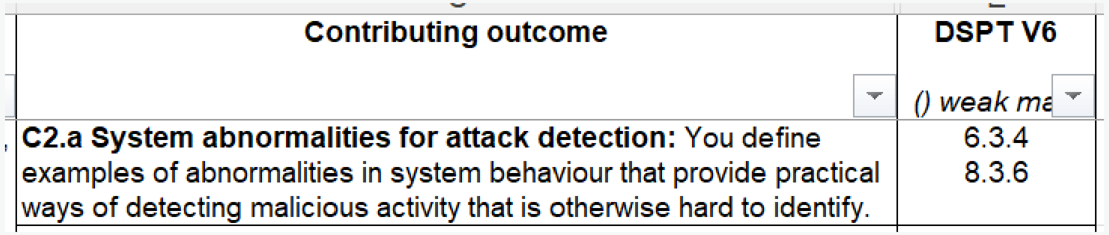
Principle:

C2 Proactive security event discovery

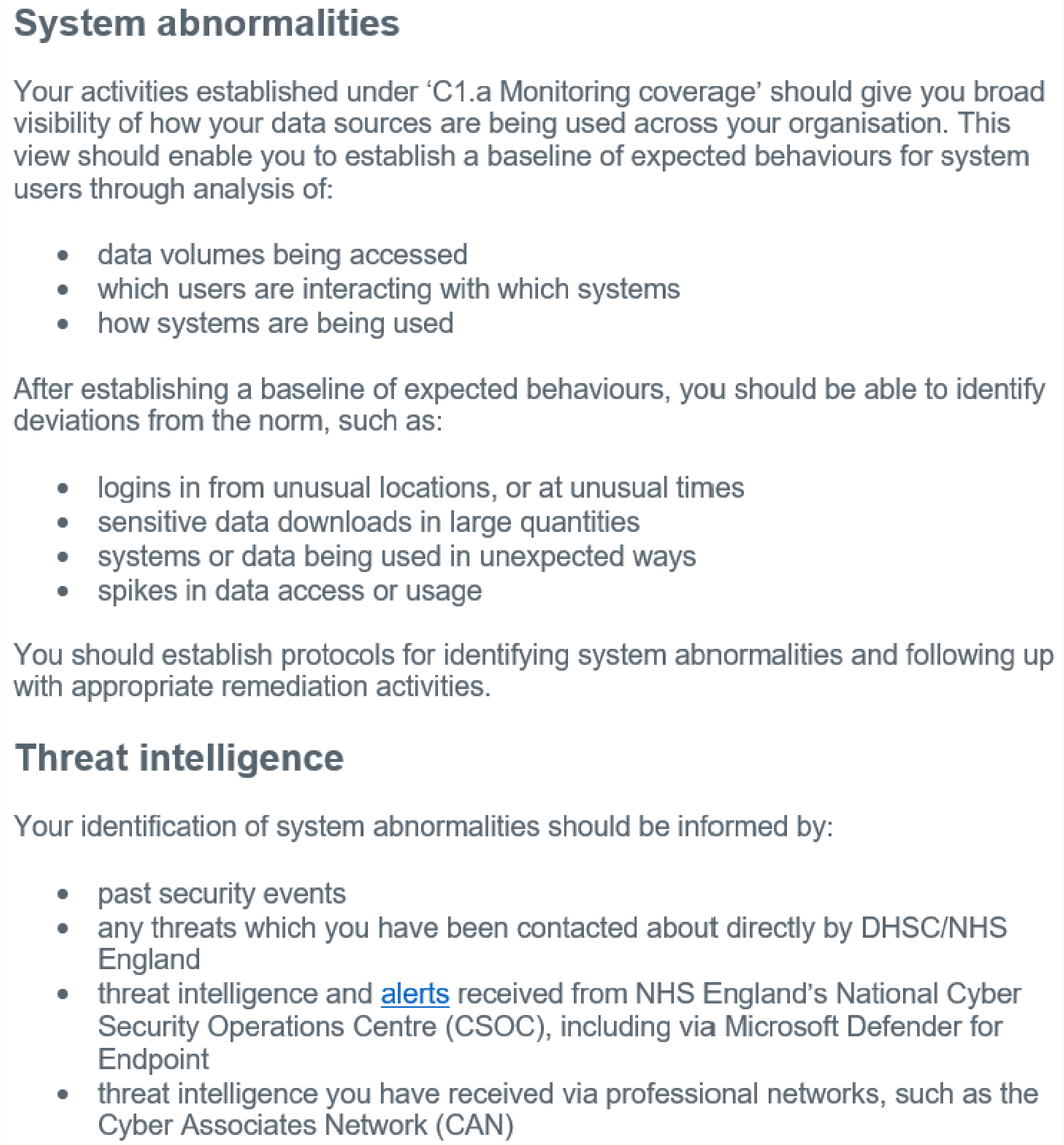
Contributing outcome:

C2.a System abnormalities for attack detection

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 () weak ma
C2.a System abnormalities for attack detection: You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.	6.3.4 8.3.6



System abnormalities

Your activities established under ‘C1.a Monitoring coverage’ should give you broad visibility of how your data sources are being used across your organisation. This view should enable you to establish a baseline of expected behaviours for system users through analysis of:

- data volumes being accessed
- which users are interacting with which systems
- how systems are being used

After establishing a baseline of expected behaviours, you should be able to identify deviations from the norm, such as:

- logins in from unusual locations, or at unusual times
- sensitive data downloads in large quantities
- systems or data being used in unexpected ways
- spikes in data access or usage

You should establish protocols for identifying system abnormalities and following up with appropriate remediation activities.

Threat intelligence

Your identification of system abnormalities should be informed by:

- past security events
- any threats which you have been contacted about directly by DHSC/NHS England
- threat intelligence and alerts received from NHS England’s National Cyber Security Operations Centre (CSOC), including via Microsoft Defender for Endpoint
- threat intelligence you have received via professional networks, such as the Cyber Associates Network (CAN)

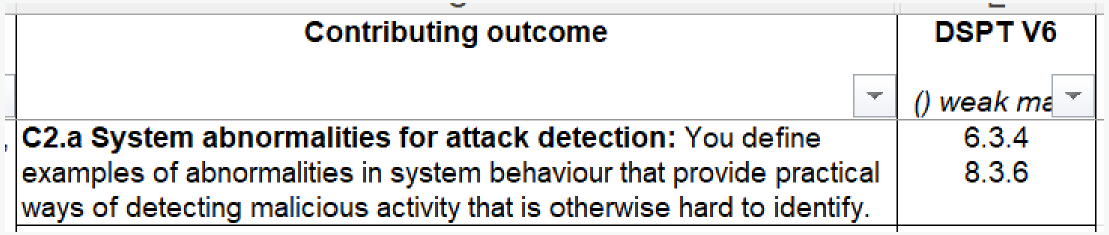
Principle:

C2 Proactive security event discovery

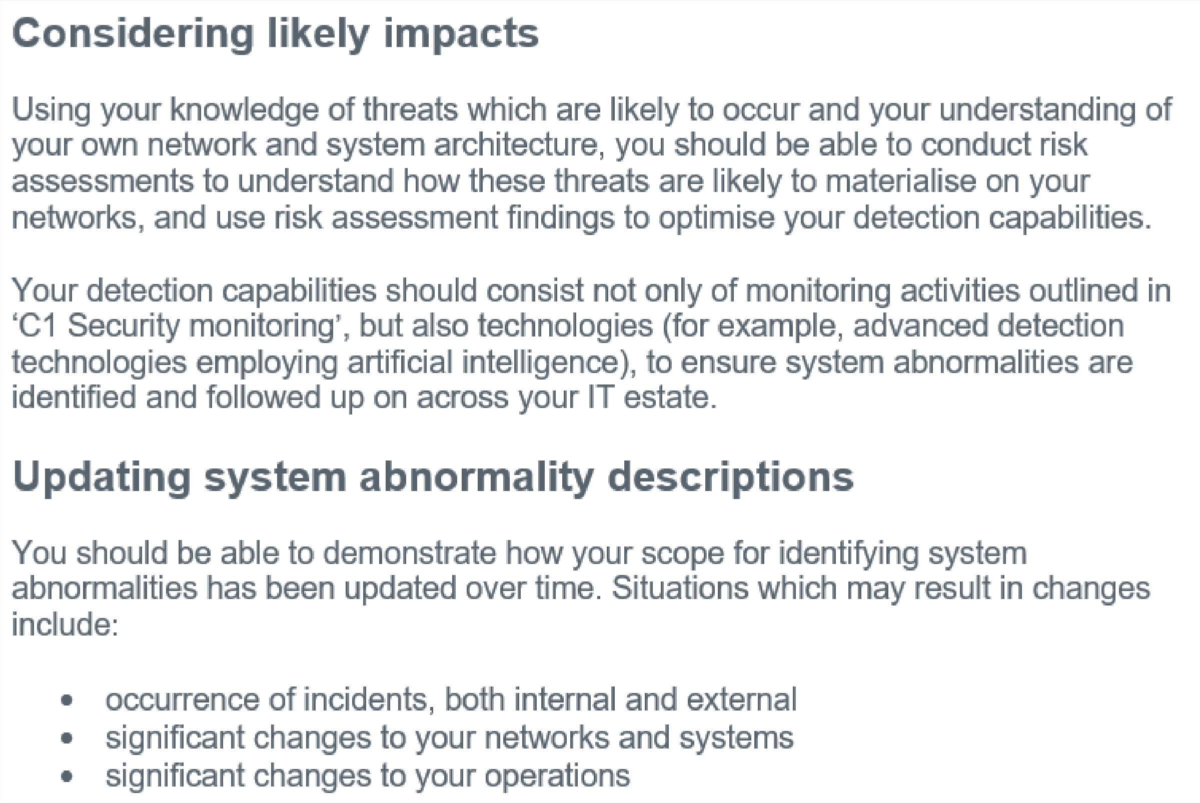
Contributing outcome:

C2.a System abnormalities for attack detection

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 *() weak ma*
C2.a System abnormalities for attack detection: You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.	6.3.4 8.3.6



Considering likely impacts

Using your knowledge of threats which are likely to occur and your understanding of your own network and system architecture, you should be able to conduct risk assessments to understand how these threats are likely to materialise on your networks, and use risk assessment findings to optimise your detection capabilities.

Your detection capabilities should consist not only of monitoring activities outlined in 'C1 Security monitoring', but also technologies (for example, advanced detection technologies employing artificial intelligence), to ensure system abnormalities are identified and followed up on across your IT estate.

Updating system abnormality descriptions

You should be able to demonstrate how your scope for identifying system abnormalities has been updated over time. Situations which may result in changes include:

- occurrence of incidents, both internal and external
- significant changes to your networks and systems
- significant changes to your operations

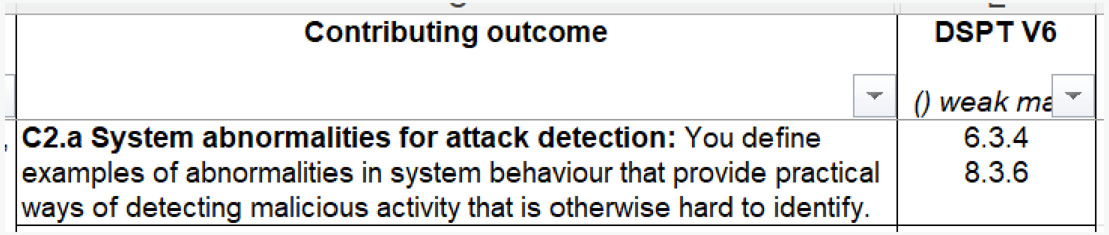
Principle:

C2 Proactive security event discovery

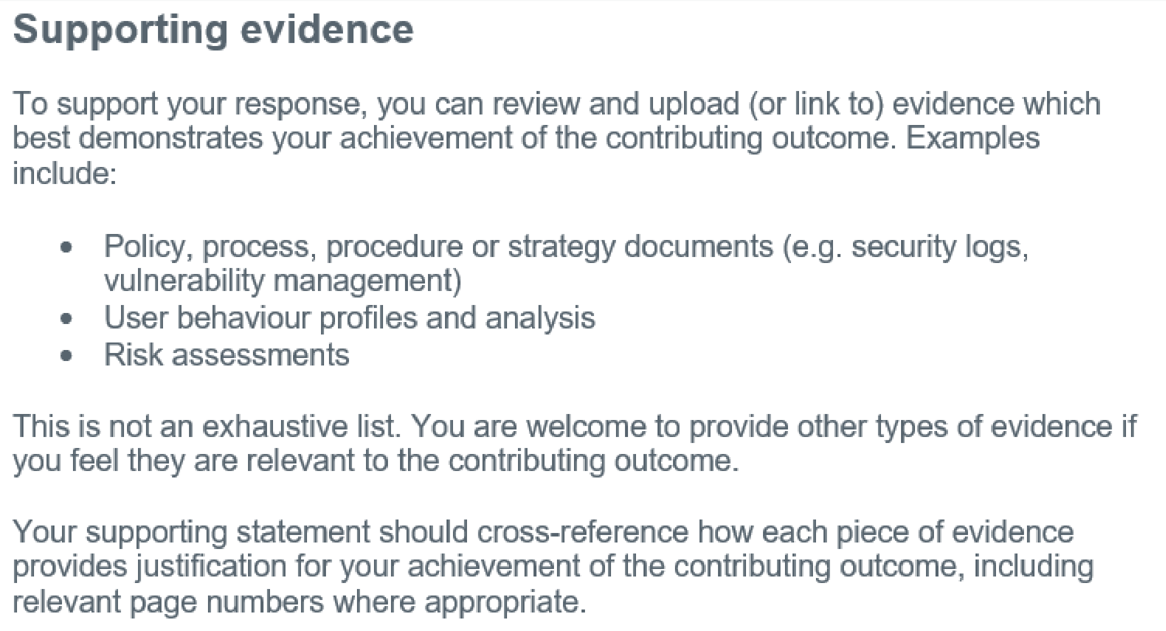
Contributing outcome:

C2.a System abnormalities for attack detection

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 () weak ma
C2.a System abnormalities for attack detection: You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.	6.3.4 8.3.6



Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- Policy, process, procedure or strategy documents (e.g. security logs, vulnerability management)
- User behaviour profiles and analysis
- Risk assessments

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

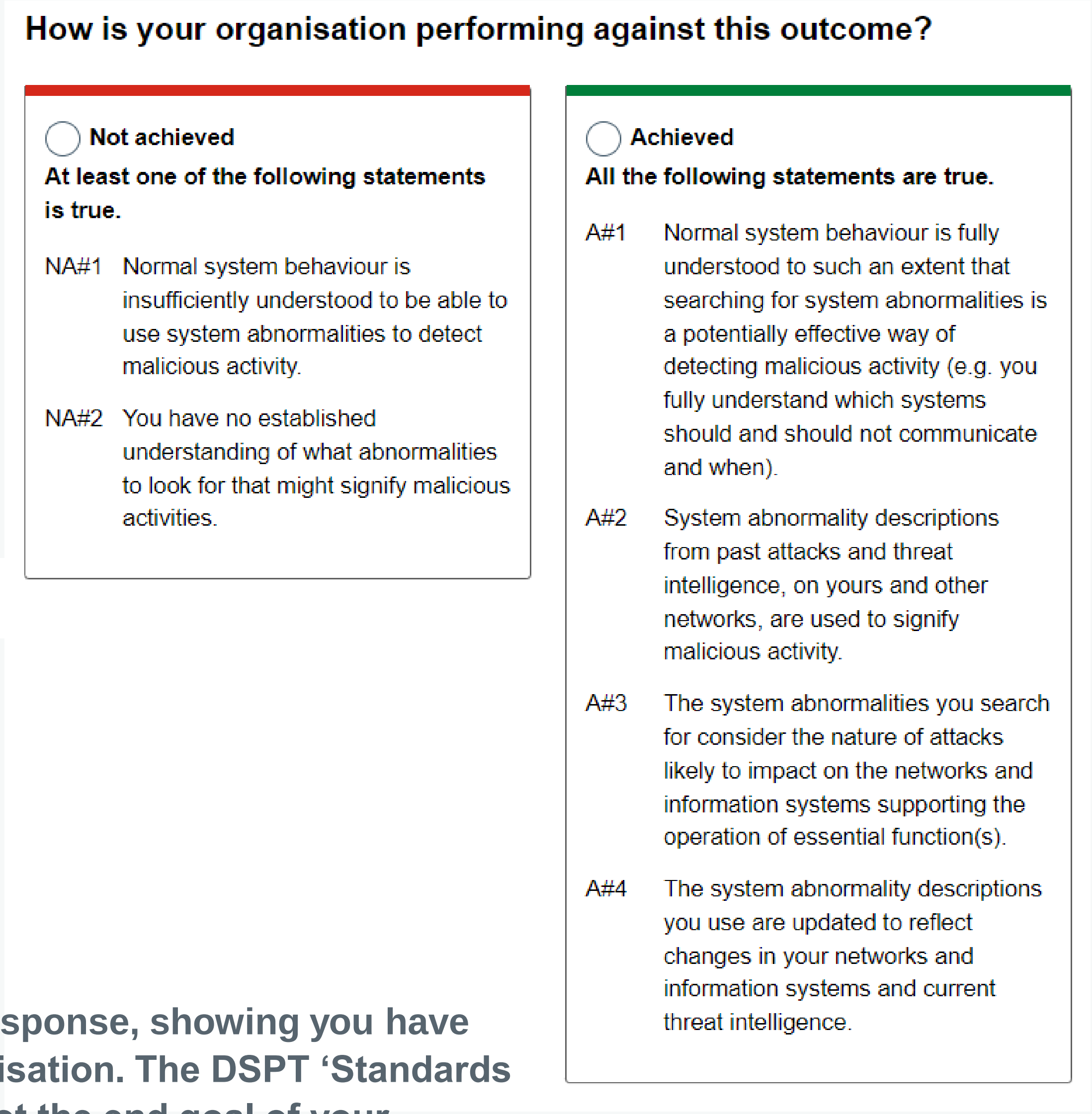
Principle:
C2 Proactive security event discovery

Contributing outcome:
C2.b Proactive attack discovery

You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity

Expectation

The baseline expectation for this contributing outcome is ***Not achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 Normal system behaviour is insufficiently understood to be able to use system abnormalities to detect malicious activity.

NA#2 You have no established understanding of what abnormalities to look for that might signify malicious activities.

○ **Achieved**

All the following statements are true.

A#1 Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity (e.g. you fully understand which systems should and should not communicate and when).

A#2 System abnormality descriptions from past attacks and threat intelligence, on yours and other networks, are used to signify malicious activity.

A#3 The system abnormalities you search for consider the nature of attacks likely to impact on the networks and information systems supporting the operation of essential function(s).

A#4 The system abnormality descriptions you use are updated to reflect changes in your networks and information systems and current threat intelligence.

You are still required to assess your achievement level and provide a response, showing you have considered the implications of the contributing outcome for your organisation. The DSPT 'Standards met' expectation should be regarded as a minimum compliance level, not the end goal of your organisation's cyber security and IG activities.

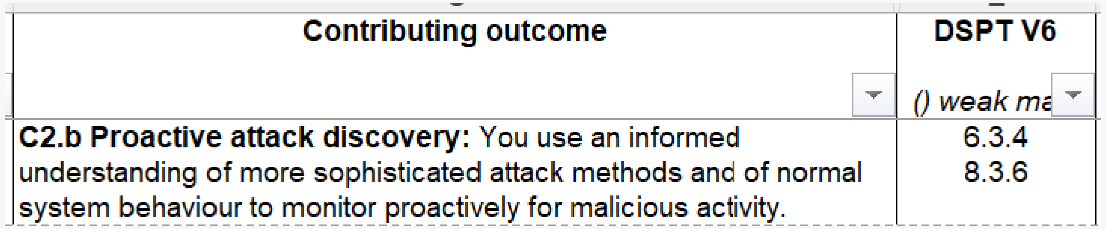
Principle:

C2 Proactive security event discovery

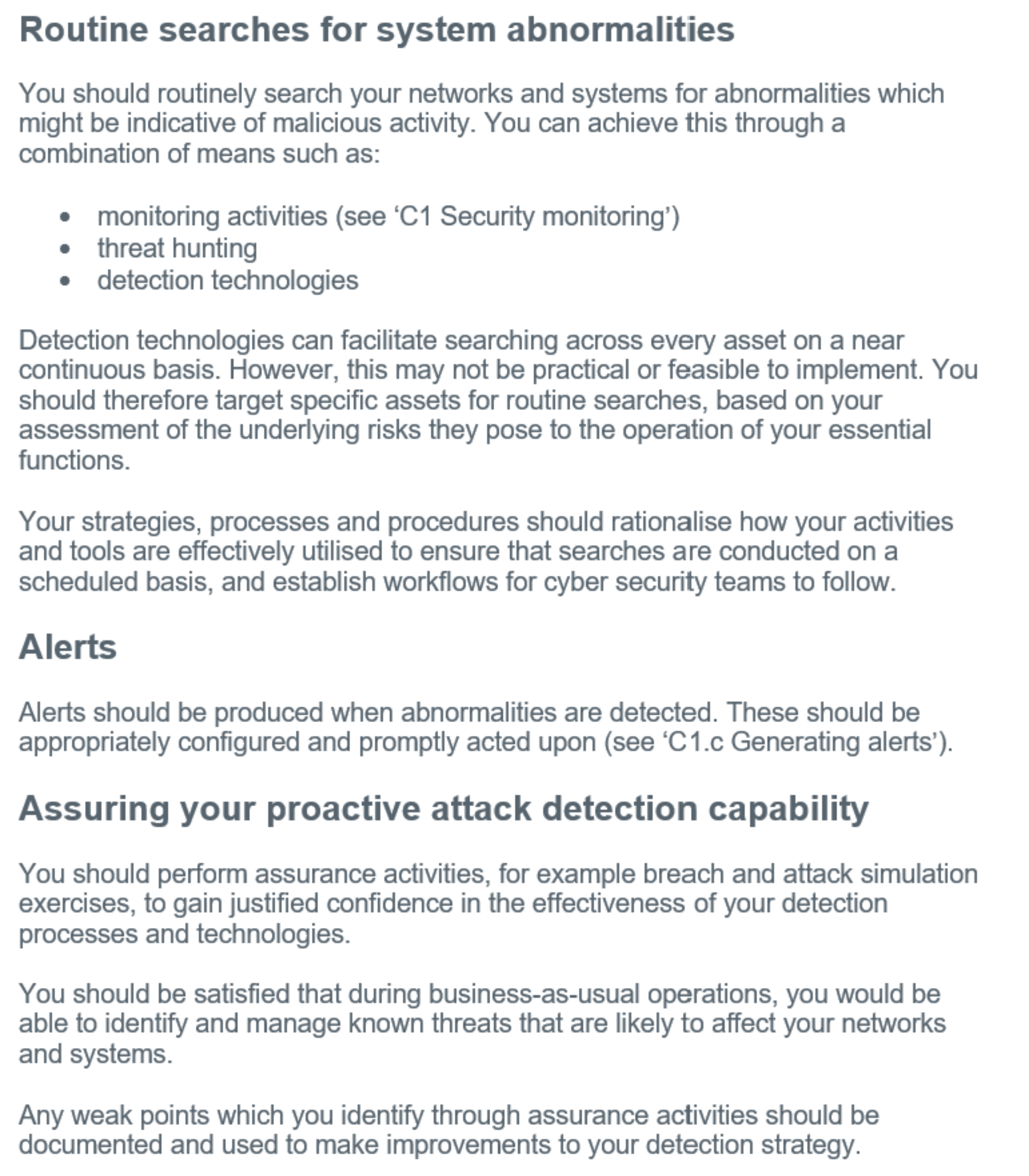
Contributing outcome:

C2.b Proactive attack discovery

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6
	() weak ma
C2.b Proactive attack discovery: You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.	6.3.4 8.3.6



Routine searches for system abnormalities

You should routinely search your networks and systems for abnormalities which might be indicative of malicious activity. You can achieve this through a combination of means such as:

- monitoring activities (see ‘C1 Security monitoring’)
- threat hunting
- detection technologies

Detection technologies can facilitate searching across every asset on a near continuous basis. However, this may not be practical or feasible to implement. You should therefore target specific assets for routine searches, based on your assessment of the underlying risks they pose to the operation of your essential functions.

Your strategies, processes and procedures should rationalise how your activities and tools are effectively utilised to ensure that searches are conducted on a scheduled basis, and establish workflows for cyber security teams to follow.

Alerts

Alerts should be produced when abnormalities are detected. These should be appropriately configured and promptly acted upon (see ‘C1.c Generating alerts’).

Assuring your proactive attack detection capability

You should perform assurance activities, for example breach and attack simulation exercises, to gain justified confidence in the effectiveness of your detection processes and technologies.

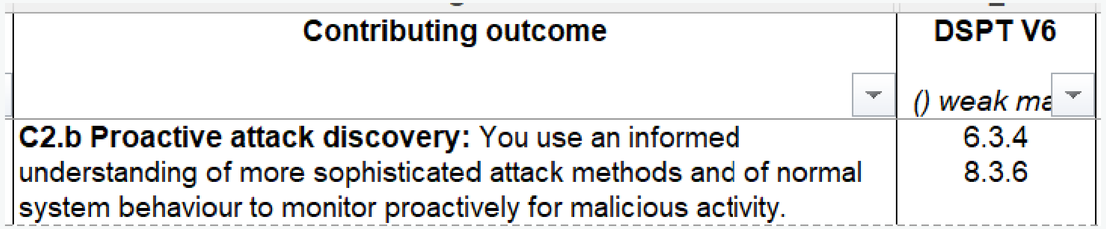
You should be satisfied that during business-as-usual operations, you would be able to identify and manage known threats that are likely to affect your networks and systems.

Any weak points which you identify through assurance activities should be documented and used to make improvements to your detection strategy.

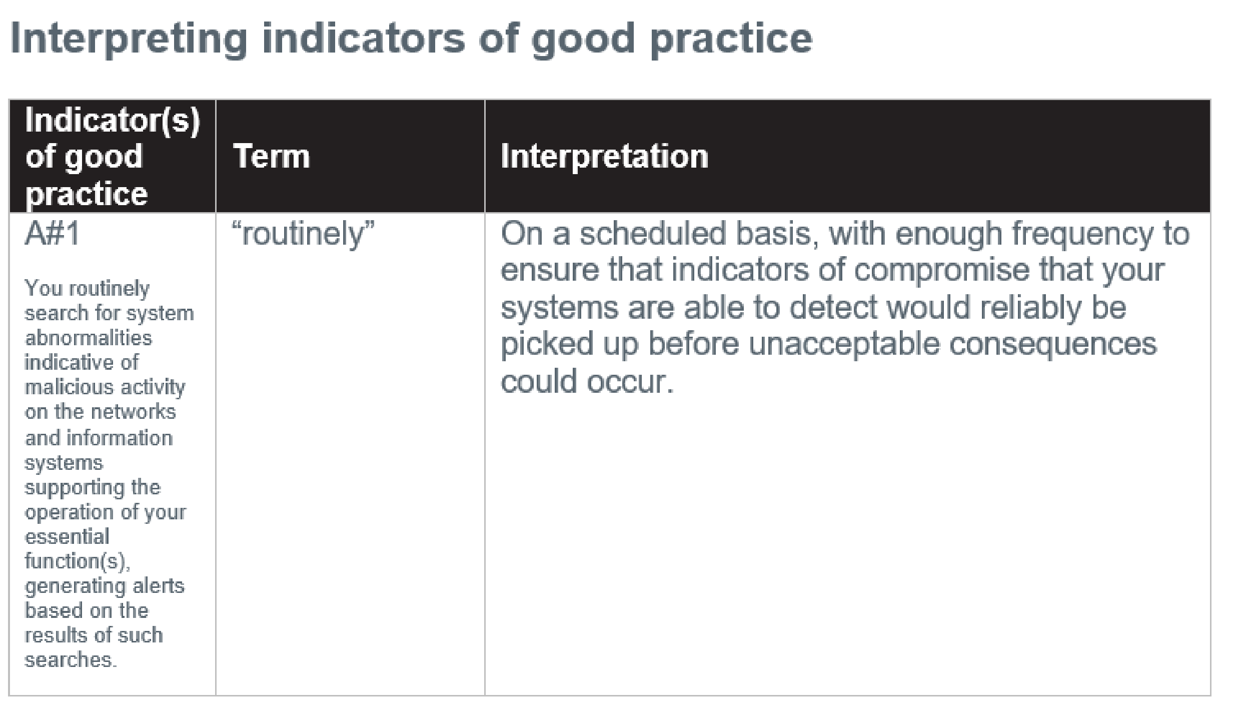
Principle:
C2 Proactive security event discovery

Contributing outcome:
C2.b Proactive attack discovery

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6 () weak ma
C2.b Proactive attack discovery: You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.	6.3.4 8.3.6



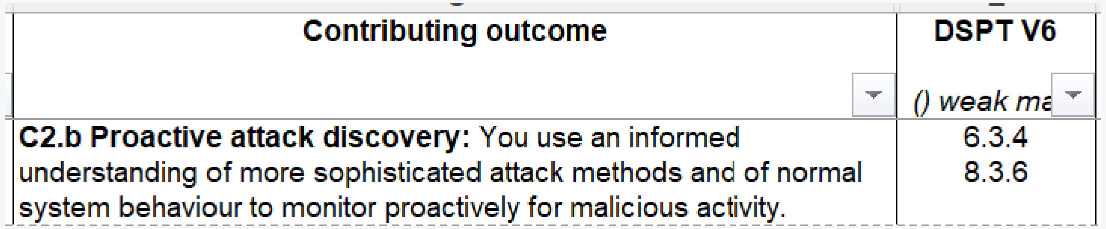
Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
A#1 You routinely search for system abnormalities indicative of malicious activity on the networks and information systems supporting the operation of your essential function(s), generating alerts based on the results of such searches.	"routinely"	On a scheduled basis, with enough frequency to ensure that indicators of compromise that your systems are able to detect would reliably be picked up before unacceptable consequences could occur.

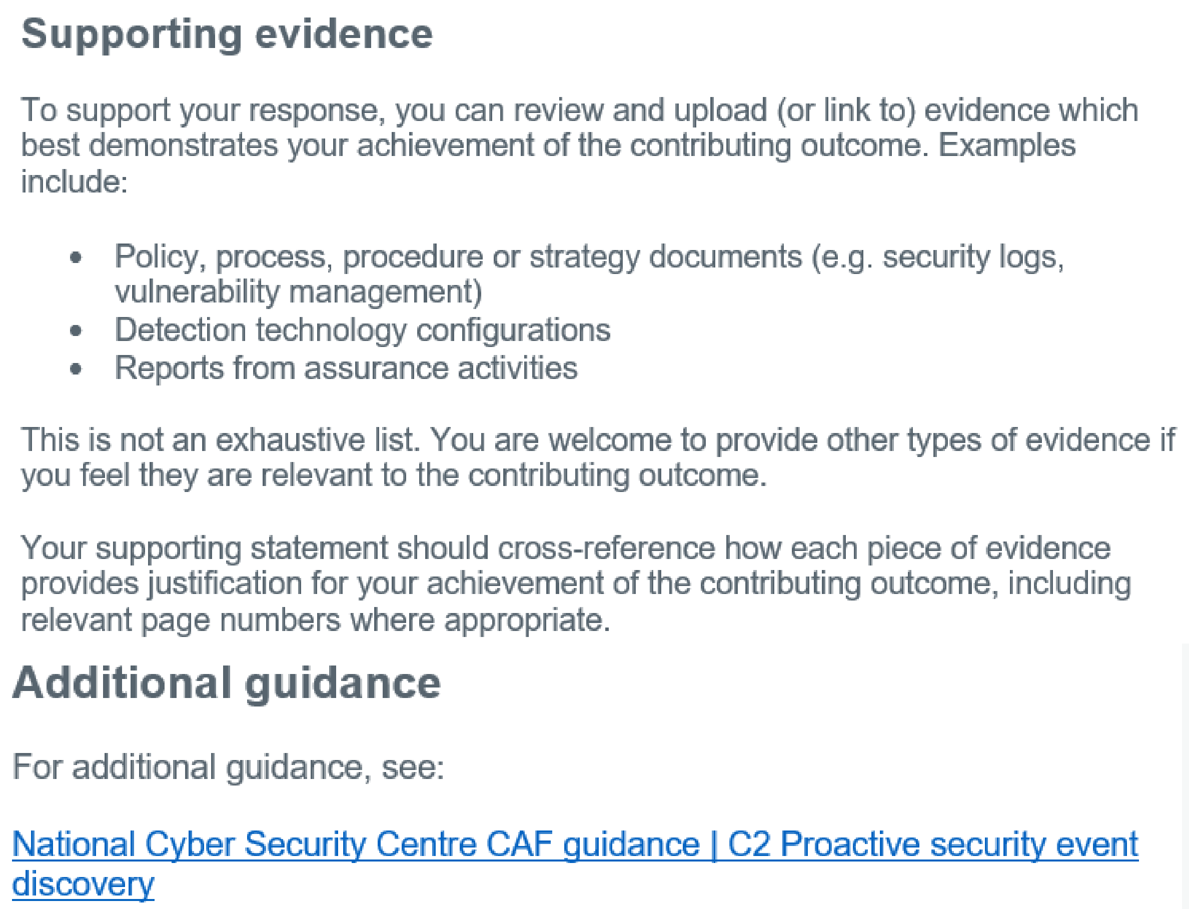
Principle:
C2 Proactive security event discovery

Contributing outcome:
C2.b Proactive attack discovery

Mapping, Guidance and Evidence to upload



Contributing outcome	DSPT V6
	() weak ma
C2.b Proactive attack discovery: You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.	6.3.4 8.3.6



Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- Policy, process, procedure or strategy documents (e.g. security logs, vulnerability management)
- Detection technology configurations
- Reports from assurance activities

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

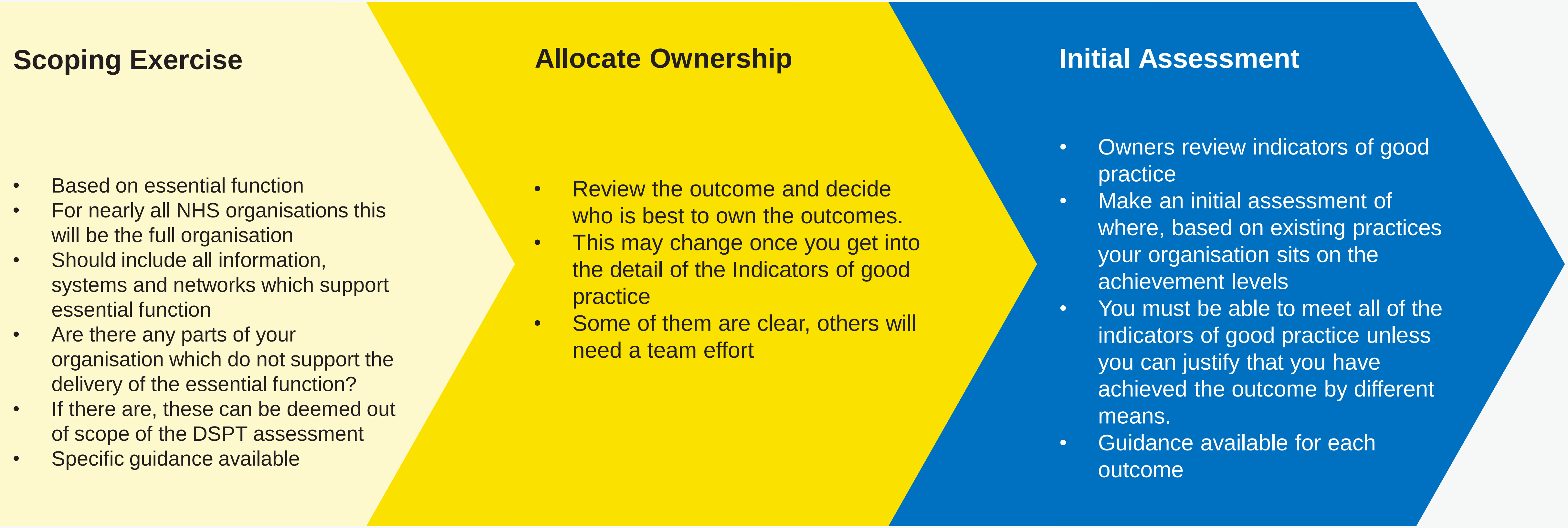
Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | C2 Proactive security event discovery

Planning for DSPT in 24-25

Completing the DSPT 24-25 – Initial Review



Scoping Exercise

- Based on essential function
- For nearly all NHS organisations this will be the full organisation
- Should include all information, systems and networks which support essential function
- Are there any parts of your organisation which do not support the delivery of the essential function?
- If there are, these can be deemed out of scope of the DSPT assessment
- Specific guidance available

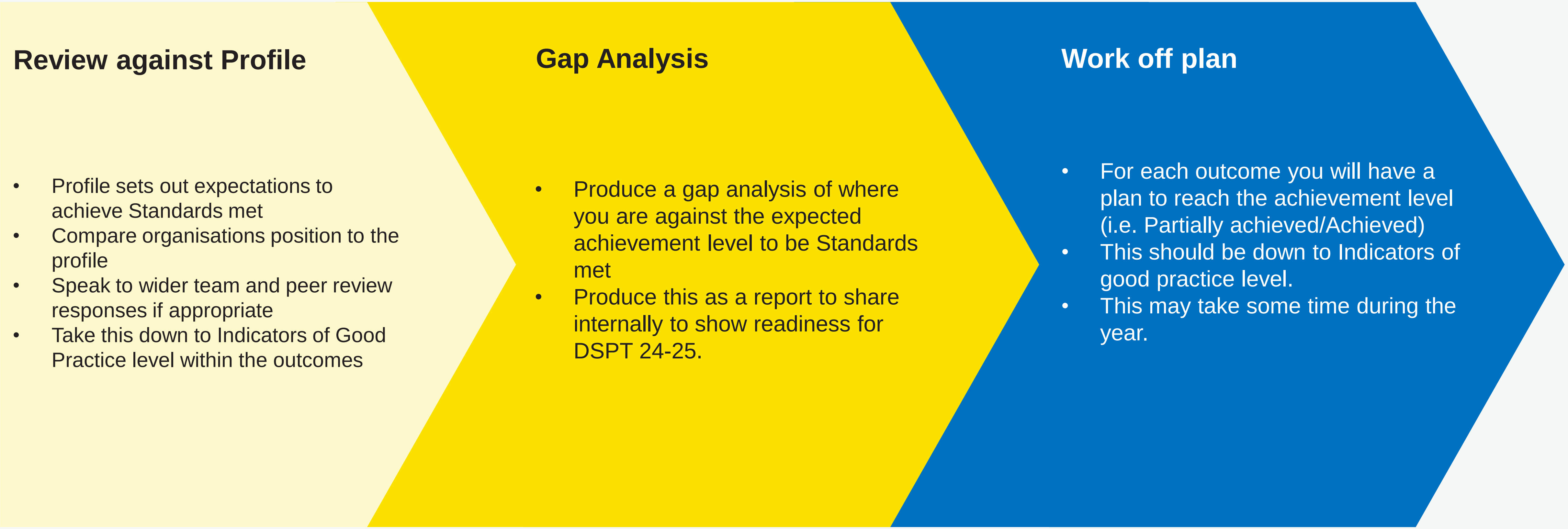
Allocate Ownership

- Review the outcome and decide who is best to own the outcomes.
- This may change once you get into the detail of the Indicators of good practice
- Some of them are clear, others will need a team effort

Initial Assessment

- Owners review indicators of good practice
- Make an initial assessment of where, based on existing practices your organisation sits on the achievement levels
- You must be able to meet all of the indicators of good practice unless you can justify that you have achieved the outcome by different means.
- Guidance available for each outcome

Completing the DSPT 24-25 – Planning to deliver



Review against Profile

- Profile sets out expectations to achieve Standards met
- Compare organisations position to the profile
- Speak to wider team and peer review responses if appropriate
- Take this down to Indicators of Good Practice level within the outcomes

Gap Analysis

- Produce a gap analysis of where you are against the expected achievement level to be Standards met
- Produce this as a report to share internally to show readiness for DSPT 24-25.

Work off plan

- For each outcome you will have a plan to reach the achievement level (i.e. Partially achieved/Achieved)
- This should be down to Indicators of good practice level.
- This may take some time during the year.

Webinars

Date and time	Topics to be covered
Tuesday 17th September 2024 12.30-13.30 Tuesday 15th October 2024 12.30-13.30 Tuesday 19th November 2024 12.30-13.30 Tuesday 17th December 2024 12.30-13.30 Tuesday 21sth January 2025 12.30-13.30 Tuesday 18th February 2025 12.30-13.30 Tuesday 18th March 2025 12.30-13.30 Tuesday 15th April 2025 12.30-13.30 Tuesday 20th May 2025 12.30-13.30 Tuesday 17th June 2025 12.30-13.30	Overview of 24-25 DSPT Completing the DSPT Changes or updates to 24-25 DSPT Demonstration of 24-25 DSPT Question and answer session

Audit update

DSPT Audit for 24-25 for NHS Trusts, ICBs, CSUs and ALBs

Audit guide

Developing an Audit guide for 24-25

Who is working on it?

Working with an audit partner

When will be able to see them?

Guides will come out after the DSPT 24-25 launch.

Summary first followed by detailed guide for auditors

Engagement

Webinars for both auditors and organisations

Looking for ‘volunteers’ to test the framework before launch

Link to guidance and IGPs

Health and care overlay, Indicators of good practice and guidance key documents

Question and answer session

NHS England

Thank You

@nhsengland

company/nhsengland

england.nhs.uk