AUD 07-25

HTA ARAC meeting, 11 February 2025

Agenda item	**3.2 Cyber Assessment Framework Update**
Purpose: for information or decision?	Information
Decision making to date?	Standing item to each Audit and Risk Committee
Recommendation	Audit and Risk Committee is asked to note the latest updates for the Cyber Assessment Framework
Which strategic risks are relevant?	Risk 5: Digital
Strategic objective	Use of Information
Core operations / Change activity	Core operations
Business Plan item	Data – production and analysis of rich data and records to inform both our strategic direction and operational capabilities (including CAF, records management and information governance)
Committee oversight?	Audit and Risk Assurance Committee
Finance and resource implications	N/A
Timescales	N/A
Communication(s) (internal/external	N/A
Identified legislative implications	N/A

Cyber Assurance Framework

Interim submission & update on next steps

ARAC 11 February 2025

HTA
Human Tissue Authority

Background

HTA
Human Tissue Authority

- As of September 2024, the Data Security Protection Toolkit (DSPT) changed to adopt the National Cyber Security Centre's Cyber Assurance Framework (CAF) as the basis for cyber security and Information Governance (IG) assurance.

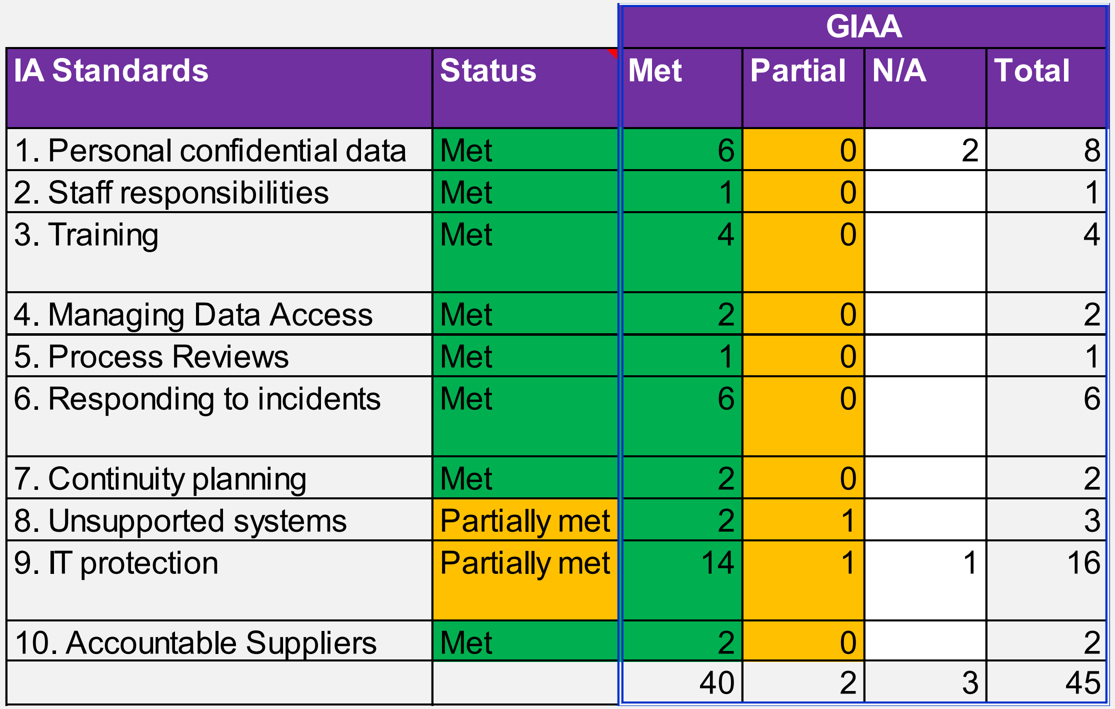
- This change has already started for large organisations including the HTA. As an Arm's Length Body (ALB), the HTA is an **early adopter** of the CAF.

- Tracking compliance against the 10 National Data Guardian Standards has been replaced by CAF **Objectives, Principles** and **Outcomes compliance.**

- CAF achievement levels scored as 'Not Achieved', 'Partially Achieved', or 'Achieved' for each contributing outcome. To get "Partially Achieved" or "Achieved", you must have all statements assessed as True, and no statements in "Not Achieved" assessed as True, however if one is "True" it will default the entire outcome to "Not Achieved".

Changes in the Frameworks

DSPT self-assessment 2023-24 based on the National Data Guardian's security standards



		GIAA			
IA Standards	**Status**	**Met**	**Partial**	**N/A**	**Total**
1. Personal confidential data	Met	6	0	2	8
2. Staff responsibilities	Met	1	0		1
3. Training	Met	4	0		4
4. Managing Data Access	Met	2	0		2
5. Process Reviews	Met	1	0		1
6. Responding to incidents	Met	6	0		6
7. Continuity planning	Met	2	0		2
8. Unsupported systems	Partially met	2	1		3
9. IT protection	Partially met	14	1	1	16
10. Accountable Suppliers	Met	2	0		2
		40	2	3	45

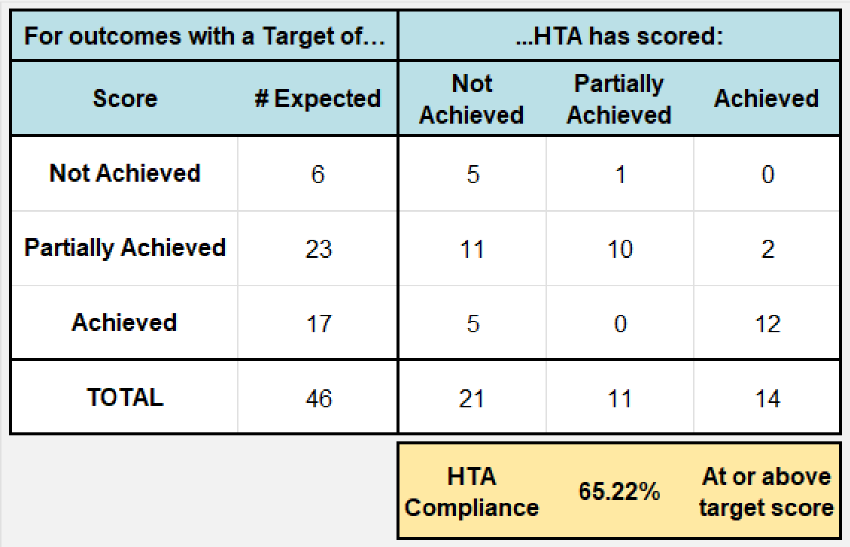
2024-25 self-assessment based on the National Cyber Security Centre's Cyber Assurance Framework (CAF)

- **Objective A -** Managing risk
- **Objective B -** Protecting against cyber-attack and data breaches
- **Objective C -** Detecting cyber security events
- **Objective D -** Minimising the impact of incidents
- **Objective E** - Using and sharing information appropriately

HTA
Human Tissue Authority

Interim Assessment
December 2024

Interim assessment – December 2024



For outcomes with a Target of…		...HTA has scored:		
Score	# Expected	Not Achieved	Partially Achieved	Achieved
Not Achieved	6	5	1	0
Partially Achieved	23	11	10	2
Achieved	17	5	0	12
TOTAL	46	21	11	14
		HTA Compliance	65.22%	At or above target score

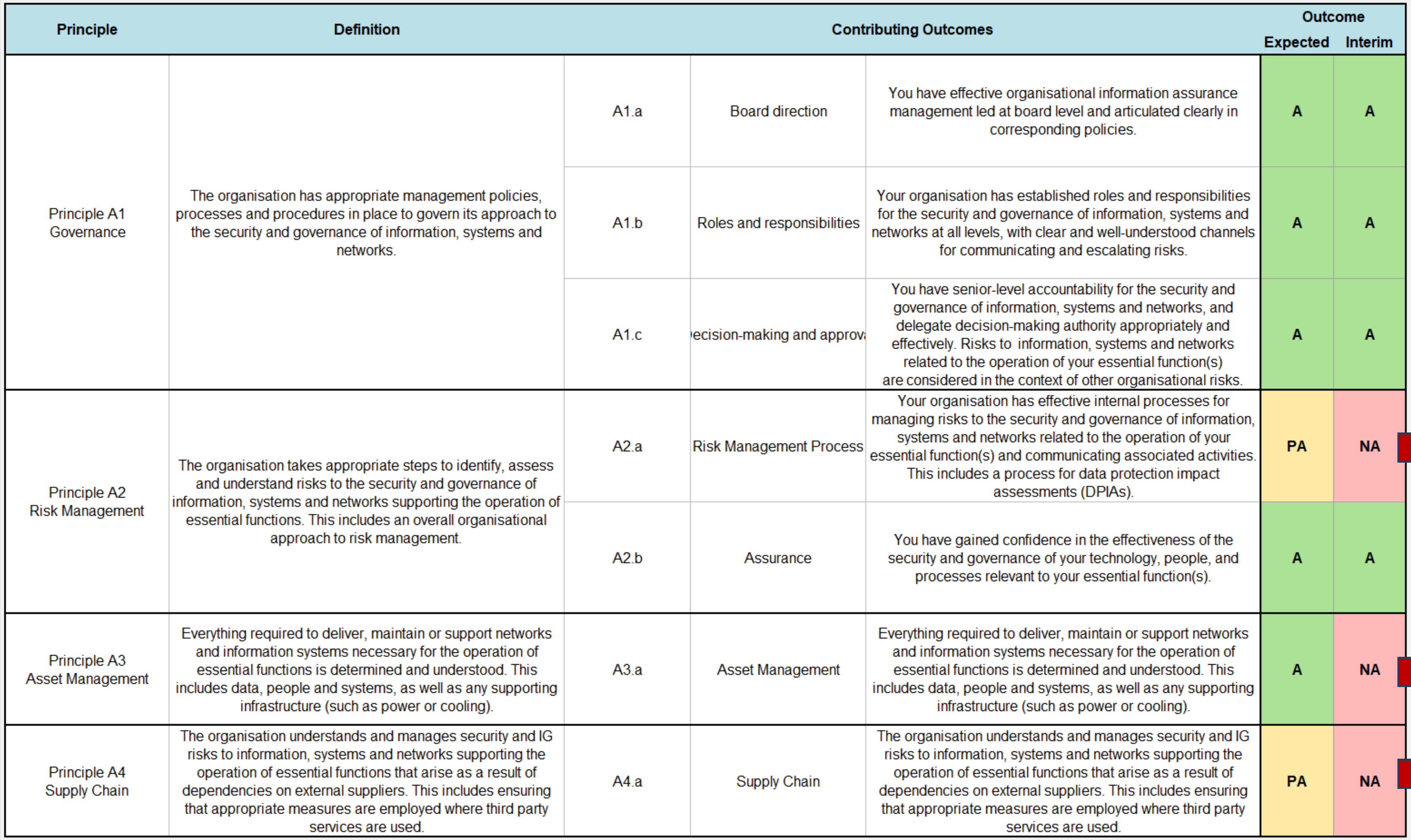
As baseline assessment the HTA are 65.22% compliance against the expected outcomes outlined by the NHSE. This could change positively or negatively once the finalised position is presented in May ahead of the final submission as a more critical review of our assurance.

These assessments are based on our technical knowledge and may under scrutiny of the Audits and further engagement with the organisation be changed to reflect a more accurate position.

As this is the first interim audit and as the HTA are early adopters along with large organisations and other ALBs the assessment was completed against NHS set targets.

Although there are 47 outcomes the HTA are only responding to 46. E4.b is related to Clinical Coding of which is not relevant to the HTA.

Objective A – Managing Risk
(Interim assessment)



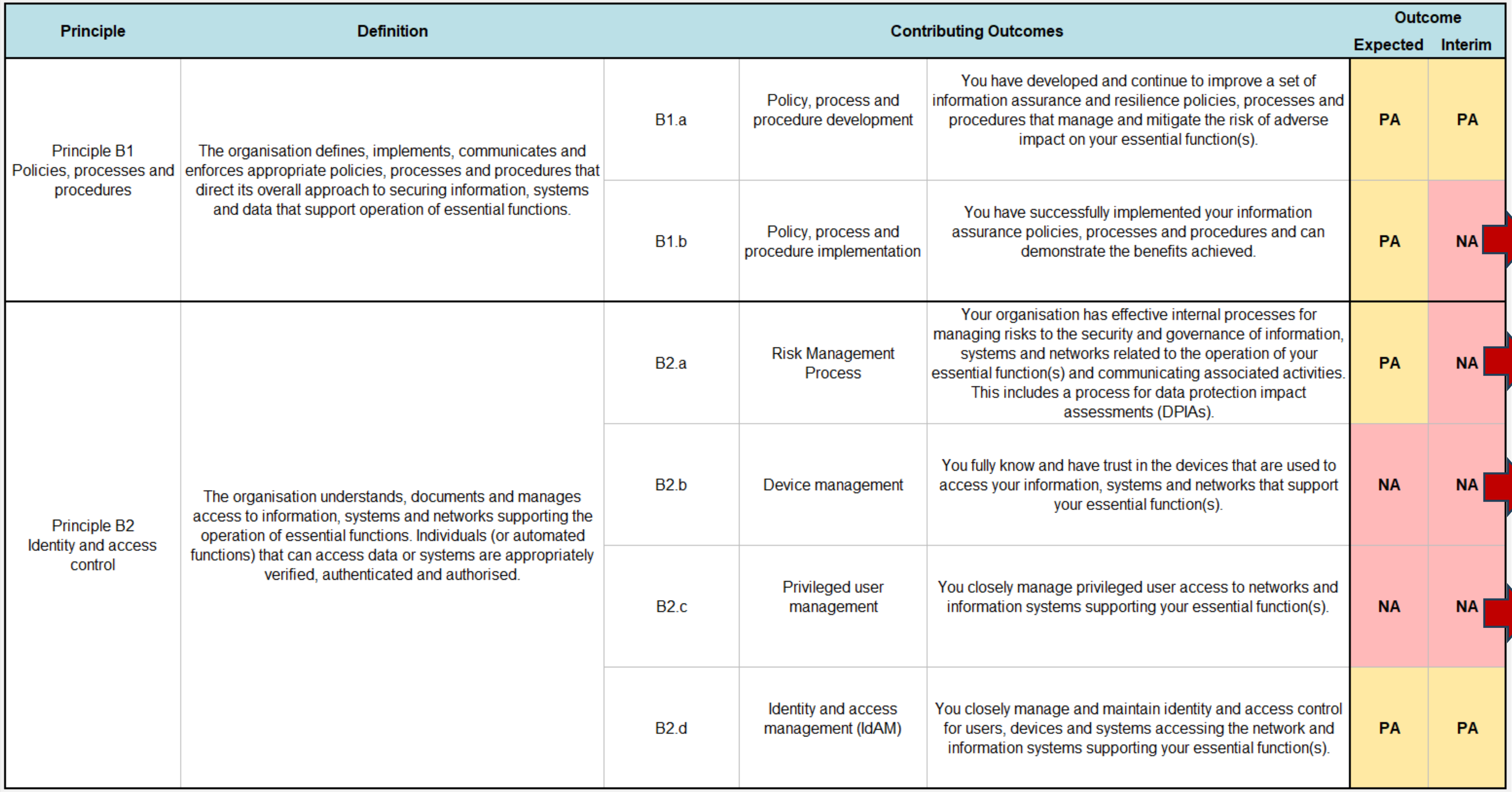
Principle	Definition	Contributing Outcomes			Outcome	
					Expected	Interim
Principle A1 Governance	The organisation has appropriate management policies, processes and procedures in place to govern its approach to the security and governance of information, systems and networks.	A1.a	Board direction	You have effective organisational information assurance management led at board level and articulated clearly in corresponding policies.	A	A
		A1.b	Roles and responsibilities	Your organisation has established roles and responsibilities for the security and governance of information, systems and networks at all levels, with clear and well-understood channels for communicating and escalating risks.	A	A
		A1.c	ecision-making and approv	You have senior-level accountability for the security and governance of information, systems and networks, and delegate decision-making authority appropriately and effectively. Risks to information, systems and networks related to the operation of your essential function(s) are considered in the context of other organisational risks.	A	A
Principle A2 Risk Management	The organisation takes appropriate steps to identify, assess and understand risks to the security and governance of information, systems and networks supporting the operation of essential functions. This includes an overall organisational approach to risk management.	A2.a	Risk Management Process	Your organisation has effective internal processes for managing risks to the security and governance of information, systems and networks related to the operation of your essential function(s) and communicating associated activities. This includes a process for data protection impact assessments (DPIAs).	PA	NA
		A2.b	Assurance	You have gained confidence in the effectiveness of the security and governance of your technology, people, and processes relevant to your essential function(s).	A	A
Principle A3 Asset Management	Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).	A3.a	Asset Management	Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).	A	NA
Principle A4 Supply Chain	The organisation understands and manages security and IG risks to information, systems and networks supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	A4.a	Supply Chain	The organisation understands and manages security and IG risks to information, systems and networks supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	PA	NA

Risk Management and Assessments

Physical and Digital Asset Management Processes

Contractual and Operational Management Functions

Objective B – Protecting against Cyber Attacks and Data Breaches (Interim assessment) – Part 1



Principle	Definition	Contributing Outcomes			Outcome	
					Expected	Interim
Principle B1 Policies, processes and procedures	The organisation defines, implements, communicates and enforces appropriate policies, processes and procedures that direct its overall approach to securing information, systems and data that support operation of essential functions.	B1.a	Policy, process and procedure development	You have developed and continue to improve a set of information assurance and resilience policies, processes and procedures that manage and mitigate the risk of adverse impact on your essential function(s).	PA	PA
		B1.b	Policy, process and procedure implementation	You have successfully implemented your information assurance policies, processes and procedures and can demonstrate the benefits achieved.	PA	NA
Principle B2 Identity and access control	The organisation understands, documents and manages access to information, systems and networks supporting the operation of essential functions. Individuals (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised.	B2.a	Risk Management Process	Your organisation has effective internal processes for managing risks to the security and governance of information, systems and networks related to the operation of your essential function(s) and communicating associated activities. This includes a process for data protection impact assessments (DPIAs).	PA	NA
		B2.b	Device management	You fully know and have trust in the devices that are used to access your information, systems and networks that support your essential function(s).	NA	NA
		B2.c	Privileged user management	You closely manage privileged user access to networks and information systems supporting your essential function(s).	NA	NA
		B2.d	Identity and access management (IdAM)	You closely manage and maintain identity and access control for users, devices and systems accessing the network and information systems supporting your essential function(s).	PA	PA

No Policy Monitoring in place to improve Score

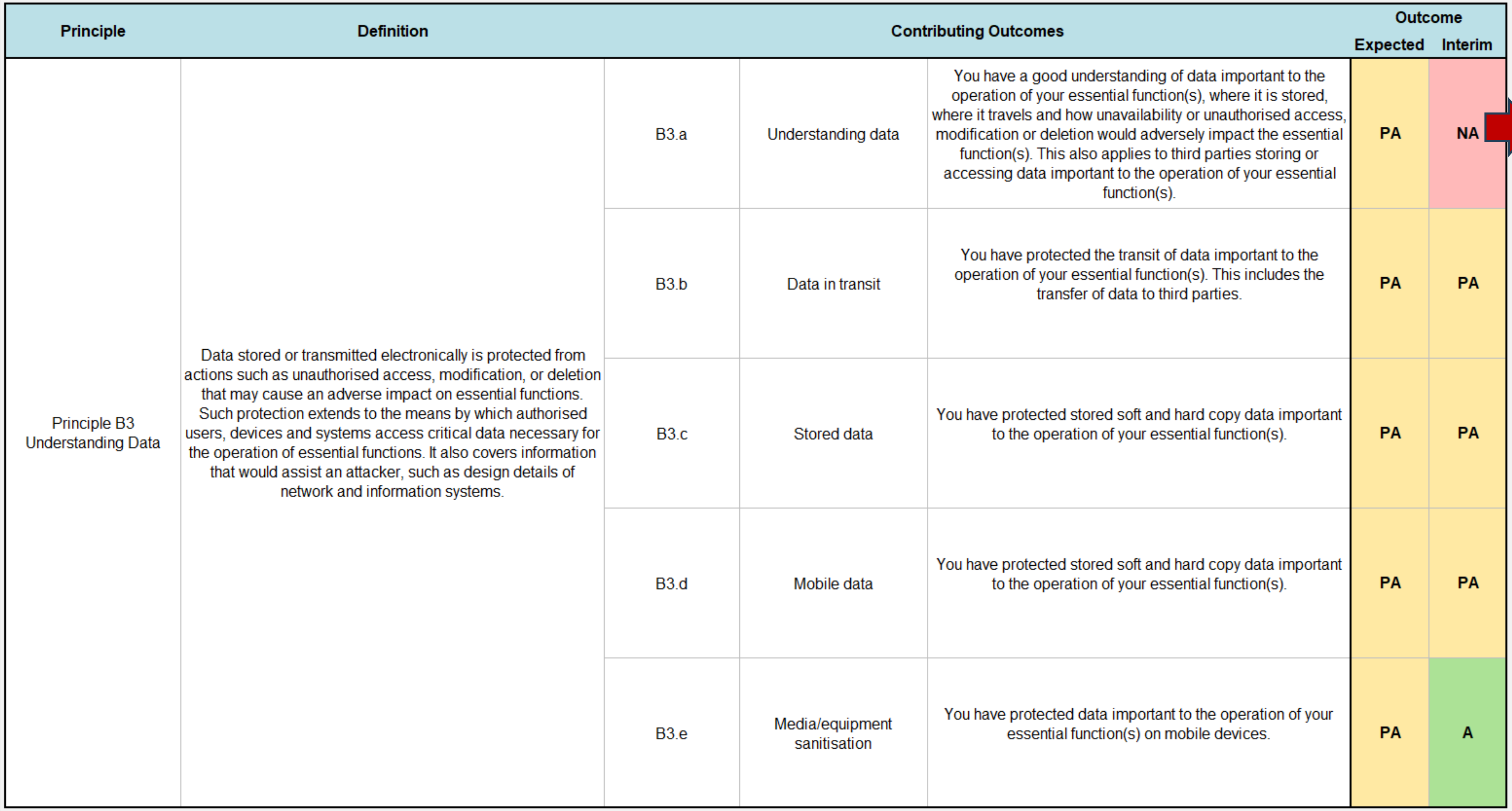
MFA in place but not Best Practice

Users can access HTA Systems using own devices

All privileged user access to network and systems must use MFA

Objective B – Protecting against Cyber Attacks and Data Breaches (Interim Assessment)

HTA
Human Tissue Authority

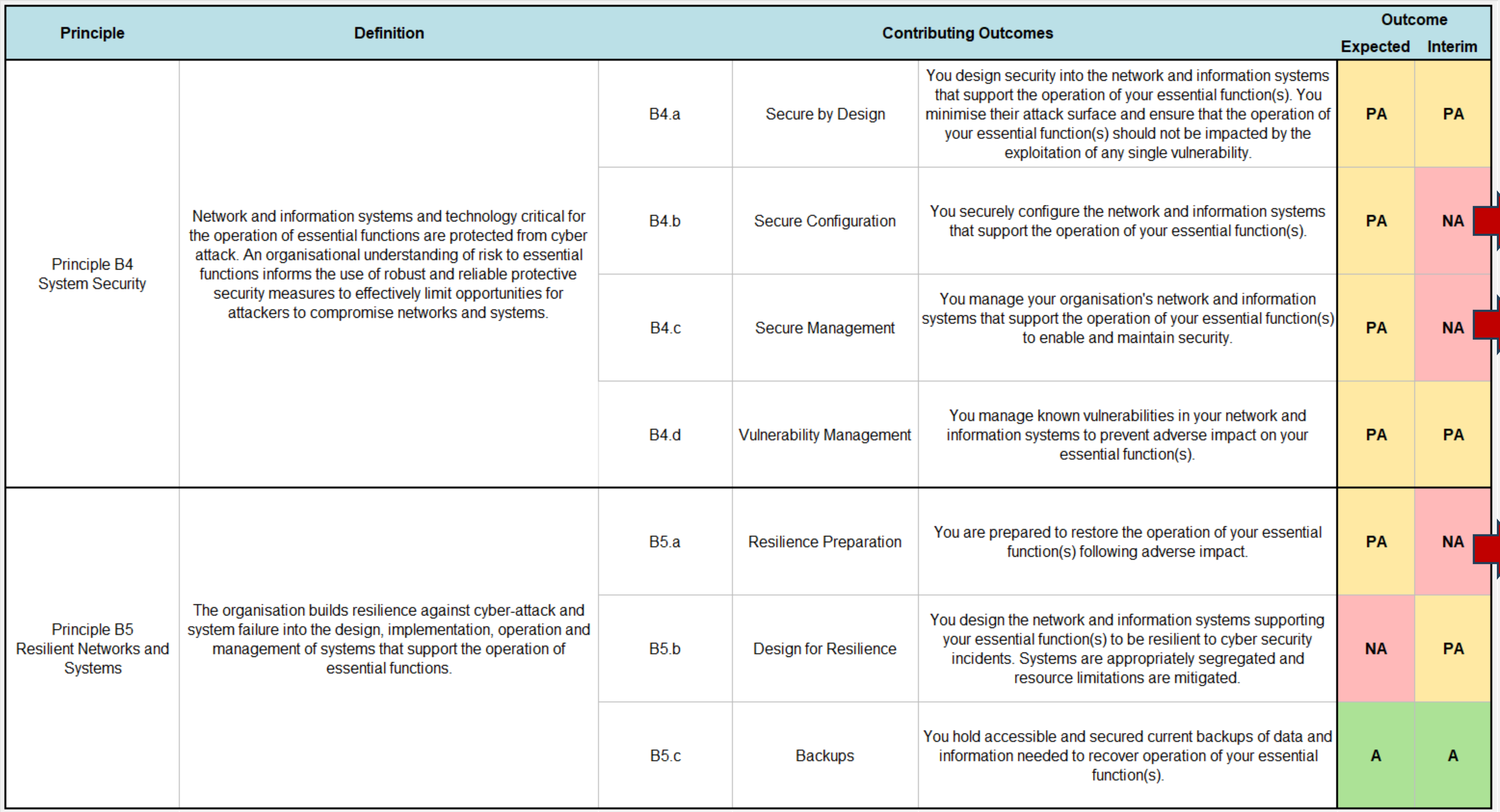


Principle	Definition	Contributing Outcomes			Outcome	
					Expected	Interim
Principle B3 Understanding Data	Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on essential functions. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of essential functions. It also covers information that would assist an attacker, such as design details of network and information systems.	B3.a	Understanding data	You have a good understanding of data important to the operation of your essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to the operation of your essential function(s).	PA	NA
		B3.b	Data in transit	You have protected the transit of data important to the operation of your essential function(s). This includes the transfer of data to third parties.	PA	PA
		B3.c	Stored data	You have protected stored soft and hard copy data important to the operation of your essential function(s).	PA	PA
		B3.d	Mobile data	You have protected stored soft and hard copy data important to the operation of your essential function(s).	PA	PA
		B3.e	Media/equipment sanitisation	You have protected data important to the operation of your essential function(s) on mobile devices.	PA	A

Multiple False statement in PA and A

Objective B – Protecting against Cyber Attacks and Data Breaches (Interim assessment)

HTA Human Tissue Authority



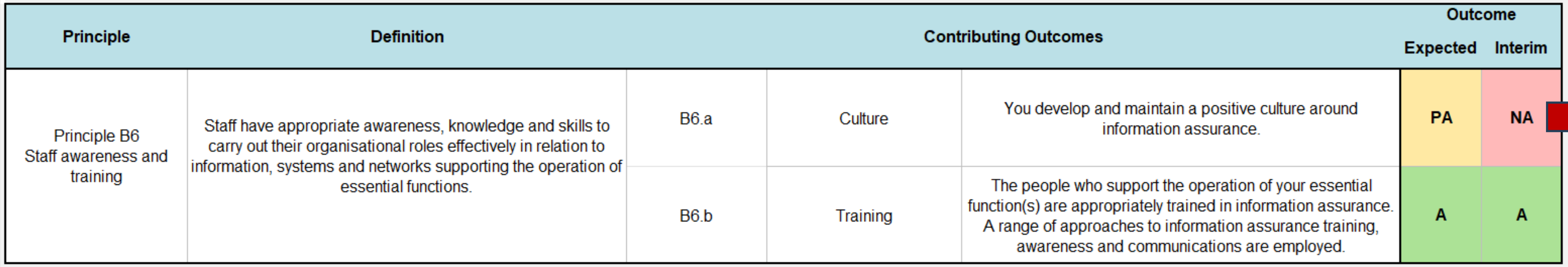
Principle	Definition	Contributing Outcomes			Outcome	
					Expected	Interim
Principle B4 System Security	Network and information systems and technology critical for the operation of essential functions are protected from cyber attack. An organisational understanding of risk to essential functions informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.	B4.a	Secure by Design	You design security into the network and information systems that support the operation of your essential function(s). You minimise their attack surface and ensure that the operation of your essential function(s) should not be impacted by the exploitation of any single vulnerability.	PA	PA
		B4.b	Secure Configuration	You securely configure the network and information systems that support the operation of your essential function(s).	PA	NA
		B4.c	Secure Management	You manage your organisation's network and information systems that support the operation of your essential function(s) to enable and maintain security.	PA	NA
		B4.d	Vulnerability Management	You manage known vulnerabilities in your network and information systems to prevent adverse impact on your essential function(s).	PA	PA
Principle B5 Resilient Networks and Systems	The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation and management of systems that support the operation of essential functions.	B5.a	Resilience Preparation	You are prepared to restore the operation of your essential function(s) following adverse impact.	PA	NA
		B5.b	Design for Resilience	You design the network and information systems supporting your essential function(s) to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.	NA	PA
		B5.c	Backups	You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s).	A	A

Generic 'LocalAdmin' account is configured on all Devices

BCC administrate our Network from non-managed devices

BCC administrate our Network from non-managed devices

Objective B – Protecting against Cyber Attacks and Data Breaches (Interim assessment)

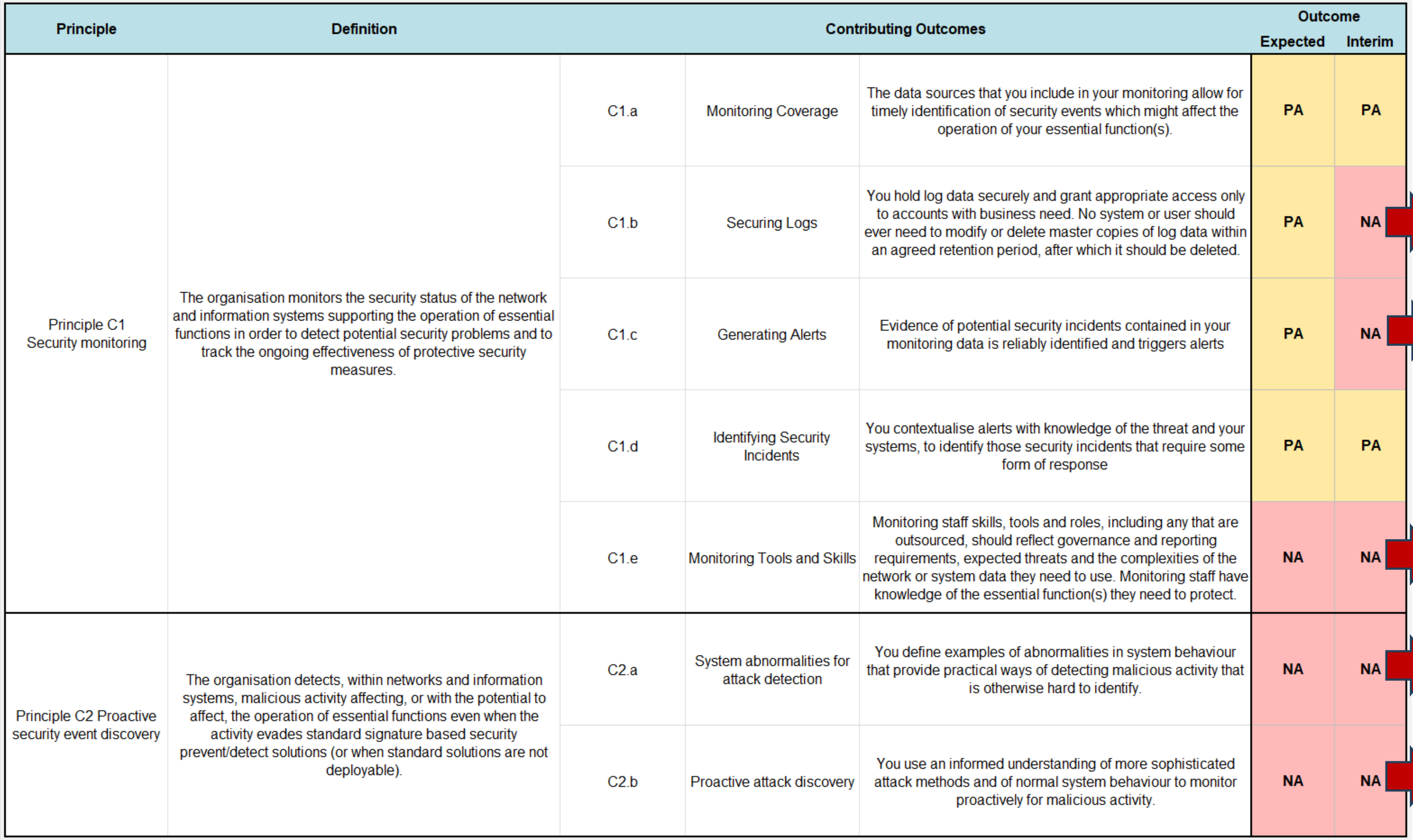


Principle	Definition	Contributing Outcomes			Outcome	
					Expected	Interim
Principle B6 Staff awareness and training	Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to information, systems and networks supporting the operation of essential functions.	B6.a	Culture	You develop and maintain a positive culture around information assurance.	PA	NA
		B6.b	Training	The people who support the operation of your essential function(s) are appropriately trained in information assurance. A range of approaches to information assurance training, awareness and communications are employed.	A	A

Multiple TRUE statements in Not Achieved

Objective C – Detecting Cyber Security Events (Interim assessment)

HTA
Human Tissue Authority



Principle	Definition	Contributing Outcomes			Outcome	
					Expected	Interim
Principle C1 Security monitoring	The organisation monitors the security status of the network and information systems supporting the operation of essential functions in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.	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).	PA	PA
		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.	PA	NA
		C1.c	Generating Alerts	Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts	PA	NA
		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	PA	PA
		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.	NA	NA
Principle C2 Proactive security event discovery	The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature based security prevent/detect solutions (or when standard solutions are not deployable).	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.	NA	NA
		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.	NA	NA

Monitoring access to log data
NA#3 is TRUE PA#3 is FALSE

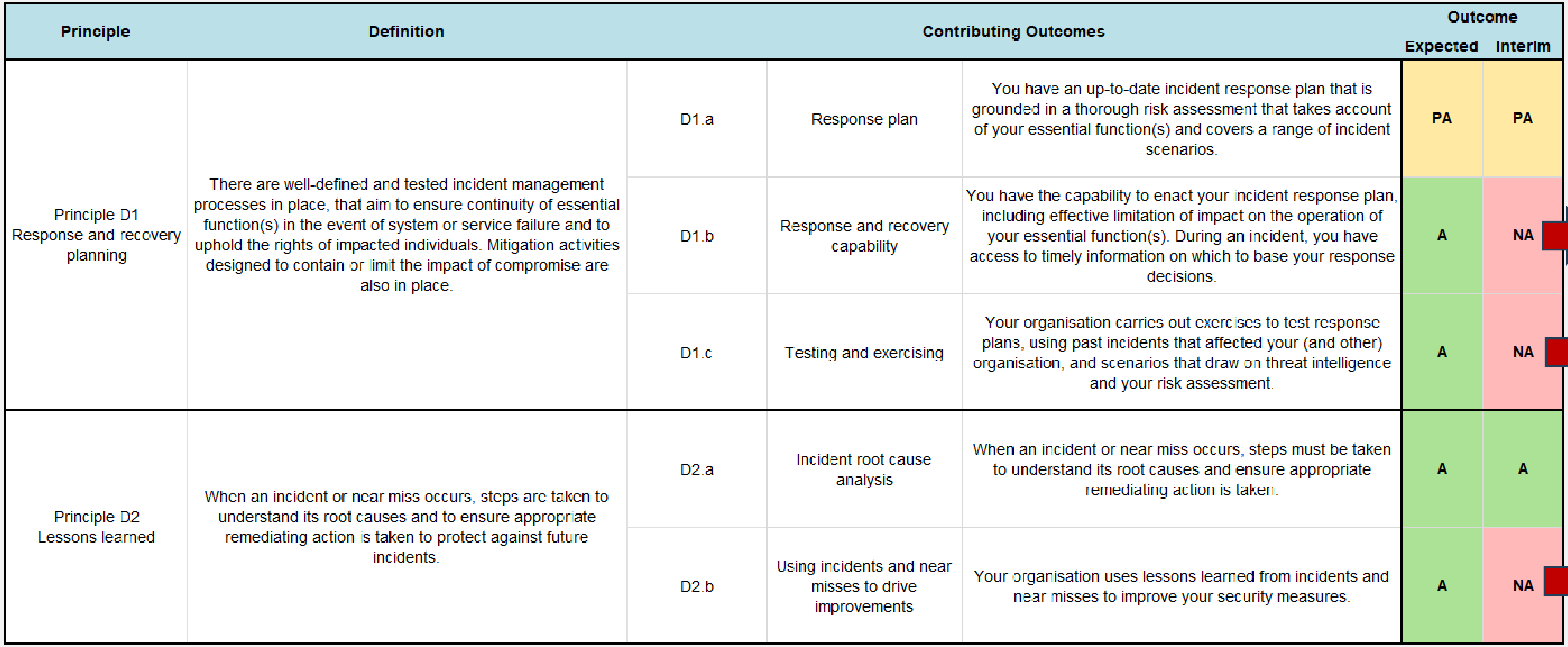
No Schedule of Logs
NA#5 is TRUE PA#5 is FALSE

Multiple TRUE statements in Not Achieved – No dedicated Monitoring Team/Resources

All Statements in Achieved are FALSE

Routine searching for Abnormalities is not performed
A#1 FALSE

Objective D – Minimising the impact of Incidents (Interim assessment)



Principle	Definition	Contributing Outcomes			Outcome	
					Expected	Interim
Principle D1 Response and recovery planning	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.	D1.a	Response plan	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.	PA	PA
		D1.b	Response and recovery capability	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.	A	NA
		D1.c	Testing and exercising	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.	A	NA
Principle D2 Lessons learned	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.	D2.a	Incident root cause analysis	When an incident or near miss occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.	A	A
		D2.b	Using incidents and near misses to drive improvements	Your organisation uses lessons learned from incidents and near misses to improve your security measures.	A	NA

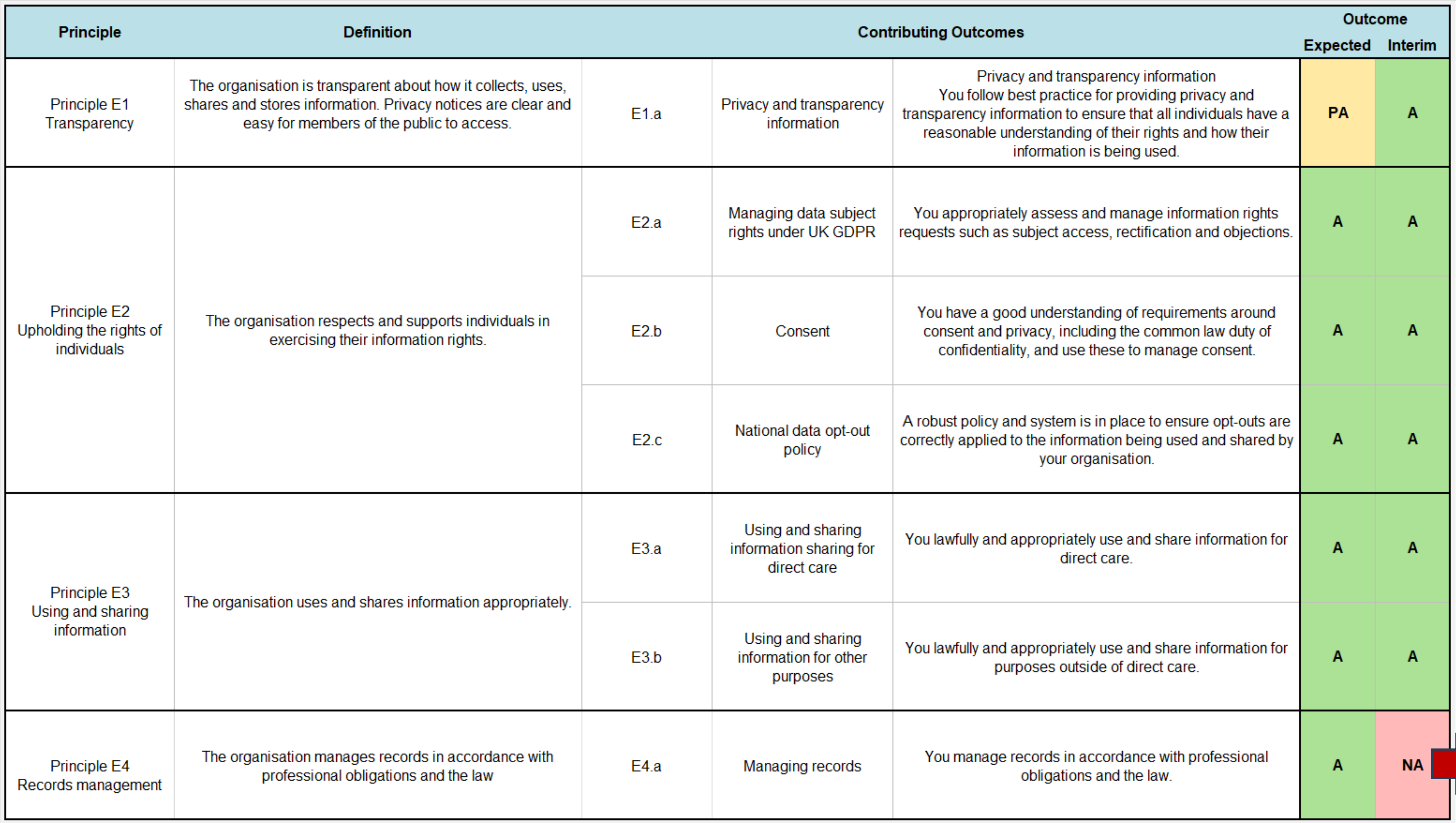
Multiple TRUE statements in the Not Achieved

Multiple TRUE statements in the Not Achieved

Insufficient organisation priority to improvements from Lessons Learned

Objective E – Using and Sharing of Information Appropriately (Interim assessment)

HTA
Human Tissue Authority



Principle	Definition	Contributing Outcomes			Outcome	
					Expected	Interim
Principle E1 Transparency	The organisation is transparent about how it collects, uses, shares and stores information. Privacy notices are clear and easy for members of the public to access.	E1.a	Privacy and transparency information	Privacy and transparency information You follow best practice for providing privacy and transparency information to ensure that all individuals have a reasonable understanding of their rights and how their information is being used.	PA	A
Principle E2 Upholding the rights of individuals	The organisation respects and supports individuals in exercising their information rights.	E2.a	Managing data subject rights under UK GDPR	You appropriately assess and manage information rights requests such as subject access, rectification and objections.	A	A
		E2.b	Consent	You have a good understanding of requirements around consent and privacy, including the common law duty of confidentiality, and use these to manage consent.	A	A
		E2.c	National data opt-out policy	A robust policy and system is in place to ensure opt-outs are correctly applied to the information being used and shared by your organisation.	A	A
Principle E3 Using and sharing information	The organisation uses and shares information appropriately.	E3.a	Using and sharing information sharing for direct care	You lawfully and appropriately use and share information for direct care.	A	A
		E3.b	Using and sharing information for other purposes	You lawfully and appropriately use and share information for purposes outside of direct care.	A	A
Principle E4 Records management	The organisation manages records in accordance with professional obligations and the law	E4.a	Managing records	You manage records in accordance with professional obligations and the law.	A	NA

Insufficient organisation priority to improvements from Lessons Learned

Independent assessment by GIAA

As per previous DSPT assessments the CAF will be subject to independent assessment in Q1 2025/26. Following this stage of the process, the HTA will confirm its assessment against the NHS Cyber Assessment Framework.

Recent guidance has been provided on the assessment process Guide for CAF-aligned DSPT independent assessors - NHS England Digital. This guidance confirms the assessment against 8 mandated outcomes.
A2.a Risk management process
A4.a Supply chain
B2.a Identity verification, authentication and authorisation
B4.d Vulnerability management
C1.a Monitoring coverage
D1.a Response plan
E2.b Consent
E3.a Using and sharing information sharing for direct care

In January the SMT considered and agree a further 4 outcomes to be tested as part of the assessment. The additional outcomes represent areas of risk or concern, where the HTA would welcome assurance against the baseline assessment due to the potential significance of the risk if realised. The outcomes are:
B5b Design for resilience
B5c Backups
B6a Culture
D1c Testing & Exercise

Next steps

Project Management approach & arrangements

Over the emainder of the quarter, we will be engaging and confirm with colleagues the arrangement to validate the interim ASSESSMENT, collect & collate EVIDENCE and prepare for the AUDIT. This includes:

- Identification of leads against each of the outcomes
- Sharing of templates for consistency in documenting the assessment, action plans and evidence. Emerging areas to focus action include:
- Engagement to confirm activities:

  February – validating assessment to generate the baseline and identifying evidence and or remedial action. For mandatory outcomes we will be starting to collect the evidence.

  March – focus on evidence collation and discussions on risk acceptance based on remedial plans against the baseline position
- Internal reporting arrangements to track progress under development