Paper Number AUD 28-24

CONFIDENTIAL

ARAC 17th October 2024

Internal Audit

Paper Number AUD 29-24

CONFIDENTIAL

ARAC 17th October 2024

Audit Tracker

Paper Number AUD 30-24

CONFIDENTIAL

ARAC 17th October 2024

Cyber Security Update

[AUD 31-24]

CAF-Aligned DSPT 2024-2025 ARAC Overview

Sam Mortimer

October 24

HTA
Human Tissue Authority

HTA
Human Tissue Authority

CAF DSPT Changes

CAF alignment to DSPT Changes

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 started for large organisations. NHS Trusts, CSUs, **ALBs** and ICBs see a different interface when they log in to the NHS portal. They are reporting compliance against 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 Information Governance (IG) controls are reasonably comparable to the current DSPT, and have been tightened only in areas where NHSE and DHSC believe the higher standard is a necessary obligation

Why is the DSPT changing?

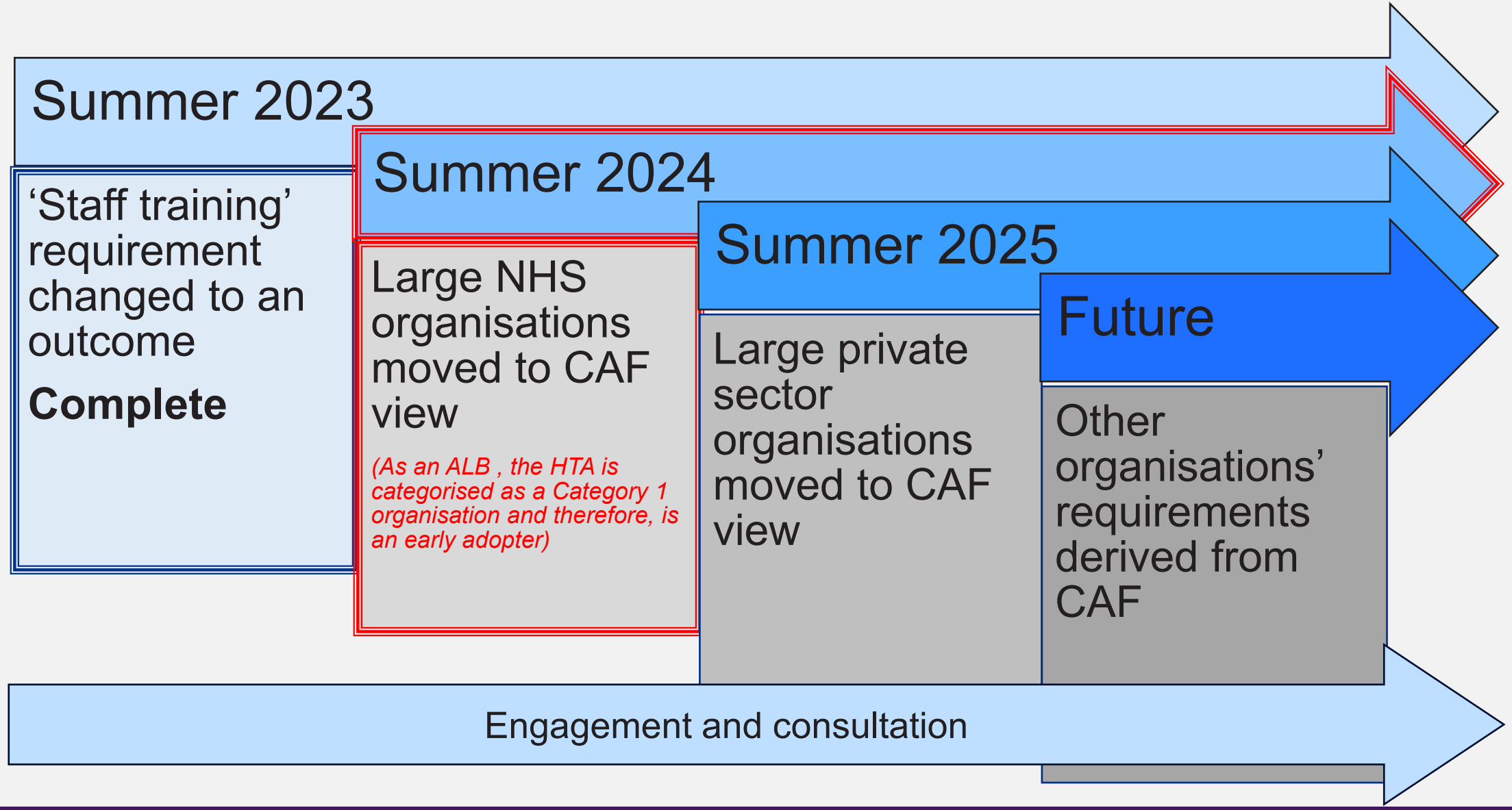
HTA
Human Tissue Authority

The goals of moving to the CAF aligned DSPT are to:

- ☑ Emphasise good decision-making over compliance, with better understanding and ownership & management of information risks at the local organisation level
- ☑ Support a culture of evaluation and improvement, organisations will need to understand the effectiveness of their practices to meet the desired outcomes, and expend effort on what works
- ☑ Create opportunities for better practice, by enabling organisations to remain current with new security measures to meet new threats and risks

Staged approach to move from DSPT to CAF

HTA
Human Tissue Authority



How this impacts on the HTA

Preparatory work has already started to achieve CAF aligned DSPT timescales:

Deadline	Action	Notes
Sep 24	Cyber Assurance Framework (CAF) adopted	Commenced
31 Dec 24	Baseline assessment	Brought forward from Feb 25
~ Apr / May 25	GIAA Internal Audit	CAF ToR under development
30 Jun 25	Final Assessment	

HTA
Human Tissue Authority

CAF Structure

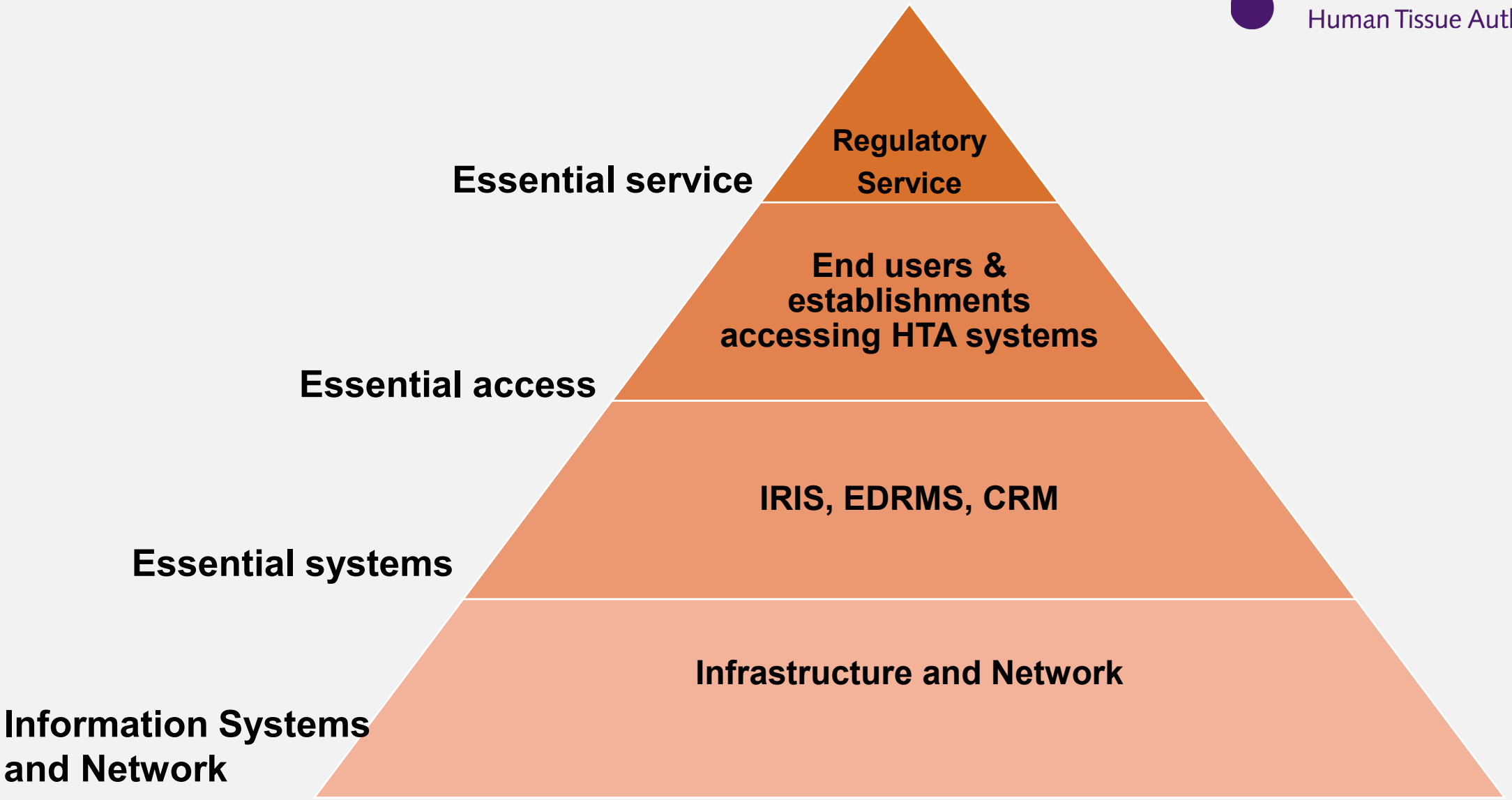
CAF Structure Definitions

HTA Human Tissue Authority

Structure	Purpose
Objectives (x 5)	Overarching goals of the organisation's cyber security and information governance (IG) activities
Principles (x 18)	Concepts which underpin the organisation's cyber security and IG 'objectives
Outcomes (x 47)	Contributing outcomes, key markers against which the organisation will judge the effectiveness of your cyber security and IG practices. These are the key element of the toolkit which you will be prompted to record results against. The combination of all recorded 'contributing outcome' results will determine whether your organisation has achieved 'standards met'
Expected achievement levels	Each outcome has a minimum achievement level set for the standard to be met. Expected achievement were determined by NHSE & DHSC to ensure that standards are no less stringent than the 2024-25 DSPT
Indicators of Good Practice (IPG)	Concrete examples of procedures and processes which help to inform the organisation's decision about whether it has achieved a contributing outcome. Each contributing outcome, will show indicators of good practice and the option to select 'Not achieved', 'Partially achieved' or 'Achieved'.

Essential HTA Service Model

HTA
Human Tissue Authority



Essential Functions Criteria

HTA
Human Tissue Authority

If **ANY** of these conditions apply to HTA information, assets, systems & networks, they **are** classified as essential functions:

- ❑ Supports the provision of our essential service
- ❑ Holds personal data
- ❑ If compromised by an incident, could have a cascading impact across other systems and networks

HTA
Human Tissue Authority

CAF compliance: Objectives, Principles & Outcomes

CAF Structure

5 Objectives grouped into 18 principles

47 Outcomes evidenced

- **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

Principle: B6 Staff Awareness and Training

Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the operation of essential functions.

Outcome

B6.a Cyber Security Culture

You develop and maintain a positive cyber security culture.

Indicators of Good Practice

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
People in your organisation don't understand what they contribute to the cyber security of the essential function. People in your organisation don't know how to raise a concern about cyber security. People believe that reporting	Your executive management understand and widely communicate the importance of a positive cyber security culture. Positive attitudes, behaviours and expectations are described for your organisation. All people in your organisation understand the contribution	Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff. Your organisation displays positive cyber security attitudes, behaviours and expectations People in your organisation

Objective A - Managing Risk

HTA Human Tissue Authority

Expectations for Standards met:

CAF element		Profile		
Principle	**Outcome**	**NA**	**PA**	**A**
Objective A - Managing risk				
Governance	A1.a Board Direction			A
	A1.b Roles and Responsibilities			A
	A1.c Decision-making			A
Risk Management	A2.a Risk Management Process		PA	
	A2.b Assurance			A
Asset Management	A3.a Asset Management			A
Supply Chain	A4.a Supply Chain		PA	

Total:	4	7	0	2	5

Objective B - Protecting against cyber-attack & data breaches

Expectations for Standards met:

CAF element		Profile		
Principle	**Outcome**	**NA**	**PA**	**A**
Objective B - Protecting against cyber attack and data breaches				
Service Protection Policies and Processes	B1.a Policy and Process Development		PA	
	B1.b Policy and Process Implementation		PA	
Identity and Access Control	B2.a Identity Verification, Authentication and Authorisation		PA	
	B2.b Device Management	NA		
	B2.c Privileged User Management	NA		
	B2.d Identity and Access Management (IdAM)		PA	
Data Security	B3.a Understanding Data		PA	
	B3.b Data in Transit		PA	
	B3.c Stored Data		PA	
	B3.d Mobile Data		PA	
	B3.e Media / Equipment Sanitisation		PA	
System Security	B4.a Secure by Design		PA	
	B4.b Secure Configuration		PA	
	B4.c Secure Management		PA	
	B4.d Vulnerability Management		PA	
Resilient Networks and Systems	B5.a Resilience Preparation		PA	
	B5.b Design for Resilience	NA		
	B5.c Backups			A
Staff Awareness and Training	B6.a Cyber Security Culture		PA	
	B6.b Cyber Security Training			A
Total:	**6**	**20**	**3**	**15**	**2**

Objective C - Detecting cyber security events

HTA Human Tissue Authority

Expectations for Standards met:

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		
Total:	**2**	**7**	**3**	**4**	**0**

Objective D - Minimising the impact of incidents

HTA Human Tissue Authority

Expectations for Standards met:

CAF element		Profile		
Principle	**Outcome**	**NA**	**PA**	**A**
Objective D - Minimising the impact of incidents				
Response and Recovery Planning	D1.a Response Plan		PA	
	D1.b Response and Recovery Capability			A
	D1.c Testing and Exercising			A
Lessons Learned	D2.a Incident Root Cause Analysis			A
	D2.b Using Incidents to Drive Improvements			A
Total:	**2**	**5**	**0**	**1**	**4**

Objective E - Using and sharing information appropriately

Expectations for Standards met:

CAF element		Profile		
Principle	**Outcome**	**Not Achieved (NA)**	**Partially Achieved (PA)**	**Achieved (A)**
Objective E - Using and sharing information appropriately				
Transparency	E1.a Privacy and transparency information		PA	
Upholding the rights of individuals	E2.a Managing data subject rights under UK GDPR			A
	E2.b Consent			A
	E2.c National data opt-out policy			A
Using and sharing information	E3.a Using and sharing information for direct care			A
	E3.b Using and sharing information for other purposes			A
Records management	E4.a Managing records			A
	E4.b Clinical coding			A
Total:	**4**	**8**	**0**	**1**	**7**

Not applicable for HTA