Control Serial Number	Control Objective Source	Overarching Control Objective:	Detailed Control Objective Including Justification	Control Guidance		Response to Control Objective Response options are YES, PARTIAL, NO , or N/A		Narrative to support Control Objective response (if PARTIAL, NO or N/A in columns G and/or H)	Document Reference (Name, Version, Page, paragraph) - please supply referenced documents	Accreditor's response/ recommendation
				MEDIUM	HIGH	MEDIUM	HIGH			
1	ISO 27001 6.2	*This column has been redacted citing S41&S43*								
			This column has been redacted citing S41&S43	*This column has been redacted citing S41&S43*	*This column has been redacted citing S41&S43*	N/A	Not Required	Essentially the PCA service is SaaS and is not cloud hosted. Pervade support and management arrangements of the central environment are reviewed through the assurance of Pervade, not this CCSS. Remote support of the PCA agent by Pervade, which is hosted in a Force DMZ is discussed in detail in the IRAR. PCA does not process any data classified as HIGH.	See IRAR for further detail on architectural principles and supporting documentation.	
						N/A	Not Required			
						Not Required	N/A			
						Yes	Not Required			
						Not Required	Yes			
						Yes	Not Required			
						Not Required	Yes			
						N/A	Not Required			
						Yes	Not Required			
						Not Required	Yes			
						Yes	Not Required			
						Not Required	Yes			
						N/A	Not Required			
						N/A	Not Required			
						Not Required	N/A	Essentially the PCA service is SaaS and is not cloud hosted. Pervade support and management arrangements of the central environment are reviewed through the assurance of Pervade, not this CCSS. Remote support of the PCA agent by Pervade, which is hosted in a Force DMZ is discussed in detail in the IRAR. PCA does not process any data classified as HIGH.	See IRAR for further detail on architectural principles and supporting documentation.	
						N/A	Not Required			
						Not Required	N/A			

Control Serial Number	Control Objective Source	Overarching Control Objective:	Detailed Control Objective Including Justification	Control Guidance		Response to Control Objective Response options are YES, PARTIAL, NO , or N/A		Narrative to support Control Objective response (if PARTIAL, NO or N/A in columns G and/or H)	Document Reference (Name, Version, Page, paragraph) - please supply referenced documents	Accreditor's response/ recommendation
				MEDIUM	HIGH	MEDIUM	HIGH			
						Yes	Not Required			
						Not Required	Yes			
						Not Required	N/A			
						Yes	Not Required			
						Yes	Not Required			
						Not Required	Yes			
						Yes	Not Required			
						Not Required	Yes			
						Yes	Not Required			
						N/A	Not Required			
						N/A	Not Required			
						N/A	Not Required			

Control Serial Number	Control Objective Source	Overarching Control Objective:	Detailed Control Objective Including Justification	Control Guidance		Response to Control Objective Response options are YES, PARTIAL, NO , or N/A		Narrative to support Control Objective response (if PARTIAL, NO or N/A in columns G and/or H)	Document Reference (Name, Version, Page, paragraph) - please supply referenced documents	Accreditor's response/ recommendation
				MEDIUM	HIGH	MEDIUM	HIGH			
2	ISO 27017 5.1					N/A	Not Required	Essentially the PCA service is SaaS and is not cloud hosted. Pervade support and management arrangements of the central environment are reviewed through the assurance of Pervade, not this CCSS. Remote support of the PCA agent by Pervade, which is hosted in a Force DMZ is discussed in detail in the IRAR. PCA does not process any data classified as HIGH.		
						N/A	Not Required			
3	ISO 27001 7					Yes	Not Required	Covered in the Pervade contract	Available on request.	
						Not Required	Yes			
4	ISO 27001 8.1					N/A	Not Required	SaaS		
						Not Required	N/A	SaaS		
						N/A	Not Required	Not Cloud		
5	ISO 27001 8.3					N/A	Not Required	SaaS - Covered through assurance of supplier.	See IRAR supporting doc's, i.e. Supplier Assurance Questionnaire.	
						Not Required	N/A	SaaS - Covered through assurance of supplier.		
6	ISO 27001 9.1					Yes	Not Required		See IRAR - provides detail.	
						Not Required	Not Required	Not Cloud		

Control Serial Number	Control Objective Source	Overarching Control Objective:	Detailed Control Objective Including Justification	Control Guidance		Response to Control Objective Response options are YES, PARTIAL, NO , or N/A		Narrative to support Control Objective response (if PARTIAL, NO or N/A in columns G and/or H)	Document Reference (Name, Version, Page, paragraph) - please supply referenced documents	Accreditor's response/ recommendation
				MEDIUM	HIGH	MEDIUM	HIGH			
						Not Required	Not Required	Not Cloud		
7	ISO 27001 9.4					Yes	Not Required		Assurance Questionnaire in IRAR	
						Yes	Not Required			
						Yes	Not Required			
						N/A	Not Required	Not CLOUD		
						Not Required	N/A			
8	ISO 27017 9.4					N/A	Not Required	Not CLOUD		
9	ISO 27001 10					Yes	Not Required		See IRAR for further detail.	
						Not Required	Yes			
						N/A	Not Required	Not LOUD		
						Not Required	N/A			
						Not Required	N/A			
10	ISO 27001 11							Pending PASF from NPIRMT (Post Covid). Data Centre is ISO27001 and 90001 certified.		
						N/A	N/A	SaaS - Addressed through Supplier Assurance	See Supplier Assurance Questionnaire in IRAR	
								Pending PASF from NPIRMT (Post Covid). Data Centre is ISO27001 and 90001 certified.		
11	ISO 27001 12.3					Yes	Yes	SaaS - Addressed through Supplier Assurance	See Supplier Assurance Questionnaire in IRAR	

Control Serial Number	Control Objective Source	Overarching Control Objective:	Detailed Control Objective Including Justification	Control Guidance		Response to Control Objective Response options are YES, PARTIAL, NO , or N/A		Narrative to support Control Objective response (if PARTIAL, NO or N/A in columns G and/or H)	Document Reference (Name, Version, Page, paragraph) - please supply referenced documents	Accreditor's response/ recommendation
				MEDIUM	HIGH	MEDIUM	HIGH			
12	ISO 27001 12.4					N/A	Not Required	SaaS - Addressed through Supplier Assurance	See Supplier Assurance Questionnaire in IRAR	
						Not Required	N/A	SaaS - Addressed through Supplier Assurance	See Supplier Assurance Questionnaire in IRAR	
						N/A	N/A	SaaS - Addressed through Supplier Assurance	See Supplier Assurance Questionnaire in IRAR	
						N/A	Not Required	Not Cloud		
13	ISO 27001 12.6					N/A	N/A	SaaS - Addressed through Supplier Assurance	See Supplier Assurance Questionnaire in IRAR	
						N/A	N/A	SaaS - Addressed through Supplier Assurance	See Supplier Assurance Questionnaire in IRAR	
14	ISO 27001 13.1					N/A	Not Required	SaaS - Addressed through Supplier Assurance	See Supplier Assurance Questionnaire in IRAR	
						Not Required	N/A			
						N/A	N/A			
						N/A	N/A			
						Not Required	N/A			
						N/A	N/A			
						N/A	N/A			
						N/A	N/A			
15	ISO 27001 13.2					Yes	Yes		**Embedded Doc - 2021.04.26 PDS Information Risk Assessment Report v1.0 (PCA) (Embedded doc 4 - Data Sharing Agreement)**	

CANDIDATE CONTROL SET FOR SERVICES (CCSS)

The CCSS is based on the BS ISO/IEC 27001:2013 Information Security Management System (ISMS) requirements and is intended to provide guidance to National Accreditors, Project Managers and Information Assurance personnel involved in the design and delivery of National Policing systems as to the controls considered essential in providing assurance of the adequate protection of Policing data. Application of the controls identified within the CCSS should assist projects in understanding where gaps may exist and enable efficient resource direction.

The CCSS can also be applied to force or regional system and is recommended for programmes co ordinated by NPCC

Additional benefit for programmes, projects and delivery teams following the CCSS methodology is gained through achieving the essential BS ISO/IEC 27001:2013 project management controls:

6.1.5 - Information Security in Project Management
18.2.2 - Compliance with Security Policies and Standards
18.2.3 - Technical Compliance Review

The CCSS is an annex to the guidance on 'Handling of Policing Data within OFFICIAL' paper and should be read in conjunction with it.

The CCSS does not cover any requirements relating to end user devices. The latter is covered by the Governance and Information Risk Return (GIRR).

GUIDANCE ON COMPLETION OF THE CANDIDATE CONTROL SET FOR SERVICES

The CCSS requires explicit response against 15 controls to ensure a consistent baseline level of assurance. Some controls are applicable to services mainly handling MEDIUM data, some controls will be applicable to systems mainly handling HIGH data and some controls may be applicable to both data types, but with different control standards identified in columns G and H. An option from Columns G/H should be selected to confirm whether a control objective is MET, PARTIALLY MET, NOT MET or N/A. If the response in the column(s) is MET then additional information is not required. However, if the response in the column(s) is PARTIALLY MET, NOT MET or N/A then additional information must be provided in column I.

Column J should be completed to reference where evidence of a control being MET or PARTIALLY MET may be found.

With 2 sets one at MEDIUM and another at HIGH it is important to note they must be treated independantly and do not build upon each other.

It is expected that other controls and standards listed under common assumptions are also met. Where this is not the case you must explicitly confirm which controls are not met and provide a brief explanation.

If designing a system hosted on a force network the GIRR controls should be referred to in addition to the CCSS controls.

Completed CCSS should be submitted to the National Accreditor for Police Systems responsible for the National Police system. Copies of the documents referenced in column J should be supplied with the CCSS.

Assumptions

It is assumed, and documents may be requested to provide evidence (or audits may be conducted) to check that assumptions have been met. The service owner will need to sign off against these assumptions as part of the ongoing Accreditation of the service.

1 Relevant international standards from the ISO 27000 series have been considered and applied in the development appropriate controls.

2 An Information Security Management system as defined by ISO27001 (or equivalent) has been implemented to support the service through out it's life cycle.

3 Relevant NCSC and Cabinet Office guidance and standards have been considered in the design, development and ongoing support of the solution

4 Relevant NIST security standards have been considered in the development, design and ongoing support of the solution.

5 Relevant legislation has been considered in the security design (e.g. DPA, FOI, RIPA, PACE, POFA, etc.)

6 National Policing policies, standards and guidance (e.g. National Vetting Policy, MOPI, PASF, etc.) have been considered and applied where applicable.

7 Accreditation/Assurance documentation, such as risk assessment, risk mitigation, residual risk acceptance and IRAR, have been produced for the service.

8 As a minimum an ITHC should be undertaken before go live, on an annual basis and when new functionality is introduced in agreement with the service Accreditor with remediations implemented as agreed by the accreditor

9 Business Continuity and Disaster Recovery planning and testing has been implemented to ensure the service level requirements.

10 Controls have been implemented to support any investigation of either misuse of access or compromise of the service i.e. forensic readiness.