Privacy and security impact assessment (PSIA)

Crimson

1. Project overview

1.1 Summary

Provide a summary of the project including any relevant background information and the key aims/objectives that the project must achieve.

Project ID:	BDG – 0013
Project Title:	Casework migration from Meridio
Project Manager:	Jenny Manock
Purpose and Aims:	Criminal investigation tool to allow investigations, especially those large in size to be conducted and managed.

Project ID:	BDG – 0160
Project Title:	Procurement of Investigation tool
Project Manager:	Sue Shepherd
Purpose and Aims:	Re-procurement of Criminal investigation tool for investigations

Formatted: Font: 11 pt

1.2 Describe the information flows

Describe the collection, creation, storage, use, transfer and disposal of information. You may find it useful to refer to a flow diagram or another way of explaining information flows. You should also say how many individuals are likely to be affected by any project that involves the processing of personal data.

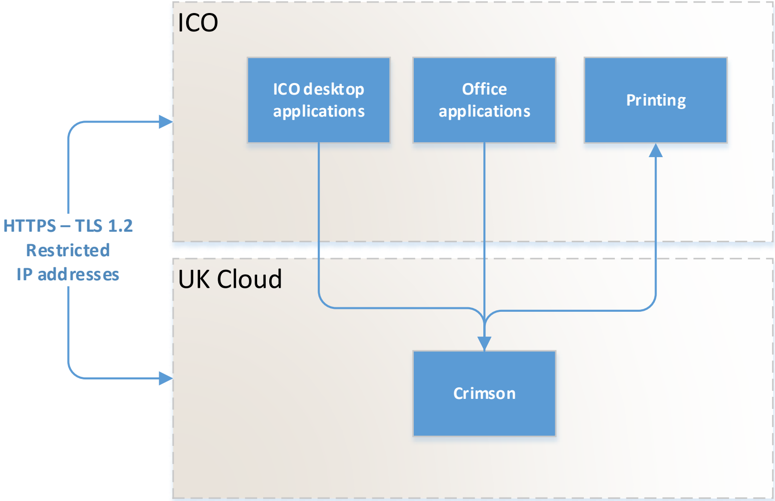
Crimson is an investigation management software solution designed to support investigators working in the public and private sector. It delivers an intelligent secure database for any type of organisation that has a need to investigate incidents, allegations or any type of criminal activity.

From complex investigations to straightforward lower level crime management, Crimson will support every stage of the investigative process.

Crimson will be hosted in the Cloud by UK Cloud, utilising Skyscape – please see attached document for privacy and security specification.

Crimson will be accessed through a web browser from the ICO network by members of the criminal investigations team. Crimson does not allow for the editing of documents within the tool. We will editing the documents such as witness statements and then uploading these once the first draft is ready. We will upload any subsequent versions as well. Documents can be deleted from Crimson by those with a certain security privilege. We will create business process which will be followed by the Criminal Investigation team around the management of documents.

The diagram below shows the information flows.



1.3 Describe the consultation process

Explain what practical steps you will take to ensure that you identify and address the privacy and security risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the PSIA process.

We have consulted our ICO IT assurance team. They have provided advice about how to ensure we have reviewed risks relevant to the solutions we are developing. They have provided input into this document at several points. They have also reviewed our mitigations, and our evaluation of those mitigations.

ICO have due diligence controls in place such as supplier assessments and legal contracts. A supplier assessment has been conducted and completed satisfactorily by Crimson. The contract will be signed off by our external legal advisors and signed by both parties before implementation.

2. Initial assessment

The purpose of the initial assessment is to determine the project's risk profile and whether further assessment is required to identify, assess and manage risks.

2.1 Privacy questions

ID	Screening question	Yes/No
1.	Will the project involve the collection of new information about individuals?	N
	Comments: There is no change to the information being collected by an investigation.	
2.	Will the project compel individuals to provide information about themselves?	N
	Comments: There is no change to the information being collected by an investigation.	
3.	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Y
	Comments: Information will be hosted by UK Cloud and may be accessed by UK Cloud for the purposes of service provision and maintenance.	
4.	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N
	Comments: There is no change to the information being collected by an investigation.	
5.	Does the project involve using new technology which might be perceived as being privacy intruding for example biometrics or facial recognition?	N
	Comments: The project does not introduce new technology which will cause intrusive privacy issues.	

6.	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	N
	Comments: The tool may allow information to be collated and viewed in a different way, but this will not change the decisions or action we take.	
7.	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example health records, criminal records, or other information that people are likely to consider as private?	Y
	Comments: The information will relate to criminal investigations.	
8.	Will the project require you to contact individuals in ways which they may find intrusive?	N
	Comments: There will be no changes to the way we contact individuals.	

2.2 Security questions

ID	**Screening question**	**Yes/No**
1.	Will the service involve the processing and storage of large volumes (eg more than 100,000) of hardcopy and/or digital records?	Y
	Comments: Although this is a short term solution, some investigations will contain large volumes of digital records. We won't be migrating data so the number of records will start small and grow over time.	
2.	Will the service involve the processing and storage of very sensitive hardcopy and/or digital information classified above OFFICIAL?	N
	Comments: Information held in the system will be Official.	
3.	Will the service involve the addition of multiple components to the core network (eg hardware, software, etc.)?	N
	Comments: There is one new application, this will not be hosted by the ICO and will be accessed through a web browser.	

4.	Will the service be delivered by multiple suppliers?	Y
	Comments: Crimson will deliver the software and UK Cloud with host the service.	
5.	Will the service be externally hosted with multiple external connections to suppliers?	N
	Comments: It will be one external connection to UK Cloud.	
6.	Will the service involve the processing and storage of hardcopy records and digital storage media outside our secure premises?	N
	Comments: The data will be hosted by UK Cloud, utilising Skyscape.	

3. Further assessment

Identify the key privacy and security risks. Larger-scale PSIAs might record this information on a more formal risk register.

3.1 Identify the privacy risks

Privacy issue	Risk to individuals	Compliance risk	Corporate risk
Collection and use Collection and use of data is unfair and unlawful.	Adverse impact to individuals' privacy.	Breach of legal and regulatory responsibilities (eg principles 1 and 2 of DPA).	Reputational damage and fines.
Data quality Collection, use and retention of poor quality data.	Adverse impact to individuals' privacy.	Breach of legal and regulatory responsibilities (eg principles 3, 4 and 5 of DPA).	Reputational damage and fines.
Individual rights Data processed without regard for statutory rights.	Adverse impact to individuals' privacy.	Breach of legal and regulatory responsibilities (eg principles 6 of DPA).	Reputational damage and fines.
Data security Confidentiality, integrity and availability of data compromised.	Adverse impact to individuals' privacy.	Breach of legal and regulatory responsibilities (eg principles 7 of DPA).	Reputational damage and fines.
Overseas transfers Data transferred to jurisdiction that doesn't adequately protect statutory rights and freedoms.	Adverse impact to individuals' privacy.	Breach of legal and regulatory responsibilities (eg principle 8 of DPA).	Reputational damage and fines.

3.2 Identify the security risks

The CESG/NCSC guidance for use of Cloud services identifies areas of risk and provides guidance on assessing and mitigating these. The 14 Cloud Security Principles cover all aspects of using a Cloud service and are sufficient to cover the scope of the UK Cloud, utilising Skyscape services.

Risks against the CESG 14 Cloud Security Principles

Security issue	Risk to information	Compliance risk	Corporate risk
Data protection in-transit Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.	If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Asset protection and resilience Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.	If this principle is not implemented, inappropriately protected consumer data could be compromised.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Separation between consumers Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.	If this principle is not implemented, service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.

Security issue	Risk to information	Compliance risk	Corporate risk
Governance framework The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.	If this principle is not implemented, any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Operational security The service provider should have processes and procedures in place to ensure the operational security of the service.	If this principle is not implemented, the service can't be operated and managed securely in order to impede, detect or prevent attacks against it.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Personnel security Service provider staff should be subject to personnel security screening and security education for their role.	If this principle is not implemented, the likelihood of accidental or malicious compromise of consumer data by service provider personnel is increased.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Secure development Services should be designed and developed to identify and mitigate threats to their security.	If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.

Security issue	Risk to information	Compliance risk	Corporate risk
Supply chain security The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.	If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Secure consumer management Consumers should be provided with the tools required to help them securely manage their service.	If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications and data.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Identity and authentication Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.	If this principle is not implemented, unauthorised changes to a consumer's service, theft or modification of data or denial of service may occur.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
External interface protection All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.	If this principle is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.

Security issue	Risk to information	Compliance risk	Corporate risk
Secure service administration The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.	If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Audit information provision to consumers Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.	If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Secure use of the service by the consumer Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.	If this principle is not implemented, the security of cloud services and the data held within them can be undermined by poor use of the service by consumers.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.

4. Identify solutions

Describe the actions you could take to reduce the risks and any future steps that will be necessary (eg the production of new guidance or security testing for new systems).

4.1 Privacy solutions

Risk	Solution(s)	Result	Justified, compliant and proportionate response
Collection and use Collection and use of data is unfair and unlawful.	We process personal data for specified and lawful purposes, and make fair processing information available to individuals. The service will not affect the categories or specified purposes for which we process personal data. We will produce policies and procedures on how information and records should be managed within SharePoint and Crimson. We will provide training and guidance to ensure staff are aware of how data should be used.	Treated Residual risk of human error	Yes
Data quality Collection, use and retention of poor quality data.	We have processes to ensure the data we collect and use is adequate, accurate and not kept for longer than is necessary. The service will not affect data quality. Where appropriate, controls in place to prevent inappropriate disclosures of personal data. We will provide training and guidance to ensure staff are aware of how documents/records should be managed. Retention will be applied to data in line with our	Treated Residual risk of human error	Yes

	retention and disposal schedule.		
Individual rights Data processed without regard for individuals' rights.	We have processes to recognise and respond to information requests. The service will not abrogate individuals' rights.	Treated	Yes
Data security Confidentiality, integrity and availability of data compromised.	The service will provide appropriate security in line with the government's Cloud Security Principles. Please refer to section 4.2 for detail. Any processing of personal data by the provider must be carried out under contract in compliance with principle 7 of the DPA; and, include provisions regarding control of the data in the event we want to terminate or transfer the service. The security model will only allow users to see data they have privileges to see. We will create user groups with set privileges. Users will then be assigned to these groups. A list of these groups and their privileges will be part of the business procedures and included in the SDD. We have attributed responsibility for creation and removal of users to IT help. This will be incorporated into the starters, movers and leaver's procedure. Managers within Criminal Investigations will be responsible for granting read and editing access from the list of users to incidents and investigations within Crimson. Auditing within the system will be switched on. This will record any changes to the system. This information will	Treated	Yes

Formatted: Font color: Auto

Formatted: Font color: Auto

	be viewable within the system. Viewing of information within Crimson is also recorded within the system, this information can be retrieved upon request by IT administrators. Where information has been added to Crimson in error, only the system administrators have permission to delete information from the system~~Where information has been added to Crimson in error, a request will be sent to IT help to ask for this to be removed. Only the Administrator group has permission to delete information from the system~~.		
Overseas transfers Data transferred to jurisdiction that doesn't adequately protect statutory rights and freedoms.	The service will not process personal data outside the EEA, and UK data centres will be used wherever possible. Please refer to section 4.2 for detail.	Treated	Yes

4.2 Security solutions

Risk	Solution(s)	Result	Compliant and Proportionate?
Data protection in-transit If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.	**Protection between our end user devices and the service:** Crimson is accessed using HTTPS over TLS 1.2. Any documents that are uploaded are transferred using the same protocols and assurances. Cryptographic protocols in place are TLS 1.2. We will use Internet explorer 11 or above to access Crimson. Crimson will be accessed over the internet (HTTPS) but with access restricted to specific IP addresses. **Internal protection within the service:** Assured (formerly IL0-IL2) services: traffic transiting within the service (e.g. between UKCloud's data centres) is protected using resilient fibre optic connections which have been independently validated by the CESG Assured Service – Telecoms (CAS-T) scheme. Service has been tested within regular PGA scoped IT Security Health Checks conducted by a "Green Tick" CHECK service provider. **Between the service and other services:** UKCloud also has a range of products such as "Secure Remote Access" and "Walled Garden" which further facilitate the secure transit of data between services. Further, UKCloud has designed and implemented a secure API proxy service to protect exposed APIs which reduces the vulnerabilities inherent to some standards-based APIs.	Treated	Yes

Risk	Solution(s)	Result	Compliant and Proportionate?
Asset protection and resilience If this principle is not implemented, inappropriately protected consumer data could be compromised.	**Data location:** All data centres and data management used by UKCloud are in the UK-domain and have certification assessments to ISO27001. **Data centre security:** Independent validation physical security of data centres complies with ISO27001 to help prevent unauthorised access, theft or compromise of systems. **Data protection at rest:** UKCloud uses physical access controls to satisfy this requirement. Storage media which may contain customer data is physically contained with the dedicated, secure data suites inside the data centres used by UKCloud. Crimson backups are stored in UK Cloud but in a secondary data centre, also hosted in the UK. UKCloud complies with ISO027001 for all their data centres. **Secure deletion:** UKCloud undertakes "other secure erasure processes" to satisfy this requirement. The UKCloud Asset Management Policy (UKC-POL-24) mandates that all equipment (hardware and software assets) no longer required or subject to replacement must be subject to (a) secure disposal, or (b) secure cleansing prior to re-use. More specific information is provided within the UKCloud Secure Data Erasure Policy (UKC-POL-32), which details all aspects of data sanitisation including specific cloud service approaches for redeployment of resources (e.g. when a customer stops using a cloud service).	Treated	Yes

Risk	Solution(s)	Result	Compliant and Proportionate?
Separation between consumers If this principle is not implemented, service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.	UKCloud's services are provided as a "community cloud", one which is provisioned for the exclusive use of a specific community of consumers from organisations that share concerns (e.g. data sovereignty, security requirements, compliance considerations etc.). UKCloud only provides its cloud services to validated UK public sector organisations. Consumers are robustly separated within the service at multiple layers. At the network layer, each consumer is assigned an exclusive range of public IP addresses. All traffic into and out of the service as well as traffic within the service (i.e. between customers on the platform) is protected by an UKCloud managed firewall as well as the consumer's self-managed virtual firewall. Crimson is part of a multi-tenanted server environment within UKCloud. Separation between customers is ensured with completely individual databases dedicated to the customer along with dedicated credentials. Service has been tested within regular PGA scoped IT Security Health Checks conducted by a "Green Tick" CHECK service provider.	Treated	Yes

Risk	Solution(s)	Result	Compliant and Proportionate?
Governance framework If this principle is not implemented, any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments.	UK Cloud complies with the ISO-27001 information security standard, covering the scope of the service delivered. This requires them to have a secure organisation in plan e.g. roles, responsibilities, policies and procedures; risk management, legal and regulatory compliance in place. UK Cloud is regularly audited by independent external auditors who are recognized by UKAS. WPC Software (Crimson) is certified against Cyber Essentials Plus, although we are not currently certified against ISO27001. Last year they introduced an ISMS, totally based upon ISO27001, and are looking to formally complete certification later this year. This means they have self-assertion in place to ensure that governance goals are met with a commitment to achieve certification to a recognised standard. Independent validation that governance goals are being met by WPC is shown through their compliance with recognised standards in place for UK Cloud. At the time of re-procurement, October 2019, WPC Software confirmed they were now certified to ISO 27001 for their SaaS services, of which Crimson is a part.	Treated	Yes
Operational security If this principle is not implemented, the service cannot be operated and managed securely in order to impede, detect or prevent attacks against it.	Configuration, change management, incident response and protective monitoring are all demonstrated by UK Cloud's compliance with the ISO-27001 (information security standard). UK Cloud is tested via a PGA scoped IT Security Health Check conducted by a "Green Tick" CHECK service provider.	Treated	Yes

Formatted: Font: 10 pt, Font color: Auto

Formatted: Font: 10 pt, Font color: Auto

Risk	Solution(s)	Result	Compliant and Proportionate?
Personnel security If this principle is not implemented, the likelihood of accidental or malicious compromise of consumer data by service provider personnel is increased.	All employees and contractors (if applicable) are required to have BPSS clearance as a minimum as part of the recruitment checks. This is appropriate for access to Official information. Evidence of the status of personnel security clearances can be provided by assertion from the UKCloud SIRO, and has previously been validated by the CESG Pan Government Accreditor.	Treated	Yes

Risk	Solution(s)	Result	Compliant and Proportionate?
Secure development If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.	**UK Cloud** UKCloud has implemented and follows an agile development methodology, prioritisation for the development of features is evaluated based upon risk and customer impact. UKCloud's Development Teams use Test Driven Development (TDD) practices where applicable. Software can only be released to production servers once it has been approved by the Change Approval Board (CAB) and customers are then advised of the pending release. All release activities are protected by rollback plans to a previous version. Evidence of the software configuration management, including the policies and related procedures has been evidenced during external assessments of UKCloud's ISO20000 certification undertaken by LRQA. The activities surrounding coding, testing and deployment have been independently validated by a CESG Pan Government Accreditor scoped IT Security Health Check, conducted by a "Green Tick" CHECK service provider. **Crimson** All development is undertaken through a defined software development lifecycle, outlined through our Quality Management System (accredited to ISO9001). Information security is a key component at each stage of our software development lifecycle is aligned to OWASP principles where possible. Regular penetration tests are performed and results of these available to customers as required. Crimson's development environment is included within the scope of their Cyber Essentials Plus accreditation. Crimson will provide a build/handover documentation.	Treated	Yes

Risk	Solution(s)	Result	Compliant and Proportionate?
Supply chain security If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.	UKCloud require any suppliers to comply with ISO27001 and each partner is to complete and submit a security controls framework and declaration, which illustrate this on an annual basis. UKCloud's Compliance Team also undertakes ad-hoc (including unannounced) on-site inspections with Alliance Partners to validate their submissions and ongoing adherence to security best practice. Evidence of third party security capabilities been evidenced during external assessments of UKCloud's ISO9001 and ISO27001 certifications, undertaken regularly by LRQA. Additionally, many "Alliance Partner" suppliers have previously been subject to on-site assessments and submission validations undertaken directly by the CESG Pan Government Accreditor.	Treated	Yes
Secure consumer management If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications and data.	UKCloud has implemented and operates a number of technical controls to ensure only authorised individuals are able to authenticate to and access the UKCloud services for which they have an identified and approved business need. As part of the implementation plan ICO will agree with Crimson the names of users that are able to log calls and request changes. We can also operate a password policy for this if required.	Treated	Yes

Risk	Solution(s)	Result	Compliant and Proportionate?
Identity and authentication If this principle is not implemented, unauthorised changes to a consumer's service, theft or modification of data or denial of service may occur.	UKCloud has implemented a secure Customer Portal for graphical administration, alongside API functionality for programmatic control of the customer's environment. Combined, both sets of features ensure that customers are only able to access their own virtualised environments, and have no means of accessing other customer environments. User access requires their unique username, password and characters from their memorable word, and separate access processes are required for the Assured and Elevated Platforms. UKCloud personnel additionally are required to use 2FA authentication tokens. The authentication of users and the levels of access which they have are regularly assessed as part of external audits of UKCloud's ISO27001 certification, undertaken by LRQA. User's accessing Crimson will require a two-step authentication process, where a user is required to log-in to access the service prior to logging into the application itself.	Treated	Yes
External interface protection If this principle is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it.	Crimson will be accessed over the internet (HTTPS) but with access restricted to specific IP addresses. These external services are dynamically routed across independent connections into each site. All connections are protected with UKCloud managed physical firewalls, and are configured in strict accordance with the Codes of Connections specified by the provider of each secured network. Service has been tested within regular PGA scoped IT Security Health Checks conducted by a "Green Tick" CHECK service provider.	Treated	Yes

Risk	Solution(s)	Result	Compliant and Proportionate?
Secure service administration If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.	UKCloud has adopted ITIL v.3 as its service management framework, and has aligned component processes within the workflows of its service desk software. Service management activities are managed and operated within separate, isolated networks for the Assured Platform. Access to this network is provided via a secure connection from the UKCloud support network, using a dedicated server only accessible to SC cleared Support Analysts. The separation and security of the service management framework has been validated as part of UKCloud's regular IT Security Health Check activities, undertaken by a "Green Tick" CHECK service provider. In addition, the effectiveness and compliance of the individual ITIL processes are regularly assessed by LRQA during their surveillance audits required by the UKCloud ISO20000 certification.	Treated	Yes
Audit information provision to consumers If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.	In accordance with the NIST defined characteristics of cloud computing, UKCloud's on-demand services have been engineered to provide customers with self-service functionality, and offer: (a) Account logs – reports which outline service consumption, incident management tickets, change management tickets and service requests which are applicable to a customer's account. (b) Audit logs – reports which detail all authentication requests by username and IP address with date and time stamps for each customer's account. (c) Firewall logs – exposing customer firewall log data which capture firewall rule breaches and traffic activities passing through the customer's virtual firewall (vShield Edge). Crimson records all changes made within the software in an Audit log. This is accessible to users of the system if they have the appropriate permissions.	Treated	Yes

Risk	Solution(s)	Result	Compliant and Proportionate?
Secure use of the service by the consumer If this principle is not implemented, the security of cloud services and the data held within them can be undermined by poor use of the service by consumers.	Crimson will provide a tailored training and ensure that the system is configured correctly as part of the implementation package. ICO will document any business processes that need to be followed by staff and deliver this as part of the training. ICO will ensure that any device that is used to access Crimson such as an iPad or iPhone is configured in line with EUD guidance. All ICO mobile devices are built to this standard.	Treated	Yes

5. Sign off and record the outcomes

Who has approved the privacy and security risks involved in the project? What solutions do you need to implement?

Risk	Solution	Approved by
Privacy risks identified above	See above mitigations	Steve Eckersley
Security risks identified above	See above mitigations	Steve Eckersley

6. Integrate the outcomes back into the project plan

Who is responsible for integrating the PSIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy and security concerns which may arise in the future?

Action to be taken	Date for completion	Responsibility for Action
New information management policies/ procedures produced and provided to staff.	Q1 2017-18	Mike Shaw / Anna Feetam
Training provided for all staff using Crimson	Q1 2017-18	Anna Feetam - Training provided by Crimson
Set up a restricted IP addresses with Crimson	Q1 2017-18	Anna Feetam / Dave Wells
Implementation of Crimson to required standard	Q1 2017-18	Crimson / Anna Feetam
Area within EDRM SharePoint to hold documents related to investigations.	Q1 2017-18	Anna Feetam
Review retention settings in line with retention and disposal policy before end of contract. Current retention is 6 years.	April 19	Mike Shaw

Contact point(s) for future privacy concerns	Steven Rook
Contact point(s) for future security concerns	Steven Rook, David Wells

7. Change history

To be completed by project manager.

Version	Date	Author	Change description
V 0.1	27.2.17	Anna Feetam	First draft
V0.2	21.3.17	Anna Feetam	Amended following review by Steven Rook.
V0.3	23.4.17	Anna Feetam	Amended to incorporate comments from Steven Rook
V1.0	23.4.17	Anna Feetam	Sent for approval from Emma Deen and Steve Eckersley
V1.1	24.4.17	Anna Feetam	Comments from Steve Eckersley and Mike Shaw
V2.0	25.4.17	Anna Feetam	Amended to incorporate comments from Steve Eckersley and Mike Shaw
V3.0	22.5.17	Anna Feetam	Amended as part of implementation planning and email exchange with Dave Wells to include restriction of IP addresses.
V4.1	09.10.19	Sue Shepherd	PSIA review and update following re-procurement of contract

8. Document control

Title	Privacy and Security Impact Assessment Template
Version	1.1
Status	Released
Owner	Information Security Manager
Approved by	Information Governance Steering Group
Release date	August 2016
Review date	March 2017