Questionnaire to assess risk of identity fraud to online government services

Basic functionality

Please pick one of the following:

This is an assessment for an existing digital service *e.g. may wish to add GOV.UK Verify to existing online product*	
This is an assessment for an existing digital service after changes (independent of GOV.UK Verify) *e.g. re-structuring digital service*	
This is an assessment for a prospective service *e.g. new digital service, or transformed existing paper service to digital*	
Please give additional context if needed:	

1. Please give a high level overview of your service (max 300 words):

What is the service called? **What does the service do?** **Why do users need the service/ what problem does it aim to solve?** **Describe the full end to end user journey at a high level, including all online and offline steps (technical detail is not required)**

3. Please tell us if your service includes any of the following functionalities.
   Cross box for all that apply

Create new account or application *(application/registration for a service)*	
Form entry that includes personal data *(users enter personal data)*	
Basic data entry *(users asked to input data that cannot be edited, viewed or tracked after submission)*	
Authentication *(leave and return to the service to access the same account using a credential)*	

Save and resume *(pause an application or data entry process and return later)*	
Data release *(display or provide information that was not submitted by the user)*	
Change of circumstances *(allow users to change the information already about them by the service e.g. address)*	
Change of eligibility *(allow users to change the information already held on them by the service in a way that enables or denies them access to the service)*	
User can make a payment *(allows users to make a payment to the service, e.g. paying council tax)*	
Users can receive money, or a benefit from the service *(e.g. money or a valuable 'thing', such as a licence or a permit)*	
Alter details that may redirect the money or benefits received from the service *(allows users to alter the destination to which benefits from the service are paid, e.g. alter address or bank account details)*	
Alter the payment amount received from the service *(allows users to increase or decrease the payment they receive from the service, e.g. alter their information in a manner that increases their tax rebate)*	
The service includes issuing identity evidence *(e.g. order a new/replacement passport)*	
Allow an individual to use the service on behalf of someone else *(e.g. a vulnerable person needs a service, so their carer applies for them and controls their account)*	
Service allows a user to input third party details *(enables a user to enter information about others e.g. their child, accountant or carer)*	
Multiple parties can access an account *(accounts can be shared e.g. access can be granted to both parents, an accountant, carer, social worker, etc.)*	
Account Information can be shared to other accounts *(e.g. a divorcee client may choose to make some information on their account visible or accessible to their lawyer's account)*	

Non-digital dependencies

4. Is it necessary for a user to complete any non-digital steps before using the online digital service?
   (e.g. to access driving licence online, a user must first have passed their test in person and been issued a licence by post)

Y / N	*If yes, please describe:*

5. Does the service have an alternative, entirely non-digital route?
   (e.g. a benefits application can be completed entirely online, or entirely in person at a job center)

Y / N	*If yes, please describe the non-digital user journey:*
	If yes, please estimate the % of users that currently takes this route:

6. Are there non-digital routes for a user to reset their password or recover a locked account?
   (e.g. users can request a password reset by email OR over the phone)

Y / N	*If yes, please describe the route(s):*

7. Is there a process that links non-digital account creation and activity with online accounts?
   (e.g. if a user tried to open an account online, then again via telephone, is there a process that would identify and prevent this?)

Y / N	*If yes, please describe the process(es):*

Expected users

8. Do you provide security awareness information to users?
   (e.g. users are staff who are trained to know not to share their passwords)

Y / N	*If yes, please describe level of user training:*

9. Can the service be accessed on devices that are not managed by the authority?
   (e.g. service can be accessed by the public in an internet cafe vs. service can only be accessed via staff intranet, on work devices)

Y / N	*If no, please describe the controls in place:*

10. Do you have policies and procedures that your users are expected to comply with?
    (e.g. users are civil servants, bound by the civil service code, external users agree to terms of use)

Y / N	*If yes, please describe the nature of these procedures for all types of user (e.g. end users and internal staff). Please specify details for each group separately:*

11. Is there an expectation that users of the service may be uncooperative or reluctant?
    (e.g. a service may have users who are incentivised to be obstructive, or otherwise avoid using the service properly)

Y / N	*If yes, please describe scenario and motivations for hostile users:*

12. Is there any incentive for users to be hostile to one another?
    (e.g. User X is completing a transaction, but needs to do so with cooperation or consent from their ex-partner, User Y. User Y may have motivation to create difficulty for User X)

Y / N	*If yes, please describe scenario and motivations for hostile users:*

Information handled

13. Please tick any relevant boxes in the chart below to describe what kind of information your service handles and how:

	Personal data	Sensitive personal data	Payment info	3rd party personal data	3rd party sensitive data	3rd party payment info
Gathers data						
Stores data						
Present to data users						
System does not handle this kind of data						
Please state the approximate number of records you have						

Notes:
Gather data = Service requires user to input the information or request it from other parties
Stores data = The data remains within the service for a length of time
Presents data to users = A logged in user will be able to view the data relating to that user account
Personal data = as defined by data protection act
Sensitive personal data = as defined by data protection act
Payment information: e.g. service retains credit card details or paypal password for quick payment
3rd party information = Information related to a 3rd party, other than the main user of the account (e.g. children of the user, spouse of the user, etc.)

14. Please provide details about the data your service utilises (as indicated in the table above) and specify whether it is held online or in a non-digital format.

Online	*Please specify:*
Non-digital	*Please specify:*

Motivation for attack

15. On balance, what is the public sentiment towards your service?
    (i.e. is your service liked, or would it attract malicious attention)

Generally liked	Generally ambivalent	Generally disliked

16. How well known is your service?
    (i.e. is your service prominent, publicly known, and are people generally aware of it's existence?)

Prominently in the news	Prominently in the public eye	Public but not prominent	Not in the public eye

17. Please state the number of users that your service has.
    Please specify user numbers, or expected user numbers. If your service has online and non-digital versions, please state the number of users on each.

Number of users:

18. Has your current service previously been actively misused, targeted by offline fraud, cyber fraud, or cyber crime?
    (Irrespective of whether the current service is online or non-digital)

Y / N	*If yes, please specify and state whether the outcome attracted public attention:*

Tracking and accountability requirements of service

19. Is it important that you know the identity of your users?
(i.e. are pseudonyms or anonymity an issue?)

Y / N	*If yes, please specify why:*

20. Is there a requirement for your service to hold users accountable?
(e.g. in the event of service misuse)

Yes, to support criminal prosecution	Yes, to support civil recovery actions	Yes, to support service moderation	No, users are not held accountable
If yes, please explain your answer			

Perceived risks to the service

21. For your service, as it moves online (or currently, if it is already online), what do you believe are the biggest areas of risk that need to be mitigated?
    (you can pick more than one option)

Improper payouts	*Y/N*	*Please specify:*
Money laundering via the service	*Y/N*	*Please specify:*
Eligibility fraud	*Y/N*	*Please specify:*
Prosecuting misuse cases	*Y/N*	*Please specify:*
Data harvesting *(e.g. by infected customer endpoints)*	*Y/N*	*Please specify:*
Reputational damage	*Y/N*	*Please specify:*
Exposure of vulnerable people	*Y/N*	*Please specify:*
Other	*Y/N*	*Please specify:*