IPV OPERATIONS MANUAL

v2.3

Table of Contents

Purpose

1. The purpose of this document is to give detail to Identity Providers for providing identity-proofing capabilities in line with GPG 44 & 45 for the purposes of this Contract. This should be read in conjunction with the other documents provided with the contract.

2. This document contains both requirements and guidance. Within the context of this document the follow terms have a specific meaning:
   "shall" is considered a capability required to deliver the service
   "should" is considered guidance on how the IdP shall demonstrate they are acting in line with Good Industry Practice.

3. This document will be used as a controlling document by the certification body in order to determine whether the IdP has the capabilities to deliver identity-proofing services for GDS.

Identity Management

Registration

4. The IdP shall allow Customers to register for a digital identity. The information needed is dependent on the target Identity Level required at the time of registration. Where the customer has been directed to the IdP from the GDS IDA Hub the target Level of Assurance will be included in the request to the IdP therefore the IdP will be able to determine the minimum Identity Level required.

Common registration requirements

5. The IdP shall require the Customer to provide an email address. The IdP shall only have one active account that uses that email address. The IdP shall attempt to confirm that the email address is under the control of the Customer. The Evidence Details from the Identity Evidence shall be retained for future checking of contra-indicators.

Specific registration requirements for each identity level

Identity Level	Registration Requirements
2	▪ The IdP shall require the Customer to declare their Claimed Identity or require the Customer to confirm the Claimed Identity where the Claimed Identity has been captured through a process that didn't require the Customer to provide such a declaration during registration. ▪ The Personal Name shall be the official name of the Customer, aliases are not allowed. The IdP may ask for a name by which they want to be known by the IdP. ▪ The IdP shall allow the Customer to declare their gender however it is not mandatory that the Customer provide it. [redacted]
3	**Requirements for score 2 plus the following:** [redacted]

Table 1 Registration Requirements

Personal Details changed over the proofing period

6. Where the Personal Details of the Customer have changed over the period required by the proofing process the Customer shall be required to declare their previous names as part of registration process; the IdP shall attempt to Validate these changes.

7. The IdP shall attempt to gather evidence of the change of Personal Details from the Customer and the IdP shall Validate that evidence as per the requirements of GPG 45 and this document. Where this is not possible the IdP shall confirm the changed Personal Details are known to an Authoritative Source (such as Data Aggregators).

Identity Data

Address

8. The IdP shall ensure the Customer provides a valid UK postcode where the address has been assigned a UK postcode. The IdP shall ensure that the post code of a UK address is consistent with the address given, i.e. the Customer can not provide the postcode of an unrelated address. Where the Customer address is automatically, or semi-automatically, populated from a dataset (e.g. from a picker using PAF) and that dataset contains the UPRN (for a UK address) then the UPRN shall also be included in the Identity Assertion.

9. The IdP should be aware that a Customer may have multiple current addresses (e.g. where they live in different places during the week and weekends), the IdP shall encourage the Customer to provide at least the address that is related to their Identity Evidence, ideally the IdP shall collect all valid current addresses for the Customer, otherwise the proofing process may be unsuccessful.

Names

10. Where the proofing or registration process requires the Customer's official name this means the name by which they are identified in official records such as a register for births, marriages or civil partnership; or by official or legal documents that enable them to be known under that name, e.g. decree absolute, final order and deed of change of name (aka 'deed poll').

11. The IdP shall ensure that first name, surname and any middle names can consistently be identified from the data it has stored.

Dates

12. The IdP shall ensure that all dates both provided by the Customer (including date of birth, issue date, expiry date) and those generated by their own systems/data are valid dates for the given month and year (e.g. not 30/02/2011).

Historical data

13. Where the Customer has historical values for name, address and date of birth, the IdP is required to retain 3 years of historical data within the Customer record. The IdP may retain historical values for longer as long as this in line with legislation, other statutory requirements that apply to them and the terms and conditions that were agreed to by the Customer. Where gender changes the IdP shall only ever retain the current value within the Customer record.

PID

14. The IdP shall generate a PID for each Customer on registration. [redacted] The PID shall remain unchanged for the lifetime of the

account. A PID shall never be reused, e.g. a new PID shall not match a PID that has been deleted.

Personal details in the identity assertion

15. A minimum set of personal data shall be provided by the IdP in the identity assertion. Identity assertions shall only be sent in response to a request from the GDS IDA Hub after a successful authentication.

16. The Personal Details collected through the proofing process that shall be included in the identity assertion are:
    - First name, surname and middle names
    - Date of birth
    - Gender
    - Address

17. Only Personal Details that have been proofed can be marked as 'verified' in the identity assertion.

18. The identity assertion shall contain historical details (up to 3 years) for these attributes except for Gender (which shall only ever contain the current value) where the IdP has collected such data.

Maintaining Accurate Identity Data

Updating verified data

19. The IdP shall enable the Customer to update their records to reflect a change in the Customer's circumstances after successful proofing. The IdP shall take appropriate measures to ensure that when this occurs it is being done by the legitimate owner of the account. The measures may vary depending on the strength of the Credential used to authenticate the Customer to the service that allows the Customer to change their details and other risk factors (e.g. detection of malware).

Validating change in a verified personal name

20. Where the Customer informs the IdP that there has been a change in their Personal Name after successful proofing the IdP shall attempt to gather evidence of the change of Personal Name from the Customer. The IdP shall Validate the evidence as per the requirements of GPG 45. Where this is not possible the IdP shall confirm the changed Personal Name is known to an Authoritative Source (such as Data Aggregators). [redacted]

Validating change in a verified date of birth

21. This is an unusual event (but not unheard of) so where the Customer informs the IdP that there has been a change in their date of birth after successful proofing the IdP shall gather evidence demonstrating the

change of date of birth from the Customer. The IdP shall Validate the evidence as per the requirements of GPG 45 and this document.

Validating change in verified address

22. Where the Customer informs the IdP that there has been a change in their address after successful proofing the IdP is not required to Validate this at the point of notification however the address history must contain at least one Validated address at the point of assertion (see Conditions for an Identity Assertion). The IdP shall Validate the change in address either by gathering evidence from the Customer and Validating it as per the requirements of GPG 45 or by confirming that the change in address is known to an Authoritative Source (such as Data Aggregators).

Validating change in identifiers

23. Where the Customer changes an identifier where that identifier is used by the IdP as an outbound channel (e.g. a mobile phone number) then the IdP shall ensure that the identifier is in the possession or control of the Customer. Where the identifier is an email address then the IdP shall ensure that the email address is in the possession or control of the Customer (see Common registration requirements).

Verifying the Customer in order to enable a change in verified data

Representing changed details in the identity assertion

25. When the Customer updated their data only that data that has been Validated can be marked as verified in the identity assertion.

Counter-fraud checks for changes in customer data

26. When the Customer changes their data, the IdP shall perform the counter-fraud checks required for the level of the identity that are appropriate to the data items that have changed; e.g. a change of name shall only necessitate counter-fraud checks that are related to names, change in address only necessitates counter-fraud checks that are related to address. Where this process discovers a Contra-indicator then the IdP shall record that Contra-indicator against the Customer record and review the guidance in this document on dealing with Contra-indicators.

Credentials and Authentication

Credential issuance

27. All Credentials issued by the IdP for the purpose of authenticating a Customer shall:
    - Only be sent to an address or via communication channel that the IdP knows to be in control of the Customer. This shall either be via the identifier, email address, address, telephone or other communication channel that has been confirmed as part of the proofing process or has been subjected to an equivalent process.
    - Meet the requirements of GPG 44 for the specific LoA required.

Recovery of lost credential

28. The IdP shall have a process to enable a Customer who has lost their Credential to regain access to their account. The IdP shall verify that the Customer is the owner of the account [redacted] whether this be online, by telephone or in person.

Display last login

29. After a successful authentication the IdP shall display the time of the last successful login (with the IdP) to the Customer. Where possible the IdP should indicate whether the last successful login was from the same device currently being used by the Customer.

Deregistration

30. At any time the Customer may choose to leave the IdP, therefore the IdP shall allow a Customer to close their account. When the Customer chooses to do so the IdP shall suspend all Credentials issued to the Customer and prevent any further authentications and assertions using that account. The IdP may offer a reasonable cooling off period to the Customer before closing the account. The IdP shall have processes to ensure the Customer is the owner of the account, [redacted]

31. The IdP shall allow the Customer to register again in the future if the Customer chooses to do so, the re-registration of such a Customer is treated as a new Customer (i.e. they are subjected to the same registration and proofing including being issued a new unique PID).

Notifications When There are Changes to a Customer's Account

32. The IdP shall notify the owner of the account that their details have been changed using contact details that were not changed by the Customer at that time. This includes where a Customer has requested to close their account.

33. [redacted].

34. The notification shall occur via a process that is out of band to the service that is allowing the Customer to change their details (e.g. via email, instant message, text, telephone, letter). The IdP shall include instructions on how to recover from an unauthorised change to their details in the notification.

Identity Repair

35. A Customer may have their identity compromised by a 3rd party that could either prevent the legitimate Customer registering with an IdP or cause an existing account to be suspended by the IdP. The IdP shall ensure they have the capability to register a Customer where they have been the subject of identity theft whilst being able to prevent the 3rd party doing so. The IdP shall ensure they have the capability to recover a closed Customer account where the account was closed by a 3rd party.

Identity Evidence (IPV Element A)

Determining Whether Identity Evidence is Applicable

36. The Identity Evidence shall be evaluated against the criteria set out in GPG 45. It shall only achieve the score from GPG 45 where is meets all the required properties for that score.

Linking The Claimed Identity to the Identity Evidence

37. The IdP shall ensure that the Claimed Identity given during registration is the same individual identified by the Identity Evidence. Ideally the Personal Name of the Claimed Identity shall match the Personal Name demonstrated by the Identity Evidence. Where the Personal Name from the Identity Evidence and the Claimed Identity differ then the IdP shall determine that they relate to the same individual, e.g. where the Claimed Identity forename is Bill and the Identity Evidence is William (i.e. they are matching synonyms).

38. The date of birth of the Claimed Identity must match the date of birth as demonstrated by that Identity Evidence. If the date of birth differs then the IdP shall ensure the Claimed Identity has the correct date of birth by either updating the Claimed Identity using the date of birth from **validated** Identity Evidence (see Validation) or requesting the Customer to correct it. However if the IdP believes the Identity Evidence to have the incorrect date of birth (based on other information they have) then the Identity Evidence with the believed incorrect date of birth shall be void.

Validation (IPV Element B)

Determining whether Identity Evidence is Genuine

Examination of the security features of a physical document

39. This chapter provides the specific requirements for physical validation of the physical Identity Evidence (i.e. physical documents) provided by the Customer in order to determine whether the Identity Evidence is **Genuine**.

40. The IdP capability to Validate identity documents will affect the determined level of identity assurance. The following table provides the personnel training and equipment capabilities that are required from an IdP in relation to the IPV score required for Validation.

Score	Equipment Requirements	Training Level
1	[redacted]	AWARE
2		BASIC
3		ADVANCED
4		ADVANCED

Table 2 Document Inspection Equipment and Training

41. Each of the training levels in the following table builds on the training of the previous level, e.g. to achieve BASIC level training the trainee shall have either previously completed a training programme for AWARE or that the training required for AWARE is also covered in the BASIC training programme.

Training Level	Training Requirements
AWARE	[redacted]

BASIC	[redacted]
ADVANCED	

Table 3 Document Training Requirements

42. [redacted]

43. [redacted]

44. [redacted]

45. Training Material for Document Verification
    - http://www.cpni.gov.uk/documents/publications/2007/2007044-gpg_document_verification_guidance.pdf
    - http://www.hoidfraudawareness.co.uk/

46. Reference Material (not a definitive list)
    - Prado (http://prado.consilium.europa.eu)
    - CPNI Document Verification
      http://www.cpni.gov.uk/documents/publications/2007/2007044-gpg_document_verification_guidance.pdf
    - Catalogue of Identity Documents
      http://www.catalogueofcurrencies.com/en/identity-documents.html
    - Security Features Guide
      http://www.catalogueofcurrencies.com/en/security-features-guide.html
    - Photocard Driving Licence
      http://www.nidirect.gov.uk/the-photocard-driving-licence-explained
    - Passports
      https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118767/introducing-new-passport.pdf
      https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118783/basic-passport-checks.pdf
    - Secure Payment Cards
      http://acquiring.elavon.com/documents/pdfs/card%20present_en_final.pdf
      http://www.discovernetwork.com/merchants/fraud-protection/prevention.html
      https://secure.cmax.americanexpress.com/Internet/International/japa/SG_en/Merchant/PROSPECT/WorkingWithUs/AvoidingCardFraud/HowToCheckCardFaces/Files/Guide_to_checking_Card_Faces.pdf
      http://www.visaeurope.com/en/businesses__retailers/retailers_and_merchants/training_your_staff/recognising_valid_visa_cards.aspx
      http://www.devon-cornwall.police.uk/CrimePrevention/AdviceBusiness/Documents/Counterfeit_Fraud.pdf

Physical document containing cryptographically protected information

47. For physical documents provided by the Customer that contain cryptographically protected information (e.g. RFID in passports, EMV Smartcard):
    - Read the embedded chip with a compatible reader. Where the information is secured using basic or enhanced access control provide the required decryption key from the information on the document. Where the cryptographic system requires a PIN the Customer shall enter it themselves.

- If the chip was successfully read then compare the retrieved information with the Personal Details and Evidence Details (where the such details are held) on the document to ensure they are consistent.
- Confirm the digital signature is correct.
- Confirm the signing key is valid with the Issuing/Authoritative Source.
- Confirm the signing key is the correct key for the Identity Evidence with the Issuing/Authoritative Source (i.e. this is the correct key used by the issuer of this evidence)..

Electronic evidence containing cryptographically protected information

48. For electronic Identity Evidence (e.g. PDF):
    - Confirm the electronic signature is correct.
    - Confirm the signing key is valid with the Issuing/Authoritative Source.
    - Confirm the signing key is the correct key for the Identity Evidence with the Issuing/Authoritative Source (i.e. this is the correct key used by the issuer of this evidence).

Checking if the Identity Evidence is Valid

49. Identity Evidence must be valid at the time of registration, therefore, in the first instance, the IdP shall ensure that the Identity Evidence has not reached its expiry date (where the Identity Evidence has an expiry date). Checks performed against the Issuing/Authoritative Source are likely to fail if the Identity Evidence is no longer valid.

50. Some forms of Identity Evidence include features such as check digits and specific identifier structures, the IdP should confirm the information provided is consistent with these features otherwise any check performed against the Issuing/Authoritative Source is likely to fail. The following are examples for some of the Identity Evidence:

51. **DVLA Driver Number**

    The driver number assigned by DVLA is a compound identifier made from information about the driver and some DVLA specific information. It is constructed as follows:
    - Characters 1 to 5 - first five letters of the surname; if the surname has fewer than five letters, the remaining spaces padded using the number 9 (e.g. MAN99). Note: some names may have been concatenated by DVLA to improve uniqueness, e.g. MAC is shortened to MC.
    - Character 6 - the decade from the year of birth (e.g. 6 for 1964).
    - Characters 7 & 8 - the month taken from the date of birth. If the Customer's gender is female, a value of '5' is added to character 7 (e.g. a woman born in October would have '60' for these characters).

- Characters 9 & 10 - day of the month from the date of birth (e.g. 14 for 14/04/1983).
- Character 11 - the last digit from the year of birth (e.g. 4 for 1964).
- Characters 12 to 13 - the first two initials of the Customers given names. Unused characters are usually padded with '9' however to ensure uniqueness other numbers are sometimes used.
- Character 14 is usually padded with a '9' however to ensure uniqueness other numbers are sometimes used.
- Characters 15 & 16 - security digits generated by DVLA.
- Characters 17 & 18 - issue number however these may not be present for all current drivers.

Reference documentation:
http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/@motor/documents/digitalasset/dg_4011281.pdf

52. **ISO/IEC 7812 Compliant Number** (e.g. bank/credit cards)
ISO/IEC 7812 is the international standard that specifies "a numbering system for the identification of issuers of cards that require an issuer identification number (IIN) to operate in international, interindustry and/or intra-industry interchange". It is constructed as follows:
    - Characters 1 to 6 - The issuer identifier number (IIN) as assigned by "ISO Register of Card Issuer Identification Numbers" (Character 1 is also the major industry identifier (MII) number as defined by ISO/IEC 7812).
    - Characters 7 to second last (maximum of 12 digits) – Account number as given by the card issuer.
    - Last digit - check digit calculated using the Luhn algorithm as defined in Annex B of ISO/IEC 7812-1.

53. To check if information is accurate the Personal Details and Evidence Details need to be confirmed as Valid by the Issuing/Authoritative Source. In practice this means the Personal Name, Address and/or DoB, at least one unique number (where the Identity Evidence has a unique number) and expiry date (where the Identity Evidence has an expiry date) from the Identity Evidence shall be confirmed by the Issuing/Authoritative Source as being identical to their records. Identity Evidence can not be determined to be Valid from inspection of the Identity Evidence itself (see **Genuine**). The following are examples for some of the Identity Evidence:

54. **ICAO 9303 Passport**
    - Passport number
    - Code (issuing state)
    - Given Name(s)
    - Surname
    - Date of birth

- Date of expiry
- Optionally: Date of issue
- Optionally: Place of birth
- Optionally: Authority
- Optionally: Type
- Optionally: Sex (the Customer shall not be mandated to provide this)

55. **Directive 2006/126/EC compliance driving licence**
    - 5 (driver number)
    - Issuing member state
    - 1 (surname)
    - 2 (given name)
    - 3 (date and place of birth)
    - 4a (issue date)
    - 4b (expiry date)
    - 4c (issuing authority)
    - Optionally: 8 (address)
    - Optionally: Issue number

Failing Validation

56. If the IdP is unable to Validate the Identity Evidence they shall record the failure against the Customer record (score 0). Where the process discovers a Contra-indicator then the IdP shall record that Contra-indicator against the Customer record and review the guidance in this document on dealing with Contra-indicators.

Verification (IPV Element C)

Static Knowledge Based Verification (KBV)

57. A static KBV secret may only be exchanged via a delivery method where the IdP has confirmed that method is linked the Claimed Identity, for example physical address is required to be proofed as part of the Validation step therefore it is acceptable to exchange the shared secret by post; telephone number may only be used where the IdP can confirm the phone number is owned/used by the Claimed Identity by information from an independent and reliable source.

58. Where the IdP sends a the static KBV secret to the address of the Claimed Identity the following conditions shall apply:

Identity Level	Delivery Requirements
2	No special conditions for delivery to a UK address. For non UK addresses the IdP shall apply the conditions for a Level 3 Identity.
3	The static KBV Secret shall be sent via a method that records the details about the recipient and requires them to acknowledge its receipt (e.g. registered post, courier etc).

Table 4 Static KBV Delivery Requirements

59. Where an IdP sends a token, device or other Credential to the address of the Claimed Identity for the purposes of being used as part of the authentication process the first time use of it effectively meets the requirement of a Static KBV assuming that the token/device/Credential can not be used for authentication in isolation (i.e. interception of this would not grant the holder access to the Customer's account).

60. An external trusted source where the Customer already has such a relationship can be used as a Static KBV. Where an external trusted source is used the process shall be able to confirm to the IdP that an individual with matching Personal Details has successfully passed the static KBV process for example the 3-D Secure (e.g. Verified by Visa, Mastercard SecureCode etc).

Dynamic Knowledge Based Verification

61. Dynamic KBV requires the IdP to gather information about the Claimed Identity from Issuing/Authoritative sources and for the Customer to demonstrate that they have such knowledge about the Claimed Identity that it is likely they are the owner of that identity.

Dynamic KBV principles

62. There must be a sensible balance between achieving assurance that the Customer is the owner of the Claimed Identity and presenting an attractive Customer journey. With this in mind the IdP shall follow a number of KBV principles:

- The KBV questions shall be relevant, sensible and proportionate
- KBV questions shall be carefully constructed as to be clear and obvious to the Customer what is being asked.
- There shall be an expectation that the owner of the Claimed Identity can reasonably be expected to know the answer.
- KBV questions shall be constructed so that the theft of a possession such as a wallet or purse would not provide the required information to answer those questions to an impostor.
- Where the IdP offers the Customer a selection of suggested answers (i.e. multiple choice) then all the answers shall be plausible and the correct answer should not be easily guessed or determined using publicly available information.
- KBV questions shall be constructed so that it is unlikely that the answers can be drawn from information available from social networking sites and public registers.
- The IdP shall use KBV data of the highest quality (see following section) where possible, a fewer questions about KBV data that is highly unlikely to be known by someone other than the owner of the Claimed Identity is preferable to many questions about KBV data that is more likely to be available to others.
- KBV questions shall be based on a range of KBV data and not reliant upon one single KBV source; for these purposes a source is considered to be an organisation in its entirety however where that organisation has within itself separate acceptance and proofing processes then data that originates from those separate processes can be considered a separate source (e.g. Bank account and mortgage from the same provider could count as different sources if the processes to obtaining them is different).
- KBV questions should cover facts about the Claimed Identity that fall into different Evidence Categories; ideally where the Customer has only provided 2 forms of Identity Evidence then questions based on high quality data relating to the unused Evidence Category should be included.
- It must be recognised that the process cannot account for every eventuality when using KBV, e.g. it must accepted that certain KBV data items may be known to close family members.
- The IdP shall ensure that where multiple questions are presented that one question doesn't effectively answer another; e.g. the IdP shall not ask "You took out a mortgage with HSBC in April 2013, what is your monthly payment?" and "You took out a mortgage in 2013, who was it with?" (as clearly the first question answers the second).
- Data that does not change regularly over long periods of time (e.g. initial mortgage borrowing, credit limit, etc) does not qualify as Dynamic KBV because it does not vary often enough for it to be unpredictable.
- The IdP shall ensure that KBV questions can not be answered by the information already provided by the Customer e.g. they shall not ask

"Which of these is your previous address?" where the Customer has already provided that address to the IdP (either during registration or by the Customer later updating their account).

- The IdP shall ensure that the KBV questions do not reveal personal information to the Customer that they have not already provided (e.g. "You have a joint account with Jane Doe, which bank is this with?" where the relationship to Jane Doe was not already provided by the Customer).
- KBV questions shall cover data gathered from multiple sources; where Data Aggregators are used then the IdP shall ensure that the KBV questions do not relate to the same source.

Dynamic KBV data

63. The degree of assurance that can be taken from the KBV process is linked to the quality and availability of the data used to generate the questions. The following describes how to consider the quality of the data. In this context "source" is considered to be the organisation that captures the original data, not any intermediary, such as a Data Aggregator, that is used to gain access to that data. KBV data is only valid if it refers to an individual whose Personal Details match those of the Claimed Identity (also see Data Aggregators).

KBV Quality	Properties of KBV Data
Low	▪ KBV data shall pertinent to the Claimed Identity. ▪ The KBV data could be researched with no financial commitment and with ease. ▪ The source of the KBV data protects the integrity of the KBV data.
Medium	**Requirements for "Low" plus the following**: ▪ The source of the KBV data confirmed the Claimed Identity through a proofing process. ▪ The KBV data is not known, or likely, to be in the public domain. ▪ The KBV data may be available to others but would require a financial commitment that would be a deterrent to others and a time commitment that would noticeably delay the Customer's ability to provide the correct answer during the IPV process. ▪ The KBV data may be known to relations and friends who are not the Claimed Identity's immediate family. ▪ The source of the KBV data protects the confidentiality of the KBV data.
High	**Requirements for "Medium" plus the following**: ▪ The source of the KBV data confirmed the Claimed Identity in a manner that complies with the identity checking requirements of The Money Laundering Regulations 2007. ▪ KBV data shall not be in the public domain including any public register. ▪ KBV data should not be known to others apart from the owner of the Claimed Identity (and immediate family). ▪ Someone other than the Claimed Identity (and immediate family) should not be able to obtain the KBV data without committing either a civil or criminal offence. ▪ The source of the KBV data have security practises that prevent unauthorised access, modification or generation of KBV data by insiders, either acting alone or with outside coercion.

	▪ The source of the KBV data shall be subject to regulation by a statutory or an independent body.

Table 5 KBV Quality

64. KBV data shall not be used where it is known, or likely, that it is in the public domain. Information in the public domain means that the KBV data can be accessed by another person either with or without a degree of research or is contained within an open/public facing website.

Dynamic KBV scoring

65. To ensure that there is a consistent approach for demonstrating that the Customer has sufficient knowledge about the Claimed Identity the IdP shall follow this scoring model for Dynamic KBV. The following table demonstrates the scoring profile for Dynamic KBV. The score is dependent on two factors, the KBV Quality and the method by which the answer is elicited from the Customer. In this context "Unprompted" means a question where the Customer is free to enter any response they wish (e.g. free text response) and "Prompted" means that the response from the Customer is constrained or limited by the IdP (e.g. multiple choice). Customers start the KBV process with a success score of '0' and failure score of '0'. Where a Customer correctly answers a KBV question their success score is incremented by the score as detailed below; where the Customer fails to correctly answer a KBV question their failure is decremented by the score as detailed below. The success and failure scores are **not** added together, they are distinctly separate counters.

KBV Quality	Unprompted Success	Unprompted Failure	Prompted Success	Prompted Failure
Low	[redacted]	[redacted]	[redacted]	[redacted]
Medium	[redacted]	[redacted]	[redacted]	[redacted]
High	[redacted]	[redacted]	[redacted]	[redacted]

Table 6 KBV Scoring

Restarting/Resuming Dynamic KBV

66. Where the IdP allows the Customer to suspend and resume the proofing process care shall be taken to ensure that they cannot use this feature to gather information relating to the Claimed Identity from the Dynamic KBV process.

67. [redacted]

68. Where the IdP allows the Customer to suspend and resume the Dynamic KBV process then the IdP shall ensure it does not reveal to the Customer whether they have correctly answered any question until they have completed the whole KBV process.

69. [redacted].

70. If the Customer fails to return or, upon return, fails to complete KBV then the IdP shall treat this in the same manner as a Customer failing KBV.

Passing and failing Dynamic KBV

71. [redacted]

Identity Level	[redacted]							
2								
3								

Table 7 KBV Pass/Fail Scoring

Physical Comparison

72. The physical comparison step of verification requires the Customer to be verified by a visual confirmation that they appear to be the person to whom the Identity Evidence was issued. There are two methods by which this may be completed, a traditional in person/face-to-face process and a remote process (e.g. using a video/video streaming link). Below is a table of quality controls that shall be considered when performing either process.

Physical Verification Method	Quality controls
In person	▪ If a person is performing the comparison they shall have sufficiently good eyesight (when wearing any prescribed corrective lenses) to be able to accurately see the image/photo and the Customer. ▪ If a person is performing the comparison they shall have been trained in detecting impostors [redacted] ▪ [redacted]. ▪ Any electronic matching capability used shall have been independently assessed by a reliable and independent body as being able to demonstrate a high degree of accuracy in distinguishing between people of similar characteristics. ▪ Size and quality of the original image/photo shall be good enough for someone to be identified [redacted]
Remote	**Requirements for "in person" plus the following:** ▪ [redacted]

	[redacted]. ▪ The visual representation of the Customer shall be of sufficient quality [redacted] and be clearly recognisable. ▪ The IdP shall take sufficient procedural and technical measures to ensure that the visual representation of the Customer is of a real person and not a photo or other mock up.

Table 8 Physical Verification Quality Controls

Biometric Comparison

73. Biometric comparison requires the Customer to be verified by a biometric confirmation that they appear to be the person to whom the Identity Evidence was issued. [redacted] The capture of the biometric for comparison shall have sufficient measures to detect the spoofing of biometric identifiers.

Failing Verification

74. If the IdP is unable to Verify the Customer as the owner of the Identity they shall record the failure against the Customer record (score 0). Where the process produces a Contra-indicator then the IdP shall record that Contra-indicator against the Customer record and review the guidance in this document on dealing with Contra-indicators before deciding whether to fail this IPV Element.

Counter-fraud Checking (IPV Element D)

Counter-fraud Checking

75. The IdP capability to perform counter-fraud checks will affect the determined level of identity assurance. The following table describes the Customer data and the counter fraud sources that the IdP is required to use to perform the counter fraud checks in relation the corresponding score for the IPV element. For clarity the counter-fraud check does not include checking the provided Identity Evidence (see Validation and Identity Evidence Review).

Score	Counter fraud checking scope
2	[redacted]
3	**Requirements for "2" plus the following:** [redacted]

Table 9 Counter-fraud Scope

Counter-fraud Capabilities

76. As part of the counter fraud checks the IdP shall have, either through their own internal data sets, or via reliable and independent sources, the following counter fraud checking capabilities:
    - Whether the Claimed Identity has been subject to identity theft, regardless of whether it was successful or not.
    - That the Claimed Identity is known to reliable and independent sources (i.e. not a zero footprint identity).
    [redacted]
    - Whether the address is associated with identity fraud.
    - Whether the Claimed Identity is deceased.
    - Whether the address history of the Claimed Identity is consistent with the declaration by the Customer.

77. The IdP shall record within their own data sets the Personal Details of Claimed Identities for which they have sent Fraud Warnings. The IdP shall check whether the Claimed Identity is in this data set.

Failing Counter-Fraud Checks

78. If the IdP determines that the Customer has failed IPV due to information gained from the counter-fraud checking process they shall record the failure against the Customer record (score 0). Where the process discovers a Contra-indicator then the IdP shall record that Contra-indicator against the Customer record and review the guidance in this

document on dealing with Contra-indicators before deciding whether to fail this IPV Element.

Activity History (IPV Element E)

79. Activity History is derived from a process based on the following information and analysis:
    - Qualifying Activity Events
    - Quality of the Activity Events
    - Weighting of Activity Events
    - Demonstration of a Continuous History

80. It is the combination of these things that indicates that the Claimed Identity has an existence over time.

Qualifying Activity Events

81. In order to determine Activity History there must be a collection of qualifying Activity Events to assess. To qualify, the Activity Event shall relate to an interaction between the Claimed Identity and a source of Activity Events. This can be in either direction, e.g. the Claimed Identity using the services of the source or the source initiating an interaction with the Claimed Identity including issuing something to the Claimed Identity.

82. Activity Event data is only valid if it refers to an individual whose Personal Details match those of the Claimed Identity, allowing for any changes in Claimed Identity that have occurred over the time period being assessed for the Activity History.

83. The requirements for the spread of Evidence Categories required are described in GPG 45. These requirements apply to the Activity Event Package as a whole, not within each Evidence Category. For example GPG 45 requires there to be Activity Events in each of the Citizen, Money and Living categories. Finding one event in Citizen Category (that is within the Activity History period required) satisfies the requirement for the Activity Event Package to contain events from the Citizen Evidence Category.

84. In order to meet the Evidence Category requirements the IdP may extend the Activity History period to include more qualifying Activity Events. In such cases the Activity History must be 'continuous' (see Continuous History) from the oldest Activity Event to the most recent (e.g. electoral role entry is 280 days ago but the minimum requirement is 180 days then there shall be a continuous history for 280 days in order to include the electoral roll entry).

Activity Event Quality

85. The degree of assurance that can be taken from the Activity History process is linked to the quality of the data used. Each Activity Event shall be measured against the quality criteria before assessment of the Activity History, however in practise the quality is likely to be determined by the source (generally a source tends to produce data of the same quality). The

following describes how to consider the quality of that data and attributes a Quality Score to each. In this context "source" is considered to be the organisation that captures/generates the original data [redacted] and not any intermediary, such as Data Aggregators, that is used to collate or access that data.

Quality	Score	Properties of Activity Event Quality
Low	1	▪ Data shall be pertinent to the Claimed Identity. ▪ The data source shall record accurate timestamps against the Activity Event. ▪ The data source shall protect the integrity of the Activity Event.
Medium	2	**Requirements for "Low" plus the following**: ▪ An individual could generate the Activity Events but it would require a financial commitment or a level of difficulty that would be a deterrent. ▪ The identity linked to the data within the data source was confirmed through an identity proofing process. ▪ The Activity Events are independently verifiable. ▪ The data source has a process for reporting and rectifying identity-related issues such as identity theft.
High	3	**Requirements for "Medium" plus the following**: ▪ The identity linked to the data within the data source was confirmed in a manner that complies with the identity checking requirements of The Money Laundering Regulations 2007. ▪ The data source shall have security practises that prevent unauthorised modification or generation of data by insiders, including acting alone or with outside coercion. ▪ The data source shall be subjected to regulation or audit by a statutory or an independent body.

Table 10 Activity Event Quality

Weighting of Activity Events

86. It has to be recognised that low quality events that have a long history are useful in assessing Activity History and high quality events that only have a short history may simply be the result of someone attempting to create a false identity. Therefore the Quality Score shall be weighted in relation to the length history available of the Claimed Identity from that source [redacted]

Weighting Condition	Weighting
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	
[redacted]	[redacted]

Table 11 Activity Event Weighting

87. The following table summarises how the quality and weighting combine to produce a score for the Activity Event.

		Longevity of Claimed Identity known by source											
		[redacted]											
Activity Event Quality	L		[redacted]			[redacted]			[redacted]			[redacted]	
	M		[redacted]			[redacted]			[redacted]			[redacted]	
	H		[redacted]			[redacted]			[redacted]			[redacted]	

Table 12 Activity Event Scoring

Continuous History

88. To achieve the Activity History criteria as defined by GPG 45 then the IdP shall determine that the Activity History appears to be continuous over the period required for the level of identity. [redacted].

Identity Level	Activity Event Total
2	[redacted]
3	[redacted]

Table 13 Activity Event Totals

89. [redacted] (see Qualifying Activity Events).

90. The [redacted] assessment [redacted] must meet the required Activity Event Total for the Activity History to be considered continuous. [redacted]

Failing Activity History

91. If the IdP is unable to determine the required Activity History they shall record the failure against the Customer record (score 0). Where the process produces a Contra-indicator then the IdP shall record that Contra-indicator against the Customer record and review the guidance in this document on dealing with Contra-indicators before deciding whether to fail this IPV Element.

External Sources

Data Aggregators

92. A Data Aggregator is an organisation involved in compiling information on individuals from various sources. For the purposes of IPV they shall also meet the criteria for being a reliable and independent source.

Matching records against those from a Data Aggregator

93. As Data Aggregators compile information from multiple sources there is no guarantee that all Personal Details from every source will match exactly to the Claimed Identity provided by the Customer on every single entry (e.g. there maybe keying/rekeying errors, OCR misreads, transpositions etc). The view of the dataset (of the Personal Details) taking in to consideration the likelihood of the source having the correct details, predictable inconsistencies and weightings shall be considered the most likely representation of the actual Personal Details (e.g. most common version of the name given the likelihood of the sources collecting the official name and not synonyms).

94. When matching the Claimed Identity against such datasets the following rules shall apply:

Item	Matching Rules
Personal Name	▪ Matching shall be allowed to take in to consideration known synonyms for given names (e.g. Bill & William). [redacted]
Date of Birth	[redacted]
Address	▪ Matching shall always match exactly on postcode (for a UK address that appears to have been assigned a postcode). ▪ Matching shall always match the main property identifier (e.g. House No. 1 Flat 1A matches House No.1 Flat A).

Table 14 Matching with Data Aggregators

Data Aggregators and KBV

95. Where KBV data is sourced through a Data Aggregator then the aggregator shall have a strong data handling process, ensuring compliance with Law, that the data is only supplied to appropriate organisations/persons and protect against unlawful and accidental disclosure. Protection of the confidentiality and integrity of this data is key to ensuring that KBV has value; if someone's KBV data is lost or stolen then that will fundamentally undermine its effectiveness in the IPV process.

Data Aggregators and Activity History

96. Where Activity Event data is sourced through a Data Aggregator then the aggregator shall have a strong data handling process, ensuring compliance with Law, that the Activity Event data is only supplied to appropriate organisations/persons and protect against unlawful and accidental disclosure. Protection of the integrity of this data is key to ensuring that Activity Events have value. If Activity Events can easily be falsified then that will fundamentally undermine their usefulness in the IPV process.

Reliable and Independent Sources

97. As part of the proofing the IdP shall check the various pieces of information with a reliable and independent source.

    A source is considered to be reliable and independent where **all** of the following conditions are met:

    - Recognised as being a suitable source for identity information within Good Industry Practice.
    - Demonstrate they can provide a dependable service.
    - Demonstrate that the staff and processes operate independently from those involved in the identity proofing processes within the IdP.

Contra-indicators

What makes a contra-indicator

98. Contra-indicators are essentially pieces of information that either contradict statements from the Customer or raise some doubt over whether the Customer is legitimate. Contra-indicators are discovered either during the proofing process or during the lifetime of the Customer's account, some arise from the Validation, Verification and Activity History steps but they are most commonly discovered during the counter-fraud checking process.

99. The discovery of a contra-indicator does not necessarily mean that the Customer is not legitimate. Most contra-indicators will require further investigation in order to confirm they are not a false-negative. Some contra-indicators are warnings to the IdP that they may need to perform more stringent checks, e.g. the Claimed Identity has been the subject of identity theft and the IdP needs to ensure that the Customer is indeed the owner of the Claimed Identity and not an impostor.

Analysing a contra-indicator

100. During the proofing process a number of contra-indicators may be discovered. The IdP shall review the contra-indicators and make an assessment on whether they believe the Customer may be making a false claim to an identity.

101. The IdP shall ensure that they have taken reasonable steps to determine whether a contra-indicator is false-positive. The Contra-indicator Table is a list of contra-indicators that the IdP may encounter and includes guidance on how to interpret and react to them. Each contra-indicator is referenced by an identifier (ID), this ID shall be used for exchanging contra-indicators between the IdP and the GDS IDA Hub Operations Centre.

Contra-indicator scoring and mitigating actions

102. The Customer is to start the proofing process with a contra-indicator score of "0". Each contra-indicator that is discovered attracts a score adjustment as described by the "found" value in the Contra-indicator Table.

103. If the IdP is able to resolve the contra-indicator by following the guidance as set out in the corresponding "Mitigating Actions" the risk score is further adjusted by the corresponding "pass" score. Where the IdP does not have the capability to perform the mitigating action then they cannot apply the 'pass' score. Many of the Mitigation Actions may in themselves raise further contra-indicators (where those Mitigating Actions fail), in such cases the new contra-indicator is simply treated as a contra-indicator in its own right.

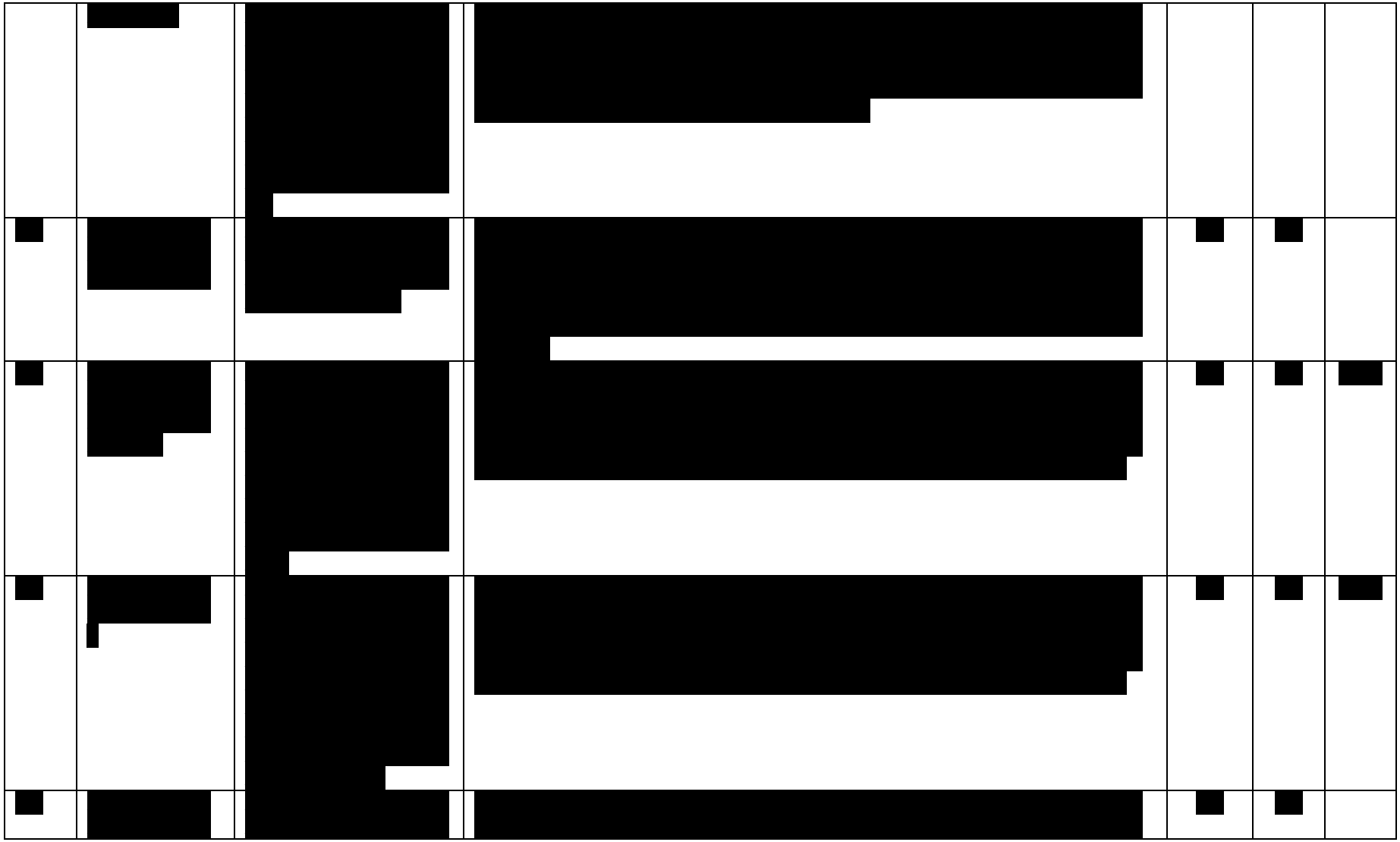
Contra-indicators after registration

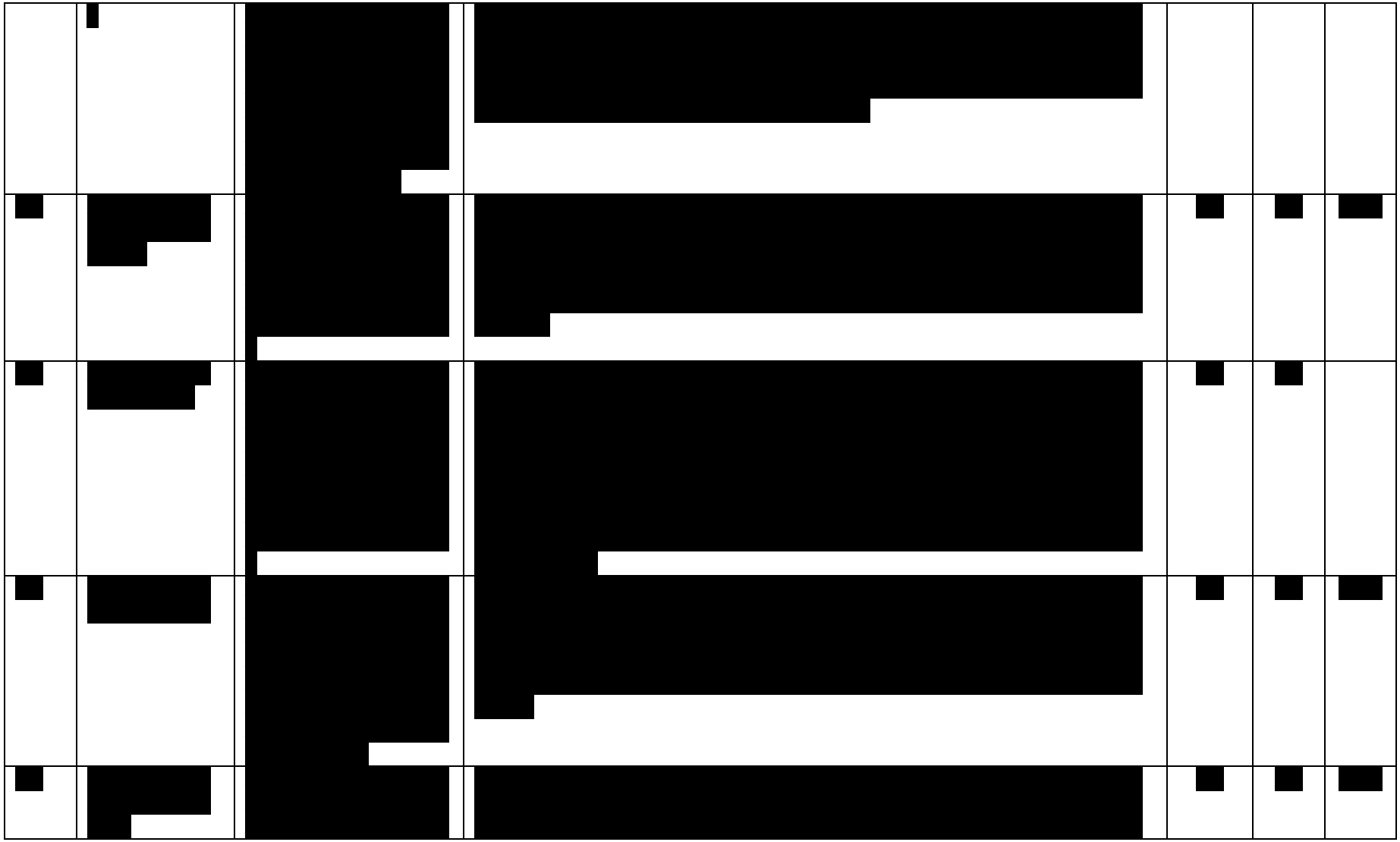
104. The IdP shall react to contra-indicators discovered after registration in the same manner as if they occurred during registration. The IdP shall evaluate whether they need to review the Customer's account to determine if they should continue to assert the Claimed Identity based on the information discovered.

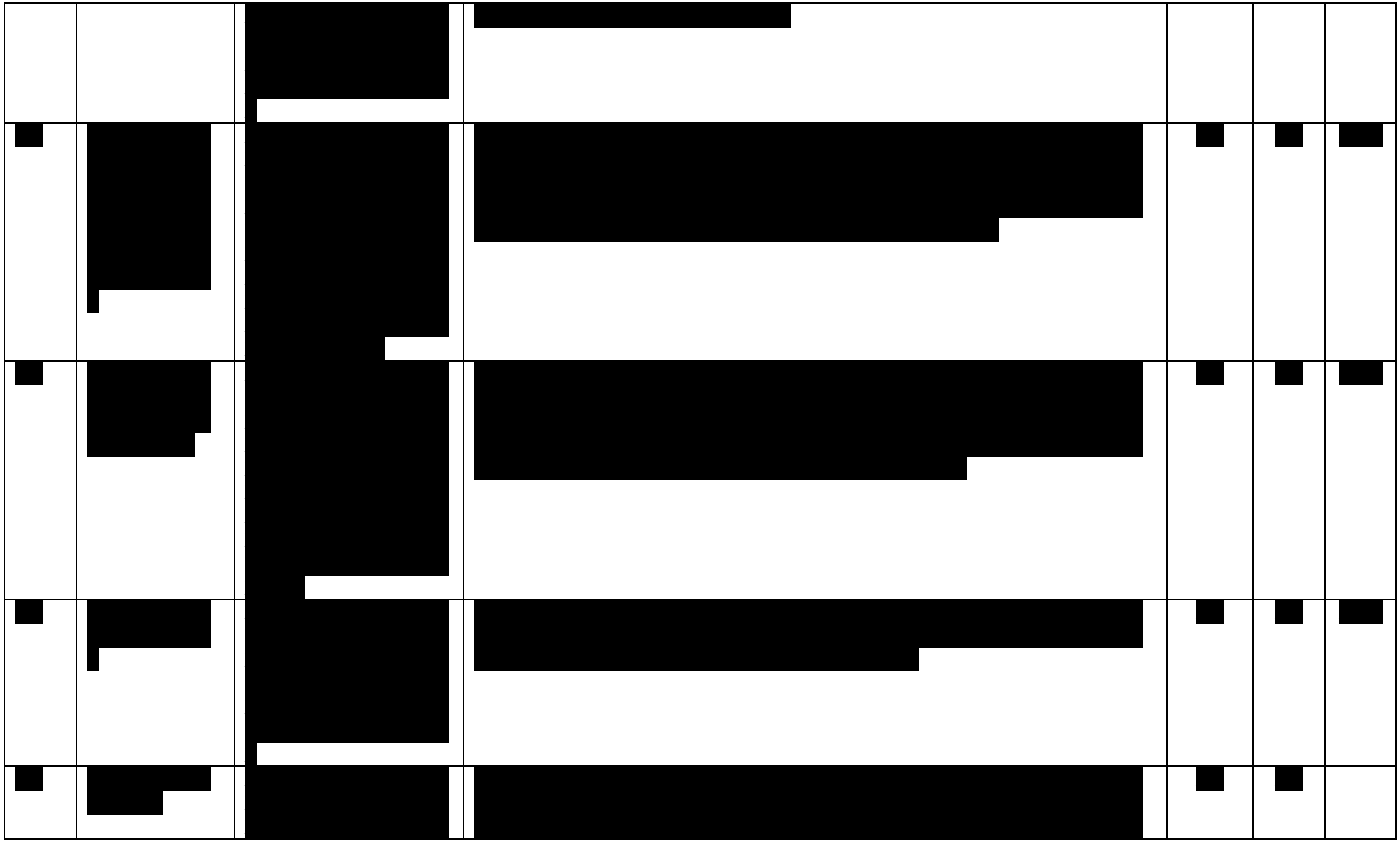
105. In cases where the same check is performed at different times (for example those described by the Conditions for an Identity Assertion) then the following rules apply:
    - The result for the most recent check takes precedence e.g. where a check returned [redacted] but later when the **same** check didn't return [redacted] then it is considered that there is now no [redacted] contra-indicator present from this check.
    - Results from different checks, regardless of the time between when they were done are considered as a whole, e.g. new contra-indictors discovered [redacted] after registration are added to all active contra-indicators discovered from the previous checks.

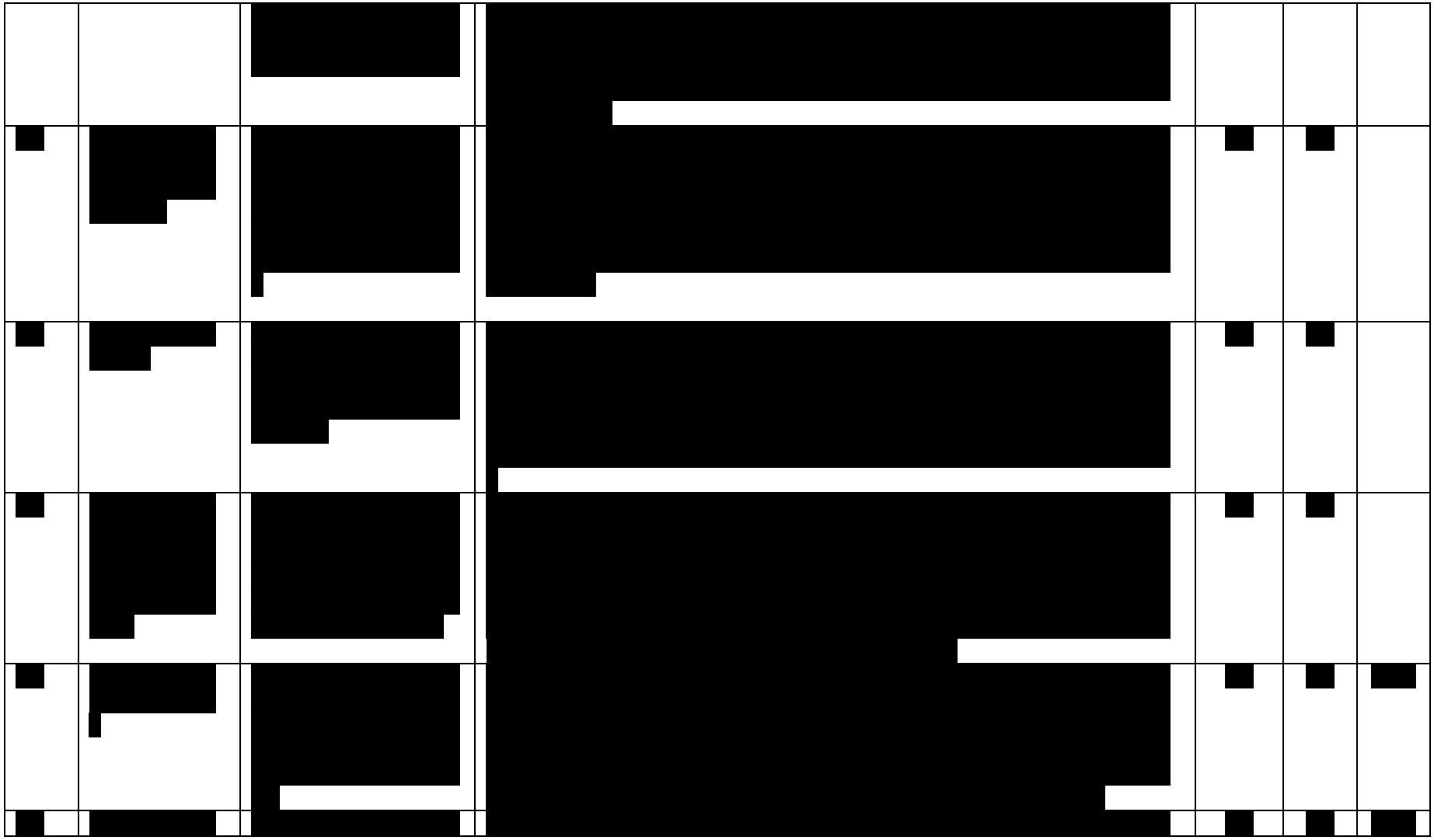
IPV Contra-indicators

ID	Contra-indicator	Details	Mitigating Actions	Found	Pass	FID
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]









[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	

Table 15 Contra-Indicators

Suspicion of Fraud

Relationship between contra-indicators and potential fraud

106. Some contra-indicators may be discovered because the Customer is trying to register an identity that is not their own or are using falsified Identity Evidence. In cases where this is possibility a contra-indictor is also associated to a Fraud Identifier (FID).

107. Simply because the IdP has discovered a contra-indicator that is associated with a FID does not in itself imply that there is an actual fraud only that there is a risk of fraud. In order to determine that there are reasonable grounds to suspect that a fraud may be taking place the FID shall need to be confirmed by following the mitigating actions associated with the contra-indicator.

108. Where the IdP does not have the capability to perform the mitigating action then they cannot apply the 'pass' score and by definition the FID cannot be 'confirmed'.

109. If the IdP is able to resolve the contra-indicator then there is no suspicion of fraud and the FID shall be ignored, however, if after taking the mitigating actions the IdP is still unable to resolve the contra-indicator then the FID shall be considered as being confirmed.

110. FIDs are mutually exclusive warnings and are prioritised as set out in the table below (Table 16 FID Prioritisation). Where an IdP has multiple confirmed FIDs then the one with the highest priority shall take precedence when returning a Fraud Warning to the GDS IDA Hub.

Priority	FID
1	[redacted]
2	[redacted]
3	[redacted]

Table 16 FID Prioritisation

Requirements for Assertion

Identity Review (Including Revalidation)

111. The IdP shall have a review process in order to determine whether the Identity Evidence that has been validated under IPV Element B was reported lost , stolen or revoked soon after the original registration and/or whether the email address used has been confirmed as being under the control of the Customer.

112. The review required is dependent on the level of the identity and are described in the following table. When the timescale for the relevant review has been reached, the IdP must then perform the review before sending the assertion to the GDS IDA Hub. Whether the identity review is performed at the time of an assertion or on the relevant date is a choice for the IdP.

Identity Level	Identity Review Requirements
2	▪ [redacted] the IdP shall ensure that all Identity Evidence that was confirmed as Valid during registration is still Valid, before the next assertion is made. ▪ The IdP shall have confirmed that the email address is under the control of the Customer [redacted].
3	▪ [redacted], the IdP shall ensure that all Identity Evidence that was confirmed as Valid during registration is still Valid, before the next assertion is made. ▪ The IdP shall have confirmed that the email address is under the control of the Customer [redacted].

Table 17 Identity Review

113. If Identity Evidence is found to no longer be valid at the review period then the IdP shall gather replacement Identity Evidence in line with GPG 45. Any new Identity Evidence shall be validated in accordance with GPG 45 and this document and shall be subject to the same review period, [redacted]

114. If Identity Evidence is determined to still be Valid after the final review period then no further reviews are required.

Availability of external sources

115. Where the IdP uses a service provided by a 3rd (e.g. the 'Document Checking Service') for Validation they may also allow an extension to the timeframes above in instances when the 3rd party service is unavailable to the IdP. This extension is limited to a [redacted] and only when it is due to the unavailability of the 3rd party service, this does not apply in

instances where issues within the IdP prevent it accessing the 3rd party service.

Evaluating the Identity

116. The IdP shall make a decision based on the information discovered from the IPV process on whether they should assert the Customer as the Claimed Identity. The IdP shall be confident that they can demonstrate the processes they performed and how they reached their decision in a court of law if required.

Conditions for an Identity Assertion

117. The table below gives guidance on the conditions and circumstances required for asserting the Claimed Identity to the GDS IDA Hub. The conditions for All Levels apply in addition to the specific requirements at Level 2 and Level 3.

Identity Level	Conditions for Assertion
Common	The IdP shall only assert the identity to the GDS IDA Hub when all of the following conditions are met: ▪ The IPV process is compliant with GPG 45 and this document. ▪ The IdP is confident that the Customer meets the requirements of the Identity Level requested as set out in GPG 45 and this document. ▪ The Credential (including process for issuance) is compliant with GPG 44 and this document. ▪ The Customer has successfully authenticated with the IdP using the relevant Credential. ▪ The IdP holds the relevant identity data in accordance with GPG 45 and this document. ▪ The IdP holds the relevant audit data as required by the Contract. [redacted] ▪ All applicable Identity Review conditions have been met.
2	**Requirements for "Common" plus the following**: [redacted]
3	**Requirements for "Common" plus the following**: [redacted]

	[redacted]

Table 18 Conditions for Assertion

Conditions for a Fraud Warning

118. The table below gives guidance on the conditions and circumstances required for sending a Fraud Warning to the GDS IDA Hub and the appropriate code to be included.

Fraud Warning Code	Description	Conditions for code
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 19 Conditions for Fraud Warnings

Fraud warning package

119. When the IdP sends a SAML response indicating that they have rejected a Customer because of a Fraud Warning they shall make available the following information to the GDS IDA Hub Operations Centre on request:
    - A fraud event number unique within the IdP
    - The Claimed Identity
    - All other information gathered/used during the IPV process

- PID
- The FID code
- All the contra-indicators discovered, the source of the contra-indicators and details of the remedial actions taken
- Scores for the each of the IPV elements
- Any other information the IdP used to determine that the Customer may not be genuine

[redacted]

- Date, time and identifier of authentication request from the GDS IDA Hub
- Date, time and identifier of the SAML response from the IdP

SAML Response to GDS IDA Hub

120. If the IdP has met all the Conditions for an Identity Assertion then the IdP shall assert that the Customer has met the level of assurance to the GDS IDA Hub with the Claimed Identity, relevant history and other identity information required as defined by this document and the SAML profile.

121. If the IdP has determined that the Customer has failed to reach the level of assurance required but has not met the conditions for a Fraud Warning then the IdP shall assert that the Customer has failed to reach the level of assurance to the GDS IDA Hub.

122. If the IdP has determined that the Customer has failed to reach the level of assurance required and has met the conditions for a Fraud Warning then the IdP shall return the Fraud Warning Code to the GDS IDA Hub.

Security Operations Function

123. IdP Security Operations functions shall communicate with the GDS IDA Hub Operating Centre over an agreed channel, for the purposes of incident response, vulnerability warnings, security breaches and other Information Assurance and Security matters.

124. It is important that all Security Operations teams work closely with each other, providing mutual support, cooperation and coordination on all matters that relate to the security of the IDA ecosystem or IDA data.