Identity IQ
8.1 Independence of resources ................................................................. 8
9.0 Analytics ............................................................................................. 9
9.1 Service usage metrics ......................................................................... 9
9.2 Metrics type ........................................................................................ 9
9.3 Reporting types .................................................................................. 9
10.0 Resellers ........................................................................................... 9
10.1 Supplier type ..................................................................................... 9
11.0 Staff security ..................................................................................... 9
11.1 Staff security clearance ...................................................................... 9
11.2 Government security clearance ......................................................... 9
12.0 Asset Protection ................................................................................ 9
12.1 Knowledge of data storage and processing locations ......................... 9
12.2 Data storage and processing locations .............................................. 9
12.3 User control over data storage and processing locations ................... 9
12.4 Datacentre security standards ........................................................... 9
12.5 Penetration testing frequency ............................................................. 9
12.6 Penetration testing approach ............................................................. 10
12.7 Protecting data at rest ....................................................................... 10
12.8 Data sanitisation process .................................................................. 10
12.9 Equipment disposal approach ........................................................... 10
13.0 Data importing or exporting ............................................................... 10
13.1 Data export approach ....................................................................... 10
13.2 Data export formats .......................................................................... 10
N/A ........................................................................................................... 10
13.3 Other data export formats ................................................................. 10
N/A ........................................................................................................... 10
13.4 Data import formats ......................................................................... 10
N/A ........................................................................................................... 10
13.5 Other data import formats ................................................................. 10
14.0 Data-in-transit protection .................................................................. 10
14.1 Data protection between buyer and supplier networks ....................... 10
14.2 Other protection between networks ................................................. 10
14.3 Data protection within supplier network ......................................... 10
14.4 Other protection within supplier network ......................................... 11
15.0 Availability and resilience .................................................................. 11
15.1 Guaranteed availability ...................................................................... 11
15.2 Approach to resilience ..................................................................... 11
15.3 Outage reporting .............................................................................. 11
16.0 Identity and authentication ............................................................... 11
16.1 User authentication needed .............................................................. 11
16.2 User authentication .......................................................................... 11
16.3 Other user authentication .................................................................. 11
16.4 Access restrictions in management interfaces and support channels .... 11
16.5 Access restriction testing frequency ............................................... 11
16.6 Management access authentication ................................................ 11
17.0 Audit information for users ............................................................... 11
17.1 Access to user activity audit information ......................................... 11
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2 Access to supplier activity audit information</td>
<td>12</td>
</tr>
<tr>
<td>17.3 How long system logs are stored for</td>
<td>12</td>
</tr>
<tr>
<td>18.0 Standards and Certifications</td>
<td>12</td>
</tr>
<tr>
<td>18.1 ISO/IEC 27001 certification</td>
<td>12</td>
</tr>
<tr>
<td>18.2 Who accredited the ISO/IEC 27001</td>
<td>12</td>
</tr>
<tr>
<td>18.3 ISO/IEC 27001 accreditation date</td>
<td>12</td>
</tr>
<tr>
<td>18.4 What the ISO/IEC 27001 doesn’t cover</td>
<td>12</td>
</tr>
<tr>
<td>18.5 ISO 28000:2007 certification</td>
<td>12</td>
</tr>
<tr>
<td>18.6 CSA STAR certification</td>
<td>12</td>
</tr>
<tr>
<td>18.7 PCI certification</td>
<td>12</td>
</tr>
<tr>
<td>18.8 Who accredited the PCI DSS certification</td>
<td>12</td>
</tr>
<tr>
<td>18.9 PCI DSS accreditation date</td>
<td>12</td>
</tr>
<tr>
<td>18.10 What the PCI DSS doesn’t cover</td>
<td>12</td>
</tr>
<tr>
<td>18.11 Other security certifications</td>
<td>12</td>
</tr>
<tr>
<td>19.0 Security Governance</td>
<td>13</td>
</tr>
<tr>
<td>19.1 Named board-level person responsible for service security</td>
<td>13</td>
</tr>
<tr>
<td>19.2 Security governance certified</td>
<td>13</td>
</tr>
<tr>
<td>19.3 Security governance standards</td>
<td>13</td>
</tr>
<tr>
<td>19.4 Information security policies and processes</td>
<td>13</td>
</tr>
<tr>
<td>20.0 Operational security</td>
<td>13</td>
</tr>
<tr>
<td>20.1 Configuration and change management standard</td>
<td>13</td>
</tr>
<tr>
<td>20.2 Configuration and change management approach</td>
<td>13</td>
</tr>
<tr>
<td>20.3 Vulnerability management type</td>
<td>13</td>
</tr>
<tr>
<td>20.4 Vulnerability management approach</td>
<td>14</td>
</tr>
<tr>
<td>20.5 Protective monitoring type</td>
<td>14</td>
</tr>
<tr>
<td>20.6 Protective monitoring approach</td>
<td>14</td>
</tr>
<tr>
<td>20.7 Incident management type</td>
<td>14</td>
</tr>
<tr>
<td>20.8 Incident management approach</td>
<td>14</td>
</tr>
<tr>
<td>21.0 Secure development</td>
<td>14</td>
</tr>
<tr>
<td>21.1 Approach to secure software development best practice</td>
<td>14</td>
</tr>
<tr>
<td>22.0 Public service networks</td>
<td>14</td>
</tr>
<tr>
<td>22.1 Connection to public service networks</td>
<td>14</td>
</tr>
<tr>
<td>23.0 Pricing</td>
<td>15</td>
</tr>
<tr>
<td>23.1 Price</td>
<td>15</td>
</tr>
<tr>
<td>23.2 Discount for educational organisations</td>
<td>15</td>
</tr>
<tr>
<td>23.3 Free trial available</td>
<td>15</td>
</tr>
<tr>
<td>23.4 Description of free trial</td>
<td>15</td>
</tr>
<tr>
<td>24.0 Documents</td>
<td>15</td>
</tr>
<tr>
<td>24.1 Pricing document</td>
<td>15</td>
</tr>
<tr>
<td>24.2 Service definition document</td>
<td>15</td>
</tr>
<tr>
<td>24.3 Terms and conditions document</td>
<td>15</td>
</tr>
</tbody>
</table>
Identity IQ

1. About the product

The Experian Identity Intelligent Questioning (IIQ) solution is a challenge and response system of identity authentication and verification based on the use of trusted data sources. Customers processed, for example, via a contact centre or the internet will be required to answer randomly selected questions based on the data, which only the legitimate owner of the identity should know. Identity IQ allows for multiple clients with multiple account numbers. The system is highly configurable and is primarily driven by parameters.

2. Product Features

• Available via Experian’s CrossCore Platform/Application Programming Interface (API).
• Available as real time integrated, user interface or batch.
• Easy to understand and intuitive web interface available for results.
• Confirmation of identity at current, previous and linked addresses.
• Confirmation of identity at current, previous and linked addresses.
• Utilises Credit, Voters Roll, CitizenCard, ONS, Adverse Information, Telephone Directory.
• PEPs, Sanctions and Enforcement screening available.
• Includes alerts relating: addresses, age, telephone, deceased individuals and more.
• Aligns to Joint Money Laundering Steering Group (JMLSG) guidelines.
• Full results audit trail

3. Product Benefits

• minimise manual processing and reduce the time taken to authenticate an individual at point of policy or claim
• provide quick, real-time authentication when interacting with customers by phone, internet or face to face
• Improved data audit trail and security
• Increased, real-time confidence in the identity of an individual
• Reducing operational costs and fraud losses.
• eliminating manual paper based processes, allowing resources to be redirected to customer service
• Allowing flexibility per your needs – you decide on the number of questions asked, the number of questions a customer/applicant must answer correctly

4. Service Scope

4.1 Software add-on or extension
No

4.2 Cloud deployment model
Private cloud
4.3 Service constraints
Yes. The service can only be used for identity checking purposes of individuals who have either given consent or you will need to ensure that, within your collection notices, your customer is made aware that their data will be passed to Experian.

4.4 System Requirements
Experian Issued Certificates for API access

5. User Support

5.1 Email or online ticketing support
Email or online ticketing

5.2 Support response times
To manage our client services effectively, and in line with ITIL best practices Experian have defined Service Levels across all core processes (incl. Incident, Service Request, Problem, Change Management etc.). Our Tiered Service Framework allows us to provide differing levels of service and support offerings to meet our client's needs. The Service Tier selected will define the SLAs we work to. Engagement via a SPOC our Experian Service Desk will ensure all interactions are recorded and assessed against impact and severity before being assigned a "Priority".

5.3 User can manage status and priority of support tickets
No

5.4 Phone support
Yes

5.5 Phone support availability
9 to 5 (UK time), Monday to Friday

5.6 Web chat support
No.

5.7 Web chat support availability
N/A

5.8 Web chat support accessibility standard
N/A

5.9 Web chat accessibility testing
N/A
5.10 Onsite support
POA

5.11 Support levels
Standard support is 09:00 - 17:00, enhanced packages offer up to 24/7 support availability, Enhanced support costs are determined by the user requirements.

5.12 Support available to third parties
Yes

6.0 Onboarding and offboarding

6.1 Getting Started
Full user guides available, plus paid-for integration assistance available

6.2 Service documentation
Yes

6.3 Documentation formats
PDF

6.4 End-of-contract data extraction
Upon request

6.5 End-of-contract process
At the end of the contract, the Buyer shall cease to use all Licensed Materials and Licensed Programs

7.0 Using the service

7.1 Web browser interface
Yes

7.2 Supported browsers

Internet Explorer 8
Internet Explorer 9
Internet Explorer 10
Firefox
Chrome
Safari 9+
Opera
7.3 Application to install
Yes

7.4 Compatible operating systems
Linux or Unix

7.5 Designed for use on mobile devices
No

7.6 Accessibility standards
None or don’t know

7.7 Description of accessibility
The product is available as a screen based option, or an API version which can be integrated in the client system, environment and screens.

7.8 Accessibility testing
None

7.9 API
Yes

7.10 What users can and can’t do using the API
Full service functionality provided via API

7.11 API documentation
Yes

7.12 API documentation formats
Open API (also known as Swagger)
HTML

7.13 API sandbox or test environment
Yes

7.14 Customisation available
Yes

7.15 Description of customisation
The solution allows a small amount of customisation using pre-defined parameters.

8.0 Scaling

8.1 Independence of resources
Full load balancing, multiple data centres
9.0 Analytics

9.1 Service usage metrics
Yes

9.2 Metrics type
Usage metrics are partially available across software suite.

9.3 Reporting types
API access

10.0 Resellers

10.1 Supplier type
Not a reseller

11.0 Staff security

11.1 Staff security clearance
Other security clearance

11.2 Government security clearance
None

12.0 Asset Protection

12.1 Knowledge of data storage and processing locations
Yes

12.2 Data storage and processing locations
United Kingdom

12.3 User control over data storage and processing locations
No

12.4 Datacentre security standards
Complies with a recognised standard (for example CSA CCM version 3.0)

12.5 Penetration testing frequency
At least once a year
12.6 Penetration testing approach
Another external penetration testing organisation

12.7 Protecting data at rest
Physical access control, complying with another standard

12.8 Data sanitisation process
No

12.9 Equipment disposal approach
Another external penetration testing organisation

13.0 Data importing or exporting

13.1 Data export approach
Data is not required to be imported by the Buyer to Experian's platform therefore data export is not required

13.2 Data export formats
N/A

13.3 Other data export formats
N/A

13.4 Data import formats
N/A

13.5 Other data import formats
N/A

14.0 Data-in-transit protection

14.1 Data protection between buyer and supplier networks
TLS (version 1.2 or above)
Other

14.2 Other protection between networks
SOAP endpoint sslv3/tls1.0/1.1/1.2
REST endpoint TLS1.2

14.3 Data protection within supplier network
TLS (version 1.2 or above)
14.4 Other protection within supplier network
SOAP endpoint sslv3/tls1.0/1.1/1.2
REST endpoint TLS1.2

15.0 Availability and resilience

15.1 Guaranteed availability
Per SLA

15.2 Approach to resilience
Experian data centres complies with the Experian Global Security Policy which is available on request.

15.3 Outage reporting
We will notify you of any material outages, that may affect you, by email.

16.0 Identity and authentication

16.1 User authentication needed
Yes

16.2 User authentication
Username or password
Other

16.3 Other user authentication
Secure token

16.4 Access restrictions in management interfaces and support channels
Users have their access controlled using a user role and security group function. In addition, access, can be restricted to specific client IP addresses.

16.5 Access restriction testing frequency
At least once a year

16.6 Management access authentication
Username or password

17.0 Audit information for users

17.1 Access to user activity audit information
Users contact the support team to get audit information
17.2 Access to supplier activity audit information
Users contact the support team to get audit information

17.3 How long system logs are stored for
At least 12 months

18.0 Standards and Certifications

18.1 ISO/IEC 27001 certification
Yes

18.2 Who accredited the ISO/IEC 27001
DNV GL Business Assurance Limited

18.3 ISO/IEC 27001 accreditation date
20/12/2016

18.4 What the ISO/IEC 27001 doesn’t cover
The following is covered by the scope of the certificate; the delivery and support of Experian IT infrastructure, operations, architecture and associated compliance and facilities management undertaken within the UK data centres.

18.5 ISO 28000:2007 certification
No

18.6 CSA STAR certification
No

18.7 PCI certification
Yes

18.8 Who accredited the PCI DSS certification
Trustwave

18.9 PCI DSS accreditation date
28th October 2016

18.10 What the PCI DSS doesn’t cover
Everything is covered

18.11 Other security certifications
No
19.0 Security Governance

19.1 Named board-level person responsible for service security
Yes

19.2 Security governance certified
Yes

19.3 Security governance standards
ISO/IEC 27001

19.4 Information security policies and processes
Experian have a comprehensive global security policy based on the ISO27001 standard which covers: Organisation and Management, information security, asset classification, physical and environmental security, communications and operations management, system access, systems development and maintenance, compliance, personnel and provisioning, business continuity management, third party management. The policy is owned by Experian's executive risk management committee which is an executive level body, and which assumes ultimate responsibility for Experian's risk position. Information security is a key component of the risk management framework. Experian management supports security through leadership statements, actions and endorsement of the security policy and implementing/improving the controls specified in the policy. The policy is available to all Experian employees and contractors on the intranet. Changes to the policy are announced on the company's intranet computer based information security and data protection training, and this is repeated on at least an annual basis. Compliance to policy is overseen by internal audit.

20.0 Operational security

20.1 Configuration and change management standard
Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402

20.2 Configuration and change management approach
Experian have a change management policy which is underpinned by processes and procedures based on ITIL best practice. This is a mature process. We use a service management tool that integrates change management, incident management, problem management, configuration management and knowledge management. Our change management policy, processes, and procedures are regularly audited by independent auditors. Formal risk analysis is employed using an approved information risk analysis phase for developments/changes. Security requirements for the system are identified and continue to be considered throughout the life of the product.

20.3 Vulnerability management type
Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402
20.4 Vulnerability management approach
Servers and PCs are built to a documented secure standard, which includes anti-virus and malware defences. Information assets have a defined patching schedule, determined by the system's criticality and the level of threat the patch is mitigating. Experian actively monitors threat environment and checks the effectiveness of security controls by reviewing both free and paid for sources of threat information, including, public information, major vendor feeds and also receiving information from specialist closed group mailing lists. The overall process is also plugged into an automated patch and fix strategy, underpinned with a technology infrastructure to deliver corrective updates.

20.5 Protective monitoring type
Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402

20.6 Protective monitoring approach
Monitoring processes and tools are in place to manage alarms generated by security related alerts and these are fed into the incident management process. Experian has a formally documented risk based incident management process to respond to security violations, unusual or suspicious events and incidents. In the event an incident occurs a team of experts from all relevant areas of Experian are gathered to form an incident response team, who manage activities until resolution. The incident response team are available 24/7 to resolve any incident. Out of core hours the dedicated incident hotline is routed to the command centre

20.7 Incident management type
Conforms to a recognised standard, for example, CSA CCM v3.0 or ISO/IEC 27035:2011 or SSAE-16 / ISAE 3402

20.8 Incident management approach
The incident management process incorporates a number of participants and contributors, including: Global Security Office - who facilitate and coordinate activities under the business security coordinator's guidance; Business Security Coordinator - a representative of the impacted business area, responsible for coordinating resolution activities; Incident Response Team (IRT) - IRT is made up of a membership that are empowered to make key decisions surrounding the actions to be taken to reduce impact, control actions, and impose corrective activities. A client report would be created, including: high level overview; facts; overview of events; actions taken.

21.0 Secure development

21.1 Approach to secure software development best practice
Independent review of processes (for example CESG CPA Build Standard, ISO/IEC 27034, ISO/IEC 27001 or CSA CCM v3.0)

22.0 Public service networks

22.1 Connection to public service networks
No
23.0 Pricing

23.1 Price
Volume based transactional pricing 0.35p-£2.98

23.2 Discount for educational organisations
N/A

23.3 Free trial available
Proof of concept for small volume of transactions, upon request

23.4 Description of free trial
Client provides data for processing against service in an offline environment, to allow analysis of results to define strategy