Scottish Government

Online Identity Assurance Programme

Technical Discovery

Architecture Principles

Status:	Baselined
Version:	1.00
Date:	01-Jun-18

Contents

1. Introduction

This document details the Architecture Principles to which the Scottish Government Online Identity Assurance Programme adheres.

Each principle is an enduring rule that applies to the OIA Solution; therefore it is necessary for the principles to be considered when specifying, scoping, delivering, implementing or amending the OIA Solution.

The Architecture Principles have been developed on the basis of the guidance published at github.com/scottishgovernment, which in turn are based on "The Open Group Architecture Framework" (TOGAF) www.opengroup.org (see Appendix 2 for copyright notice).

TOGAF defines architecture principles as follows:

Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organization sets about fulfilling its mission. In their turn, principles may be just one element in a structured set of ideas that collectively define and guide the organization, from values through to actions and results.

The purpose of this set of architecture principles is to provide a framework for making well informed business, technical, security, privacy and commercial decisions in the OIA Programme.

It is expected that these architecture principles will change over time in response to events and as the intentions of the OIA Programme and its stakeholders develop over time.

At the present time the architecture principles are intended as guidance rather than prescriptive rules – however any intention to diverge from the architecture principles should be acknowledged and justified – and could result in a change to the principles to accommodate the non-compliant aspect.

2. Glossary

A glossary of terms used in this document is available as a separate document.

3. Scotland's Digital Future: High Level Operating Framework

The Scottish Government has published a document entitled "*Scotland's Digital Future: High Level Operating Framework*" (the "HLOF"). The HLOF is currently at version 2 and is publically available at: http://www.gov.scot/Publications.

The overview of the HLOF states "*The High Level Operating Framework provides: principles for use when designing ICT solutions, by promoting and supporting the use of commonly agreed standards and specifications, and providing an information assurance approach in turn promoting the digital first approach. The collaboration and integration that this supports, with a focus on re-use before buy, will help eliminate duplication and avoidable spend.*".

The Architecture Principles for Online Identity Assurance will build upon the core Architecture Principles set out in the HLOF which applies to all Scottish Government ICT solutions.

In general this document includes the Architectural Principles from the HLOF by reference rather than by duplication; however for convenience a summary of each HLOF principle is included here. If the HLOF is significantly revised, replaced or withdrawn in the future this document will need to be reviewed to ensure completeness, consistency and relevance.

3.1. Strategic Principles

HLOF sets out the following four "Strategic Principles":

Strategic Principle	Notes
Customer and citizen focus	Applies
Privacy and openness; using data appropriately	Applies
A skilled and empowered workforce	Applies
Collaboration and value for money	Applies

3.2. HLOF Architecture Principles supporting Customer and Citizen Focus

HLOF sets out the following architecture principles that support the strategic principle of Customer and Citizen Focus.

Reference	Architecture Principle	Notes
OFP-CC1	Digital Standards	Applies
OFP-CC2	Multi-channel	Applies
OFP-CC3	Verification and easy sign-in for citizen access	HLOF states "Public Sector organisations will use the national *myaccount* service to verify the identity of citizen access to digital public services as a default.". Whilst OIA supports the underlying objectives of this HLOF principle it is recognised that solutions in addition to (or other than) myaccount will be considered for OIA.

3.3. HLOF Architecture Principles supporting Privacy and Openness

HLOF sets out the following architecture principles that support the strategic principle of Privacy and Openness.

Reference	Architecture Principle	Notes
OFP-PO1	Data Management – Open Data	Applies – however relevance may be limited as OIA not expected to process data that is appropriate for "open publishing".
OFP-PO2	Data Management – Data Sharing	Applies – however relevance may be limited as OIA not expected to process data that is appropriate for sharing.

3.4. HLOF Architecture Principles for a Skilled and Empowered Workforce

HLOF sets out the following architecture principles that support the strategic principle of a Skilled and Empowered Workforce.

Reference	Architecture Principle	Notes
OFP-SW1	ICT Workforce Capability	Applies
OFP-SW1.2	ICT Workforce Capability – Enterprise Architecture Skills	Applies (although it is noted OFP-SW1.2 reads more as an aspiration than a principle)

3.5. HLOF Architecture Principles for Collaboration and Value for Money

HLOF sets out the following architecture principles that support the strategic principle of Collaboration and Value for Money.

Reference	Architecture Principle	Notes
OFP-CV1	Reuse, before buy, before build	Applies – OIA is broadly conceived as a reusable component
OFP-CV2	Collaboration	Applies – OIA should be a key enabler for collaboration
OFP-CV3	*not used in HLOF*	
OVP-CV4	Use of Open Standards in Software	Applies
OVP-CV5	Use of Open Source Software	Applies with amendment. OVP-CV5 states: "*Wherever possible, and subject to compliance with the principles of fair and open procurement, organisations should seek to procure new or upgraded ICT services based on Open Source software*". For OIA this will be interpreted as starting "*Wherever reasonably practicable…*".
OFP-CV6	Single approach to identity & access management for public sector employees	Applies – Relying Parties could choose to use OIA to manage identities used by system users (e.g. for role-based access control) however they will not be required so to do.
OFP-CV7	Enterprise architecture approach to ICT planning	Applies – OIA should be progressed as part of a portfolio approach to the provision of Scottish Government systems.
OFP-CV8	Service Oriented Approach (SOA) to Design of ICT Solutions	Applies (although it is noted OFP-CV8 reads more as an aspiration than a principle). Closely related to (or dependent on) OFP-CV7.

4. Business Principles – User Related

4.1. PBU01 – Trusted, Transparent and Open

4.1.1. Statement

In general the Target Cohort should understand (at a high-level) the purpose and operation of the OIA Solution and how their identity is established, used and shared.

4.1.2. Rationale

If Citizens understand how their identity is established, used and shared this will increase their confidence in the OIA Solution and will therefore encourage them to participate.

4.1.3. Implications

This principle relies on the OIA Programme's core commitment and philosophy to be open about all aspects of the programme.

Each IDP or RP must be able to justify to Citizen why their Identity data is being processed. The information provided will include a clear explanation of why any specific information has to be provided by the Citizen (e.g. in order that a particular level of identity assurance can be obtained) and identifies any related obligations on the part of the RP.

Each Citizen must be offered a clear description about the processing of Identity data in advance of any processing. IDPs must be transparent with users about their service works. Any future material changes must only come into effect if the user is made aware and consents subsequent.

The activities necessary to appropriately engage the Target Cohort in order to build a level of understanding will be a significant element of the OIA Programme running in parallel with implementing the technical solution.

4.1.4. Notes

1. Adherence to this principle could be key to the success of the OIA Programme.

4.2. PBU01A – Citizen Control

4.2.1. Statement

Citizens can exercise control over identity assurance activities affecting them and these can only take place with their consent.

4.2.2. Rationale

Users will want to exercise control over the use of their identity.

4.2.3. Implications

An IDP or RP must ensure any collection, use or disclosure of Identity Data is consented by the respective Citizen.

4.2.4. Notes

1. Based on Verify PCAG IDA Principle

4.3. PBU01B – Citizen Access

4.3.1. Statement

IDPs and RPs must provide all Identity data related to a Citizen promptly on (valid) request.

A Citizen can export or delete their Identity data from an IDP readily and at any time.

4.3.2. Rationale

Citizens have an expectation that they will be able to access their own Identity data and can readily move from their established Identity one IDP to another without this impacting their established LoA.

4.3.3. Implications

Each IDP and RP must allow, promptly on request and free of charge, each Citizen access to any Identity data relating to that Citizen.

A Citizen must be able to require an IDP to securely transfer their Identity data to another IDP in a form that is supported by all IDPs, free of charge and without impediment or delay.

IDPs must be able to exchange the LoA for a Citizen in a trusted manner without technical or commercial barriers.

4.3.4. Notes

1. This assumes multiple IDPs are participating in the OIA Solution.
2. This could be split into two separate principles for "access" and "delete/move" – and the latter could itself be split.
3. This principle may be challenging to implement and will be kept under review.

4.4. PBU02 – Worthwhile [*Citizen-Centric*]

4.4.1. Statement

In general the Target Cohort must be able to see a net benefit from using the system.

4.4.2. Rationale

If it is accepted that use of the OIA Solution by Citizens is not mandatory then Citizens will only use the system if it is preferable to the available alternatives. Online banking is a useful comparator.

4.4.3. Implications

The OIA Solution must be built from a "citizen-centric" perspective. Although Citizens may not usually interact directly with the OIA Solution (because user interfaces will be provided by RPs and IDPs) the design and processes of the OIA Solution will strongly influence User Experience (UX) (see Wikipedia).

Design of the OIA Solution must take into account the full range of use cases, particularly scenarios where issues are encountered (e.g. an Authentication is rejected or a Citizen is unable to provide required evidence when seeking to establish their Identity).

4.4.4. Notes

1. This principle aligns to the OIA Programme Service Design workstream.
2. Experience of other comparable schemes (such as GOV.UK Verify) should be taken into account.

4.5. PBU03 - Easy to Use

4.5.1. Statement

The OIA Solution must be regarded as usable by the Target Cohort.

4.5.2. Rationale

It is a basic tenet of the programme that the solution should be convenient for users to utilise so as to enable the widest possible take-up.

4.5.3. Implications

This principle will ensure that any solution element that is exclusive (i.e. there is/are no alternative(s)) and which is not generally usable by the Target Cohort is rejected. For example a solution that depends on each Citizen having a valid Driving Licence would be rejected.

4.5.4. Notes

1. Target Cohort requires definition - for example what age group does the Target Cohort start at?
2. Is some kind of quantitative measure required for example "*The OIA Solution is rated as "usable" or better by more than 90% of a representative cross-sectional sample of the Target Cohort [during the Beta Project].*"?

4.6. PBU04 - Proportionate

4.6.1. Statement

The OIA Solution must be regarded as proportionate by the Target Cohort.

4.6.2. Rationale

Use cases needing to establish a low-level of identity assurance to complete a routine task (e.g. interactions with a Local Authority about perceived service issues) should not be required (by the OIA Solution to provide the same level of evidence as use cases for more sensitive tasks (e.g. accessing medical or tax records).

4.6.3. Implications

A given Identity may have varying levels of assurance over time. In general this would be expected to be that trust in a given Identity would *increase* over time – however there may be circumstances where it is appropriate to reduce the level of trust, for example if anomalous behaviour is identified or expected.

4.6.4. Notes

1. Business processes to enable individuals to increase their level of assurance through a range of mechanisms will need to be defined, agreed and implemented and fully supported by the OIA Solution

4.7. PBU05 - Single Identity [*Tell us Once*]

4.7.1. Statement

The OIA Solution must enable a Citizen to establish their Identity "in one place" and for that Identity to then be used and trusted by all RPs.

4.7.2. Rationale

This principle reflects a core driver for the OIA Solution. Adherence to this principle is effectively an objective of the OIA Programme.

4.7.3. Implications

A given Identity may have varying levels of assurance over time. In general this would be expected to be that trust in a given Identity would *increase* over time – however there may be circumstances where it is appropriate to reduce the level of trust, for example if anomalous behaviour is identified or expected.

4.7.4. Notes

1. This principle relates solely to the pure concept of an Identity not to other data that is associated with that Identity. For example whilst a Citizen may have a common Identity that is established once and then utilised in interactions say with health providers and social security if their primary address changes and is reported via one RP that updated address may or may

not be cascaded to other RPs that subscribe to that Identity. That would be a separate design choice which would have a number of variants (e.g. automated cascading vs cascading controlled by the Citizen). The ability to do this would also be influenced by the high-level solution design – for example are Personal Data Stores part of the solution?

2. The "in one place" wording of this principle is not intended to preclude the use by a Citizen of more than one IDP.

4.8. PBU06 - Accessible and Available

4.8.1. Statement

The OIA Programme intends that the OIA Solution should be available for use by as many Citizens as is reasonably practical. "Available for use" includes use by Citizens

- who have mental or physical impairments;
- who do not have access to dedicated ICT (but can access shared ICT facilities e.g. at a public library or hostel); and
- regardless of geographic location (within Scotland).

4.8.2. Rationale

If Citizens wish to use the OIA Solution there should be no barriers preventing them from doing so.

4.8.3. Implications

The phrasing "as reasonably practicable" is included so that there is not an absolute requirement to achieve 100% availability for use - which is considered to be impractical.

4.8.4. Notes

1. This principle should serve to prevent solutions being adopted that do not support the wider Target Cohort.
2. The ability to meet this principle will be influenced by the success of other initiatives for "digital inclusivity" or the equivalent.
3. The ability to meet this principle will be influenced by the availability for use of RPs services – if these are not available for use then it is unlikely that access to the OIA Solution will be of any value to the Citizen concerned.

4.9. PBU07 - Usage Optional

4.9.1. Statement

Users who are not willing or able to use the OIA Solution should have reasonable alternative methods available to them to enable them to access services provided by RPs.

4.9.2. Rationale

It is not acceptable to require Citizens to use the OIA Solution.

4.9.3. Implications

All services must continue to offer access channels for Citizens that do not use the OIA Solution.

Whilst it would not be acceptable for RPs to provide deliberately arcane alternative channels it should be accepted that non-digital alternatives may be less convenient than the use of mainstream digital services.

Usage of the OIA Solution could be more complex than a simple "yes/no" (binary) decision. Potentially Citizens may wish to be able to:

- use the OIA Solution for some supported services but not others; and/or
- use some functionality of the OIA Solution but not all; or
- some combination of the above.

Design decisions will need to be made as to whether this flexibility should be included in the system specification and if so with what priority.

4.9.4. Notes

4. This principle may apply more to RPs than to the OIA Programme or the OIA Solution because in general it would not be the responsibility of the OIA Programme to offer solutions that are not the OIA Solution. For example claiming a social security benefit in person rather than via a digital service would be a channel offered and provided by the specific agency e.g. Social Security Scotland, not by the OIA Programme.

4.10. PBU08 - Limited Scope

4.10.1. Statement

Interactions using the OIA Solution shall use only the minimum necessary Identity data.

4.10.2. Rationale

The OIA Solution should only be used by an RP where a genuine need has been established and only to the appropriate minimum Level of Assurance.

4.10.3. Implications

Identity data processed by an IDP or an RP to undertake Authorisation of a requested transaction by a Citizen must be the minimum necessary in undertake that Authorisation in a secure and (if necessary) auditable manner.

When a Citizen ends their relationship with an IDP, the Citizen's identity data must be deleted by the IDP. Data may be retained only where required for specific, targeted fraud, security or other criminal investigation purposes.

4.10.4. Notes

1. Based on Verify PCAG IDA Principle

5. Business Principles – Data Related

5.1. PBD01 – Ownership & Control

5.1.1. Statement

Any data relating to the identity of a specific Citizen that is stored or processed by the OIA Solution shall remain the property of that Citizen and processed on their behalf by the OIA Solution.

5.1.2. Rationale

Citizens will have a reasonable expectation that they will retain control over their identity profile.

5.1.3. Implications

This principle may shape technical and commercial approaches for the provision of the OIA Solution as different approaches may offer different levels of ownership & control to the Citizen.

5.1.4. Notes

1. There will be a need in the future to determine the detail of what is meant by "ownership & control".

5.2. PBD02 – Data Standards

5.2.1. Statement

The OIA Solution will require all participants to adhere to defined and agreed OIA Data Standards.

5.2.2. Rationale

The OIA Solution will "source and sink" data to and from a number of RPs and IDPs. Individual participants will have internal data stores (and supporting algorithmic processing). The meaning of data and information shared via the OIA Solution must be consistent in presentation, metadata and level of confidence.

5.2.3. Implications

The OIA Programme will need to define appropriate OIA Data Standards and publish these.

Testing and assurance will be required to demonstrate that participants are able to meet the OIA Data Standards.

5.2.4. Notes

1. OIA Data Standards should be open not proprietary.
2. Existing industry standards should be reviewed to determine if they are appropriate for adoption as all or part of the OIA Data Standards.

5.3. PBD03 – Legislative Compliance

5.3.1. Statement

The OIA Solution and the use thereof will be compliant with all relevant legislation including, but not limited to the General Data Protection Regulation (GDPR).

5.3.2. Rationale

The solution and the way that it is used must meet or exceed all legal standards.

5.3.3. Implications

As the OIA Solution is developed the OIA Programme must ensure legislative compliance, including if necessary, taking appropriate steps to ensure the legislative compliance of vendors and third parties including IDPs and RPs.

5.3.4. Notes

1. Whilst it may seem obvious that the solution and the way that it is used must meet or exceed all legal standards it is considered worth stating as a principle to encourage compliance to be considered throughout the lifecycle.

6. Business Principles – Commercial Related

6.1. PBC01 – Compliant with Procurement Regulation

6.1.1. Statement

The OIA Programme must be compliant with all applicable public procurement regulations at all stages of the lifecycle.

6.1.2. Rationale

As a major public sector initiative the programme will be subject to the public procurement regulations and failure to comply would add significant risk to the programme's ability to deliver in accordance with the agreed objectives and potentially could result in litigation.

6.1.3. Implications

The applicability of public procurement regulations could constrain the technical solution and delivery model for the OIA Programme and the OIA Solution. Awareness of this will enable any constraints to be acknowledged at every stage from shaping the proposed Alpha Phase.

6.1.4. Notes

1. It is beyond the scope of this document to consider potential procurement implications in detail. This principle is intended to serve as a prompt to ensure that procurement matters are given due consideration.

6.2. PBC02 – Intellectual Property Rights

6.2.1. Statement

The OIA Programme must be clear about the provenance and ownership of all intellectual property used or generated during the lifecycle of the OIA Solution.

6.2.2. Rationale

The intellectual property inherent in the OIA Solution could have significant value. Clearly any existing proprietary products that are selected to be included in the solution will be owned by the respective vendors.

6.2.3. Implications

Ownership of each individual's identity data needs to be fully understood. It is assumed that such data would either be retained by the Citizen or would be owned by the Scottish Government or by a trusted third party such as an arm's length body (or some combination). Identity data would not be the property of any software provider, cloud services provider etc.

Any existing proprietary products that are selected to be included in the solution will be owned by the respective vendors who will retain the related IP.

6.2.4. Notes

1. Where proprietary products or services (including PaaS or SaaS) are being used the IP considerations will be more complex and vendors' standard terms and conditions may not align fully to the needs and expectations of the OIA Programme.
2. This principle is subject to expert review.

6.3. PBC03 – Participation Agreement

6.3.1. Statement

Each IDP and RP will be required to enter into a formal Participation Agreement that will govern how they interact with the OIA Solution.

6.3.2. Rationale

A formal agreement is required to set out what is (and potentially is not) acceptable use of the OIA Solution. For example this could:

- require appropriate protection of sensitive data;
- require a level of vetting of individuals accessing the OIA Solution;
- prohibit use of the OIA Solution other than for specific agreed purposes; and
- prohibit use of the OIA Solution for commercial gain.

6.3.3. Implications

IDPs and RPs will be clear about their responsibilities and the implications of any failure to comply.

6.3.4. Notes

1. It may be that a single Participation Agreement can apply to both IDPs and RPs or conversely that specific variants are necessary to reflect the different interactions of the two roles.

7. Technology Principles - Standards

7.1. PTS01 – Scottish Government Standards

7.1.1. Statement

The OIA Solution must (wherever practicable) adhere to all applicable technical standards issued, mandated or recommended by the Scottish Government.

7.1.2. Rationale

As part of the infrastructure for the Scottish Government and the wider public sector of Scotland the OIA Solution should align to common standards as this should in general:

- improve quality;
- support sharing;
- support integration;
- reduce costs;
- promote re-use; and
- increase security.

7.1.3. Implications

This principle will ensure that the OIA Solution is engineered so as to be capable of forming a core element of the Scottish digital infrastructure for the long term.

7.1.4. Notes

1. Information is required to determine where such standards are published. Is there a common, core set?

8. Technology Principles - Sustainability

8.1. PTU01 – Flexibility

8.1.1. Statement

The OIA Solution must be positioned to be able to adopt changes in Identification, Authentication and Authorisation using such an identity.

8.1.2. Rationale

The OIA Solution is intended to be a long term element of public sector digital service provision in Scotland. Identity assurance is an area with constant change and evolution. This includes changes in citizen's knowledge, appetites and expectations of digital services and identity management as well as new technical solutions (and enhancements to existing technical solutions) and new ways of providing and consuming digital services.

In order to be able to develop a solution against this constantly "moving target" it is critical to build flexibility in to the design and implementation of the solution the OIA Solution.

8.1.3. Implications

The architecture of the OIA Solution should take into account the need for flexibility and balance this against the ability to meet agreed "Day 1" requirements.

The OIA Solution is never likely to be complete (or "done" in Agile terminology).

The OIA Solution should have a clear roadmap (both before and after go-live) that sets out a programme of enhancements over time. The roadmap will be adjusted as necessary if priorities change and new opportunities emerge and will be informed by the Product Backlog see: https://www.scrumguides.org/productbacklog or equivalent.

8.1.4. Notes

1. Whilst this principle currently references an Agile approach the core principle will apply regardless of methodology.

8.2. PTU02 – Scalability

8.2.1. Statement

The OIA Solution must be able to operate efficiently and affordably across a range of business volumes.

8.2.2. Rationale

There will be several potential business volume metrics for the OIA Solution such as:

- number of RPs;
- number of Citizens having registered identities; and

- average number of authentication requests per Citizens.

Take-up of the service will be determined by RPs and Citizens and cannot be determined by the service owner, i.e. the "roll-out" of the service is demand-driven. This means that the business volumes, which in turn set the necessary processing capacity of the OIA Solution, are not readily predictable.

For these reasons a solution is required that can operate initially with low business volumes and yet can scale up to the maximum supported business volumes – whilst recognising that in practice these volumes may or may not be reached in practice.

8.2.3. Implications

Architecture, hosting, licensing (if any) and the supporting commercial terms for the solution must address the necessary scalability of the OIA Solution.

Testing and assurance of the solution (particularly performance and stress testing) should be specified so as to prove the scalability of the system at the earliest possible stage.

8.2.4. Notes

1. It is recommended that a clear range of (minimum and maximum) business volumes to be supported is documented by the OIA Programme at an early stage. Once in place this can be used to validate and compare solution options and potential costs.

8.3. PTU03 – Lifecycle Costs

8.3.1. Statement

The OIA Solution must be shaped with appropriate consideration for all costs that will be incurred from initiation to decommissioning to ensure that the most economically advantageous[1] approach is adopted.

8.3.2. Rationale

Costs for the OIA Solution will be incurred across the full system lifecycle such as:

- initiation;
- specification;
- design;
- configuration, implementation and/or build;
- testing and assurance;
- hosting (inc. cloud), operation and licences;
- support and maintenance; and
- decommissioning.

[1] "most economically advantageous" can be broadly interpreted for the purposes of this document as meaning the optimum balance of costs against benefits.

8.3.3. Implications

A solution is required that is affordable across the full lifecycle.

The allocation of costs across the user base must be clear, equitable and incentivise adoption.

8.3.4. Notes

None

8.4. PTU04 – Continuous Improvement

8.4.1. Statement

The OIA Solution will be developed and operated in accordance with the principles of continuous improvement.

8.4.2. Rationale

Implementing effective processes to capture and address opportunities for the OIA Solution to improve performance or address weaknesses will increase its value to Citizens and RPs and/or reduce costs.

8.4.3. Implications

Each individual involved in the provision of the OIA Solution should be aware of the commitment to continuous improvement and how they should support that commitment.

Technical solutions and methodologies that are compatible with the principles of continuous improvement should be preferred.

Continuous improvement will need to be implemented within a change and release management discipline.

8.4.4. Notes

1. It may be that an aspiration to adhere to and benefit from continuous improvement is better documented elsewhere rather than as an architecture principle.

8.5. PTU05 – Supportability

8.5.1. Statement

The OIA Solution must provide a high quality of service across its full operational lifecycle.

8.5.2. Rationale

The OIA Solution is expected to form a core element of the Scottish digital infrastructure for the long term and will be relied upon by Citizens and RPs and therefore must be reliable and available at all times.

8.5.3. Implications

The OIA Solution will require maintenance and support arrangements that are compliant with industry best practice to be in place throughput.

Selection of solution components should take into account their maintainability and supportability.

The OIA Solution should include a capability for self-monitoring to proactively identify issues as they occur (or are believed likely to occur) and to flag these conditions automatically to the support team for action.

8.5.4. Notes

1. ITIL® is a mature and widely adopted approach to service management - see: https://www.axelos.com/itil.

9. Technology Principles - Management

9.1. PTM01 – Audit

9.1.1. Statement

The OIA Solution must support an audit function.

9.1.2. Rationale

The nature of the OIA Solution means that potentially it could be used (or attempts made to use it) for unauthorised purposes. Therefore it is important that there is a means to monitor activity and flag unexpected activity as an "event" in real time and/or log that activity for later analysis and investigation.

9.1.3. Implications

The audit function could in itself be subject to misuse (or attempted misuse) and this must be factored into its design and the processes, controls and authorisation for access to audit data.

Audit requirements (in a general sense) should be considered as part of the solution requirements (e.g. the Product Backlog) to ensure they are fully taken into account.

9.1.4. Notes

1. The relationship (or trade-off) between audit capability and privacy will need to be carefully managed.

9.2. PTM02 – Management Information

9.2.1. Statement

The OIA Solution must provide usage data including uncompleted usage episodes

9.2.2. Rationale

Take-up will be a key success indicator for the OIA Solution. Therefore having a rich understanding of how the system is being used and what actual or perceived barriers may exist is important as it will enable the user experience to be improved over time on the basis of reliable evidence.

9.2.3. Implications

Management information should not include any information specific to any individual and hence should not conflict with privacy concerns

9.2.4. Notes

None.

10. Technology Principles - Integration

10.1. PTI01 – Solution Scope

10.1.1. Statement

The OIA Solution will handle Identification and Authentication actions for RPs but not Authorisation which will be the responsibility of the RP's internal systems.

10.1.2. Rationale

Authorisation (broadly the question "what actions is the individual who has authenticated with Identity X permitted to undertake?") is an internal matter for each RP and the means of implementation (e.g. Role Based Access Control) will be dependent on their internal systems and processes.

10.1.3. Implications

This principle has the effect of constraining and clarifying the scope of the OIA Solution.

10.1.4. Notes

1. RPs may need to adapt their internal systems and processes in order to use Identities authenticated by the OIA Solution.

10.2. PTI02 – Defined Interfaces

10.2.1. Statement

The technical interfaces to be used by IDPs and RPs to fully interoperate with the OIA Solution must be documented and must take into account ease of use and lifecycle cost from the IDP and RP perspective.

10.2.2. Rationale

IDPs and RPs need to have a well-defined and stable specification against which to build their solutions.

10.2.3. Implications

Change Management of interfaces specifications and Release Management for solution components that implement those specifications will need to be carefully orchestrated. The OIA Programme will not be able to amend interfaces without following due process – which could impact responsiveness.

10.2.4. Notes

1. If an Agile approach to solution implementation is adopted adherence to this principle could become a constraint – although it may be possible to mitigate this by ensuring "backwards compatibility".

10.3. PTI02A – Conformance Accreditation

10.3.1. Statement

IDPs and RPs will need to through an accreditation process specified by the OIA Programme before being able to join the OIA Eco-system.

10.3.2. Rationale

IDPs and RPs present potential vulnerabilities to the security and service quality of the OIA Eco-system. Such weaknesses may could be related to systems, physical security or personnel (for example).

10.3.3. Implications

The OIA Programme would need to develop and agree a proportionate accreditation process.

10.3.4. Notes

1. How the costs of designing, implementing and operating the accreditation process would be met must be agreed.

10.4. PTI02B – Implementation Support

10.4.1. Statement

The OIA Programme will make available reasonable assistance available to IDPs and RPs as they adapt and assure their systems to interoperate with the OIA Solution.

10.4.2. Rationale

All IDPs and (separately) all RPs will have similar technical challenges in adapting their systems to operate with the OIA Solution. Overall time, risk, and cost (across the public sector in Scotland) will be reduced if the OIA Programme makes tools and information available to the IDPs and RPs as they undertake these activities.

10.4.3. Implications

One element of the OIA Solution would need to be any necessary ancillary products (such as code "stubs" replicating the behaviour of integration components. Therefore these would need to be taken into account through the system lifecycle.

10.4.4. Notes

1. This should be taken into account in the Business Case as it will have both costs and benefits.

10.5. PTI03 – Non-proprietary

10.5.1. Statement

The integration mechanisms used by IDPs and RPs to fully interoperate with the OIA Solution must not require the licensing of any commercial (proprietary) software by IDPs or RPs.

10.5.2. Rationale

IDPs or RPs should not have to pay for software in order to be able to access the OIA Solution.

Avoiding the use of proprietary software for integration mechanisms will avoid a dependency on one or more vendors (with attendant risks such as that they could vary charges, change interfaces or withdraw support).

10.5.3. Implications

This principle will ensure that lifecycle costs for IDPs or RPs are predictable and will encourage them to build interfaces to a defined and stable specification which will incentivise take-up.

10.5.4. Notes

1. It may be that consideration is given to waiving this principle if there is an overwhelming technical and/or commercial justification.

10.6. PTI04 – Functional Isolation

10.6.1. Statement

The OIA Solution will be agnostic as to how IDPs and RPs specify, provision and operate their digital and manual processes

10.6.2. Rationale

IDPs or RPs must be free to operate existing, modified or new processes as they see fit as long as they continue to meet their related obligations (in particular but not limited to regarding the use of Citizens sensitive data) and adhere to the integration standards set by the OIA Programme.

10.6.3. Implications

The OIA Solution will be responsible for the Identification and Authentication functions. RPs (and their systems) will be responsible for the Authorisation function.

10.6.4. Notes

1. This approach will require less re-engineering of RP systems and a lighter-weight OIA Solution than would be the case if Authorisation were also a function of the OIA Solution. It will also provide RPs with greater flexibility.

10.7. PTI05 – Sector-specific Identifiers and Data

10.7.1. Statement

The OIA Solution will not recognise, process or store or otherwise support existing or future sector-specific identifiers or data used by RPs.

10.7.2. Rationale

The OIA Solution should contain the minimum practicable amount of identity data. This is necessary to eliminate or significantly reduce the possibility of the OIA Solution being used to link the records of Citizens across multiple RPs (such linking being undesirable for privacy reasons). In addition this could reduce vulnerability of the OIA Solution to attack by reducing the utility of the assets stored in a single (physical or virtual).

10.7.3. Implications

RPs would need to be able to match an OIA ID to a customer account (or equivalent) in their own systems. It is assumed that this would be done as part of the Identification stage and therefore the mapping could be re-used during ongoing Authentication and Authorisation instances.

Change and potential re-verification (prompted by elapsed time or event occurrence) must be catered for.

10.7.4. Notes

1. Discussion required to determine if it is necessary or beneficial for the OIA Solution to provide OIA IDs that are specific to particular RPs, i.e. for one single Identity RP “A” is consistently served one OIA ID whereas RP “B” is consistently served a different OIA ID to potentially increase separation of RPs.
2. Consideration to be given as to whether existing sector identifiers (such as CHI) should be supported.

10.8. PTI06 – Message Integrity

10.8.1. Statement

The OIA Solution will use appropriate techniques to prove the veracity of all messages exchanged with RPs and IDPs.

10.8.2. Rationale

It is vital that the OIA Solution and the associated participants have absolute confidence that for each message:

- the source of that message is known and trusted;
- the message is appropriately authorised; and
- the content of the message has not been tampered with en-route.

10.8.3. Implications

Only solutions that can support this principle (for example by use of a public-key infrastructure to support signing and encryption) should be considered.

10.8.4. Notes

None

Appendix 1 – Version Control

Version	Date	Summary of Changes
0.03	27-Apr-18	First draft for internal review (only)
1.00	01-Jun-18	Initial Baseline – addressing review comments

Appendix 2 - Acknowledgements

TOGAF Copyright Acknowledgement

This document includes material derived from “The Open Group TOGAF 9 Templates and Examples”. The Open Group grants permission to use, copy, modify, and distribute these materials subject to the inclusion of the following notice.

GOV.UK Verify Acknowledgement

This document includes some material from the GOV.UK Verify principles published under the Open Government Licence 3.0.