COMMONWEALTH OF VIRGINIA

IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT 2
Identity Trust Frameworks

In accordance with Section 2.2-436 of the *Code of Virginia*, the Secretary of Technology, after consultation with the Secretary of Transportation, approved this Guidance Document regarding identity trust frameworks. This Guidance Document shall be effective as of December 1, 2017 and shall remain in force and effect unless rescinded or amended by further action pursuant to Section 2.2-436 of the *Code of Virginia*.

Table of Contents

1 Publication Version Control

The following table contains a history of revisions to this publication.

Publication Version	Date	Revision Description
1.0	05/02/2016	Initial Draft of Document
1.0	05/02/2016	Document revised by IMSAC at public workshop
1.0	06/23/2016	Document revised by VITA staff based on comments from IMSAC during May 2, 2016, public workshop
1.0	09/12/2016	Document revised by VITA staff based on public comment received pursuant to § 2.2-437.C, *Code of Virginia*
1.0	09/30/2016	Document revised by VITA staff based on comments from IMSAC during September 12, 2016, public meeting
1.0	05/01/2017	Document revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by the Identity Management Standards Advisory Council (IMSAC)
1.0	06/05/2017	Document recommended by IMSAC for adoption by the Secretary of Technology

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) at the direction of the Identity Management Standards Advisory Council (IMSAC).

- The document was reviewed by IMSAC during a council workshop, May 2, 2016.

- The document was revised based on public comment received in written and verbal form during the 30-day comment period, pursuant to § 2.2-437.C.

- The document was revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by IMSAC.

3 Purpose and Scope

Pursuant to §§ 2.2-436 and 2.2-437, this guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to establish minimum specifications for digital identity systems so as to warrant liability protection pursuant to the Electronic Identity Management Act ("the Act"), §§ 59.1-550 to -555. This guidance document was prepared to provide information or guidance of general applicability to the public for interpreting or implementing the Act. This guidance document was not developed as a Commonwealth of Virginia Information Technology Resource Management (ITRM) Policy, Standard, and Guideline, pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive branch agencies of the Commonwealth of Virginia.

4 Statutory Authority

The following section documents the statutory authority established in the Code of Virginia for the development of minimum specifications and standards for identity trust frameworks. References to statutes below and throughout this document shall be to the Code of Virginia, unless otherwise specified.

Governing Statutes:

Secretary of Technology
§ 2.2-225. Position established; agencies for which responsible; additional powers
http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/

Identity Management Standards Advisory Council
§ 2.2-437. Identity Management Standards Advisory Council
http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/

Commonwealth Identity Management Standards
§ 2.2-436. Approval of electronic identity standards
http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/

Electronic Identity Management Act
Chapter 50. Electronic Identity Management Act
http://law.lis.virginia.gov/vacode/title59.1/chapter50/

5 Terminology and Definitions

The core terms used within the digital identity management domain may be assigned a wide range of definitions, depending on the context or community of interest. For the purpose of the IMSAC guidance document series, the terminology has been defined in the *IMSAC Reference Document: Terminology and Definitions*, which may be accessed at http://vita.virginia.gov/default.aspx?id=6442475952

The IMSAC terminology aligns with the definitions published in the following documents:

- National Institute of Standards and Technology Special Publication 800-63-3 March 31, 2017 Public Review version, available at https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3
- Electronic Identity Management Act (§ 59.1-550), available at http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550
- International Telecommunication Union, Recommendation X. 1255, available at http://www.itu.int/ITU-T/recommendations/rec.aspx?id=11951&lang=en

6 Background

In 2015, the Virginia General Assembly passed the Electronic Identity Management Act (§§ 59.1-550 to -555) to address demand in the state's digital economy for secure, privacy enhancing digital authentication and identity management. Growing numbers of communities of interest have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – identity providers, credential service providers and relying parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly created the Identity Management Standards Advisory Council (IMSAC) to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix 1**.

IMSAC recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an identity trust framework, as defined in § 59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§§ 59.1-550 to -555); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Purpose Statement

This guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to provide information or guidance of general applicability to the public for interpreting or implementing the Electronic Identity Management Act. Specifically, this guidance document establishes minimum specifications for identity trust frameworks supporting digital identity systems.

The document defines minimum requirements, components, and related provisions for identity trust frameworks. The document assumes a specific identity trust framework will address the business, legal, and technical requirements for each distinct digital identity system; these requirements will be designed based on the specific assurance model supported by the system; and the identity trust framework will be compliant with applicable laws, regulations, and statutes.

The document limits its focus to identity trust frameworks. Separate IMSAC guidance documents in this series define minimum specifications for other components of a digital identity system.

7 Minimum Specifications

The Commonwealth of Virginia's Electronic Identity Management Act defines identity trust framework as a digital identity system with established identity, security, privacy, technology, and enforcement rules and policies adhered to by certified identity providers that are members of the identity trust framework (§ 59.1-550). Identity trust frameworks consist of multiparty agreements among members, which enforce requirements and ensure trust in the acceptance of identity credentials.

This document establishes minimum specifications for identity trust frameworks. Identity trust frameworks should be designed to document the business, legal, and technical components for enterprise architecture, business processes, governance models, operational policies and practices, and member obligations within the system. Identity trust frameworks also should contain the requirements for meeting the assurance model supported by the system. Subsequent guidance documents in the IMSAC series have addressed other components of digital identity systems, pursuant to § 2.2-436 and § 2.2-437.

Trust Framework Components

The following section outlines the minimum specifications for the business, legal and technical components of a standard identity trust framework. These components have been identified through a rigorous assessment of existing identity trust frameworks in the identity ecosystem and other domains, as outlined in Section 8 of this report. The components also align with the Identity Ecosystem Framework (IDEF), adopted by the Identity Ecosystem Steering Group in October 2015.[1]

Business Components

- Limitations on Use of Data: Collection, maintenance, and use of a person's identity information solely for the purpose for which it was collected.
- Governance Authority & Change Processes: Governance model for the identity trust framework built on a transparent, clearly defined structure and change-management process.
- Operating Policies & Procedures: Policies and procedures for the operations, maintenance, and business continuity of the identity trust framework's operational authority, and across the digital identity system.
- Security, Privacy & Confidentiality (Business): Compliant business processes and documentation for notifying a person of the security, privacy, and confidentiality provisions

[1] Identity Ecosystem Framework (IDEF) Baseline Functional Requirements (v.1.0), Identity Ecosystem Steering Group (IDESG), may be accessed at: https://workspace.idesg.org/kws/public/download/83/IDEF-Baseline-Requirements-v1.0-FINAL-10152015.pdf&wg_abbrev=idesg_document.

in the identity trust framework and for gaining consent from the person for using identity information.
- Suspension & Termination (Voluntary & Involuntary): Provisions for suspending or terminating a member due to failure to meet the obligations in the agreement, or the member's self-suspension or termination of participation in the identity trust framework.
- Data Elements & Data Classification: Attribute-level documentation, classification, and labeling of the person identity information used within the identity trust framework to support compliant handling of the data through the entire data lifecycle.
- Expectations of Performance: Provisions in the identity trust framework that set the performance and service criteria for all members – IdPs, CSPs, and RPs – including requirements for breach response and resolution, system(s) interruption or failure, and other risk situations.
- Use Cases (Exchange & Member Types): Documented examples for roles and responsibilities of members of the identity trust framework and data flows across the digital identity system.

Legal Components

- Definition/Identification of Applicable Law: Provisions requiring members of the identity trust framework to comply with all governing laws, statutes, rules, and regulations of the jurisdiction in which each member operates.
- Legal Agreements for Exchange Structure: Statement of requirements for the architecture, performance, and service specifications, and member obligations for the operation and maintenance of the exchange of person identity information within the identity trust framework.
- Security, Privacy & Consent Provisions (Legal): Terms and conditions establishing member obligations for the collection, labeling, operational use, and maintenance of person identity information and for gaining consent from the person for using identity information.
- Assignment of Liability & Risk for Members: Articles that define how liability and risk within the identity trust framework will be distributed among members, with indemnification provisions for violation of the agreement.
- Representations & Warranties: Statements of factual principles in the identity trust framework upon which members may rely, and assurances of the implied indemnification obligation in the event the principles are violated or proven false.
- Grant of Authority: Provisions requiring members of the identity trust framework to assign to the Governance Authority decision-making authority over the identity trust framework.
- Dispute Resolution: Statement of requirements and processes for mediation and the resolution of disputes among members in the identity trust framework in a manner that avoids adjudicative procedures.
- Authorizations for Data Requests by Members: Articles defining role-based rules, requirements, and processes for members of the identity trust framework to access person identity information.

- Open Disclosure & Anti-Circumvention: Provisions requiring transparency in the rules, policies, and practices for operations and governance of the identity trust framework, and prohibiting the circumvention of technical protections within the digital identity system for the handling of person identity information.
- Confidential Person Information: Statements documenting the business, legal and technical requirements for the classification, labeling and handling of confidential person identity information.
- Audit, Accountability & Compliance: Terms of conditions documenting and requiring members of the identity trust framework to comply with audit procedures, and the consequences of members failing to comply with the audit findings and corrective action plan to address deficiencies.

Technical Components

- Performance & Service Specifications: Architecture and infrastructure specifications, protocols, and requirements for all members – IdPs, CSPs, and RPs – covering full end-to-end integration for the digital identity system supported by the identity trust framework, including technical, solutions, and information architecture.
- Security, Privacy & Confidentiality: Architecture and infrastructure specifications, protocols, and requirements within the digital identity system supported by the identity trust framework designed for the collection, labeling, operational use, and maintenance of person identity information and for gaining consent from the person for using identity information.
- Breach Notification: Processes, protocols, and requirements compliant with applicable law for notifying the appropriate authorities in the event of a breach of person identity information, and related risk situations, within the identity trust framework.
- System Access: Standards-based, open architecture processes, protocols, and requirements for member authentication and access to the digital identity system supported by the identity trust framework.
- Provisions for Future Use of Data: Terms and conditions defining limitations on, and permitted purposes for, the use of person identity information after the information has been used for the Registration event and the issuance of a credential by a credential service provider.
- Duty of Response by Members: Terms and conditions requiring identity trust framework member systems to respond to and process messaging requests – inbound and outbound – within the digital identity system, normally establishing the time in which the member system must respond and process the request.
- Onboarding, Testing & Certification Requirements: Documented processes, protocols, specifications, and requirements for onboarding, testing, and certifying prospective member systems in the identity trust framework.
- Handling of Test Data v. Production Data: Terms and conditions compliant with applicable law preventing the use of production data in a test environment.

- Compliance with Governing Standards: Terms and conditions identifying and stating requirements for member compliance with governing external standards for the identity trust framework, including standards for information processing, Electronic Authentication, and Authorization.

8 Alignment Comparison

The minimum specifications for identity trust frameworks established in this document have been developed based on a detailed comparison analysis of identity trust frameworks and related governance models currently operational in the identity management ecosystem. Specifically, the minimum specifications build upon core components of existing identity trust frameworks while adapting or extending them to meet the requirements of IMSAC, pursuant to §2.2-436-§2.2-437. The analysis covered identity trust frameworks on a global scale, including a detailed review of the Open Identity Exchange (OIX) Trust Framework Model (OIX/OITF) and the European Union (EU) standards.

The following identity trust frameworks were evaluated by IMSAC. Results from the alignment comparison analysis have been compiled into matrix form in **Appendix 2**.

- State Identity, Credential and Access Management (SICAM) Guidance and Roadmap – Strategic framework published by the National Association of State Chief Information Officers (NASCIO) to promote alignment with FICAM within state government.[2]
- AAMVA DL/ID Security Framework – Set of requirements, recommendations and standards maintained by the American Association of Motor Vehicle Administrators (AAMVA) for use by Motor Vehicle Administrations to ensure driver's license and identification security.
- eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA) – Trust framework established to support the exchange health information and messaging within eHealth Exchange, the Nationwide Health Information Network.
- InCommon Trust Framework – Trust framework designed to facilitate authentication and identity management for students, faculty, staff and other service providers for institutions of higher education.
- Kantara Initiative Trust Framework – Trust framework developed on a for-profit, subscription basis to enable secure, identity-based, online interactions in a secure environment.
- Open Identity Exchange (OIX)/OITF Model – Set of guidelines and recommended mechanisms (assurance model and level of protection) for developing and implementing an identity trust framework for secure, confidence-based exchange of information (global).

[2] The Federal Identity, Credential, and Access Management (FICAM) program was created 2008 to address challenges, implementation issues, and design requirements for digital Identity, credential, and access management for federal agencies. For more information, visit: https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000XNYG

Appendix 1. IMSAC Charter

COMMONWEALTH OF VIRGINIA
IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL
CHARTER

Advisory Council Responsibilities (§ 2.2-437.A; § 2.2-436.A)

The Identity Management Standards Advisory Council (the Advisory Council) advises the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to § 2.2-436.

The Advisory Council recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an identity trust framework, as defined in § 59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-550 et seq.); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Membership and Governance Structure (§ 2.2-437.B)

The Advisory Council's membership and governance structure is as follows:

1. The Advisory Council consists of seven members, to be appointed by the Governor, with expertise in electronic identity management and information technology. Members include a representative of the Department of Motor Vehicles, a representative of the Virginia Information Technologies Agency, and five representatives of the business community with appropriate experience and expertise. In addition to the seven appointed members, the Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex officio member of the Advisory Council.

2. The Advisory Council designates one of its members as chairman.

3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure of the Governor, and may be reappointed.

4. Members serve without compensation but may be reimbursed for all reasonable and necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.

5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.

The formation, membership and governance structure for the Advisory Council has been codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

The statutory authority and requirements for public notice and comment periods for guidance documents have been established pursuant to § 2.2-437.C, as follows:

C. Proposed guidance documents and general opportunity for oral or written submittals as to those guidance documents shall be posted on the Virginia Regulatory Town Hall and published in the Virginia Register of Regulations as a general notice following the processes and procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§ 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written comments following the posting and publication and shall hold at least one meeting dedicated to the receipt of oral comment no less than 15 days after the posting and publication. The Advisory Council shall also develop methods for the identification and notification of interested parties and specific means of seeking input from interested persons and groups. The Advisory Council shall send a copy of such notices, comments, and other background material relative to the development of the recommended guidance documents to the Joint Commission on Administrative Rules.

This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the minutes of the meeting and related IMSAC documents, visit:
https://vita.virginia.gov/About/default.aspx?id=6442474173

Appendix 2. Trust Framework Alignment Comparison Matrix

	Trust Framework (TF) Components for IMSAC			
	Business	**Legal**	**Technical**	**Other**
Trust Framework (TF) Comparison Matrix	• Limitations on Use of Data ("Permitted Purpose") • Governance Authority & Change Processes • Operating Policies & Procedures • Security, Privacy & Confidentiality-Business: Consent/Auth.) • Suspension & Termination (Voluntary & Involuntary) • Data Elements & Data Classification (Attribute Level/Person Identity Information) • Expectations of Performance • Use Cases (Exchange & Member Types)	• Definition/Identification of "Applicable Law" • Legal Agreements for Exchange Structure • Security, Privacy & Consent Provisions • Assignment of Liability & Risk for Members • Representations & Warranties • Grant of Authority • Dispute Resolution • Authorizations for Data Requests by Member • Open Disclosure & Anti-Circumvention • Confidential Person Information • Audit, Accountability & Compliance	• Performance & Service Specifications • Security, Privacy & Confidentiality (Technical: Infrastructure/ Architecture) • Breach Notification • System Access (ID/Authentication) • Provisions for Future Use of Data • Duty of Response by Members • Onboarding, Testing & Certification Requirements • Handling of Test Data v. Production Data • Compliance Governing Standards	• Openness & Transparency • TF Lifecycle Management ("Living Agreement") • Support & Capacity Building (IGs) • Scalability to Support Array of Members (Horizontal/Vertical) • Glossary of TF Terms/Definitions • Component-based Approach for TF Elements

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	**Legal**	**Technical**	**Other**
State Identity, Credential and Access Management (SICAM) Guidance and Roadmap	+ Limitations on Use of Data (§6.6) + Governance Authority & change processes (§6.6) + Operating policies & procedures (§6.6) + Security, privacy & confidentiality (§6.6) + Suspension & termination (§6.6) + Data elements & data classification (attribute level/PII) (§5.5, §6.5, §6.6) + Expectations of performance (§6.6)	+ Compliance w/ applicable law (§6.6) + Legal agreements for exchange structure (§6.6) + Security, privacy & consent (§6.6) + Liability (§6.6) + Representations & warranties (§6.6) + Grant of authority (§6.6) + Dispute resolution (§6.6) + Authorizations for data exchange (§6.6) + Non-exclusivity (§6.6) + Confidential Person Information (§6.6, §6.3) + Audit (§6.6) + Accountability & compliance (§6.9)	+ Performance & service specifications (§5, §6.4) + Security, privacy & confidentiality (§5, §6.4) + Breach notification (§5, §6.4; §6.6) + System access (§6.6) + Provisions for future use of data/services (§6) + Expectations of Members (§6.6) + Duty of response by Members (§6.6) + Onboarding, testing & certification (§6.6) + Compliance with governing standards (§5, §6.6)	+ Openness & transparency (§6.6) + TF lifecycle management (§6.6) + Scalability to support array of Members (§6.8) + Glossary of TF terms/definitions (§1.4) + Component-based approach for different Member types (§6.6)

NASCIO, State Identity, Credential and Access Management (SICAM) Guidance and Roadmap, Sept. 2012.

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	**Legal**	**Technical**	**Other**
AAMVA DL/ID Security Framework	+ Data element-level verification and validation (§1.3 #9, §1.4 #10, §1.4 #13, §3.3.4, §7.4, Appdx.) + Data (Name) collection, use and maintenance (§3.3.4, § 7.1, Appdx.) + AAMVA DL/ID Personal ID Card Design Specification (§1.4 #12, §3.3.4, 7.3, Appdx.) + Procedures for initial customer ID and validation (§3.3.3, §6.0) + Record & document use, permitted purpose (§3.3.5, §4.6, §7.1, §8.0) + Benefits/ business drivers (§2.0, §3.1) + Business-driven agreement among MVAs (§3.1, §3.3, §4.5) + Business requirements for P&Ps, document issuing systems, and internal controls, Driver License Agreement (DLA) (§3.3.1, §4.2, §4.5, Appdx.)	+ Assumes MVA compliance with applicable law, document use, data sharing (§1.5 All Recs., §3.1, §3.2, §3.3.5, §4.5, §8.3, Appdx.) + Enforcement thru business requirements (§2.0, §3.1, §4.5) + Audit plan (§1.1 #2, §1.2 #5, §3.3.2, §5.1, Appdx.) + Compliance and oversight, internal controls (§3.3.2, §4.4, §5.2) + Risk assessment & management (§1.1 #3, §3.3.5, § 4.2, §4.4, §8.0) + Privacy (§1.1 #4, §4.2, Appdx., §3.3.4, §3.3.5, §4.5, §4.6, §7.1, §7.4, §8.3) + Common set of verifiable resources (§1.3 #8, §3.3.3, §6.2, Appdx.) + Machine-Readable Technology (MRT) (§3.3.5, §8.2, Appdx.) + Restrictions, minimum penalties and sanctions (§3.3.5, §8.1, Appdx.)	+ Electronic verification (w/issuing entity) of DL/ID data elements (§1.3 #9, §3.3.3, §6.3) + Standards for MVA system integrity, interoperability & reciprocity (§2.0, §3.1, §3.3.2, §4.2, §4.5) + Compliance with governing standards (§3.3.2, §4.5, §5.2) + System integrity, security & privacy (§4.6)	+ Compliance and implementation support thru FDR employee training (§1.1 #1, §3.3.1, §4.1) + Common definition of "residency" (§1.3 #6, §3.3.3) tied to DL/ID verification (§1.3 #7, §3.3.3, §6.1) + "End of stay" on immigration doc. as expiration date for DL/ID - data element derivation (§1.4 #11, §3.3.4, §7.2, Appdx.) + Horizontal scalability thru reciprocity (§3.1) + Openness enforced thru privacy provisions (§4.6, §7.1) + Limits on disclosure enforced thru privacy provisions (§4.6, 7.1) + Glossary of abbreviations/ acronyms (§9.0) + LE Use Case (§1.5 Rec. #8, data sharing §3.3.5, §8.3, Appdx.)

AAMVA. DL/ID Security Framework, Feb. 2004.

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	**Legal**	**Technical**	**Other**
eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA)	+ Limitations on use of data (§1.jj; §3; §5.01-5.03) + Governance Authority (§4) & change processes (§10.03; §11.03) + Operating policies & procedures (§11; Appdx.; change process in §11.03) + Security, privacy & confidentiality (§7; §8; §14) + Suspension & termination (§19) + Data elements & data classification (attribute level/PII) (§1.v; §1.w; §1.kk) + Expectations of performance (§12)	+ Definition/compliance w/ applicable law (§1.a; §15.11; §23.01; Appdx.) + Legal agreements for exchange structure (recitals; §1.ee; §3.01; §23.07) + Security, privacy & consent (§14) + Liability (§18) + Representations & warranties (§15; disclaimers in §17) + Grant of authority (§4.03) + Dispute resolution (§21; Appdx.) + Authorizations for data exchange (§12; §13) + Open disclosure & anti-circumvention (§15; §23.04; §23.07) + Confidential Person information (§16) + Audit (§9) + Accountability & compliance (§10.01; 11.01; §15.03; §15.06)	+ Performance & service specifications (§10; Appdx.; change process in §10.03) + Security, privacy & confidentiality (§7; §8; §14) + Breach notification (§14.03) + System access (§6) + Provisions for future use of data (§5.02) + Expectations of Members (§12) + Duty of response by Members (§13) + Onboarding, testing & certification (§10.01) + Handling of test data v. production data (§15.07)	+ Openness & transparency (overview; recitals) + TF lifecycle management ("living agreement") (overview; §4; §10.03; §11.03) + Scalability to support array of Members (horizontal/vertical) (Member types defined in §1; expectations in §12.02; duties in §13) + Glossary of TF terms/definitions (§1) + Component-based approach for different Member types (types defined in §1; expectations in §12.02; duties in §13; warranties in §15)

eHealth Exchange, Data Use and Reciprocal Support Agreement, Sept. 2014.

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	**Legal**	**Technical**	**Other**
InCommon Trust Framework	+ Limitations on use of data (ICPOP; IAS; limits on use of ID information in PA §9) + Governance Authority & change processes (ICPOP; PA §17) + Operating policies & procedures (ICPOP) + Security, privacy & confidentiality (PA §6, §9; ICPOP) + Suspension & termination (PA §5.b, §5.c) + Data elements & data classification (attribute level/PII) (IAS; PA §6.b) + Expectations of performance (PA §6, §7) + Use cases and examples (InCommon Website; ICBP; Members)	+ Definition/compliance w/ applicable law (PA §15) + Legal agreements for exchange structure (ICPP; PA §6, §7.b) + Security, privacy & consent (PA §6, §9) + Liability (PA §11, includes disclaimer & limitations) + Representations & warranties (addressed in PA §7.b) + Grant of authority to executive (PA §18) + Dispute resolution process (PA §10; ICBL §5) + Authorizations for data exchange (PA §18) + Open disclosure & anti-circumvention (PA §14, §16) + Confidential Person information (PA §8, §9) + Audit (ICPOP) + Accountability & compliance (PA §15)	+ Performance & service specifications (PA §6, §7) + Security, privacy & confidentiality (ICPOP) + Breach notification (PA and addenda; ICPOP) + System access (ICPOP) + Provisions for future use of data (ICPOP) + Expectations of Members (PA §6, §7) + Duty of response by Members (PA §6, §7) + Onboarding, testing & certification (ICPOP) + Handling of test data v. production data (ICPOP)	+ Openness & transparency (ICBP) + TF lifecycle management (“living agreement”) (ICBL; PA §17) + Implementation support (ICPOP) + Scalability to support array of Members (horizontal/vertical) (Member types defined in Join §1, Members) + Glossary of TF terms/definitions (InCommon Website) + Component-based approach for different Member types (Members)

ICPOP=InCommon Member Operational Practices
PA=InCommon Participation Agreement
IAS=InCommon Attribute Summary

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	**Legal**	**Technical**	**Other**
Kantara Initiative Trust Framework	+ Limitations on use of data (KTR MTAU) + Governance Authority (BL §4; OP §2) & change/ amendment processes (BL §12; OP §9; MA §3) + Operating policies & procedures (OP) + Security, privacy & confidentiality (AP; MA) + Suspension & termination (MA §2; BL §8.11; KTR MTAU) + Data elements & data classification (KTR; KIC) + Expectations of performance (AP; KTR MTAU; KIC) + Use cases (Working groups for business cases-trusted federations)	+ Definition/identification of applicable law (KTR MTAU; see also "Governing law and jurisdiction" provision in KTR MTAU) + Legal agreement for exchange structure (MA) + Security, privacy & consent provisions + Liability (KTR MTAU) + Warranty (KTR MTAU) + Grant of authority (MA) + Authorizations for data requests by Member + Open disclosure & anti-circumvention (Other agreements in KTR MTAU) + Confidential Person information (Options set in IPRP; IPRP Art. 3) + Accountability & compliance (w/ antitrust laws in BL §17; MA)	+ Performance & service specifications (AP; KTR/KTV; KTR MTAU; KIC; Member protection & treatment in IPRP) + Security, privacy & confidentiality (AP; MA) + Technical certification & testing (AP; KIC) + Standards for technical & operational interoperability (KTR; MA goal #3; #7; KIC)	+ Open & transparent governance model (MA goals #3, #4; op; BL §3) + TF lifecycle management (MA goals #4, #6) + Support & capacity building (IGs) + Scalability to support array of Members (horizontal/vertical) (member types BL §8) + TF definitions (BL §1; OP §1; IPRP Art. 2)

BL=Bylaws; IPRP=Intellectual Property Rights Policies; MA=Member Agreement; OP=Operating Procedures
KTR=Kantara Trust Registry; KTV=KTR Trust Validation; KTR MTAU=Metadata Terms of Access & Use; KIC= Kantara Interoperability Cert.-SAML, OATH, etc.
AP= Assurance Programs; Identity Assurance Accreditation & Approval and Interoperability Certification Programs

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	**Legal**	**Technical**	**Other**
Open Identity Exchange (OIX)/OITF Model	+ Limitations on use of data (OITF §III.B, §III.C, §V) + Governance Authority & change processes (OIX; OITF §III.C) + Operating policies & procedures (OIX; OITF §II, §III.B, §III.C) + Security, privacy & confidentiality (OIX; OITF §III.A, §V) + Suspension & termination (OITF §III.C) + Data elements & data classification (attribute level/PII) (OIX; OITF §III.A, §III.B) + Expectations of performance (OIX; OITF §II, §III.C) + Use cases for agreement, transaction & Member types (OITF §I, §III; OIX)	+ Compliance w/ applicable law (OIX; OITF §V) + Legal agreements for exchange structure (OIX; OITF §II, §III.C) + Security, privacy & consent (OIX; OITF §III.A) + Liability, representations & warranties (OITF §III.C) + Grant of authority (OIX; OITF §III.C) + Dispute resolution (OITF §II, §III.C, §V) + Authorizations for data exchange (OIX; OITF §III.A) + Anti-circumvention & open disclosure (OITF §V) + Audit (OIX; OITF §II, §III.B, §V) + Accountability & compliance (OIX; OITF §II, §V)	+ Performance & service specifications (OIX; OITF §II, §III.A, §III.B) + Security, privacy & confidentiality (OIX; OITF §III.A; §V) + Expectations of Members (OIX; OITF §III.A, §III.B, §III.C) + Onboarding, testing & certification (OIX; OITF §II, §III.B)	+ Openness & transparency (OIX; OITF §I; statement in OITF §V, §VI) + TF lifecycle management (OIX; OITF §II) + Scalability to support array of Members (horizontal/vertical) (OITF §II, §III.C, §IV) + High-level definitions (OITF §I) + Component-based approach for different Member types (OIX; OITF §II, §III.C) + Use cases & examples of TFs (OITF §IV)

OITF=The Open Identity Trust Framework (OITF) Model, March 2010
OIX=Open Identity Exchange Trust Framework Requirements and Guidelines v. 1 (Draft 2)