

Exhibit 6

Risk Wiki

Draft 1.2
February 11, 2011

Discussion and Development Materials

of the

OIX Advisory Committee

and the

OIX Legal Policy Committee

This is a tool for Trust Framework risk analysis, design and development, it is also the framework for an online tool that enables broad community participation in the legal analysis.

Notes to user:

This tool has been prepared for use by the OIX Advisory Committee and the OIX Legal Policy Committee and by any other parties involved in online and telecommunications data/identity system legal standardization, risk and liability analysis, and trust framework, legislation and contract development work.

The tool is made available by OIX under a creative commons license (with attribution), so that it is broadly available to all interested parties.

These materials and the online or other discussions that use or refer to these materials are not intended to provide legal advice. They are only intended for use as a reference tool in the consideration and discussion of issues associated with the design, development and deployment of data and information resource management systems and online and telecommunications identity management systems. Parties should seek the advice of legal counsel in each relevant jurisdiction before implementing any business or personal decision that involves the establishment of legal duties, the management of legal risks or the potential for legal liability.

The online functionality at www.openidentityexchange.org is made available for public use pursuant to the terms of use [link] posted on the OIX website.

If you are not familiar with the use of this Tool, please see the “User Guide” (see table of contents).

Notes and expanded discussion relating to this tool (to be considered for inclusion in the OIX Risk Wiki) are available at [insert reference to appendix here].

The online functionality at www.openidentityexchange.org based on this tool is made available for public use pursuant to the terms of use [TOU link here] posted on the OIX website.

[OIX Administrative NOTE: The foregoing reference to a TOU is needed to collect the necessary rights from, and make needed disclosures to, persons posting content to the OIX Risk WIKI and other online tools and programs in order to accumulate and share their contributions with other stakeholders through the tool. It is anticipated that the public use of the online WIKI tool will generate postings, the continued accumulation of which will constitute a “community-generated” and “community maintained” “virtual discussion” that will keep the legal analysis dynamically current as an issue-spotting resource to inform the collective analysis and discussion, and to help identify system-relevant future modifications to the Listing information requirements for the OIX listing service and other OIX programs. We should explore designing the WIKI so that it can most easily track alternative analyses for forking (and recombining) issues (such as, for example, when an identical transactions are entered into, subject to two different countries’ laws.)]

Introduction

What is the Risk Wiki?

These materials present a structure for identification and legal analysis of risks and legal liabilities, and for risk, cost and liability management and mitigation strategies associated with online identity activities (including identification, proofing, authentication, and related activities).

The structure is intended to inform the creation of an online tool that can be accessed by stakeholders to aid them in the analysis of data/identity systems, and which will store, accumulate, and make available stakeholder discussion of problems, and proposed solutions to the benefit of data/identity stakeholders in different contexts at internet scale.

This is not an article. It is a tool for structuring the analysis of duties, risks and liabilities that are associated with online identity systems. Accordingly, the materials do not present pre-determined answers to every question (although the analysis is “pre-populated” with initial comments on scores of legal issues). Instead, use of the tool will help to generate answers to legal questions raised in the course of Trust Framework construction and other legal analysis associated with online trust framework design, development, deployment and review.

Think of this tool as a legal “answer computer.” You need to “program” it with the particular variables relevant to you (as a Trust Community, a party providing services to data subjects (users), relying parties, identity providers, and others). The “programming language” is based on identifying the common forms of “data actions” that are relied on in your existing or proposed data/identity system, and using those as a basis for analyzing system technical and legal configurations to achieve stakeholder goals.

The tool provides the structure and prompts you for facts about data and information flows and actions in your current or planned online identity system. The facts are requested in a certain structure and are included in a particular order. That order is dictated by the overall flow and hierarchy of actions that typically take place with respect to data and information systems, but is flexible to accommodate the data actions and flow that characterize the particular system being analyzed for application in a particular context.

This material and the “tool” are not legal advice and are not a substitute for consultation with legal counsel. You should consult with legal counsel prior to entering into any legal agreements, taking on legal obligations or engaging in activities that might result in legal liabilities.

Why use this structure?

Using this structured analysis can help to achieve benefits at the system, company and individual level, such as:

More highly focused (and less costly) legal liability analysis

Better matching of Tools and Rules in technology procurement through use of “Data Action” oriented analysis to achieve more effective compliance at lower cost

Better integrated and more comprehensive legal contracting functions relating to online identity services to reduce relying party and other system user complexity

More effective online identity risk mitigation strategies

Greater access to relevant “use cases” to inform your project

Systems built using the tools can enjoy easier integration of other system services that are structured with the same analysis (e.g., legal interoperability), which enables scalable “outsourcing” and “in-sourcing” of data/identity related services (for example in the “cloud computing” context).

Is the tool pre-populated with examples of identified duties, analyzed risks and liability management strategies?

Yes. In the interests of “getting the ball rolling” scores of issues have already “salted” into the analysis (and, as a prompt for close consideration of data actions – see the “verb taxonomy” (Attachment 1) for more information on data actions). These should be treated as starting points for the analysis, and the characterization of the actions, the specific data and information involved, the status of the transferor and transferee of data (e.g., in regulated industries), the circumstances in which it takes place (e.g., the legal jurisdiction(s), special status of data subjects (e.g., minors), and other relevant factors should all be accounted for in the analysis.¹

These comments and skeletal analysis (as a kind of “serving suggestion”) suggest how the tools might be used by parties and introduce many issues associated with many of the more common risk and liability questions and situations that arise in online identity management systems

This tool will always be a “work in process.” Due to the requirements of different systems, the laws of different jurisdictions, different stakeholders, different data, and different contexts, the categories of analysis applied in this tool will appear necessarily general. The intention is to provide a structure for analysis, rather than to pre-define the result of that analysis. It is anticipated that users of the tool will “build out” various parts of the tool as it is used.

In furtherance of the end of building a robust identity community repository of risk, liability and mitigation analyses, OIX is exploring creating a WIKI or similar online functionality for broad

¹ This is a “forest and trees” issue. Extending the “ecosystem” analysis, an ecosystem can only be properly analyzed if you first understand its components. For example, you wouldn’t analyze the nutritional and reproductive needs of penguins and cactus in the analysis of a study of tropical rainforest ecosystems. Similarly, you wouldn’t include *disposal* Tools and Rules (such as degaussing, shredding, and affidavits of data destruction) in the analysis of the process of data *collection*.

public use of the tool. To check on the status of that functionality [here][NOTE: Insert link to online tool].

When will this document be completed?

This document will never be finalized. It will always be a working draft. This is because advances in technology will continue to give rise to new capacities and challenges in SOT/IDM systems, which will alter the needs of Trust Communities, Relying Parties and Data Subjects. It will also change the needs of IDPs, Assessors and other participants in the system who will be called upon to deliver SOT/IDM related services at measurable, reliable and predictable LOAs, LOPs and LOCs, which will require them to make changes in their service offerings to match the corresponding changes in Trust Frameworks. The only constant will be change.

To the extent that these materials provide descriptions, discussion and analyses of legal issues, theories and principles, it is in an effort to capture the comments and concepts involved in the continuing discussion and analysis associated with the work in developing the structured analysis. Discussion and analysis is intended to be inclusive of issues raised by various parties in the U.S. and in other legal jurisdictions around the world, and inconsistencies in the analysis may be present.

Nothing in these materials represents a position or conclusion of OIX or any of its members, board members, representatives, its legal counsel or other advisors or OIX contributors. These materials are not meant to present a comprehensive treatment of the issues, but are intended as an analytical “sandbox” in which stakeholders can work together to develop the legal issues.

Why was this tool developed by OIX?

The creation of a uniform legal risk and liability analysis tool will help drive consistency of analysis across multiple Trust Framework and online identity system development exercises. This will permit the consideration of risk and liability management and mitigation strategies within a uniform analytical framework, which will be expressed in a more consistent configuration of Tools and Rules, which in turn will foster greater interoperability across online identity services. Specifications make Tools interoperable. Trust Frameworks make Rules interoperable.

Greater interoperability will make systems more measurable and monitorable and subject to greater stakeholder control (such as user-centric controls). Measurement will enable the generation of broadly recognized simple system metrics such as the current LOA, and future LOP and LOC metrics. The identification of relevant system metrics (that are developed to enable the easy characterization of online identity management systems by participants) will, in turn, inform the design, development and implementation of OIX member registration and Listing Service information requirements that are intended to collect identity market relevant information for distribution to stakeholders to inform decision making. This creates a market information “feedback loop” that helps to incorporate all stakeholder risk profiles, liability concerns, and mitigation strategies in future OIX Listing requirements, the collection and public availability of which allows system participants to refine and develop system design, development and marketing parameters.

Also, this tool, when used in combination with information available on the OIX Listing Service can help individuals and businesses to identify appropriate Trust Framework structures and available online identity management services suitable to a particular individual’s or entity’s online risk and liability profile. This will help to reduce the costs to individuals and entities of organizing and operating secure online transaction/identity management (“SOT/IDM”) support systems.

I see why this helps Trust Communities and other stakeholders put together online identity management systems, but why is this analysis useful to OIX?

Using the Risk WIKI and other tools permits the collective, ongoing analysis of existing liabilities by various stakeholders in online identity systems. Examination of current cumulative analysis allows OIX to find out what types of market data it should collect and distribute (through the OIX Listing Service) to help all stakeholders to guide the SOT/IDM market to maturity (i.e., to achieve greater reliability, predictability, interoperability, transparency and to engender greater “trust”).

Also, use of the structured analysis, combined with market data, and the presence of broadly adopted system metrics (such as LOA, and future LOP, and LOC metrics) will permit stakeholders, parties listed in the OIX Listing Service and other parties using OIX market data to design and deploy SOT/IDM systems in a way that *mitigates* unintended and counter-functional

liabilities, but clarifies and enforces liabilities (such as for negligent or intentionally fraudulent behavior) that serve to discourage participant behavior that is not consistent with SOT/IDM system goals.

The feedback loop is primed and sustained by stakeholder-relevant information. System design information is generated by the participation of different groups in Trust Framework design activities and contract drafting exercises. Information is made uniform by standardized analytical and design approaches. Uniform analytical information yields improved opportunities for relevant market information sharing and market development opportunities, and results in interoperable systems.

The quality of the information in the feedback loop is improved as the percentage of market participants generating the information increases. The adoption curve will be improved to the extent that systems are designed and deployed based on *consensus* among the parties as to their respective duties and the mechanisms that are put in place to enforce them and to mitigate their unintended liabilities. The consensus on those issues will be achieved through in-person conversations by representatives, reports (such as those issued by the ABA and government entities) and (in order to accommodate the broader participation in such “conversations”) in the use of online functionality to engender discussion persistence and recordation, such as the OIX Risk WIKI.

These will be opt-in systems, so the achievement of consensus at the design stage presages broader adoption at the deployment stage. This consensus will be documented in a series of (more or less) standardized agreements that will create mutual dependencies based on enforceable promises to perform data and information-related duties consistent with clearly defined, system-consistent standards.

Please note that this material is intended to provide a structure for analysis. It is not a comprehensive listing of all of the relevant sources of liability or ideas on how they might be mitigated and addressed. It is hoped that the establishment of this structure for the analysis will serve to make the analysis more efficient and accessible to the variety of stakeholder groups for which it is potentially relevant.

In addition, OIX is exploring how best to present this tool as an online functionality, such as a WIKI, that will permit users to benefit from the analyses engaged in by other parties. To check on the current status of that effort, please go to www.openidentityexchange.org and search for OIX Risk WIKI.

Table of Contents

Cover page.....

Introduction.....

Why was this tool developed by OIX?

Table of Contents.....

How to Use This Tool and Analysis.....

Description of the “I-AM” process
(**I**dentify Duties, **A**nalyze Risks and **M**itigate Liabilities)

I. “I” - Identify Duties

Overview of “Identifying Duties” Process.....

Identification of Duties associated with
9 separate SOT/IDM Data Actions.....

Action 1 – System setup – TF Construction.....

Action 2 – System setup – IDP Certification.....

Action 3 – Pre-SOT - Identification
(step 1 – Data Proofing)

Action 4 – Pre-SOT - Identification
(step 2 – Credential/Token Issuance)

Action 5 – SOT – Pre-Authentication Communications.....

Action 6 – SOT – Authentication Credentials and Tokens...
- Transfers

Action 7 – SOT - Authentication Credentials and Tokens...
- Review and Reliance

Action 8 – SOT – Post – Authentication.....
Authorization by Relying Party

Action 9 – Post-SOT – Data and Credential Management....

II. “A” - Analyze Risks

Overview of “Analyze Risks” Process.....

Analysis of Risks associated with
9 separate SOT/IDM Data Actions.....

Action 1 – System setup – TF Construction.....

Action 2 – System setup – IDP Certification.....

Action 3 – Pre-SOT - Identification
(step 1 – Data Proofing)

Action 4 – Pre-SOT - Identification
(step 2 – Credential/Token Issuance)

Action 5 – SOT – Pre-Authentication Communications.....

Action 6 – SOT – Authentication Credentials and Tokens...
- Transfers

Action 7 – SOT - Authentication Credentials and Tokens...
- Review and Reliance

Action 8 – SOT – Post – Authentication.....
Authorization by Relying Party

Action 9 – Post-SOT – Data and Credential Management....

III. “M” - Mitigate Liabilities

Overview of “Mitigate Liabilities” Process.....

Management Strategies for Liabilities associated with
9 separate SOT/IDM Data Actions.....

Action 1 – System setup – TF Construction.....

Action 2 – System setup – IDP Certification.....

Action 3 – Pre-SOT - Identification
(step 1 – Data Proofing)

Action 4 – Pre-SOT - Identification
(step 2 – Credential/Token Issuance)

Action 5 – SOT – Pre-Authentication Communications.....

Action 6 – SOT – Authentication Credentials and Tokens...
- Transfers

Action 7 – SOT - Authentication Credentials and Tokens...
- Review and Reliance

Action 8 – SOT – Post – Authentication.....
Authorization by Relying Party

Action 9 – Post-SOT – Data and Credential Management....

How to Use This Tool and Analysis

This document presents an analytical tool designed to aid in the construction of Trust Frameworks.

The creation of Trust Frameworks, and more importantly “trusted” online identity systems, starts with the analysis of risk and liability. Here is how that works.

Trust Frameworks can only earn the name “trust” if they are *reliable*, i.e., if they provide the same result in successive trials. Reliability enables *predictability*, i.e., where the result can be declared in advance. System reliability and predictability enable repeatability and the identification of measurable levels of performance.

Measurement enables quantification of online identity system metrics (such as for Levels of Assurance, Levels of Protection and Levels of Control), and the quantification, valuation, monitoring and regulation of system parameters. It also provides the opportunity to understand and predict the behavior of online identity systems, which implies opportunities for control to assure conformity with stakeholder-derived consensus rules.

The establishment of system metrics simultaneously establishes parameters for measurement of interoperability (e.g., the establishment of a measurement called “LOA 3” allows the subsequent use of that metric to declare all services “at LOA 3” to be functionally equivalent (for relevant, measured system purposes) with respect to the factors assessed to earn that certification).

Of central importance here, the factors that are relevant in the establishment of system metrics also informs the Identification of Duties, the Analysis of Risks and the Management of Liabilities that is part of the Trust Framework construction exercise. [NOTE: This is why the risk and liability profiles vary among different LOA levels; the costs and duties are both higher at higher LOAs]. The Duties, Risks and Liabilities analysis is the legal continuation of the technical work done to establish LOAs (and the same process will proceed for other system metrics such as LOP and LOC when technologies and duties are “standardized” to enable their respective relevant metrics).

Trust begins with reliability.

This tool helps all parties in a Trust Community (and across Trust Communities) look at risk and liability *together*, in order to craft consensus solutions and mitigations that support all stakeholder goals in an *agreed upon* fashion. In that way, the tool helps parties to “envision” the risk and liability landscape through a common perspective, providing a shared starting point for working through mitigation strategies (whether contractual, regulatory or legislative).

How can Trust Frameworks (and this analysis) help achieve reliable systems?

Information systems (including the portion that is used to provide online identity management systems) are made up from two basic components: *Technology* (hardware, software, networks, and the like), and *people* who make decisions in the system.

Technology Tools are rendered reliable by specifications, which enable them to be designed and deployed in ways that are more reliable, predictable and measurable.

The performance of People is rendered reliable by Rules, i.e., enforceable policies and laws.

Rules of all types (whether from statute, regulation, administrative practice, contract, policy, industry practice, etc. are intended to establish “duties.” A duty is the legal obligation to perform an action in a certain way.² Legal duties curb the discretion associated with human action.³ Contracts document the promises to perform future duties in a certain way.

The receipt of those contract promises enables parties to know that the party to which that duty is assigned will be more likely to behave in a manner (at least within the scope of the described duty) that is reliable and predictable. The duty is backed up by incentives or by punishments (or a combination) that may be enforced through sovereign action or by other parties (or a combination).

The bottom line is that enforceable rules (*aka* background laws and contracts) render human behaviors more reliable by assigning enforceable duties. This tool enables the application of a standard analysis in an effort to drive interoperability at the legal layer of online identity systems.

Integrated systems that depend on the reliability of both technology and people (such as online identity systems), and the construction of Trust Frameworks to guide their design and deployment, can benefit from a duty, risk, liability and mitigation analysis that permits the simultaneous consideration of Technology Tools and Legal Rules. Using this tool, stakeholders can develop “hybrid” analyses that can integrate the reliability drivers of both technology and people working together in information systems. That analysis informs the content of Trust Frameworks.

The “hybrid” analysis is achieved by focusing on the central concern of most technology and legal analysis in online identity systems, i.e., the specific *actions* involved in the movement and use of data and information.

² Black’s law dictionary defines “duty” alternatively as “Legal or moral obligation. Obligatory conduct or service. Mandatory obligation to perform.” “Obligation, to which law will give recognition and effect, to conform to particular standard of conduct toward another.” Finally citing the Restatement of Torts Sec. 4, “to denote the fact that the actor is required to conduct himself in a particular manner at the risk that if he does not do so he becomes subject to liability to another to whom the duty is owed for any injury sustained by such other, of which that actor’s conduct is a legal cause.

³ The word “shall” is found throughout legal texts for a reason. It is a definitive invocation of the sovereign or of a party to a contract setting indicating an instruction and expectation that a described duty will be performed in a certain manner.

The hybrid analysis is necessary because each Data Action requires its own special set of Tools and Rules to be carried out consistently with system needs. For example, the Tools and Rules associated with the action of transferring data for proofing that contains social security number by e mail (it must be encrypted as a matter of law), are different than those associated with action of [insert contrasting data action example]

Description of the “I_AM” Duty/Risk/Liability Analysis Process

What does “I_AM” stand for?

“I_AM” stands for:

Identify Duties

Analyze Risks, and

Manage (or Mitigate) Liabilities

These are the three basic steps in the analysis applied to each of the nine separate data and information-related actions (the “Data Actions”) identified in these materials.

Each Data Action is illustrated in a separate diagram [insert link to diagrams here]. Please note that in these early iterations of the tool, the Data Actions are somewhat generally defined. It is expected that as the online identity ecosystem community uses the tool, and contributions are accumulated in the tool, the coverage of the analysis presented in the tool will expand in breadth and depth.

Step 1 - Identify Duties

The *identification* of duties is the first step. Parties engaging in the Trust Framework construction process need to consider their online identity system performance goals and needs to identify what duties need to be assigned to system participants to achieve those goals. The exercise of describing this in a draft Trust Framework “term sheet” is roughly equivalent to drafting a statement of work for a service contract. The preparation of the related legal agreements that create binding duties from Trust Framework guidelines is roughly equivalent to drafting the service contract itself.

The duties that are relevant to maintaining online identity systems relate primarily to how ALL people participating in the system *act with respect to identity data and information* in the system that is being analyzed (or designed, as the case may be). These are referred to as their respective “Data Actions.” The numbered diagrams illustrate the nine data actions that are fundamental to online identity data systems.

The analysis is organized around the different functional categories of Data Actions (placed in an order based on whether one action satisfies a condition precedent to other actions – actions that are prerequisites to other actions being described first). Thus, for example, the Data Actions associated with the issuance of a credential are identified before the Data Actions associated with the use of that credential). This is done in order to facilitate the analysis of issues in clusters at various levels of the Data Action stack. It is expected that many levels of refinement will be added to the types of Data Actions listed as additional parties engage in the analysis.

Why start with duties?

For purposes of putting together a reliable, predictable, interoperable online identity system, like drafting a statement of work for a service contract, Trust Communities of any overall composition have at least one thing in common: they are interested in accomplishing the specific overall goal of influencing the behavior of other companies and individuals sufficiently to cause an online identity system to be available to them that suits their needs (i.e., their specific needs to address risk). All stakeholders' desire for system reliability and integrity is served by mutual enforceable promises to engage in certain behaviors. That influence is carried into effect by an integrated set of contracts.

Those contracts create enforceable duties to accomplish Trust Framework goals. To assemble the legal part of the "Tools and Rules" structure, identifying and establishing "duties" is the place to start. The presence or absence of legal duties determines the extent of legal liability. If there is a desire to control liability, it starts with legal duties.

Step 2 - Analyze Risks

The second step is the I_AM process is to analyze the risks. There are basically two types of "risks" to any party. First, are the risks associated with breach of duty by another party. Second, are the risks associated with a party's own breach of duty. Within these broad categories, there are many subcategories depending on the nature of the particular legal duty involved. The analysis of either type of risk is subject to the influence of myriad variables.

In an effort to "tame" the variables, and as a prerequisite to Step 3 in which strategies for mitigating liability are considered, the analysis of risks should consider the various ways in which the overall "risk" profile associated with a specific duty is affected by the separate legal elements that are prerequisites for the conclusion that a liability should be imposed. In other words, Section 2 should apply risk categories that anticipate and make easier the effort in Step 3.

In the initial analysis, this requires resort to the "plain vanilla" legal liability analysis (at least in the case of negligence) which is based on the nested sub-analyses of *duty*, *breach*, *causation and damages*. Those sub-analyses are "baked into" Section 2, but that basic analysis should be modified to fit the particular situation being analyzed (for instance by relevant analytical elaborations of each of the breach, causation and damages analysis).

Step 3 – Manage and Mitigate Liabilities

The final step in the "I_AM" process is to manage and mitigate the liabilities that are associated with the risks analyzed in Step 2. The OIX Risk WIKI helps to perform this analysis by providing a review format in Step 3 through which the individual liabilities analyzed in Step 2 are brought forward and listed in Step 3, and then subjected to a tailored review of potential Statutory, Regulatory, Administrative and Contractual mitigation strategies.

The intention in this section is to engage in a simultaneous detailed and comprehensive review of potential liability management and mitigation strategies, with the expectation that mitigation strategy themes will then arise among the various separate mitigation strategies that will suggest

overall mitigation strategies that can then inform the content of market normalizing legislation, adaptations in regulation or administrative enforcement initiatives or the preparation of standardized contract terms to address broad swaths of the liability mitigation landscape.

In completing this section, it is important to recall that there are “good” and “bad” liabilities, and that those determination are not entirely subjective. “Good” liabilities are those that support the performance of consensus driven, system-consistent behaviors. Bad liabilities are those that are unanticipated by one or more of the parties and undermine overall data/identity system performance.

I. IDENTIFY DUTIES

Who should use this section

You should reference this section if:

You are performing a data and information flow *legal issues audit* of online identity processes

You are putting together a Trust Framework

You are working with tech folks to design data and information handling systems

You are analyzing legal risk or liability associated with a data and information action scenario

[NOTE: Other?]

How to use this section

In this section, you will be identifying duties associated with online identity data and information management systems. The “duties” will be applied to guide (or “evaluate” in existing systems) the human and institutional (acting through their employees and contractors) behaviors that need to occur in the system to cause the system to perform desired online identity data and information actions reliably and predictably. Those Data Action “goals” can be derived from a single Trust Framework, other (“normatively referenced” Trust Frameworks), working with system design consultants and the like.

Because so many behaviors need to happen in a coordinated fashion in order for online identity systems to function, and particularly for them to function at multiple levels of system metrics such as LOAs (and the proposed LOPs and LOCs), this section provides a structure for identifying such duties in detail. Each desired behavior and duty is matched to the specific Data Action, organized roughly in the order in which they occur in an online identity system.

There are nine general “Data Action” categories, each of which calls out a different data movements and/or use. Each Data Action is a different subsection of this section.

Matching behaviors and duties with specific Data Actions permits the correlation of duties, liabilities, management/mitigation strategies with discreet technological subsystems (such as those involved with proofing, authorizing, etc.), which will aid in implementation of appropriate system-stabilizing sets of coordinated Tools and Rules.

How to use the Data Action Diagrams

It is suggested that you print out, and have handy, a copy of the nine Data Action Diagrams to help you visualize the data and information flows in each Data Action while reviewing the separate “Identification,” “Analysis,” and “Management” steps. Each sub-step in this section 1 presents a “narrative” that describes the data and information movements that take place in each Data Action diagram.

How to use the Data Flow Mapping Tool

The Data Flow Mapping Tool is a blank “data action diagram” on which you can draw your own data flow map. This provides you with a picture of the data flows that you will examine and analyze using the Data Flow Survey Tool and the Risk Wiki.

How to use the Data Flow Survey Tool

Sometimes it is not obvious how a company engages in different Data Actions, particularly where data and information take place in systems that are decentralized, are poorly or incompletely mapped or understood, or are taken for granted by employees. Also, the Data Flow Survey Tool helps to alert the reader to the way in which a single Data Action can give rise to different duties for different parties.

For example, when you are playing catch with a ball, one pitch can involve your *throw* and your friends *catch*. Catching and throwing are different actions (verbs), both taken with respect to the same throw. Similarly, a transfer of data (the “throw” if you will) is a sharing by one person, and a *collecting* or *accessing* by another. Each party in a single data transfer will engage in different actions (“verbs”) that will invoke different legal duties and liability profiles. The Data Flow Survey Tool helps to identify these initially subtle details.

The more detailed the analysis of duties, the more accurate the risk analysis and liability management/mitigation steps can be. Duties are described with respect to specific actions. Toward this end, please refer to the Data Flow Survey Tool which asks various questions relating to generic Data Actions that are intended to help “tease out” the details of the specific types of sub-actions that together comprise the nine basic Data Actions, which might not be obvious at first.

The Data Flow Survey questions have been designed to solicit information about the particular verbs associated with the Data Actions that are relevant under various legal regimes and tests that are applicable to data and information under current U.S. law. It is expected that the list of verbs will expand to include relevant concepts under other relevant law as use of the tool expands.

The initial generic “Data Verbs” listed in the Data Flow Survey Tool are as follows: (additions and refinements to come):

Collecting data,
Accessing data,
Sharing data with others,
Holding data,
Using data, and
Disposing of data.

Each of the nine Data Action Steps of SOT/IDM transactions involves one or more of these generic 6 Data Verb categories. For instance, the Data Action Step of “proofing” includes the

collection of data by an IDSP, the *sharing* of data by a User, the *holding* of data by an IDSP, the *using* of data by the IDSP, etc. Because it involves separate steps, each of which could generate a separate and distinct legal duty, risk and liability, it is not appropriate to start with an analysis of generic “proofing.” Instead, each of the separate Data Action steps should be separately analyzed, with the results then combined to provide an overall profile of the identified duties, the analyzed risks and the mitigated liabilities associated with the overall “proofing” Data Action Step. Each action category has different risk profiles, different liability potential, and calls for different management strategies.

For each of the 9 Data Action Steps, the following pages provide:

- a. A number and title assigned to the “action” for cross reference.
- b. A data flow diagram of the SOT Sub-Transaction
- c. A narrative of the data flow, with reference to the “Action Categories” involved in that step.
- d. A listing of identified, potential liabilities of each SOT/IDM participant

Action 1 – System setup – Trust Framework Construction

- a. Number and title assigned to the action for cross reference.
See attached diagram number 1
- b. Data flow diagram of the SOT Sub-Transaction.
See attached diagram number 1
- c. Narrative of the data flow diagram.

Diagram number 1 sets forth the interaction between the Trust Community (TC) advisors, OIX and third party technical and legal consultants to advise a TC that is putting together its Trust Framework (TF).

The TF sets forth the SOT/IDM needs of the TC and its requirements for specific technology tools and legal rules (the “legal rules” in the form of TF requiring conformity with applicable background law (such as GLB, HIPAA, COPPA, etc.)), the TF’s establishment (or adoption) of standard definitions, contract terms and other legal requirements, or other structural, policy, enforcement, governance or other similar issues relevant to the TC.

The TF may call for specific IDSP/Assessor/Auditor or RP qualifications. TCs will generally be encouraged to take advantage of existing “best practices” regarding TF construction, LOA and LOP characterization, and legal rules.

- d. Listing of identified, potential duties of each SOT/IDM participant
 - i. IDSP – N/A
 - ii. RP – N/A
 - iii. User – N/A
 - iv. Assessor – N/A
 - v. Auditor – N/A
 - vi. Trust Community – [NOTE: Consider moving this to the “analyze” section]. TCs composed of commercial entities should consider anti-trust and competition laws in structuring collaboration. TCs should consider IP, governance and certification implications of TC’s production of TFs and other materials and marking conventions. Issues of whether to form separate entity (501(c)(3)? 501(c)(6)?) for initiative, or to convene as OIX working group or other entity working group.

- vii. Other – Advisors to TC? (Technology. Tools consultant, and Legal Rules consultant)

Action 2 – System setup – TF Listing and IDP Certification and Listing

- a. Number and title assigned to the action for cross reference
See attached diagram number 2
- b. Data flow diagram of the SOT Sub-Transaction
See attached diagram number 2
- c. Narrative of the data flow
Diagram number 2 sets forth the communications and data flows relating to the following system setup steps (see diagram):
 1. Register Trust Framework:
 2. OIX lists Trust Framework
 3. ISDP information provided to Assessor
 4. Assessor certifies IDSP
 5. OIX registers IDSP
 6. OIX lists IDSP
- d. Listing of identified, potential duties of each SOT/IDM participant
 - i. IDSP
Actions:
 1. Register TF - NA
 2. OIX List TF
 3. IDSP information provided to Assessor
 - i. LOA – Information must be accurate, current, etc.
 - ii. LOP – IDSP may have confidential or proprietary information that it wants to protect. IDSP should include that in terms, but restrictions may be inconsistent with transparency of assessment process.
 4. Assessor Certifies IDSP
 - i. “Responsibility” for certification is borne by assessor, but is affected by contract between Assessor and IDSP (for instance, assessor might seek to limit its liability for certifying based on false information, etc.)
 5. OIX Registers IDSP
 - i. IDSP agrees to terms of OIX membership rules, as in effect from time to time.
 6. OIX Lists IDSP

- i. IDSP agrees to terms of OIX listing rules, as in effect from time to time.
- ii. RP – N/A
- iii. User – N/A
- iv. Assessor – Note that it is assumed that for purposes of IDSP certification, the IDSP will not provide Assessor with access to any PI or other user data. If such data is required for the assessment, the LOP notes below should be expanded to include this type of protected data as well.

Actions:

- 1. Register TF – N/A
- 2. OIX List TF – N/A
- 3. IDSP Info. To Assessor
 - i. LOP – Assessor collects information from IDSP (See LOP “verbs” attachment for notes regarding Collection, Use, Disposal of Data)
- 4. Assessor Certifies IDSP
 - i. LOA – Assessor processes that are prerequisite to certification are relied on by RPs
- 5. OIX Registers IDSP
- 6. OIX Lists IDSP
 - i. LOA – OIX reliance on Assessor certification

- v. Auditor – Note that, while auditors perform similar functions to assessors, but not at the time of initial system setup, they are included here since the data flows are similar to that between an auditor and assessor.

Actions:

- 1. Register TF – N/A
- 2. OIX List TF – N/A
- 3. IDSP Info. To Auditor
 - i. LOP (Collection, Use, Disposal of Data)
- 4. Auditor Certifies IDSP
 - i. LOA risk to Auditor – potential liability if Audit was negligently rendered.
- 5. OIX Registers IDSP
- 6. OIX Lists IDSP

- viii. Trust Community - ?

Action 3 – Pre-SOT - Identification (step 1 – Proofing)

a. Number and title assigned to the action for cross reference

See attached diagram number 3

b. Data flow diagram of the SOT Sub-Transaction

See attached diagram number 3

c. Narrative of the data flow

Diagram number 3 sets forth the data flow from the user (individual, entity or object data subject) and from third parties to the IDSP to enable the IDSP to “proof” or identify the user as a prerequisite to credential and token issuance. The collection of data from third parties may be at the request and instruction of the user, or may be initiated by the IDSP (depending on the circumstances).

d. Listing of identified, potential duties of each SOT/IDM participant

i. IDSP
LOP –

- I. IDSP collects, holds and uses (see verb taxonomy) data from user and other data sources.
- II. When data is being collected from or about a User, they will be interested in:
 - a. Identity of data collector
 - b. Location from which data is being collected
 - c. Where data will be stored
 - d. What data is being collected
 - e. The reason for the collection and how it will be used
 - f. Who will have access to the information
 - g. What “User Centric” elements are present in the system
 - h. LOP information
 - i. Data retention and destruction policies.
 - j. How User can pursue interests in system
 - k. Dispute resolution

LOA – Query whether the IDSP collected data of quality and quantity necessary to permit it to perform the proofing needed to issue the credential and token at a given LOA (depending on TF requirements).

Both considerations affect the assignment of an appropriate LOA.

LOC – Is IDSP providing Data Subject “control” regarding data consistent with background law and TF requirements

ii. RP – N/A

iii. User

LOA – What are the obligations of the user to provide accurate and current information? What are the protocols and liability differences associated with the issuance of anonymous and pseudonymous identification? What are protections against misrepresentation in identification process?

- iv. Assessor – N/A
- iv. Auditor - N/A
- v. Trust Community - ?
- vi. Other parties
 - a. Other Data Sources
 - i. LOA – Did the third party data source provide accurate and current information?

Action 4 – Pre-SOT - Identification (step 2 – Credential/Token Issuance)

a. Number and title assigned to the action for cross reference

See attached diagram number 4

b. Data flow diagram of the SOT Sub-Transaction

See attached diagram number 4

c. Narrative of the data flow

Diagram number 4 sets forth the data flows associated with the issuance of the credential and token by the IDSP following its receipt and review of the identification data that it received from the User and third party information provider. Note that the Credential and/or Token may be issued to the User so that it can use it without further interaction with the IDSP. In the alternative, the Credential and/or Token may be retained by the IDSP to be sent directly by the IDSP to one or more RPs at the request of or on behalf of? the User.

d. Listing of identified, potential duties of each SOT/IDM participant

i. IDSP

LOP – To the extent that the Credential and Token are held by the IDSP, they constitute newly created identity “information” for which the IDSP needs to exercise a context-appropriate level of care in holding to prevent unauthorized use.

LOP – Is the transfer of the credential/Token secure to prevent interception or compromise by unauthorized persons?

LOA – The issuance of the Credential and the Token by IDSP causes it to be in the “chain of responsibility” for the quality of those identifiers at a given LOA. Consider how to assure that LOA levels and their corresponding level-dependent legal/policy requirements are clear in TF documents, given the multiple parties (i.e., user as data subject, IDSP as credential issuer, assessor as IDSP certifier to a given LOA) involved in delivering SOT services at a given LOA.

LOC – Is issuance process consistent with user control requirements of background law and relevant TF?

ii. RP – N/A

iii. User

a. Where User receives and holds Credential and Token –

- ii. LOP – User responsible for unauthorized use of Credentials and Tokens within its control
 - iii. LOA – User could be responsible for whether credential and token are used at LOA intended. Note that Credential and Token may be “marked” to indicate appropriate LOA to prevent abuse.
 - b. Where IDSP retains and holds Credential and Token -
 - i. LOP – IDSP could be responsible for third party unauthorized use of Credentials and Tokens within its control.
 - ii. LOA – IDSP responsible for issuing Credentials and Tokens at the appropriate LOA based on the requirements of the relevant TF and the quality and quantity of the identity data received.
 - iii. LOC – IDSP process consistent with user control requirements of background law?
 - c. Before User uses SOT/IDM system, they agree to comply with future changed or modified terms of relevant agreements and to resolve any disputes via the dispute resolution process.
- iv. Assessor – N/A
- v. Auditor – N/A
- vi. Trust Community - ?

Action 5 – SOT – Pre-Authentication Communications and Negotiation

a. Number and title assigned to the action for cross reference
See attached diagram number 5

b. Data flow diagram of the SOT Sub-Transaction
See attached diagram number 5

c. Narrative of the data flow

Diagram number 5 sets forth the “back and forth” communications that occur prior to the time that a level of “security” or authentication practice is required in a transaction. This may include, for example, the online search for publicly available information, the engagement in e-mail dialogue preliminary to entry into a transaction (such as for discussion of terms, etc.), and the like.

Even though this set of “actions” does not involve the exchange of identity related information, it is included in this liability analysis since it may involve the exchange of other information that one or the other parties is interested in protecting for some reason.

Thus, for example, providing copyrighted information to another party for their review might come with a license that permits them to duplicate it for internal review purposes. The violation of that “license” can lead to liability (infringement) associated with SOT/IDM transactions.

d. Listing of identified, potential duties of each SOT/IDM participant

- i. IDSP – N/A
- ii. RP – Exchange of “negotiation information” may be subject to particular contract terms (such as NDA and other confidentiality limitations, limited licenses, other contract terms meant to protect intellectual property and proprietary interests)
- iii. User – See RP above
- iv. Assessor – N/A
- v. Auditor – N/A
- vi. Trust Community - ?

Action 6 – SOT – Authentication Credentials and Tokens - Transfers

a. Number and title assigned to the action for cross reference

See attached diagram number 6

b. Data flow diagram of the SOT Sub-Transaction

See attached diagram number 6

c. Narrative of the data flow

Diagram number 6 sets forth the transfer of credentials and/or tokens at the initiation of an authentication interaction. Note that Action 6 describes the specific action of actual “transfer” of the credential, not the later action of review and reliance by the relying party. The act of “review, reference and reliance” is covered in Action 7.

The transfer can be from the User directly (where the IDSP has provided the User with the credential/token before hand).

In the alternative, the transfer can be from the IDSP, at the request of or on behalf of the User (where the IDSP stays in possession of the credential/token until such time as it is so requested).

It is anticipated that both types of systems will be useful in different settings as the SOT/IDM market matures, and that hybrid systems will be deployed that have elements of each approach (like client/server software).

d. Listing of identified, potential duties of each SOT/IDM participant

i. IDSP

- a. LOA – Provide safe transfer of credentials/tokens to RP to protect credential/token integrity
- b. LOP – Protect credentials/tokens from unauthorized access
- c. LOC – Are IDSP credential issuance processes consistent with user control requirements of background law?
- d. Other

ii. RP

- a. LOA
- b. LOP – Prior to collecting credentials, tokens or User-related identity information disclose RP privacy policy and the available LOP to User and IDSP.
- c. LOC – Are RP credential handling requirements consistent with data subject control requirements of background law?
- d. Other – Apply special rules for receipt of credentials/tokens relating to minors

- iii. User
 - a. LOA – Requirement that User follow processes required to assure integrity of credentials and tokens.
 - b. LOP – Requirement that User observe particular IDSP and RP protocols and processes to maintain system integrity.
 - c. Other
- iv. Assessor – N/A
- iv. Auditor – N/A
- v. Trust Community

Action 7 – SOT - Authentication Credentials and Tokens - Review and Reliance

a. Number and title assigned to the action for cross reference

See attached diagram number 7

b. Data flow diagram of the SOT Sub-Transaction

See attached diagram number 7

c. Narrative of the data flow

Diagram number 7 sets forth the “Action” of Review and Reliance by the Relying Party on credentials/tokens that it has received. While this “action” does not involve a “movement” of data, it does involve the action of “Using” data engaged in the Relying Party. (Please see the “Verbs Taxonomy” for exploration of SOT/IDM system elements associated with “Use” of data)

The “action” by the Relying Party of Review and Reliance is also part of the SOT/IDM system for which specifications can be applied to render the system more reliable, predictable and interoperable.

For example, system integrity can be improved and liability reduced if contract terms require that relying parties only rely on reasonably current credentials/tokens, and that they not accept them for transactions that require a higher LOA than that assigned to the credential/token that they have received).

Also, the exercise of reliance by the RP on a credential/token may prompt the RP to take action with respect to a third party (acting in reliance on the LOA of the credential/token) in such a way as result in potential liability for IDPs and others. Those interactions with third parties are not included on the diagrams for Action 7.

d. Listing of identified, potential duties of each SOT/IDM participant

i. IDSP

- a. LOA – Issue of detrimental reliance by RP
- b. LOP –
- c. LOC -
- d. Other -

ii. RP

- a. LOA – Issue of process steps required by RP prior to relying on credentials, tokens and other User-related information received and issue of whether there are reasonable measures to reduce risk of inaccurate and fraudulent information.
- b. LOP –
- c. LOC -
- d. Other –

- i. Apply appropriate rules for review and reliance on information provided by minors.
 - ii. Consider RP liability issues for incorrect rejection of conforming/accurate credentials/tokens and other authentication materials
 - iii. Consider evidentiary issues for RP to demonstrate detrimental reliance on faulty credentials/tokens. Need for documented internal processes. Possible need for changes to Federal and State evidentiary rules to match National Trust Framework standards for recordkeeping.
 - iii. User
 - a. LOA – To the extent that User initiated the presentation of the credential/token (either directly or by instruction to an IDSP), they are taking an action to make an identity assertion. Explore rights and responsibilities associated with detrimental reliance issue.
 - b. LOP -
 - iv. Assessor –
 - a. LOA – To the extent that the quality of the credential/token relied on is at issue, there is the potential that the quality issue could relate to a certification element for which testing could be well or poorly done. Consider potential for negligent certification.
 - v. Auditor
 - a. See LOA discussion for Assessor immediately above.
 - vi. Trust Community - ?

Action 8 – SOT – Post–Authentication Authorization by Relying Party

- a. Number and title assigned to the action for cross reference
See attached diagram number 8
- b. Data flow diagram of the SOT Sub-Transaction
See attached diagram number 8
- c. Narrative of the data flow
Diagram number 8 sets forth the data and information flow associated with post authentication authorization transactions.

Another exercise of reliance by the RP can take the form of an RP action with respect to a third party (acting in reliance on the LOA of the credential/token) in such a way as result in potential liability for IDPs and others). This potential action is reflected on the diagram for Action 8. While this action is different than providing User with access to online content, systems or services, it similarly represents a source of potential liability where the RP detrimentally relies upon faulty credentials/tokens.

- d. Listing of identified, potential duties of each SOT/IDM participant
 - i. IDSP
 - ii. RP
 - iii. User – Consider circumstances in which User will have responsibility for transactions authorized where use of credential/token was by third party.
 - iv. Assessor
 - v. Auditor
 - vi. Trust Community
 - vii. Other

Action 9 – Post-SOT – Data and Credential Management

a. Number and title assigned to the action for cross reference

See attached diagram number 9

b. Data flow diagram of the SOT Sub-Transaction

See attached diagram number 9

c. Narrative of the data flow

Diagram number 9 sets forth a subset of the potential actions associated with different uses of identity related data, credentials and tokens following their use in a particular SOT/IDM transaction.

Such actions may take the form of one or more of the following actions (Please see “Ecosystem of Duties and Liabilities - Verbs Taxonomy”).

Sharing data with Others

Using data

Holding data

Disposing of data

d. Listing of identified, potential liabilities of each SOT/IDM participant

i. IDSP

a. LOP – Protection of credentials/tokens and other User-related information in compliance with RP privacy policy.

b. Other -

ii. RP

a. LOP –

i. Protection of credentials/tokens and other User-related information in compliance with RP privacy policy.

ii. Agreement not to use credentials and other information for spam or other similar purposes.

b. Other –

iii. User

a. LOP – Requirement that User provide prompt notice to IDP or any loss or unauthorized use of credential or token.

b. Other -

iv. Assessor

a. LOP –

- b. Other –
- v. Auditor
 - a. LOP –
 - b. Other –
- vi. Trust Community - ?
- vii. Other - ?

II. ANALYZE RISKS

In Section I, for each Data Action, potential duties were identified.

This Section II carries forward the groupings of duties based on the category of Data Action involved, and adds the analysis of risk potential for each separate stakeholder with respect to each category of Data Action. This further forks the analysis, because while “duties” are assigned to a single specific party, “risks” can arise both to party that has the duty AND other parties where a duty is breached.

For example, where an IDP fails to properly “proof” a data subject and issues a credential to a fictitious data subject (i.e., a “data thief”), several parties can be at risk. The first is the IDP for “negligence risk” in issuing the credential, the second is to the identity thief for “criminal risk,” and the third is to the Relying Party for “reliance risk.” The single duty was on the IDP, but its breach caused “risk” to multiple other parties. At the inception of this analysis, only modest analytical forks are suggested. It is expected that, as the use of the online tool proceeds, a more detailed and comprehensive risk analysis will emerge.

Discussion of the Risk Analysis Process

Please note that this section is “under construction.” The work of the OIX Legal Policy Group has just started to add the summary risk analyses to this section.

Each section of this second part of the IAM analysis calls for:

- a. A stakeholder specific listing and analysis of potential risk concerns.

This is assembled as follows:

- i. “Duty” is brought forward from “Identify Duties” section in step one.
 - ii. “Breach” is analyzed for every Identified Duty. Risks to both breaching party and injured party arising from each identified Breach should be analyzed.
 - iii. “Causation” is analyzed for every “Breach” listed. The types of possible causes of “Breach” should each be listed and analyzed.
 - iv. “Damages” are analyzed for each “Causation” scenario listed. The likelihood and magnitude of potential damages should be evaluated.
- b. A listing of potential issues to be considered by Trust Communities preparing Trust Frameworks.

The listing is a summary of the significant issues identified in the overall analysis. It is intended to simplify the detail of the analysis, where appropriate, to aid in the drafting of the Trust Framework and in other work that uses the OIX Risk WIKI.

NOTE: The accurate characterization of duties may require that the consideration of that duty “bounce back and forth” between steps 1 and 2 for refinement prior to being moved to step 3. That is because it is anticipated that the analysis of duties that is engaged in under section 2 will result in refinements to the “duties” identified in section 1, i.e., that new duties (and new aspects of identified duties) will be discovered in step 2. The step 1 and step 2 processes should be repeated until sufficient refinement of the analysis is accomplished to warrant the consideration of liability management strategies in step 3.

Action 1 – System setup – Trust Framework Construction

- a. Stakeholder specific listing and analysis of potential risk concerns
 - i. IDSP
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - ii. RP
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - iii. User
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - iv. Assessor
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - v. Auditor
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - vi. Trust Community

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

b. Listing of Potential Issues for Trust Communities

List significant risk analysis issues associated with this Data Action for consideration by Trust Communities.

Action 2 – System setup – IDSP Certification

- a. Stakeholder specific listing and analysis of potential risk concerns
 - i. IDSP
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - ii. RP
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - iii. User
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - iv. Assessor
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - v. Auditor
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - vi. Trust Community

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

b. Listing of Potential Issues for Trust Communities

- A. Duty – (LOA and LOP) – Consider the interval for periodic recertification/audits by qualified auditors, and the access by market participants and the public to the results of such audits
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

- A. Duty - Consider requirements for transparency of certification process and access to assessor/audit data. [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

- A. Duty - Consider requirements for and implications of decertification. Will it be specific or general? What will happen to data held by IDSP (data portability issue).
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

- A. Duty - Consider level of detail of specifications in TF for certification process and reference to mandatory application of standardized approaches (normative references) for legal elements supporting a given LOP and LOA. Consider also suggestion of recommended practices in TF (informative references).
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

- iv. A. Duty - Consider circumstances where TF may require certification of RP. In those circumstances, consider also:

- a. Providing for RP obligation to notify IDSP and User on knowledge of SOT/IDM system breach.
- b. Providing for RP obligation to agree to future modifications and changes to TF requirements.
- c. Providing for RP obligation to resolve disputes through a specified dispute resolution process.

B. Breach [analyze risk to this and other stakeholders if this duty is breached]

C. Causation [analyze risks from causation issues]

D. Damages [analyze risks of damages magnitude and likelihood]

A. Duty - Consider mechanisms to address potential conflicts of interest when IDSPs pay assessors and auditors for certification services. [insert a duty of this stakeholder Identified in Step 1]

B. Breach [analyze risk to this and other stakeholders if this duty is breached]

C. Causation [analyze risks from causation issues]

D. Damages [analyze risks of damages magnitude and likelihood]

A. Duty - Consider requirements for assess and auditor independence, self certification and review of auditor and assessor certifications.

B. Breach [analyze risk to this and other stakeholders if this duty is breached]

C. Causation [analyze risks from causation issues]

D. Damages [analyze risks of damages magnitude and likelihood]

A. Duty (LOA and LOP) – Consider requirements for IDSPs response to findings of non-compliance with Trust Framework requirements.

B. Breach [analyze risk to this and other stakeholders if this duty is breached]

C. Causation [analyze risks from causation issues]

D. Damages [analyze risks of damages magnitude and likelihood]

b. Listing of Potential Issues for Trust Communities

List significant risk analysis issues associated with this Data Action for consideration by Trust Communities.

Action 3 – Pre-SOT - Identification (step 1 – Data Proofing)

a. Stakeholder specific listing and analysis of potential risk concerns

i. IDSP –

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

- a. LOA – What are the protocols and processes for the identity data proofing process? What type, quality and quantity of materials were referenced? What standards are applied for review? Was the process online? In Person?
- b. LOA and LOP – When information used in proofing process is received from third party, consider whether notification of User and RP is appropriate (to allow for vetting for accuracy and currency).
- c. Other –
 - i. Consider special rules relating to minors (and consider COPPA (minors), FERPA (educational records)).
 - ii. Compliance risk associated with transfer of identity related data that is “regulated data” under various state and federal laws.

ii. RP – N/A

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

iii. User

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

- a. LOA –
 - i. What are mechanisms to assure that reliable, current and relevant information have been provided
 - ii. What is the responsibility for omissions and misrepresentations of information?
- b. LOP –
- c. Other -

- iv. Assessor – N/A
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]

- v. Auditor – N/A
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]

- vi. Trust Community
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]

- b. Listing of Potential Issues for Trust Communities

List significant risk analysis issues associated with this Data Action for consideration by Trust Communities.

Action 4 – Pre-SOT - Identification (step 2 – Credential/Token Issuance)

a. Stakeholder specific listing and analysis of potential risk concerns

i. IDSP

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

a. LOA – For tokens and credentials, what systems are used to generate and support tokens and how secure are they.

- i. Consider breadth of potential liability due to expansion of range of uses for broadly interoperable SOT//IDM system. Multi-use, interoperable credentials/tokens may require stabilizing legislation or contract structures to be supported.

b. Other –

- i. Consider compliance risk associated with transfer of any credentials/tokens and identity related data that is “regulated data” under various state and federal laws.
- ii. Consider IDSP policies and assure that operations conform to description of data handling in published policies.

ii. RP

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

ii. User –

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

Consider user responsibility for keeping credential/token confidential and for authorized and some subcategory of unauthorized use (consider Reg. E and credit card analogy).

iv. Assessor –

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

- a. LOA – Indirect responsibility through certification exercise
- b. LOP - Indirect responsibility through certification exercises

v. Auditor

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

- a. LOA – See Assessor LOA discussion
- b. LOP – See Assessor LOA discussion

vi. Trust Community

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

b. Listing of Potential Issues for Trust Communities

List significant risk analysis issues associated with this Data Action for consideration by Trust Communities.

Action 5 – SOT – Pre-Authentication Communications and Negotiation

- a. Stakeholder specific listing and analysis of potential risk concerns
 - iii. IDSP –
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - ii. RP
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - iii. User
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - iv. Assessor
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]
 - v. Auditor
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]

vi. Trust Community

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

b. Listing of Potential Issues for Trust Communities

List significant risk analysis issues associated with this Data Action for consideration by Trust Communities.

Action 6 – SOT – Authentication Credentials and Tokens - Transfers

a. Stakeholder specific listing and analysis of potential risk concerns

i. IDSP

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

a. LOA –

- i. Consider whether system where IDSP or User holds credentials/tokens is preferred.
- ii. Potential liability from providing inaccurate or non-current information to RPs.

b. LOP – Protect credentials and tokens during transfers involved in issuance process. Includes analysis of both:

- i. Current standards and practices of “data protection” recognized and imposed under current law, and
- ii. New LOP concepts that are also relevant to issues of SOT/IDM system adoption, User “trust,” and system integrity. To the extent that these are determined to be required and implementable, they could be supported by contract and/or legislation. Examples of such new LOP categories for IDSPs that have been suggested for consideration by Trust Frameworks include:

1. Providing User with ability and right to decide whether information should be supplied to a particular RP.
2. Provide RPs and Users with easy access to online functions to report known system breaches and flaws undermining the maintenance of reliable, standardized LOA and LOPs.
3. Making available to User, on request, information regarding all instances in which information has been made available to any third party (RP or other).
4. To protect against LOP problems, have IDSP require RP to limit information (contained in the credentials, token or other authentication data) that they require for a given transaction.

5. Requirement that IDSP take reasonable steps to confirm authority of person making authorization request is the User or someone acting at their request or on their behalf, or where credential is held by IDSP, that the request is by an authorized RP.

c. Other –

- i. No Discrimination – IDSP provides credentials and tokens on User request to any RP that complies with applicable terms of SOT/IDM system and agreements.
- ii. Compliance risk associated with transfer of identity related data that is “regulated data” under various state and federal laws.

ii. RP

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

- a. LOP – Consider practice of “least collection principle” only collect credentials/tokens and information needed for immediate transaction.

iii. User –

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

iv. Assessor

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

v. Auditor

- A. Duty [insert a duty of this stakeholder Identified in Step 1]

- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

vi. Trust Community

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

b. Listing of Potential Issues for Trust Communities

List significant risk analysis issues associated with this Data Action for consideration by Trust Communities.

Action 7 – SOT - Authentication Credentials and Tokens - Review and Reliance

a. Stakeholder specific listing and analysis of potential risk concerns

i. IDSP

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

- a. LOA – Expanded liability potential as credentials/tokens are used in expanded markets and contexts.

ii. RP –

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

- a. Consider issues associated with general RP protocols and processes (e.g., that RP does not know of authentication problems), prior to relying on credential or token received from User or IDSP
- b. Consider whether TFs associated with specific regulated sectors (such as healthcare, banking, Massachusetts and California businesses and telecommunications companies) that impose a requirement on protecting certain information should set forth specific requirements for specific RP protocols and processes aimed at addressing the specific authentication requirements of the respective background laws of those areas.
- c. Consider liability of RP when it acts in reliance on a false credential, providing access to an unauthorized user.
- d. Consider liability of RP when it fails to act in reliance on a valid credential, denying access to an authorized user.

- iii. User
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]

- iv. Assessor
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]

- v. Auditor
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]

- vi. Trust Community
 - A. Duty [insert a duty of this stakeholder Identified in Step 1]
 - B. Breach [analyze risk to this and other stakeholders if this duty is breached]
 - C. Causation [analyze risks from causation issues]
 - D. Damages [analyze risks of damages magnitude and likelihood]

b. Listing of Potential Issues for Trust Communities

List significant risk analysis issues associated with this Data Action for consideration by Trust Communities.

Action 8 – SOT – Post – Authentication Authorization by Relying Party

a. Stakeholder specific listing and analysis of potential risk concerns

i. IDSP

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

- a. LOA – Reliance of RP on credential/token at given LOA could result in liability of IDSP

ii. RP –

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

- d. LOA - RP is the party to which a duty can be owed regarding the declaration that a particular credential/token is reliable (trusted) at a given LOA. The nature of the liability of the IDSP, Assessor, User, for an erroneous authorization made in reliance on presented credential is dependent on the type of resulting authorization. Authorizations include authorization to computer networks and network resources, the allowance of access to online data resources and communications systems.

iii. User

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]

D. Damages [analyze risks of damages magnitude and likelihood]

iv. Assessor

A. Duty [insert a duty of this stakeholder Identified in Step 1]

B. Breach [analyze risk to this and other stakeholders if this duty is breached]

C. Causation [analyze risks from causation issues]

D. Damages [analyze risks of damages magnitude and likelihood]

v. Auditor

A. Duty [insert a duty of this stakeholder Identified in Step 1]

B. Breach [analyze risk to this and other stakeholders if this duty is breached]

C. Causation [analyze risks from causation issues]

D. Damages [analyze risks of damages magnitude and likelihood]

vi. Trust Community

A. Duty [insert a duty of this stakeholder Identified in Step 1]

B. Breach [analyze risk to this and other stakeholders if this duty is breached]

C. Causation [analyze risks from causation issues]

D. Damages [analyze risks of damages magnitude and likelihood]

b. Listing of Potential Issues for Trust Communities

The nature of the authentication at issue generally dictates the LOA of the authentication. Thus, high security authorizations require high LOA authentications.

Authentication is to Authorization as passing through your office security system in the morning is like to going to work. The former is a necessary prerequisite, but ultimately the “value” is in what happens after you clear security. That latter value drives the quantification (i.e., damages calculation) in the liability analysis.

Authorization sensitivity and security drive liability issues. The different types of SOT within a given LOA will have a great many different liability profiles, as a result of differences in the economic and other implications of SOT/IDM system integrity breaches.

Action 9 – Post-SOT – Data and Credential Management

a. Stakeholder specific listing and analysis of potential risk concerns

i. IDSP

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

a. LOP – Continued protection of Identity related information, i.e., Credentials/Tokens/Identity Data. Requirements for LOP maintenance by IDSPs include both:

- i. Existing duties established under law.
 - 1. Consider situations in which duties are inconsistent with SOT/IDM overall goals and should be modified by legislation, risk sharing or spreading structures or contract provisions.
- ii. New duties that have been proposed for consideration as fostering SOT/IDM system integrity, deployment acceptance and enhanced system “trust.” Include:
 - 1. IDP obligation to destroy log files regarding User’s online activities (when obtained) within reasonable period
 - 2. IDSP obligation to notify User and RP of data and security breaches.
 - 3. Provide User with ability to revoke credentials/tokens.
 - 4. Provide data portability to address variety of situations in which IDSP services are no longer available to User.
 - 5. Provide credential/token information to RPs in a way that makes separate SOT/IDM transactions distinct and unlinkable (to avoid RP reuse of User data).
 - 6. Consider allowing user to request that IDSP not collect information on RPs to which credentials have been sent and the implications of this approach.

b. LOA – Reuse of credentials/tokens for

- i. multiple transactions
- ii. purposes not declared in agreement or policy

- iii. marketing without User consent (via opt in or opt out mechanism?)
- c. Other –

ii. RP

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

- a. LOP – Existing obligations to protect held Credentials/Tokens/Identity Data and to provide notice to Users of data breach for certain types of data.
- b. LOA –Reuse of credentials/tokens for multiple transactions
- c. Other –

iii. User

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

- a. LOP – Credentials/Tokens/Identity Data
- b. LOA –Reuse of credentials/tokens for multiple transactions
- d. Other –

iv. Assessor

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

- a. LOP – Holding, Sharing with Others, Use and Disposal of Identity Data, if any received as part of IDSP certification exercise.
- a. LOA –LOP integrity will reduce risk of identity theft related crime, where breach in LOP could allow identity thief to access the “instrumentality” (i.e., the data) of the later crime of monetary or other theft.
- b. Other –

iv. Auditor

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

[NOTE: The following issues and analyses have not yet been rendered in the standard “duty, breach, causation, damages” format]

- a. LOP – See Assessor analysis above
- b. LOA –See Assessor analysis above
- c. Other –

vi. Trust Community

- A. Duty [insert a duty of this stakeholder Identified in Step 1]
- B. Breach [analyze risk to this and other stakeholders if this duty is breached]
- C. Causation [analyze risks from causation issues]
- D. Damages [analyze risks of damages magnitude and likelihood]

b. Listing of Potential Issues for Trust Communities

Consider the “Verbs Taxonomy” as a prompt for identifying the types of actions that might be relevant to the liability analysis post-SOT. Examples include potential liability associated with such post-transaction actions such as (i) transferring data for marketing purposes contrary to statements made in a privacy policy with respect to data sharing practices, (ii) the holding of credit card information without cardholder permission following a completed transaction under PCI DSS, disposing of computer hard drives containing PI relating to residents of certain states without degaussing the drives, etc.).

To maintain interoperability, consider mechanisms for assuring that stakeholders deploying and using TF agree to comply with additional and modified future policies of TF as it changes to address then-current circumstances.

Consider role of standardized elements for dispute resolution process.

III. MANAGEMENT OF LIABILITY

In section I, for each Data Action 1-9, potential duties were identified.

In section II, for each Data Action 1-9, risks related to the potential breach of those duties were evaluated with respect to each stakeholder. The risks were analyzed with respect to the separate elements of breach, causation and damages.

In this section III, for each Data Action 1-9, the liability associated with each analyzed risk is “graded” and potential management strategies described.

The “branched analysis” of the prior sections is carried forward here to permit the more precise matching of potential management strategies with each particular context, entity and type of potential liability.

Each section of this third part of the IAM analysis provides:

- a. A stakeholder-specific listing of summary potential liability concerns.
- b. A stakeholder-specific listing of potential management strategies is called for. As a prompt to consideration of management possibilities at different levels of the legal stack, consideration of statutory, regulatory, other administrative and contractual management is solicited.

[Development note: In this and following sections, the quantitative and qualitative summary of the “Risk Analysis” should be included. Consider standardized “grading” system for liability severity, likelihood and impact analysis. Look at NIST and other factors for guidance. Align “grading” factors with potential types of management available.]

Action 1 – System setup – Trust Framework Construction

- a. Stakeholder specific summary of potential liability concerns
 - i. IDSP [include summary of “Analysis” section here]
 - ii. RP [include summary of “Analysis” section here]
 - iii. User [include summary of “Analysis” section here]
 - iv. Assessor [include summary of “Analysis” section here]
 - v. Auditor [include summary of “Analysis” section here]

- b. Listing of Potential Management Approaches
 - i. IDSP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - ii. RP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

- d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iii. User
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iv. Assessor
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - v. Auditor
 - a. Statutory Management
 - i. Nature of risk/liability to address

- ii. Potential solution
- b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
- c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
- d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

Action 2 – System setup – IDSP Certification

- a. Stakeholder specific listing of potential liability concerns
 - i. IDSP [include summary of “Analysis” section here]
 - ii. RP [include summary of “Analysis” section here]
 - iii. User [include summary of “Analysis” section here]
 - iv. Assessor [include summary of “Analysis” section here]
 - v. Auditor [include summary of “Analysis” section here]

- b. Listing of Potential Management Approaches
 - i. IDSP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - ii. RP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address

- ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
- iii. User
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
- iv. Assessor
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
- v. Auditor
 - a. Statutory Management

- i. Nature of risk/liability to address
 - ii. Potential solution

- b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

- c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

- d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

Action 3 – Pre-SOT - Identification (step 1 – Data Proofing)

- a. Stakeholder specific listing of potential liability concerns
 - i. IDSP [include summary of “Analysis” section here]
 - ii. RP [include summary of “Analysis” section here]
 - iii. User [include summary of “Analysis” section here]
 - iv. Assessor [include summary of “Analysis” section here]
 - v. Auditor [include summary of “Analysis” section here]

- b. Listing of Potential Management Approaches
 - i. IDSP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - ii. RP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address

- ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iii. User
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iv. Assessor
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - v. Auditor
 - a. Statutory Management

- i. Nature of risk/liability to address
 - ii. Potential solution

- b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

- c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

- d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

4 – Pre-SOT - Identification (step 2 – Credential/Token Issuance)

- a. Stakeholder specific listing of potential liability concerns
 - i. IDSP [include summary of “Analysis” section here]
 - ii. RP [include summary of “Analysis” section here]
 - iii. User [include summary of “Analysis” section here]
 - iv. Assessor [include summary of “Analysis” section here]
 - v. Auditor [include summary of “Analysis” section here]

- b. Listing of Potential Management Approaches
 - i. IDSP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - ii. RP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address

- ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iii. User
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iv. Assessor
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - v. Auditor
 - a. Statutory Management

- i. Nature of risk/liability to address
 - ii. Potential solution
- b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
- c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
- d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

Action 5 – SOT – Pre-Authentication Communications and Negotiation

- a. Stakeholder specific listing of potential liability concerns
 - i. IDSP [include summary of “Analysis” section here]
 - ii. RP [include summary of “Analysis” section here]
 - iii. User [include summary of “Analysis” section here]
 - iv. Assessor [include summary of “Analysis” section here]
 - v. Auditor [include summary of “Analysis” section here]

- b. Listing of Potential Management Approaches
 - i. IDSP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - ii. RP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address

- ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iii. User
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iv. Assessor
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - v. Auditor
 - a. Statutory Management

- i. Nature of risk/liability to address
 - ii. Potential solution
- b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
- c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
- d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

Action 6 – SOT – Authentication Credentials and Tokens - Transfers

- a. Stakeholder specific listing of potential liability concerns
 - i. IDSP [include summary of “Analysis” section here]
 - ii. RP [include summary of “Analysis” section here]
 - iii. User [include summary of “Analysis” section here]
 - iv. Assessor [include summary of “Analysis” section here]
 - v. Auditor [include summary of “Analysis” section here]

- b. Listing of Potential Management Approaches
 - i. IDSP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - ii. RP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management

- i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iii. User
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iv. Assessor
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - v. Auditor

- a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

- b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

- c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

- d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

Action 7 – SOT - Authentication Credentials and Tokens - Review and Reliance

- a. Stakeholder specific listing of potential liability concerns
 - i. IDSP [include summary of “Analysis” section here]
 - ii. RP [include summary of “Analysis” section here]
 - iii. User [include summary of “Analysis” section here]
 - iv. Assessor [include summary of “Analysis” section here]
 - v. Auditor [include summary of “Analysis” section here]

- b. Listing of Potential Management Approaches
 - i. IDSP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - ii. RP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address

- ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iii. User
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iv. Assessor
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - v. Auditor
 - a. Statutory Management

- i. Nature of risk/liability to address
 - ii. Potential solution
- b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
- c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
- d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

Action 8 – SOT – Post – Authentication Authorization by Relying Party

- a. Stakeholder specific listing of potential liability concerns
 - i. IDSP [include summary of “Analysis” section here]
 - ii. RP [include summary of “Analysis” section here]
 - iii. User [include summary of “Analysis” section here]
 - iv. Assessor [include summary of “Analysis” section here]
 - v. Auditor [include summary of “Analysis” section here]

- b. Listing of Potential Management Approaches
 - i. IDSP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - ii. RP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address

- ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iii. User
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iv. Assessor
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - v. Auditor
 - a. Statutory Management

- i. Nature of risk/liability to address
 - ii. Potential solution

- b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

- c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

- d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

Action 9 – Post-SOT – Data and Credential Management

- a. Stakeholder specific listing of potential liability concerns
 - i. IDSP [include summary of “Analysis” section here]
 - ii. RP [include summary of “Analysis” section here]
 - iii. User [include summary of “Analysis” section here]
 - iv. Assessor [include summary of “Analysis” section here]
 - v. Auditor [include summary of “Analysis” section here]

- b. Listing of Potential Management Approaches
 - i. IDSP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - ii. RP
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address

- ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iii. User
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - iv. Assessor
 - a. Statutory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution
 - v. Auditor
 - a. Statutory Management

- i. Nature of risk/liability to address
 - ii. Potential solution

- b. Regulatory Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

- c. Other Administrative Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

- d. Contractual Management
 - i. Nature of risk/liability to address
 - ii. Potential solution

