

**Exhibit 1**

# **OIX Trust Framework Legal Checklist**

**Draft 1.2**  
**February 10, 2011**

**Discussion and Development Materials**  
**of the**  
**OIX Advisory Committee**  
**and the**  
**OIX Legal Policy Committee**

**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](http://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].

The online functionality at [www.openidentityexchange.org](http://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**

This checklist tool provides a general guide for legal analysis by identity system:

service providers (such as IDPs and other data handlers), and

users (including relying parties and data subjects).

For service providers, the checklist can help with identity product/service development and can help to reduce costs and liability exposure.

For service users, the checklist can help with identity product review and evaluation.

Online identity achieves integrity through the application of both technology tools and legal rules. This is the a development checklist for the “Rules” portion of identity services and products (referred to as “products” herein). As such, this is a checklist for use in identity product and service development.

**Trust Framework Legal Checklist  
Short Version**

**Context Setting**

- 1. Review Participant Goals and Roles**
- 2. Review Additional Facts**
- 3. Review Existing Law**
- 4. Review Existing Contracts**

**Product Risks and Rewards Review**

- 5. Do Risk Analysis**
- 6. Configure Terms for Risk Management**
- 7. Develop Contract Terms to Realize Product Opportunities**

**Product Design and Release**

- 8. Prepare Documentation**
- 9. Launch Product and List with OIX**

**Post-Launch Change Management**

- 10. Adapt Product to Change**

## Trust Framework Legal Checklist Extended Version

### Context Setting

#### 1. Review Participant Goals and Roles

- a. Name **General Context** (Commercial, Social, Governmental)
- b. Name **Specific Context** (web, e-mail, Telco, banking, healthcare, education, consumer reporting, etc.)
- c. Name **Participant Type** (individual (adult or minor), business, governmental, etc.)
- d. Identify each **Participant Role** (e.g., IDP, RP, DS, Assessor, etc.)
- e. Identify each **Participant Goals** (e.g., design service (IDP), receive reliable credentials (RP), maintain controls to achieve “privacy” (DS))

#### **Tools:**

Exhibit 2 – OIX Data Action Diagrams  
Exhibit 3 - OIX Data Flow Mapping Tool  
Exhibit 4 - OIX Data Action Survey Tool (was “verbs taxonomy”)  
Exhibit 5 - Global Glossary Grid  
Exhibit 7 - OIX FIPPs Comparison Tool  
Exhibit 8 - OIX Harm and Solution Coordination Matrix

#### 2. Review Additional Facts

- a. Data “Nouns” - Identify **data type** (e.g., regulated data such as that covered by GLB, HIPAA, FCRA, FERPA, COPPA, etc.; is it confidential or proprietary data in commercial context)
- b. Data “Verbs” - Identify **data “flow” and specific data actions** taken (or planned) (e.g., collection, holding, transfer, correlation, use, disposal, etc.)

#### **Tools:**

Exhibit 2 – OIX Data Action Diagrams  
Exhibit 3 - OIX Data Flow Mapping Tool  
Exhibit 4 - OIX Data Action Survey Tool (was “verbs taxonomy”)  
Exhibit 5 - Global Glossary Grid  
Exhibit 6 - OIX Risk Wiki

#### 3. Review Existing Law

- a. Identify relevant jurisdictions (consider location of data subject, place of business of RP and IDP, server location (if known), choice-of-law clauses in agreements (see 4 below).

- b. Identify “hard edge” authority in jurisdiction (statutes, regulations, case law, etc.).
- c. Identify “soft edge” authority in jurisdiction (enforcement policies, vague statutory terms, conflict between relevant jurisdictions treatment, etc.).

**Tools:**

Exhibit 5 - Global Glossary Grid

Exhibit 6 - OIX Risk Wiki

Exhibit 7 - OIX FIPPs Comparison Tool

Exhibit 8 - OIX Harm and Solution Coordination Matrix

#### **4. Review Existing Contracts**

- a. **Customer-side** contracts (online TOU, Telco service agreements, privacy policies, subscription agreements, etc.)
- b. **Supplier-side** contracts (e.g., service providers (including employee agreements), content licensors/providers, etc.)

**Tools:**

Exhibit 3 - OIX Data Flow Mapping Tool

Exhibit 4 - OIX Data Action Survey Tool (was “verbs taxonomy”)

Exhibit 5 - Global Glossary Grid

Exhibit 6 - OIX Risk Wiki

### **Product Risks and Rewards Review**

#### **5. Do Risk Analysis**

- a. Economic and other **loss from your acts** (“Liability” for performance failure that breaches legal “duty” from statute, regulation or contract).
- b. Economic and other **loss from negligent acts of others** (negligence of others, e.g., service provider data loss, )
- c. Economic and other **loss from intentional acts of others** (intentional acts of others, e.g., data theft, misuse of credentials, unauthorized secondary use of data).
- d. Review available **technology solutions** to address risks if possible for maximum reliability (e.g., passwords, firewalls, etc.), and review remaining “reliability gaps” assuming technology is in place (the “gaps” will be the target of the legal “Rules” in step 6 below.)

**Tools:**

Exhibit 5 - Global Glossary Grid

Exhibit 6 - OIX Risk Wiki

Exhibit 8 - OIX Harm and Solution Coordination Matrix

## 6. Configure Terms for Risk Management

- a. Use **contract and structuring solutions** to maximize protection available under statute and regulations (e.g., draft toward favorable characterization under law, use liability insulating structures, pursue “safe-harbor” and “duty of care” qualification, etc.).
- b. Create **performance requirements for use of technology** to address risk and **performance requirements for managerial, physical, decision-making standards** and other non-technical requirements.
- c. Incorporate **risk sharing and risk shifting mechanisms** among both similar and different stakeholder groups into structure (e.g., insurance, indemnification arrangements, pooled risk structures among similarly situated participants, etc.).
- d. Apply **pricing and reserve strategies** to anticipate systemic or uncontrolled risks (consider accounting, tax and treasury function issues associated with matching against revenues).

### Tools:

Exhibit 5 - Global Glossary Grid

Exhibit 6 - OIX Risk Wiki

Exhibit 7 - OIX FIPPs Comparison Tool

Exhibit 8 - OIX Harm and Solution Coordination Matrix

**Notes:** See Attachment 1 for draft notes for consideration for Risk Wiki).

## 7. Develop Contract Terms to Realize Product Opportunities

- a. Create “**drafting solutions**” to cause other parties to perform duties that will support participant goals (LOA for RPs, LOC for DSs, and LOP for IDPs), and to fulfill other “data action” performance, revenue realization and market expansion needs.
- b. Synthesize “Tools and Rules” into hybrid structure to **cause data flows to take place reliably through both technology and human parts** of the system to achieve system performance and revenue goals.
- c. **Apply multi-level, integrated approach** to analysis of all stakeholder needs to create consensus-based structures of promises to drive adoption, achieve sustainability and to maximize “laminar” rather than “turbulent” data flows.

### Tools:

Exhibit 3 - OIX Data Flow Mapping Tool

Exhibit 5 - Global Glossary Grid

Exhibit 6 - OIX Risk Wiki

Exhibit 7 - OIX FIPPs Comparison Tool

Exhibit 8 - OIX Harm and Solution Coordination Matrix

## **Product Design and Release**

### **8. Prepare Documentation**

- a. Prepare **Trust Framework “term sheet”** to capture relevant variables to support contract preparation.
- b. Draft Agreements to establish enforceable performance duties for all participants, breach events, remedies and other issues raised that in the aggregate **create an enforceable “Trust Framework.”**
- c. Seek to **use common definitions** and terms applied in other Trust Frameworks to increase interoperability (and market penetration).
- d. **Normatively cross reference and incorporate terms and structures** applied in other Trust Frameworks to increase interoperability (and market penetration).

#### **Tools:**

Exhibit 5 - Global Glossary Grid

Exhibit 6 - OIX Risk Wiki

### **9. Launch Product and List with OIX**

- a. Become member of OIX
- b. Sign listing agreement
- c. List Trust Framework

#### **Tools:**

Exhibit 9 - OIX Trust Framework Metadata Listing Service

## **Post-Launch Change Management**

### **10. Adapt Product to Change**

- a. Anticipate future change in document terms
- b. Create processes to streamline future change processes

#### **Tools:**

Exhibit 1 - OIX Trust Framework Legal Checklist

Exhibit 2 – OIX Data Action Diagrams

Exhibit 3 - OIX Data Flow Mapping Tool

Exhibit 4 - OIX Data Action Survey Tool (was “verbs taxonomy”)

Exhibit 5 - Global Glossary Grid

Exhibit 6 - OIX Risk Wiki

Exhibit 7 - OIX FIPPs Comparison Tool

Exhibit 8 - OIX Harm and Solution Coordination Matrix  
Exhibit 9 - OIX Trust Framework Metadata Listing Service

## Attachment 1

**These notes are associated with:**

### **Checklist Step 6 – “Configure Terms for Risk Management”**

**The following are notes for consideration for inclusion in the risk wiki relating to the liability management and risk mitigation issues.**

**These are in draft form, and do not represent a cohesive narrative of the issues. These notes should be included in the risk wiki online discussion as relevant.**

#### **Notes summary:**

Analyses of potential liability mitigation strategies are multifaceted, and involve an evaluation of strategies at a variety of levels. For example, mitigation of liabilities can be effected at:

the **analytical level** (for example with respect to ways to affect elements of traditional legal analyses of duties, breach, causation, damages and liability);

the **process level** (for example by providing positive “safe harbors” to encourage desired behaviors (such as conformity to consensus-based data handling practices), and “strict liability” to curb undesirable behaviors (such as data theft);

the **strategic levels** (relating to the different sources of authority that provide the mitigation “relief” such as legislation, regulation; administrative practice, litigation and contracts (which can be result in risk shifting, or risk “eliminating” in practical effect); and

the **systemic level** (through mechanisms to address system costs that cannot be otherwise mitigated (such as through insurance (both liability insurance and no-fault schemes are potentially relevant here), fee and taxation schemes that pay costs of shifting risk to government/citizens that benefit from systems, and the like);

[Note: consider other relevant levels here].

Each of these levels is explored in greater detail below

#### **Discussion and Analysis**

Injury is relevant to injured parties and to the systems on which they depend.

Look at injury/damage from the system, as well as individual perspective.

Systems of compensation for damages, liability and liability mitigation are resource allocation mechanisms. From a system perspective, they dictate who will ultimately incur the economic costs associated with resource allocation systems when system inconsistent, unanticipated or non-system events result in additional costs.

Rules in these areas are often generalized as reflecting a "Bentham-like" notion of "the greatest good for the greatest number," particularly in the contexts where data resource management systems are depended upon by user groups in the context of large group governance structures, social communities and expansive commercial markets; where such weighting serves the need of assuring maximum system continuity and minimal displacement from issues that affect only a minority of system users.

Close examination of liability profiles in various industries, including a review of the economic effects of various existing systems of hybrid liability/mitigation schemes, reveals what many already perceive, i.e., that the efforts to impose precise liability and mitigation structures (to narrowly "channel" behaviors), are often also characterized by unplanned variables that can derail their intended economic effect.

Nonetheless, with appropriate information "feedback" mechanisms in place, such systems adjust to such variables (such as when premiums are adjusted to account for claims experience from a particular group of insured parties), and reach a sort of steady state; at which point risk is mitigated during the period that system changes occur only gradually, with occasional larger "fits and starts" (for example through new legislation or a new court case). Even if existing systems are accused of not always achieving the desired result, they at least offer some structure, which is at least a start to dealing with liability and mitigation in a structured, strategic way.

#### Risk and liability arise from duties

[Provide link and reference to the duties, risk and liability analysis presented in the section on "Liabilities."]

#### When structuring liability and mitigation structures, "liability" can be evaluated from several levels

From the *individual level*, harm is perceived as something to be remedied. The narrower individual perspective permits the ready identification of losses suffered, harms caused, insults imposed and other bases for complaint.

Importantly, the discernment of harm and its remediation involves more than just the final adjudication of responsibility (through the "duty-breach-causation-damages" structure). It is also important to consider the larger processes, and their system effects, particularly where the systems are large (many participants, many transactions, etc.) and the potential harms are typically relatively minor (such as the "costs" associated with monitoring credit reports) or are not legally cognizable under current law. In this context,

the assertion of the complaint by the party that perceives the harm, invites the energy-absorbing application of process, to provide a “time out” for deliberation and analysis of the issues by all parties.

Of course, given the already tremendous and growing volume of identity related transactions that take place daily on networked information systems (including, but not limited to, e-mail, search and phone calls), it is critical that the processes for assertion and resolution of claims be streamlined and machine assisted to the extent possible. The sheer magnitude of the conflict resolution challenge for online harms will require substantial consideration, planning, and educational efforts.

### The individual view of liability is just part of the picture

Every party that uses networked information and identity systems has the potential to experience harm as a result of its use of the system. This includes individual, commercial, governmental and other parties in various roles. Each of the parties’ interests will need to be addressed in the structuring of sustainable, adopted systems.

This multi-party perspective is often lost in the chorus of concern with the interests of individual consumer/citizens. Clearly there are also many small businesses, charitable organizations and other groups that could potentially experience harm in their roles as either data subjects, relying parties or otherwise. In addition, larger commercial and governmental players can also experience harm from their use of these systems.

These notes focus on potential harms to individuals as an initial matter in the interest of proposing an analytical construct for the harm “vector” that has gotten the most attention, and which can benefit most significantly from such structure. Other vectors of harm will be developed in the risk wiki.

The individual view of liability suggests mitigation strategies that are directed at altering the individual risk profile, and that focus on reducing risk for the individual person or entity. The individual perspective is aimed at the preservation of legal “rights” that arise as an artifact of the nature of the many “identity based” laws that define our relationships with others (such as property, contract, tort, etc.), all based on various iterations of the relationship between “self” and “other.”

The individual perspective is unique, in that it is more highly developed, and the “silos” that characterize the current state of data/identity law manifest as fragmented legal “solutions,” that establish duties for data handling parties that can be inconsistent. Also, from the individual level “risk shifting” (i.e., “make the other guy pay.”) is just as satisfactory as “risk elimination.”<sup>1</sup>

---

<sup>1</sup> In fact it may be competitively more satisfactory to have a system that recognizes that it shifts risks, since more explicit declaration of the respective connections of bad and good behaviors to “risk relief” and “risk burden” will incentive a greater number of people.

The particular concerns at the individual level yield a corresponding set of particular solutions, mostly relating to the processes that have been established to give form to the various “rights” that are applied at the individual level. The perennial issues in the area of direct versus indirect damages (how far to extend the implications of “causation”) and questions of how to set so-called “punitive, indirect, exemplary and other similar damages,” offer plenty of variables to challenge the analysis of risk and liability, even where the breach and causation variables are clear and unquestioned.

### The system view of liability

Many of the most critical issues are, however, at the system level. From the system level, those harms that cannot be eliminated are merely reallocated (as a system cost incurred due to contractual responsibility). The debate then shifts to a sort of “overall fairness” question of which party in the system is best able to shoulder which risks, and which qualify for more aggressive measures aimed at mitigation.

The issue of mitigation is ultimately a question of resource allocation (in this case in the form of cost), where system resources are finite. The question can be cast as “What are the mechanisms that can allow the entire “system of systems” to function in a sustainable manner so that a given single system within that structure can continue to deliver the benefits for which it was designed?”

In other words, in a system of finite resources, how is the “pinch” of resource limitations addressed. This is the question asked intermittently in the financial system context (for instance at the time of setting FDIC reserve levels, and at the time of setting “stimulus” funding to maintain system integrity in the “too big to fail” context).

### Mitigation must match risk

As alluded to above, liability can manifest itself at various levels, each of which invites a different solution

For example, merely placing “liability” on a single breaching party may not be an effective strategy to protect the “system” for system-level risks. It is analogous to the ineffectuality of firing a \$500,000 Wall Street trader in an effort to address a \$1 billion trading loss that resulted from that employee’s system-risking behavior. That type of risk might be better mitigated through another strategy. There are numerous situations where the imposition of liability is not sufficient protection at the system level, typically in the context of catastrophic risks. This is why, for example, the risks that were the focus of the FCC suggestion for “FDIC-type” insurance in the \_\_\_\_\_ might be better served through a mechanism more akin to “no-fault” automobile insurance.

[NOTE: More here]

Risk is dynamic in changing systems, so mitigation strategies must be dynamic as well

[NOTE: More here on notion that systems need more, they need mechanisms to dynamically prevent recurrence, recidivism, cascading failure scenarios, and other similar “network effects” of harm. For this, the systems require built in feedback mechanisms. More here]

Analytical, Process, Strategic, and Systemic approaches

[NOTE: Expand discussion of each approach in the Risk Wiki]

### **Analytical Level Strategies**

Since liability is the end point of the process of requiring parties to compensate victims for the harm that they cause by defaulting on their duties (i.e., promises of performance), any variable that goes into determining liability can potentially be relevant in crafting approaches to limiting liability. The *analysis* of these variables and the way in which they are affected by various factors (presumptions, definitions, legal tests, standards established in precedent, and the like), can yield insight into steps that can be taken to either enhance (for “good liabilities” such as those imposed on “data thieves”) or diminish (for “bad liabilities” such as those imposed based on unanticipated harms), the potential mitigation approaches.

[NOTE: More here]

### **Preventing the failure in the first place**

Significant liability limitation can be achieved by creating clear, reliable, interoperable systems. In fact, familiar systems are more resistant to harms that are both negligently caused and those that are intentional. Reliable, predictable interoperable systems are more familiar, and that familiarity can help to reduce negligence (reducing liability) simply because it will be easier for all parties to exercise appropriate levels of “due care” when they are interacting with familiar systems.

Familiarity will also reduce the system’s vulnerability to attack which causes intentional harms. This is because in familiar systems, it is harder to engage in so-called “social engineering” attacks (and related “pretexting” in relevant telecommunications legislation and regulation), such as underlies the majority of data breach events currently. It is harder to fool someone into allowing unauthorized access to data when the data rules are better known.

[NOTE: More here]

### **Separating different types of failure**

There are many potential points of failure in complex systems. Failures caused by negligence can be different than those caused by intentional actions of third parties.

Each has different tests that arose in the context of different laws and commercial and social settings. Taking those variables into account substantially expands the more “theoretical” questions raised above regarding “duties, breach, causation and damages.”

NOTE: More here on how the different factors are modified to apply in different contexts. Discuss *res ipsa locator*, causation clarification, the effect of other parties’ negligence in both comparative-negligence and contributory-negligence jurisdictions, the “doctrine of unclean hands,” etc. Also discuss insurance and other risk spreading and risk sharing mechanisms. Also, consider separate mechanisms of liquidated damages, indemnities, liability caps and other contractual mechanisms so allocate liability both before and after it is finally determined.

### **Approaches to mitigating online identity system liabilities**

NOTE: The following outlines a variety of examples of mitigation strategies. They should be presented in a manner that reflects the proposed structures above (such as division of mitigation analysis into analytic, process, strategic and systemic approaches].

In current identity management systems, two of the chief variables associated with liability are (i) unknown legal constructs and (ii) human or entity misbehavior (either negligent or intentional). Contract strategies directed toward mitigating or eliminating these sources of liability might include, for example:

#### **Contract methods**

- Indemnification
- Warranties language
- Explicit limitations of liability
- Guarantees
- Clear statement of responsibilities (duties) relating to data and information handling
- Clear drafting of terms and definitions (avoids misunderstanding)
- “As is” –type clauses
- Integration clause to avoid “parole evidence” and related issues
- Force Majeur* clause
- Cost containment mechanisms (such as requirement for arbitration, etc.)
- “Cure periods” for default
- [Other]

#### **Risk shifting methods**

- Indemnifications
- Legislative and regulatory “safe harbors”

#### **Risk spreading methods**

- Insurance (spread risk to premium payers).
- Investment (spread risk to investors)

System relief that is funded by taxes (spread risk among citizens; an additional challenge in international systems)

### **Legislative and regulatory methods**

Selection of legislative definitions and structures provide “orderly” commercial markets.

Creation of “safe harbors” to encourage system-consistent behavior (doesn’t eliminate system risk, but will normalize it for some parties). (e.g., see Reg. E in the PCI-DSS context for credit cards)

[More here:]

### **Behavioral methods**

Education

Training employees for compliance with policies

Simplification of processes

[Note articles in Science and Nature magazines on research demonstrating reductions in errors and system failures when checklists were used by pilots, surgeons, nuclear power plant workers]

### **Policy methods**

Establish clear policies for every person who might come in contact with entity’s data such as employee policy, website TOU, network use policy, phone system policy. Simple structures and broadly issued policies. Institutional “buy in” to make policies stick.

### **Technology methods**

Curb discretion that can lead to risk by limiting operations for access, transfer, etc. that can result in liability. In other words, rules are intended to curb discretion, but appropriately applied technologies such as firewalls, encryption, etc. can entirely eliminate discretion by entirely preventing access to data and information upon which discretion might otherwise be exercised.

Note that encryption (without specifics) is invoked in many statutes as a sort of “safe harbor” in the data breach notice requirements.

Consider encryption of data at rest, and in transfer, particularly PII.

### **Investigative methods**

Data flow audit – test the verbs to confirm how a company is handling data currently. Identify potential “points of failure” in both Tools AND Rules, BEFORE there is a liability asserted.

### **Systems/Structures methods**

Consider strategies to reduce the holding of sensitive data

“Least information principle”

Store information centrally where can assure timely disposal

[NOTE: Include more examples and follow structure suggested in initial discussion]