

InterPARES Trust Overview

Luciana Duranti, Project Director and Professor
School of Library, Archival and Information Studies
The University of British Columbia
Vancouver, B.C. Canada

The Overall Challenge

The nature of digital records:

- Records are **vulnerable** (easy to destroy, lose, corrupt, tamper with, or become inaccessible if not protected) and **persistent** (forever there if not purposefully destroyed)
- Record **content, structure and form are no longer inextricably linked**
- The record as a stored entity is distinct from its manifestation on a computer screen, and its **digital components** have to be considered as well as its documentary form
- When we save a record, we take it apart in its digital components, and when we retrieve it, we reproduce it creating a copy: hence **it is not possible to preserve a digital record, only the ability to reproduce or recreate it**



The Overall Challenge (cont.)

- Establishing digital records **accuracy, reliability and authenticity** and maintaining it over time so that it can be proven
- Developing an infrastructure that ensures a **seamless controlled flow** of authentic data/documents/records from the creator to the preserver irrespective of changes in technology
- Providing **transparency** while protecting secrecy where warranted
- Ensuring that the **conflicting rights** of users, clients, employees, and future generations are protected
- Ensuring the **permanent preservation** of the documentary cultural heritage in digital form

Records Online

Increasingly individuals and organizations choose to keep their records on line. The primary **uses** of the online environment are:

- Backup
 - Collaboration
 - Distribution (including social media)
 - Recordkeeping
 - Long-term storage
 - Keeping Archives
-
- Email storage is number one.

Internet vs Cloud

Internet provider refers to “entities providing users the **ability to communicate** through a computer system **that processes or stores computer data** on behalf of such communication or users.” (Budapest Convention on Cybercrime, 2001). Three “actions” relate to the definition of provider: **communication, data processing** and **data storage**.

“**Cloud computing** is a model for enabling convenient, on-demand network access to a **shared** pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” (National Institute of Standards and Technology, 2009)

The term Cloud is useful as it conveys the nebulous nature of what happens on the Internet, and the fact that, differently from other industries presenting similar characteristics, like the aero-spatial one, the services offered on the Internet are not **regulated** nor are they **transparent**.



Trust on the Internet

- We know very little about what happens on the Internet. The **standard of trustworthiness** for it is that of the ordinary marketplace, *caveat emptor*, or **buyer beware**
- Trust is defined in legal theory as a relationship of **voluntary vulnerability, dependence and reliance**, based on **risk assessment**
- The nature of trust relationships on the Internet is fraught with risks, weaknesses, and fault-lines inherent in the management of records and their storage in rapidly changing technologies where **authorship, ownership, and jurisdiction** may be questioned.

What is involved in Trust?

- In business, trust involves confidence of one party in another, based on **alignment of value systems** with respect to **specific benefits**
- In everyday life, trust involves acting without the knowledge needed to act. It consists of **substituting the information that one does not have with other information**
- Trust is also a matter of **perception** and it is often **rooted in old mechanisms** which may lead us to trust untrustworthy entities



Questions We Should Be Asking

- How can **confidentiality** and **privacy** be protected in the Internet?
- How can **forensic readiness** of an organization be maintained and **compliance with the law** ensured?
- How can an organization's records **accuracy, reliability, and authenticity** be guaranteed and verifiable?
- How can an organization's records and information **security** be enforced?
- How can an organization maintain **governance** upon the records entrusted to the Internet?
- How can the **preservation** of records of permanent value be ensured?



The Classic Response

- Choosing the Internet is a **Risk Assessment** decision where Risk = probability x impact. It is a question of comparison. If one cannot have everything, what does one give up?
- The first choice offered us is **between Transparency and Security**: the Internet offers “trust through technology.” Security involves location independence: a core aspect of Internet services delivery models.
- The second choice offered us is **between Control and Economy**: the Internet offers “trust through control on expenditures.”



The Trust Challenge

If we decide to carry out our activities online, we must find a balance between **trust** and **trustworthiness**, which is needed to ensure a balanced trust relationship.

Trust constitutes a risk which can only be mitigated by the establishment of a **trust balance**: we must trust trustworthy trustees and trustworthy records.



InterPARES Trust (2013-2018)

The **goal of InterPARES Trust** is to generate the theoretical and methodological **frameworks** that will support the development of integrated and consistent local, national and international **networks of policies, procedures, regulations, standards and legislation concerning digital records entrusted to the Internet**, to ensure public trust grounded on evidence of good governance, a strong digital economy, and a persistent digital memory.

InterPARES Trust is funded by a 5-year SSHRC Partnership grant and matching funds from UBC and all the partners (in cash and/or in kind)



InterPARES Trust Participants

- The **International Alliance** comprises 7 Teams:
 - North America
 - Latin America
 - Europe
 - Asia
 - Australasia
 - Africa
 - Transnational Organizations
- Supporting Partners
- Pro-bono Consultants
- Management Team



Partners

- Universities
- National & Regional Archives
- Libraries
- Governments
- International Organizations
- Businesses
- Individual researchers



Research Objectives

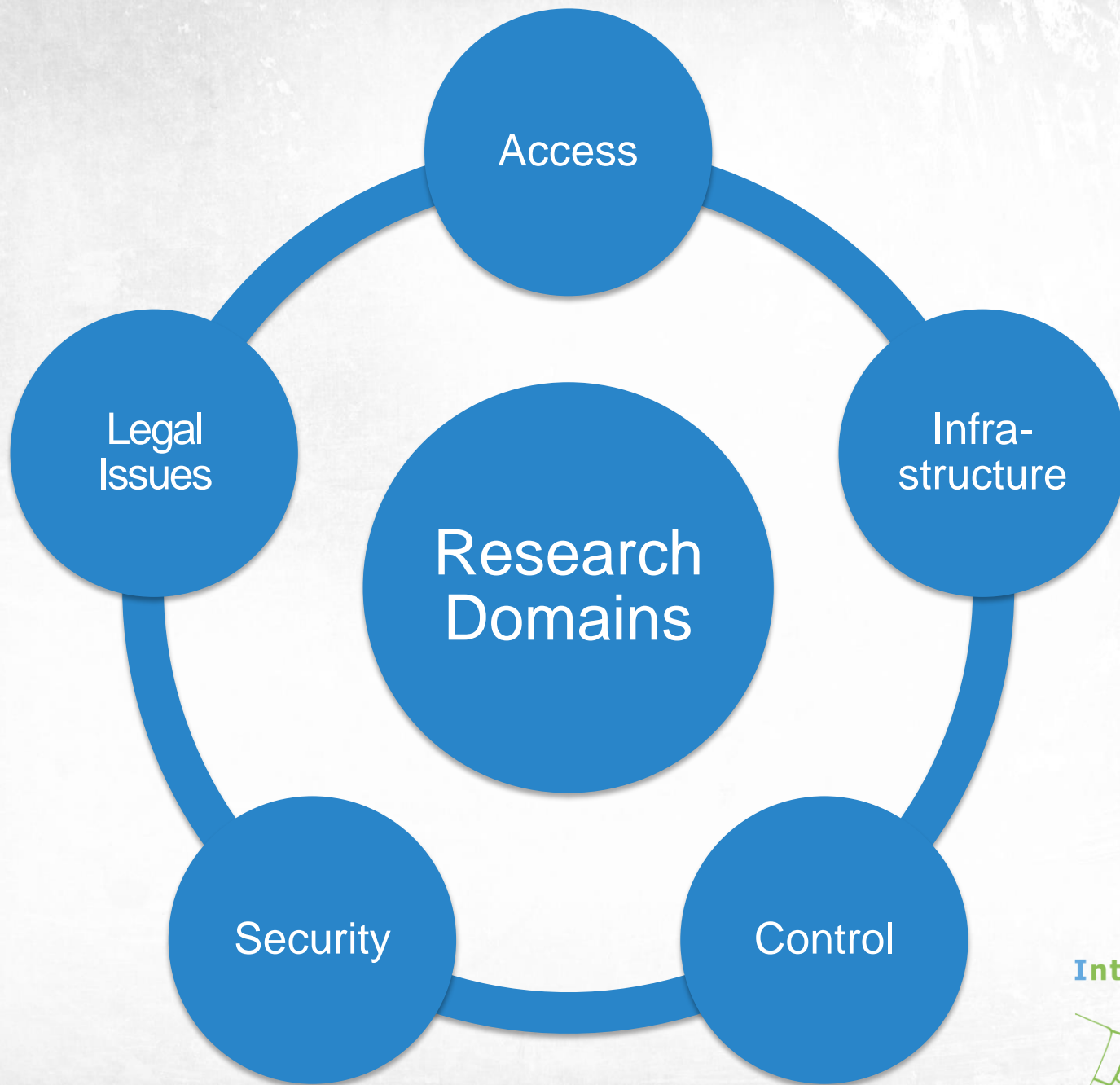
- Building the foundations for establishing a **relationship of trust** between the people and those organizations that hold the records and data related to and/or belonging to them on the Internet
- Ensuring the **trustworthiness of data and records** created in the interaction of people and organizations
- Developing a **supra-national framework embracing both developed and developing countries and all sectors**, which is capable of guiding the development of domestic legislation and regulatory instruments that are consistent across cultures and societies

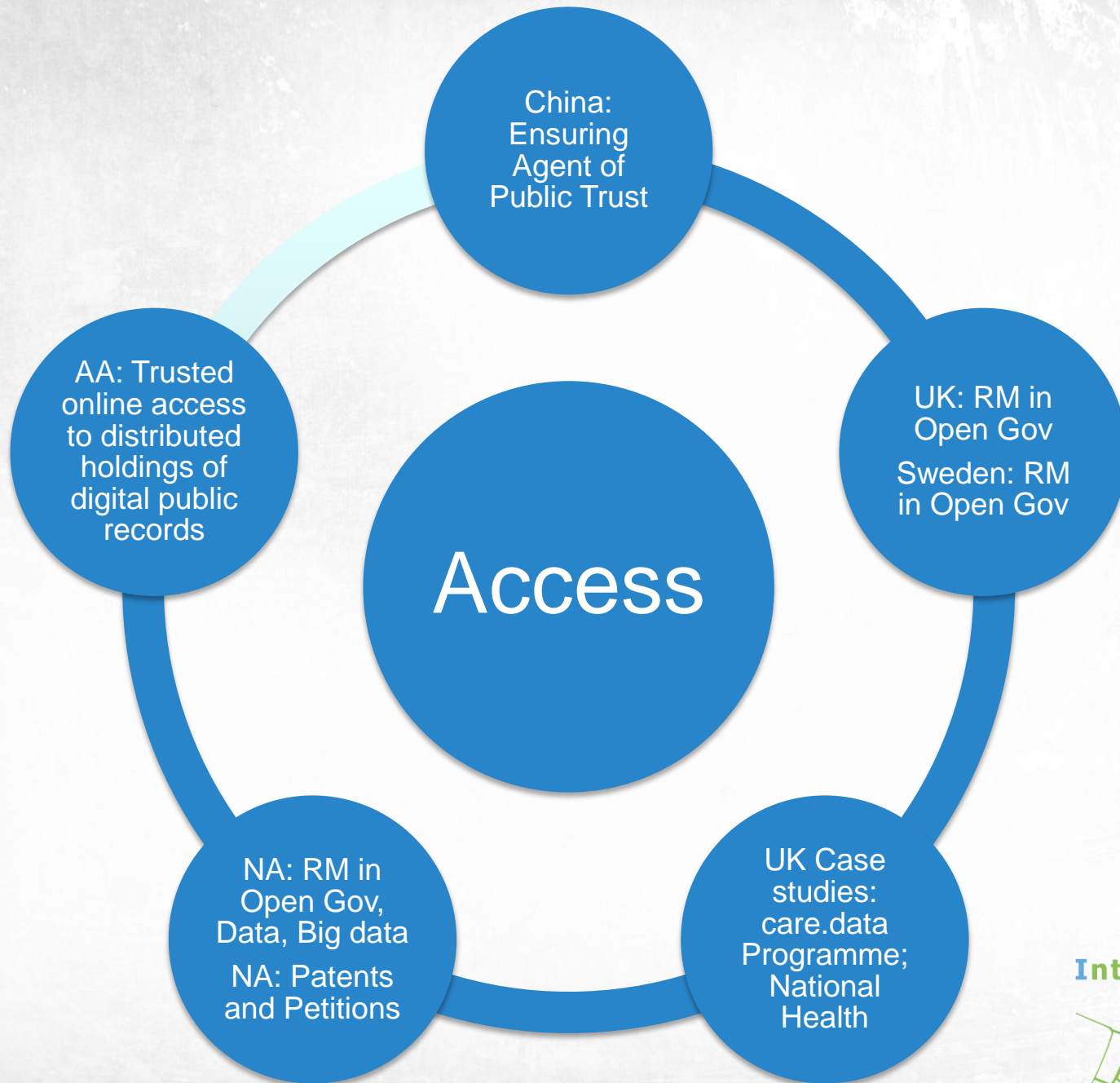


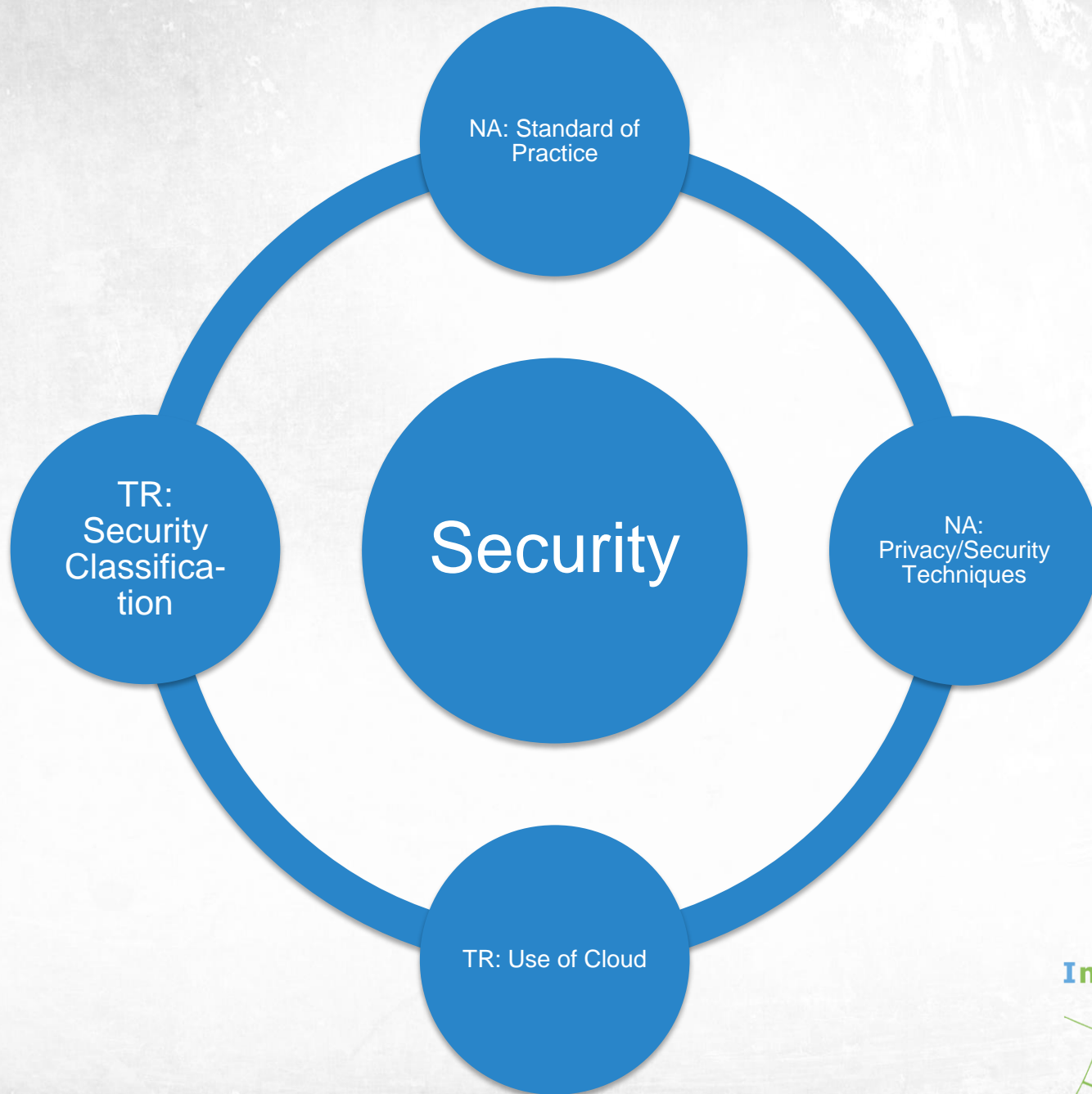
Methodology

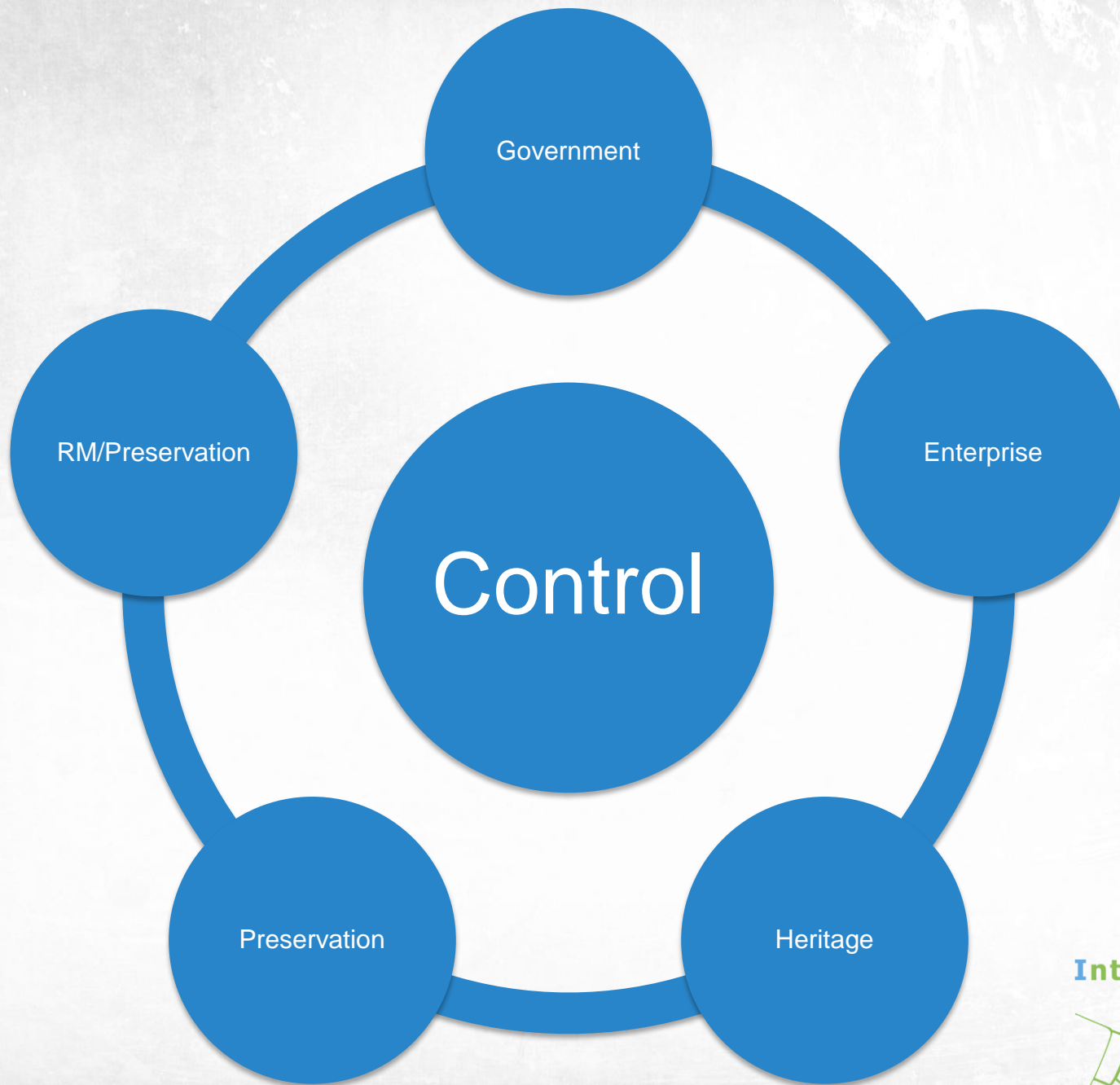
- **Archival and diplomatics methods**
- We use **auxiliary sciences** to overcome specific challenges
 - **Resource-based theory** because studies the technologic, managerial and relational means of maximizing competitive advantage
 - **Risk management** because it studies vulnerabilities and ways to mitigate them
 - **Design theory** because it studies policy in situations with unknown variable
 - **Digital forensics**, because it studies the authenticity of digital material that do not reside in the systems in which they were produced and kept
 - **Human computer interaction; aero-spatial, cybercrime, and telecommunication law; organizational theory**, etc.
- We **integrate** this knowledge into archival science, ensuring that the archival system maintain its consistency and cohesion











Control - Government

- User perceptions of trust – New Zealand
- Chain of responsibility of RM – China
- Monitoring life cycle compliance – Croatia
- Preserving/managing life cycle – Brazil
- Comparative analysis of e-services - Croatia
- Digital certificates in e-Government – China
- Website retention & disposition – Israel

Control - Government

- Case study of statements of offence – Belgium and Canada (Quebec)
- Retention & disposition in a cloud environment – North America
- Open data & open government in Latin America – Mexico & Chile
- Regulations for cloud storage – Mexico
- Policies for records of IFAI – Mexico
- Encouraging records creating agencies to use and trust digital archiving – Australasia

Control – Enterprise & Heritage

- Benefits realization management – Norway & Sweden
- Enterprise RM in the cloud – China
- IFRCjobs: SaaS Recruiting tool - Transnational
- Evaluating metadata in cultural heritage organizations – Turkey
- Users Perspectives of Trust -- Australasia

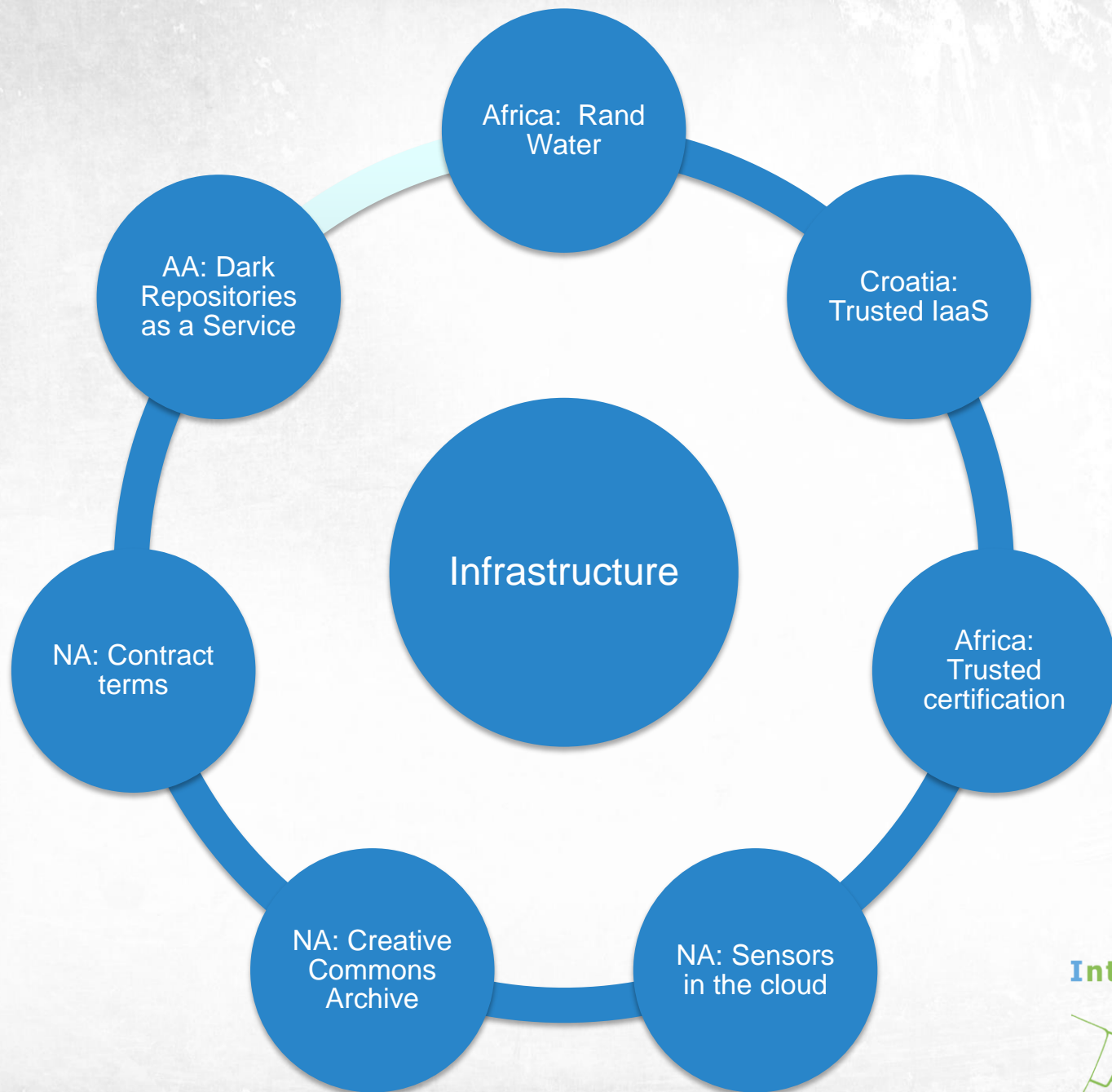
Preservation as a Service for Trust (PaaST)

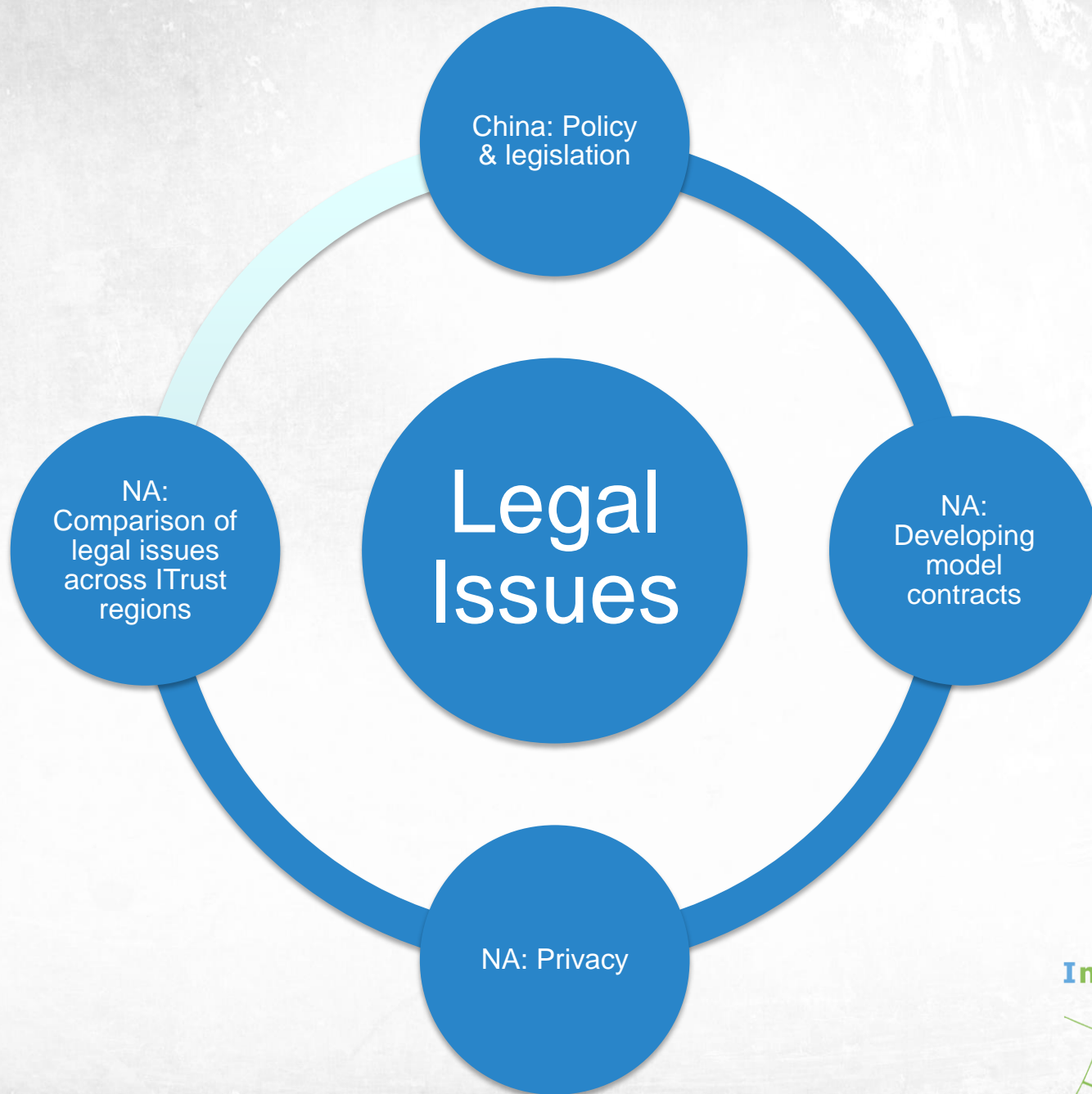
From these studies, InterPARES Trust is developing a model of **preservation as a service for trust** that every designated preserver (e.g. archives) can require CSProviders to respect

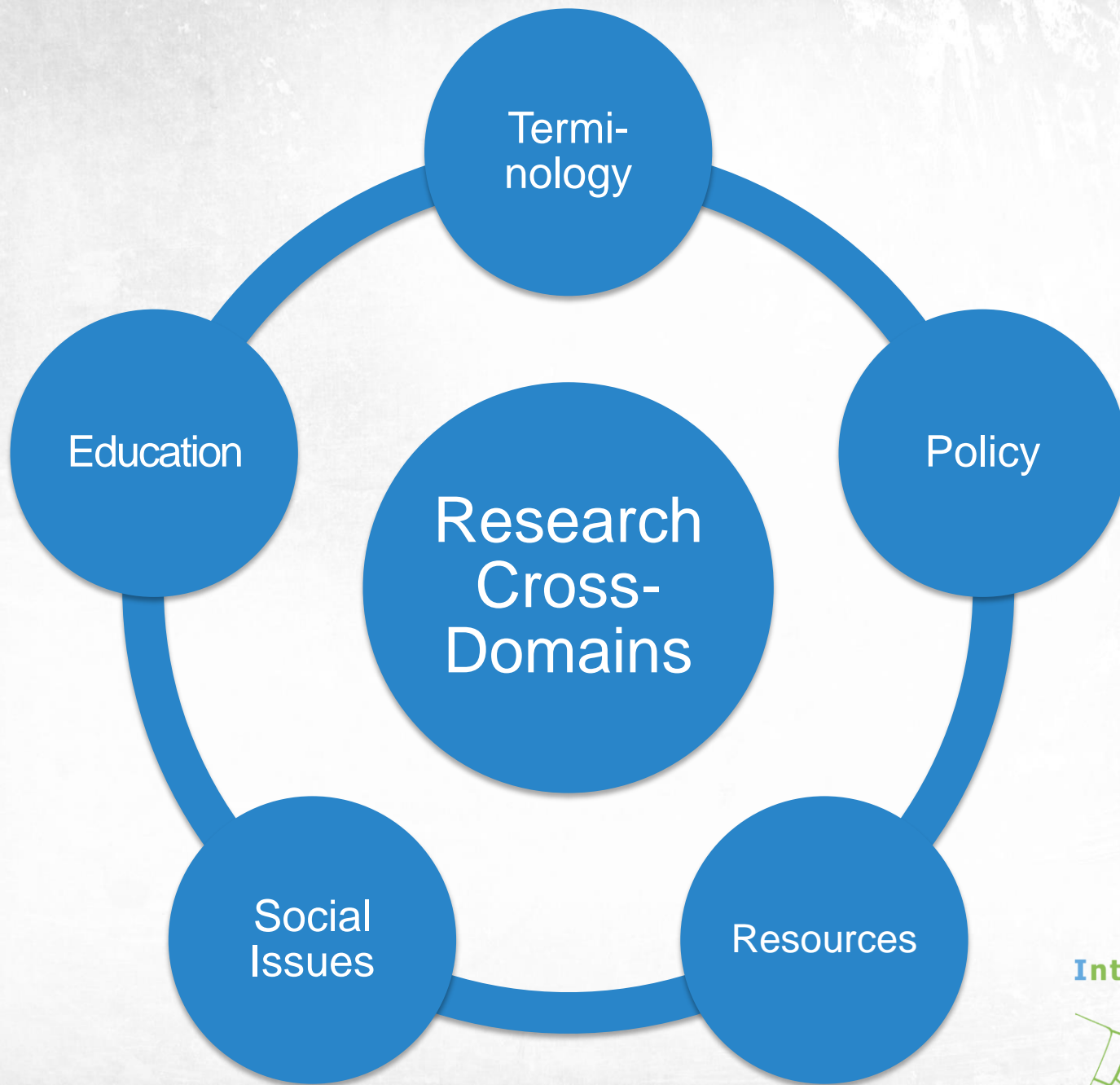
The storage of the material can be in the provider's data centers, but does not need to be in a given institution, as long as the institution is the **place where preservation services are controlled**

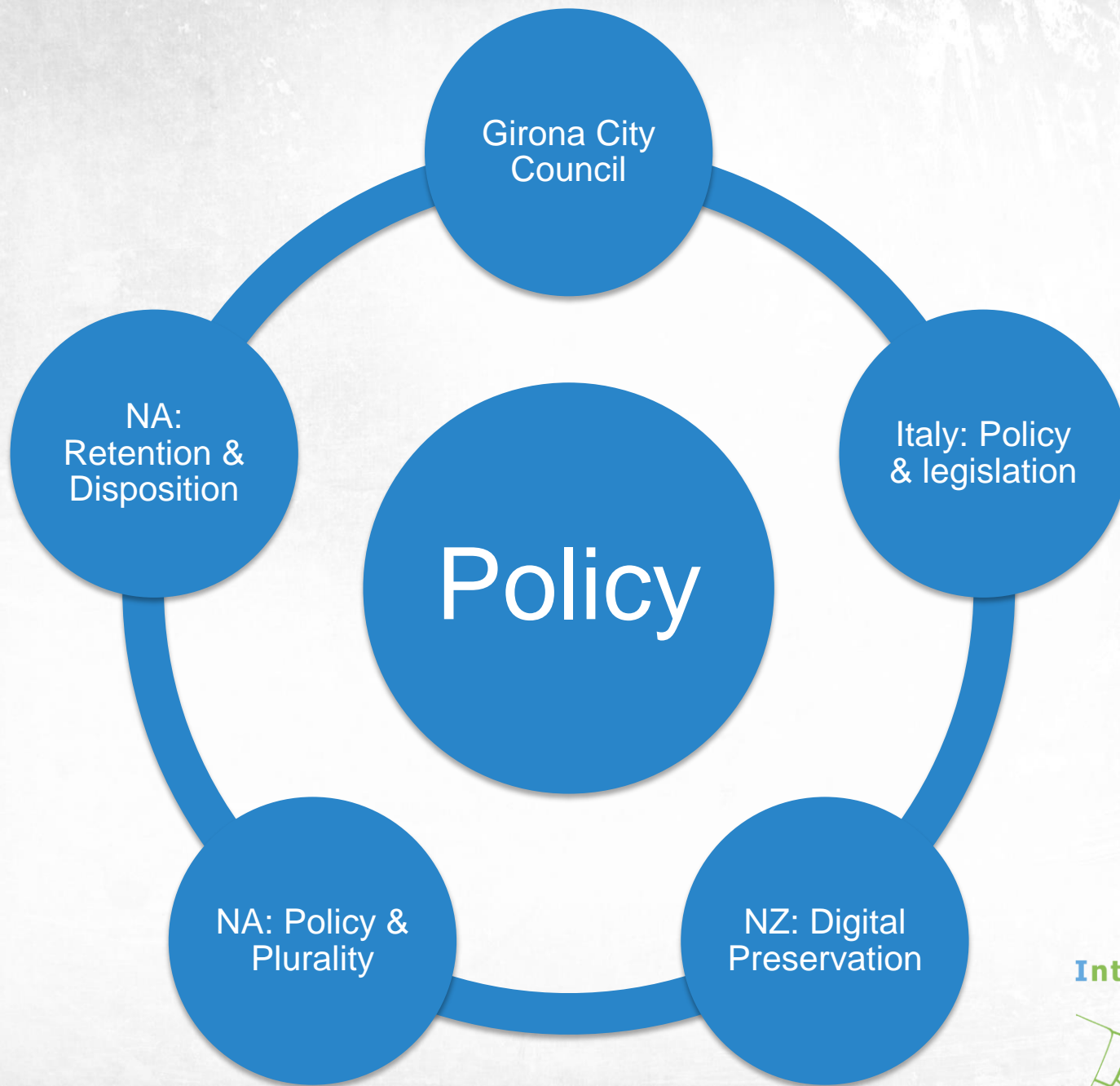
To develop a reference baseline InterPARES Trust is using UML (Unified Modeling Language) and working with the Object Management Group (OMG) detailing all the functional requirements that providers must respect.













Resources

- Literature reviews
 - Economic models (UK)
 - Open Government (UK)
 - Social media in government (NA)
 - Retention & Disposition (NA)
 - Gamification (NA)
 - HCI (NA)
 - PIM (NA)
- Reinventing business and operating models for trusted archival services (AA)

Resources & Education

- Ontology of functional activities for archival systems (TR)
- Reports (NA)
 - Notes on International Law
 - Trust in Law
 - Trust in Business
 - Trustworthy Smart Grid Infrastructures
- Review and update of Digital Records Pathways (AA)
- Curriculum Alignments at Institutions of Higher Learning in Africa (AF)

Dissemination

Research Dissemination is authored by InterPARES Trust researchers and research assistants. They will be listed below on an ongoing basis.

Search

by Author:

by Text in Citation:

Publications

[\[12 \] Books \(Including Chapters\)](#)

[\[30 \] Articles - Refereed](#)

[\[6 \] Articles - Non-Refereed](#)

[\[19 \] Conference Proceedings - Refereed](#)

[\[0 \] Conference Proceedings - Non-Refereed](#)

[\[37 \] InterPARES Trust Research Documents](#)

[\[5 \] Theses](#)

Presentations

[\[51 \] Lectures, Workshops, and Seminars](#)

[\[147 \] Conferences \(Symposia, Sessions, Panels, Papers\)](#)

Public Relations

[\[16 \] Articles and Reviews](#)

[\[6 \] Broadcast Interviews](#)

[\[4 \] Reports](#)

[\[2 \] Sponsorships](#)

[\[1 \] Videos](#)



www.interparestrust.org

www.interpares.org

www.ciscra.org

luciana.duranti@ubc.ca

InterPARES
Trust

