A Meta Model for Trust Frameworks
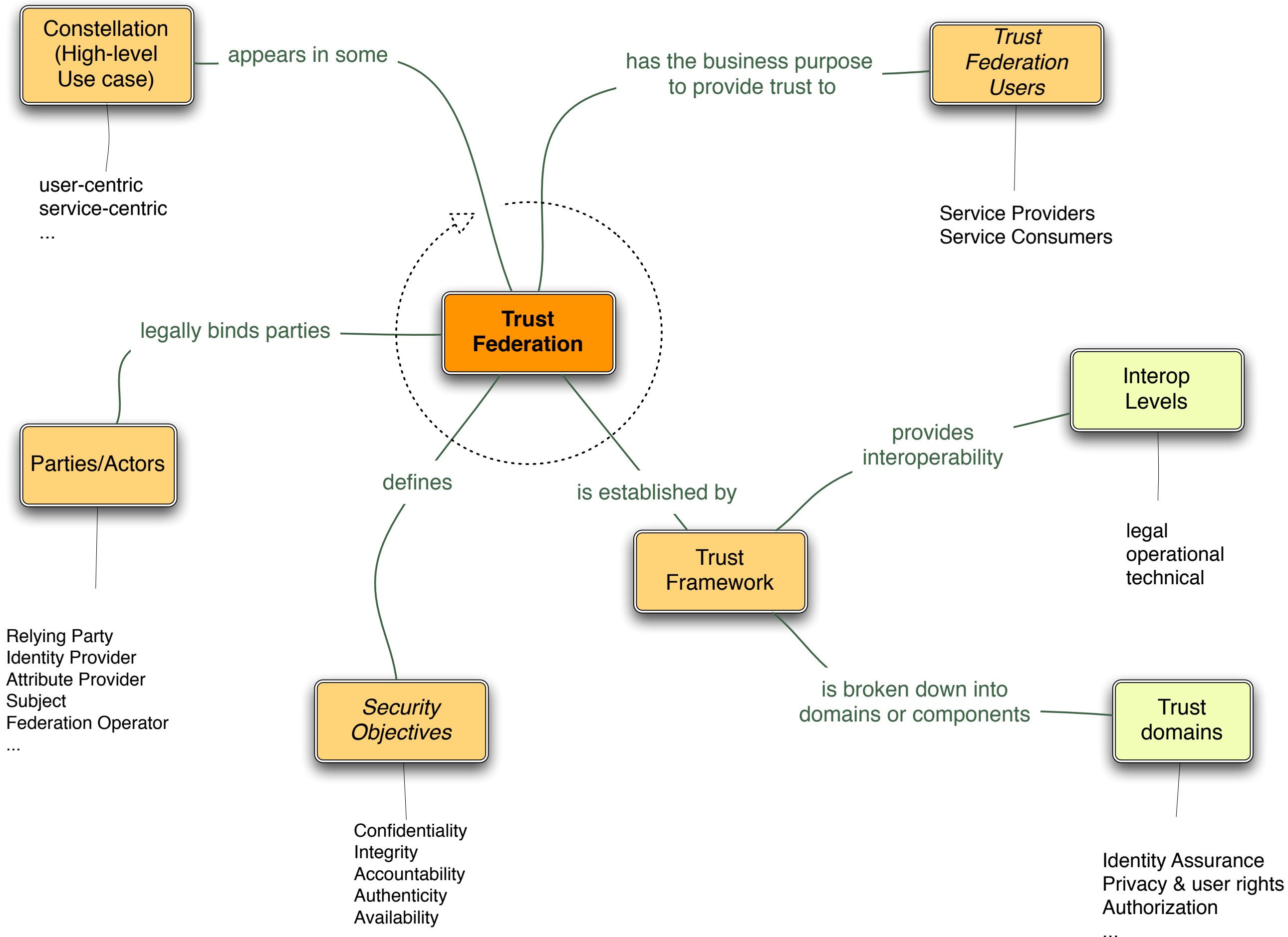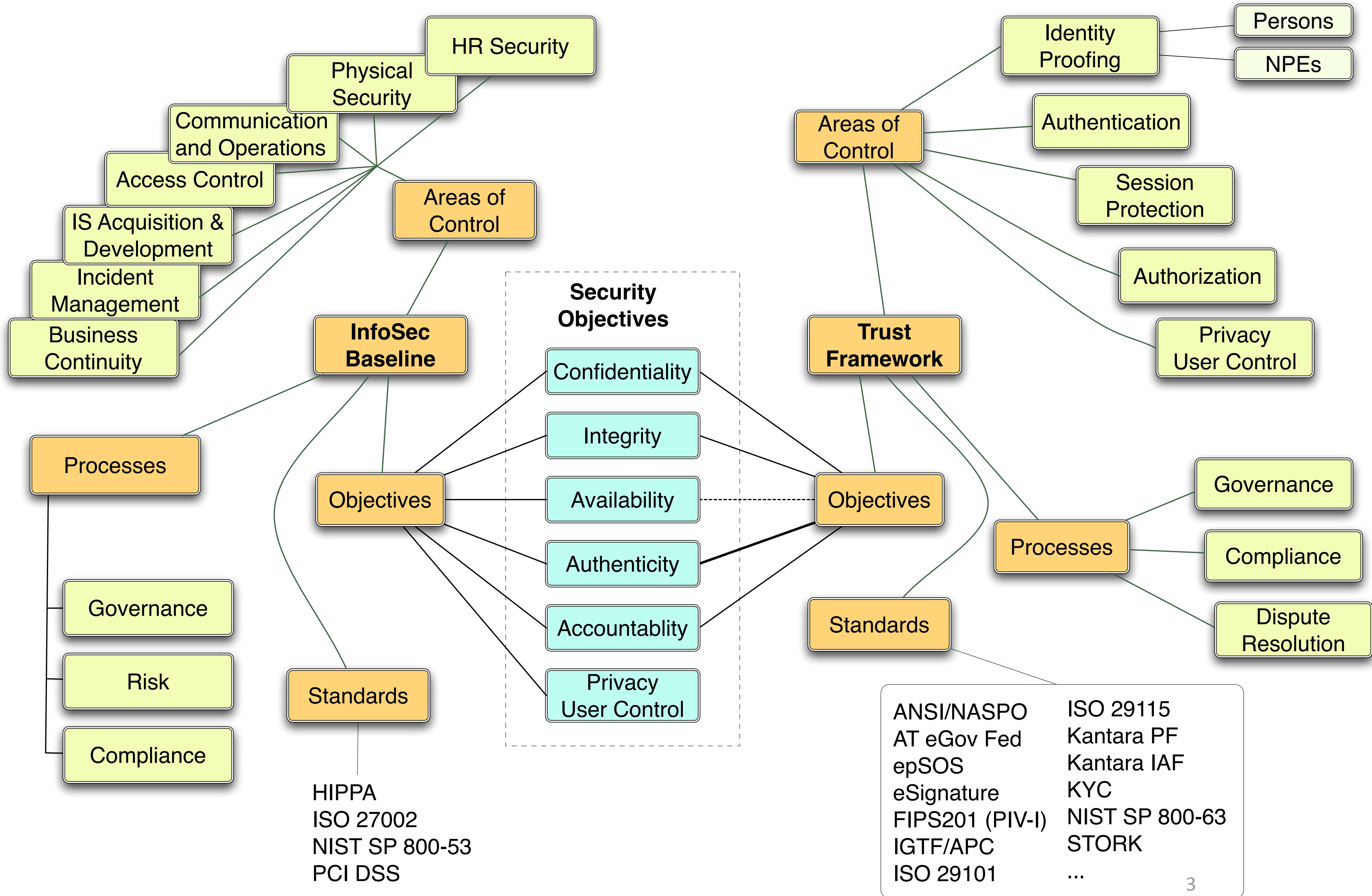
Rainer Hörbe, 28-March-2011

What is a Trust Federation?

Constellation (High-level Use case)
- user-centric
- service-centric
- ...

appears in some

has the business purpose to provide trust to

Trust Federation Users
- Service Providers
- Service Consumers

Trust Federation

legally binds parties

Parties/Actors
- Relying Party
- Identity Provider
- Attribute Provider
- Subject
- Federation Operator
- ...

defines

Security Objectives
- Confidentiality
- Integrity
- Accountability
- Authenticity
- Availability

is established by

Trust Framework

provides interoperability

Interop Levels
- legal
- operational
- technical

is broken down into domains or components

Trust domains
- Identity Assurance
- Privacy & user rights
- Authorization
- ...

HR Security

Physical Security

Communication and Operations

Access Control

IS Acquisition & Development

Incident Management

Business Continuity

Areas of Control

InfoSec Baseline

Objectives

Standards

Processes

Governance

Risk

Compliance

Security Objectives

Confidentiality

Integrity

Availability

Authenticity

Accountablity

Privacy User Control

Trust Framework

Objectives

Standards

Areas of Control

Identity Proofing

Persons

NPEs

Authentication

Session Protection

Authorization

Privacy User Control

Processes

Governance

Compliance

Dispute Resolution

HIPPA
ISO 27002
NIST SP 800-53
PCI DSS

ANSI/NASPO
AT eGov Fed
epSOS
eSignature
FIPS201 (PIV-I)
IGTF/APC
ISO 29101

ISO 29115
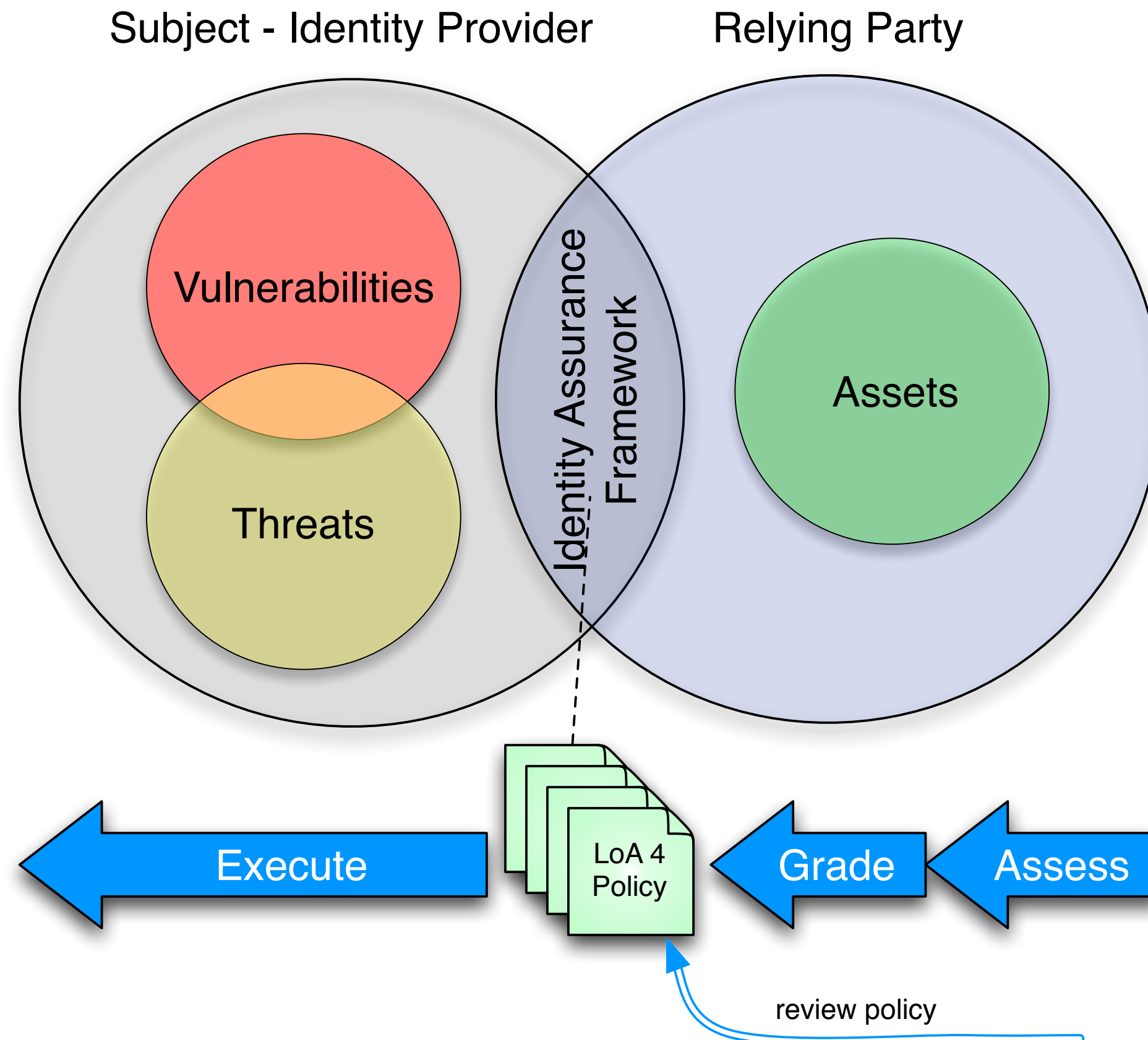Kantara PF
Kantara IAF
KYC
NIST SP 800-63
STORK
...

3

Trust Framework Capabilities

	Identity	AuthN	Session	AuthZ	Account-ability	Privacy	User Control
ANSI/NASPO	Individuals						
AT eGov Fed	all	X	X	X	X		
epSOS				X	X	X	
eSignature	Individuals	X					
FIPS201 (PIV-I)	Individuals	X					
IGTF/APC	NPE	X					
ISO 29101	Individuals	X					
ISO 29115	all						
Kanrara PF						X	X
Kantara IAF	Individuals				X		
KYC	all				X		
NIST SP 800-63	Individuals	X					
STORK	Individuals	X					

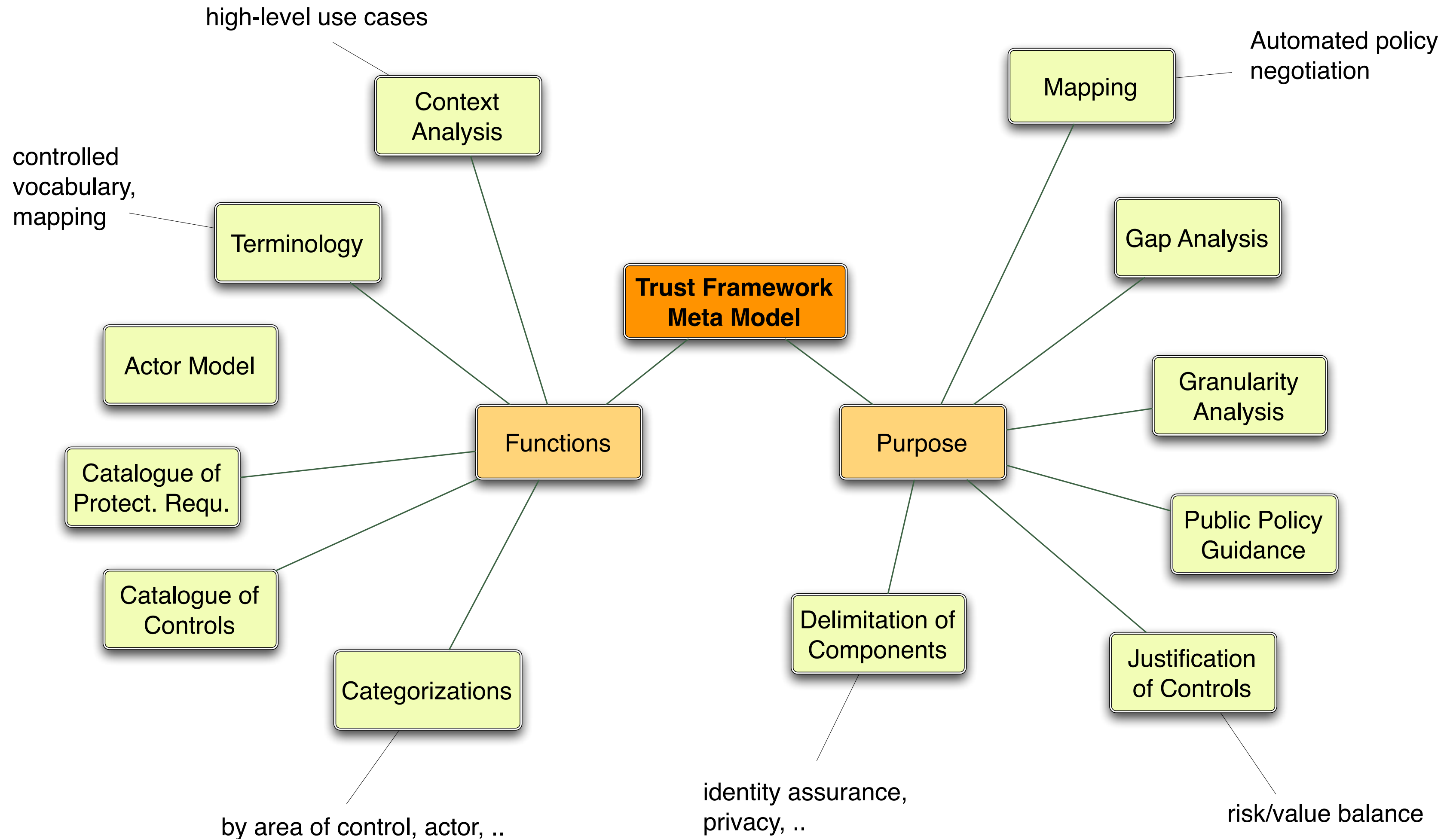**Risk management: Enterprise View**
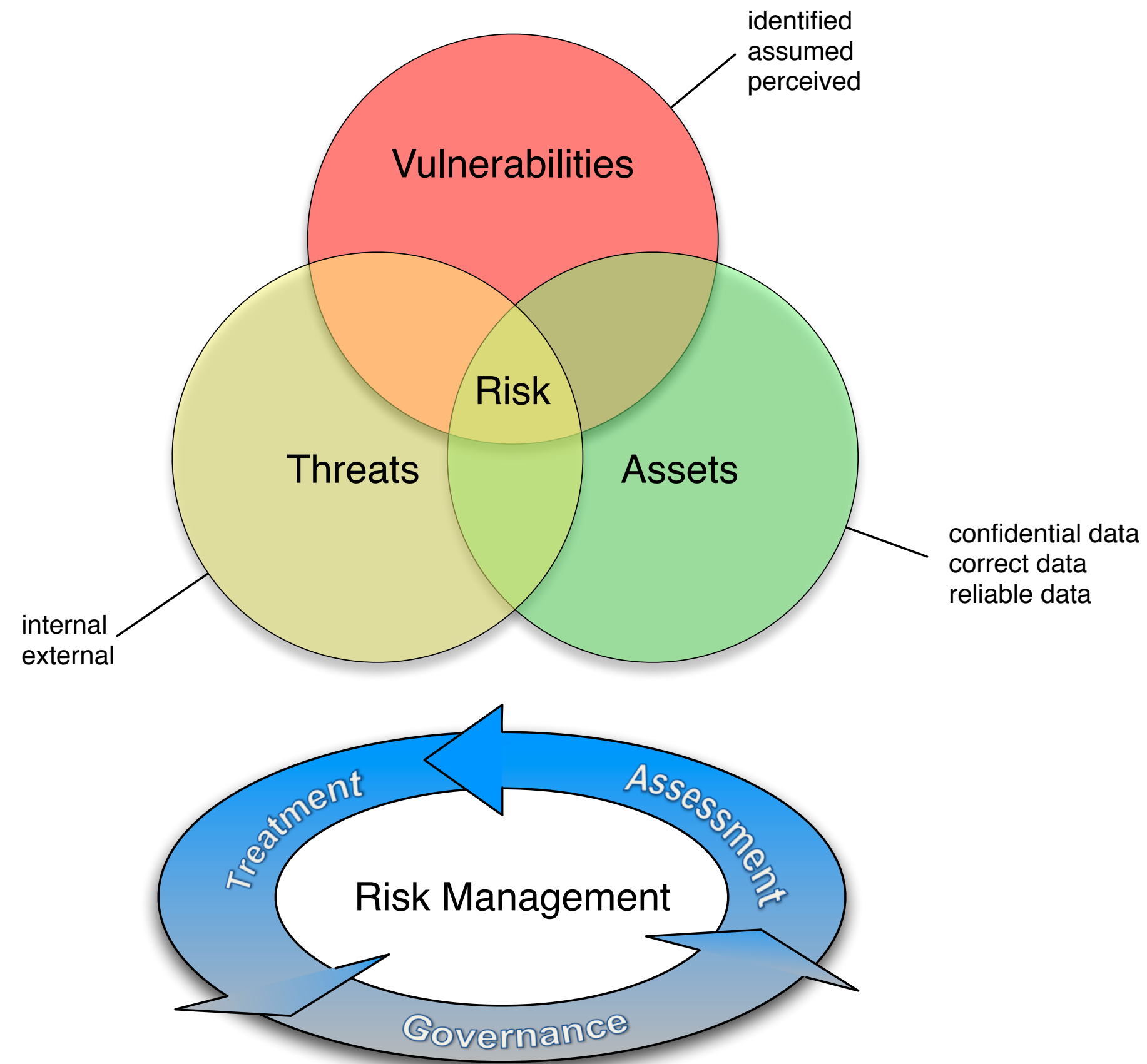
Risk management in enterprises the risk as cross section of assets, vulnerabilities and threats is determined and mitigated by safeguards and other methods. Service providers and consumers are part of the organization. IT Security is managed by handling IT-related risk. Policies can be managed and enforced centrally.

Risk management: Federation with SP-centric view

Subject - Identity Provider

Relying Party

Vulnerabilities

Threats

Identity Assurance Framework

Assets

Execute
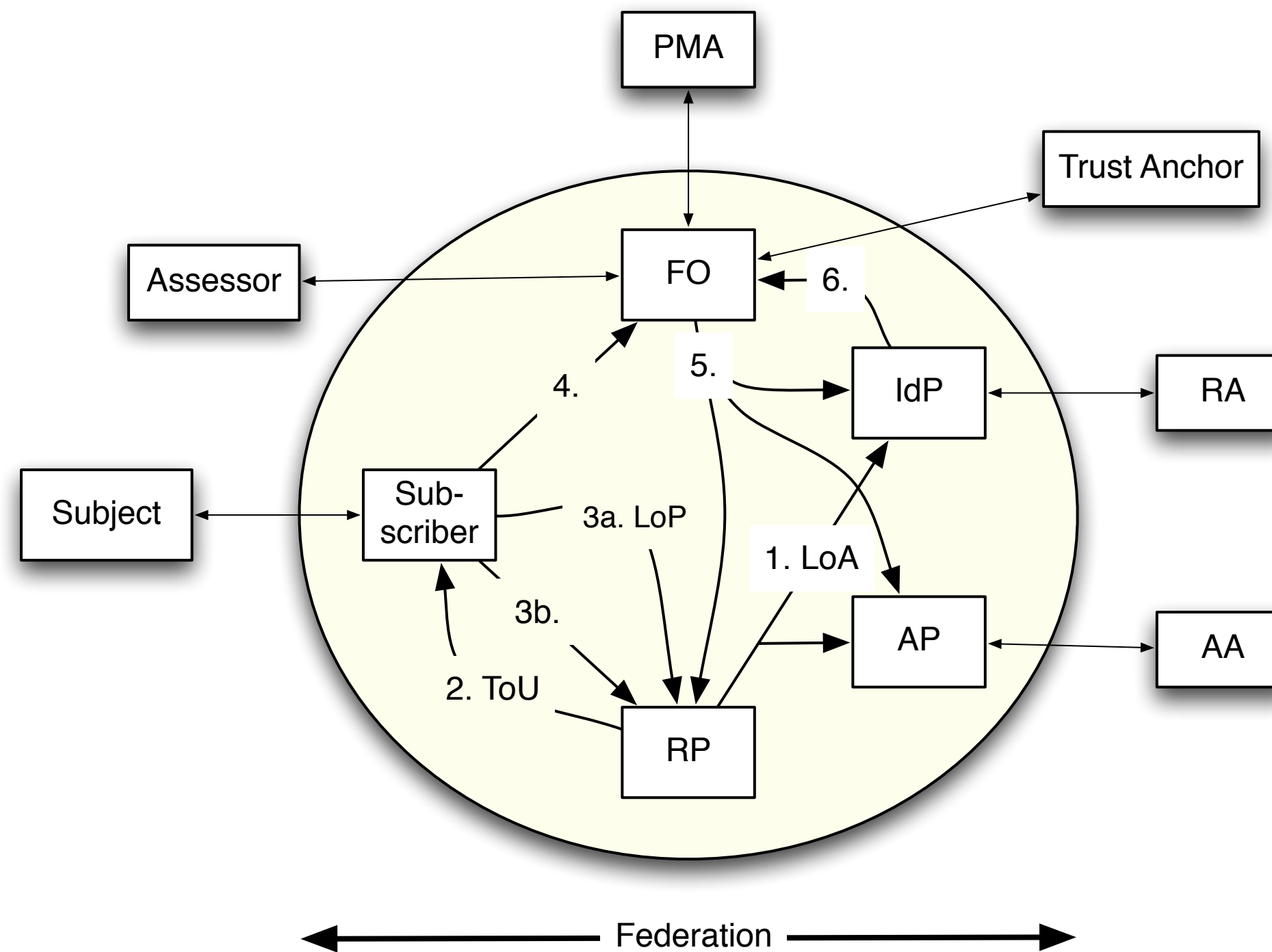
LoA 4 Policy

Grade

Assess

review policy

Risk management across enterprises disrupts the risk management process as known from enterprise risk management. Assets cannot be related to threats, mitigating vulnerabilities by safeguards to adjust risk to an acceptable level is and other methods. As autonomous actors handle their risk at a time, there is no common process for risk management. To resolve the issue, Trust Frameworks provide a baseline security policy, frequently with several assurance levels, to map the complexity of vulnerabilities and threats to a defined set of controls (or assurance criteria).

Meta Model: A basis to assess Trust Frameworks

high-level use cases

Automated policy negotiation

Context Analysis

controlled vocabulary, mapping

Mapping

Terminology

Gap Analysis

Actor Model

Trust Framework Meta Model

Functions

Purpose

Granularity Analysis

Catalogue of Protect. Requ.

Public Policy Guidance

Catalogue of Controls

Justification of Controls

Categorizations

Delimitation of Components

identity assurance, privacy, ..

risk/value balance

by area of control, actor, ..

7

Trust Relationships
Actor Model

1. Level of Assurance
2. Terms of Use
3a. Level of privacy
3b. Client device protection
4. Manage provider policy
5. Provider policy
6. Trust anchor

The previous federation models with three actors fit nicely into Venn diagrams, but many federation constellations have more actors. This diagram includes Attribute Providers (AP), a Federation Operator (FO), Registration Authority (RA), Attribute Authority (AA) and a Policy Management Authority (PMA).

The key objective of a Trust Federation is to support all these relationships.