Recording In Progress

DESIGN ASSURANCE STANDARD v1.0 OFFICIAL LAUNCH

Institute of Operational Privacy Design

MARCH 19, 2025 @ 1:00 PM (EDT)

AGENDA

1. Introduction to the IOPD
2. Purpose of the Standard
3. Introduction to the Standard
   a. Assurance Case
   b. Major Claims
   c. Risk Model
   d. Quick Start Guide
   e. Perspective in Scoping
   f. Controls
4. Future Work and How to Get Involved

Meant to be an introduction and overview, not a training session.

INTRODUCTION TO THE
Institute of Operational Privacy Design

IOPD

Incorporated 2021

Non-Profit 501c(6)

Organization

Professional Membership

Board of Directors

Standards Committee

Ad-Hoc Committees

Mission

To promote the adoption of common, free, and comprehensive standards committed to protecting individuals' privacy.

INTRODUCTION TO THE
Standards Committee of the IOPD

Chair
Nandita Narla

Organization
~20 Members

2025 Mission
Controls Catalog

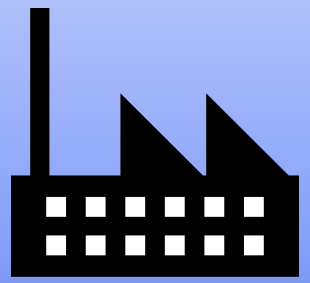
Data Protection by Design

Review Design Process Standard

PURPOSE OF THE STANDARD

Professionals

Improve privacy



Companies

External validation of “privacy by design” claims

Implementers & Auditors

Support their clients

Regulators

Review claims of “privacy by design”

Benefits of using the Standard

Improve Privacy Program

Looking at privacy from a different perspective can improve the overall health of an organization's privacy program.

Prepare for Certification

For organizations wanting to eventually get certified, starting now will give you a head start against competitors.

Remove Sales Blockages

Failure to provide adequate assurance on privacy can impede B2B sales.

Validate Marketing Claims

Claiming "Privacy by Design" without substantive backing can open up an organization to deceptive trade practices.

Holistic Regulatory Approach

Compliance can be tricky. Applying a privacy by design can cover 80% of regulatory obligations in 80% of jurisdictions and future proof products.

Improve Products and Trust

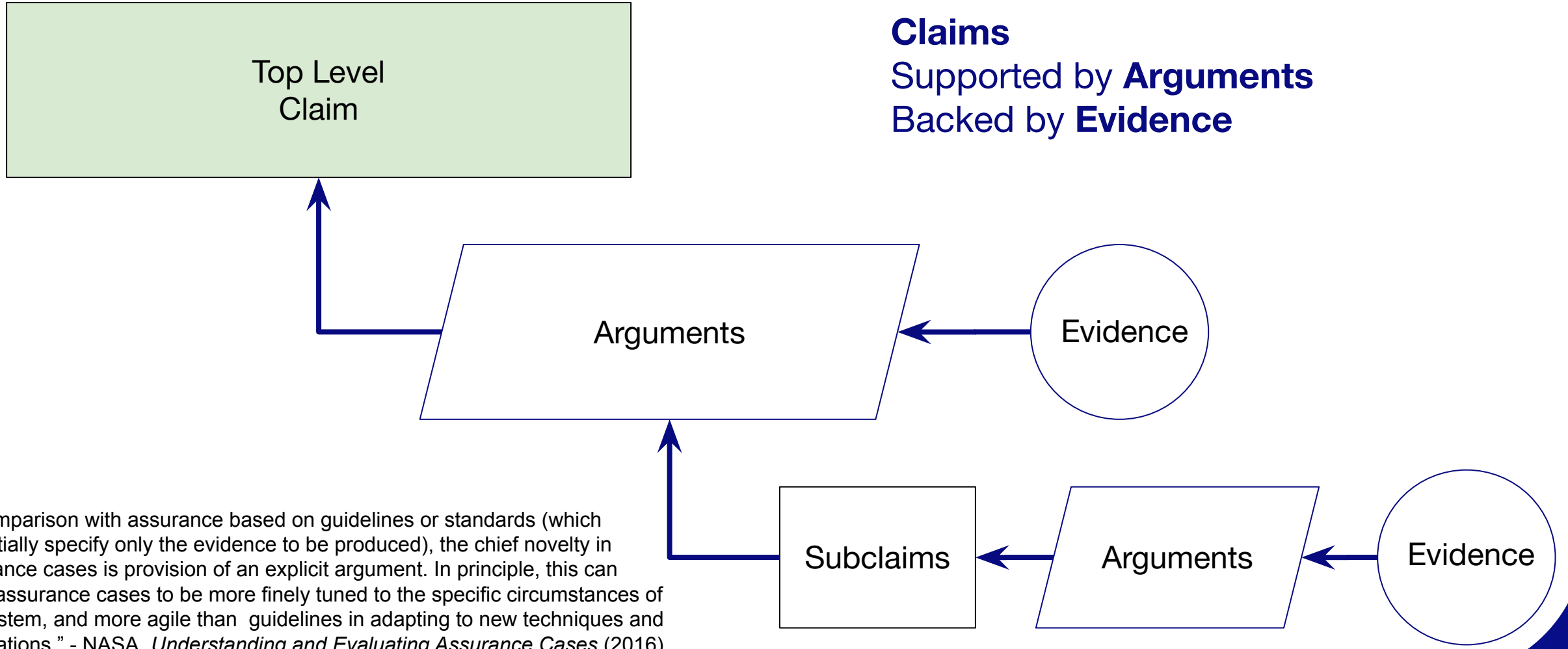
Studies show consumers want privacy and will have more favorable impression of brands that protect their privacy.

Design Assurance Standard

- Version 1.0
- Adopted March 1st, 2025
- Covers products, services and business processes

- Not a guarantee of privacy but reasonable **assurance**

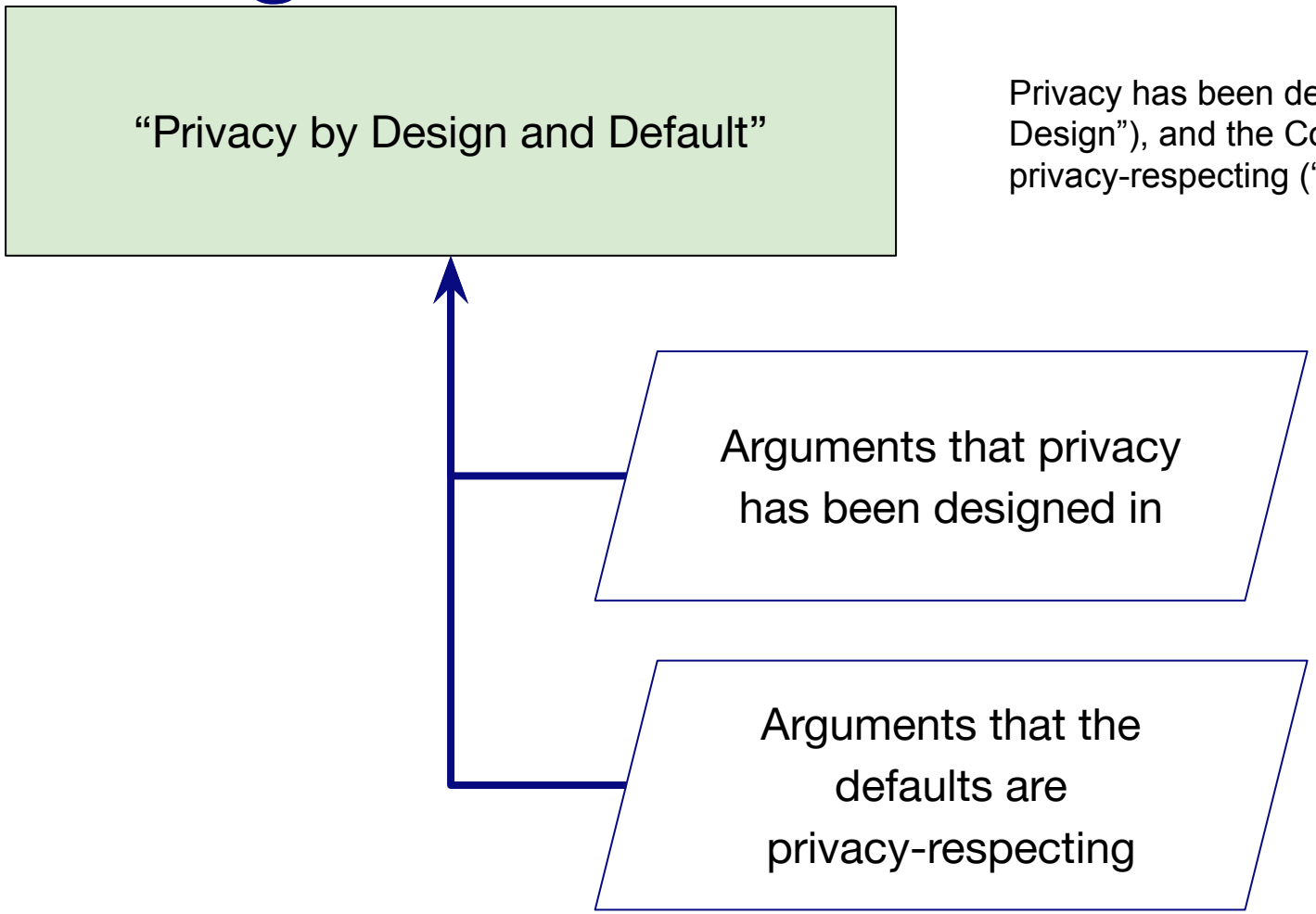
Assurance Case



Claims
Supported by **Arguments**
Backed by **Evidence**

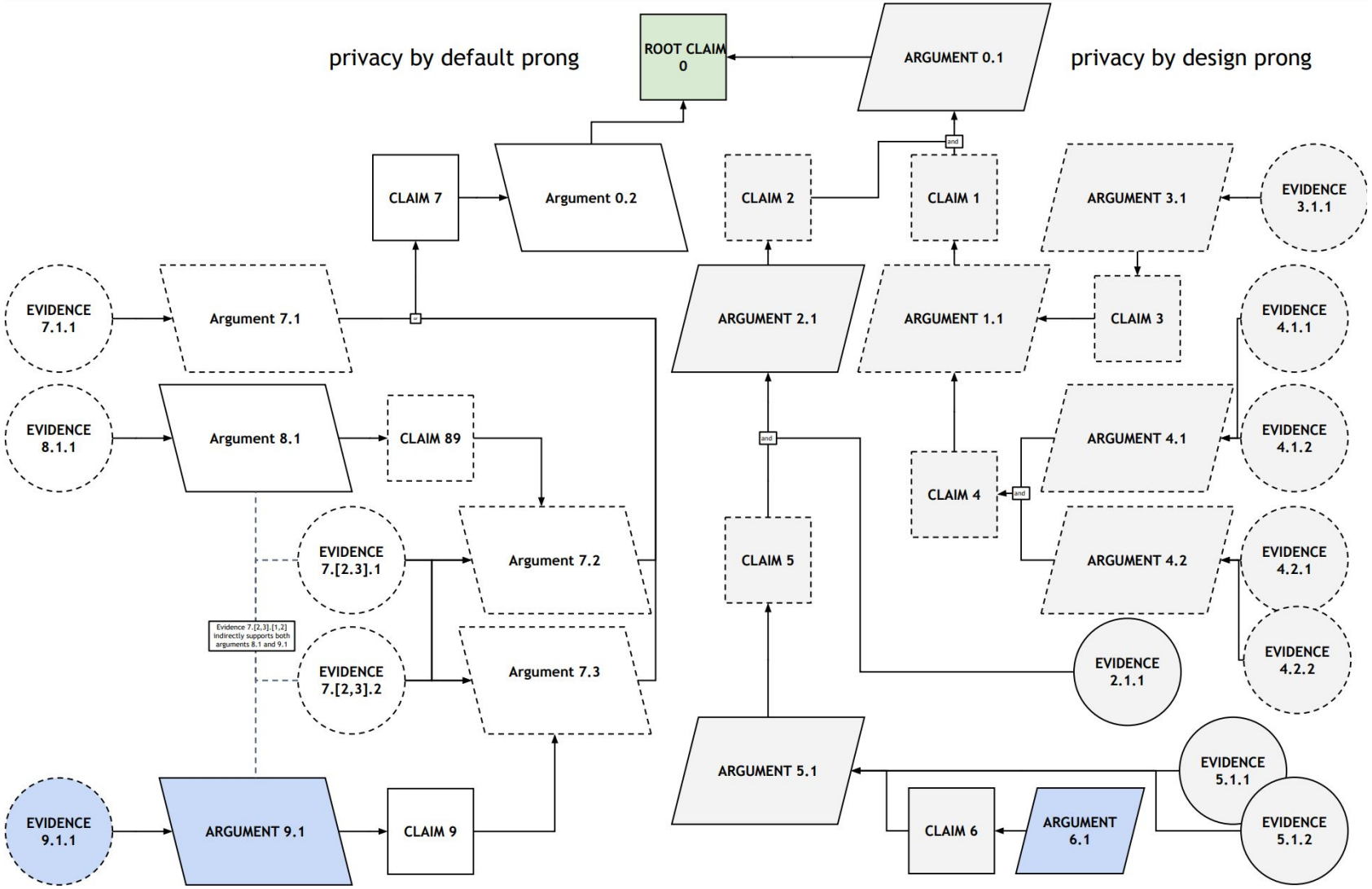
"In comparison with assurance based on guidelines or standards (which essentially specify only the evidence to be produced), the chief novelty in assurance cases is provision of an explicit argument. In principle, this can allow assurance cases to be more finely tuned to the specific circumstances of the system, and more agile than guidelines in adapting to new techniques and applications." - NASA, *Understanding and Evaluating Assurance Cases* (2016)

Design Assurance Standard



Privacy has been designed into the Target System (“Privacy by Design”), and the Configuration(s) of the Target System are privacy-respecting (“Privacy by Default”).

Design Assurance Standard (10 Claims)



Claims

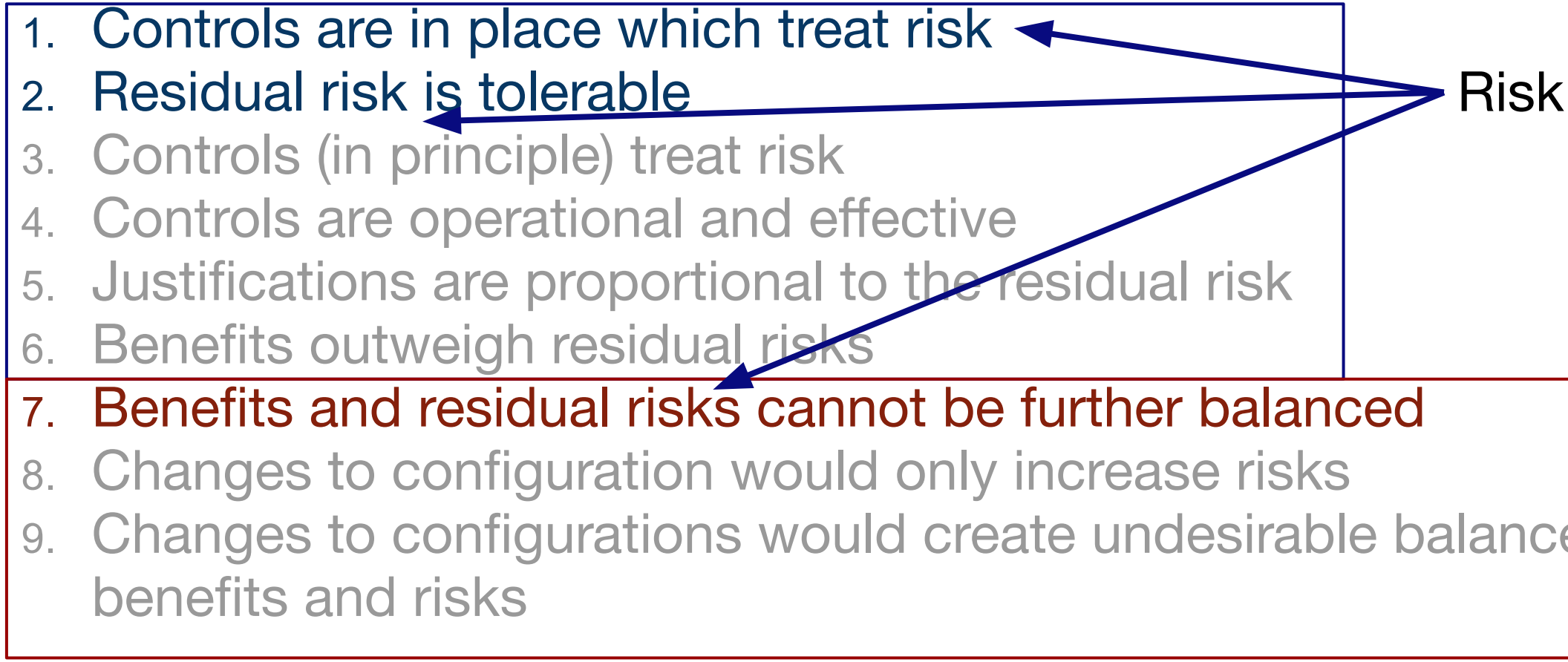
0. Privacy by design and default
1. Controls are in place which treat risk
2. Residual risk is tolerable
3. Controls (in principle) treat risk
4. Controls are operational and effective
5. Justifications are proportional to the residual risk
6. Benefits outweigh residual risks
7. Benefits and residual risks cannot be further balanced
8. Changes to configuration would only increase risks
9. Changes to configurations would create undesirable balance of benefits and risks

Claims

0. **Privacy by design** and default
1. Controls are in place which treat risk
2. Residual risk is tolerable
3. Controls (in principle) treat risk
4. Controls are operational and effective
5. Justifications are proportional to the residual risk
6. Benefits outweigh residual risks
7. Benefits and residual risks cannot be further balanced
8. Changes to configuration would only increase risks
9. Changes to configurations would create undesirable balance of benefits and risks

Claims

0. **Privacy by design** and **Privacy by default**
1. Controls are in place which treat risk
2. Residual risk is tolerable
3. Controls (in principle) treat risk
4. Controls are operational and effective
5. Justifications are proportional to the residual risk
6. Benefits outweigh residual risks
7. Benefits and residual risks cannot be further balanced
8. Changes to configuration would only increase risks
9. Changes to configurations would create undesirable balance of benefits and risks



Risk Model

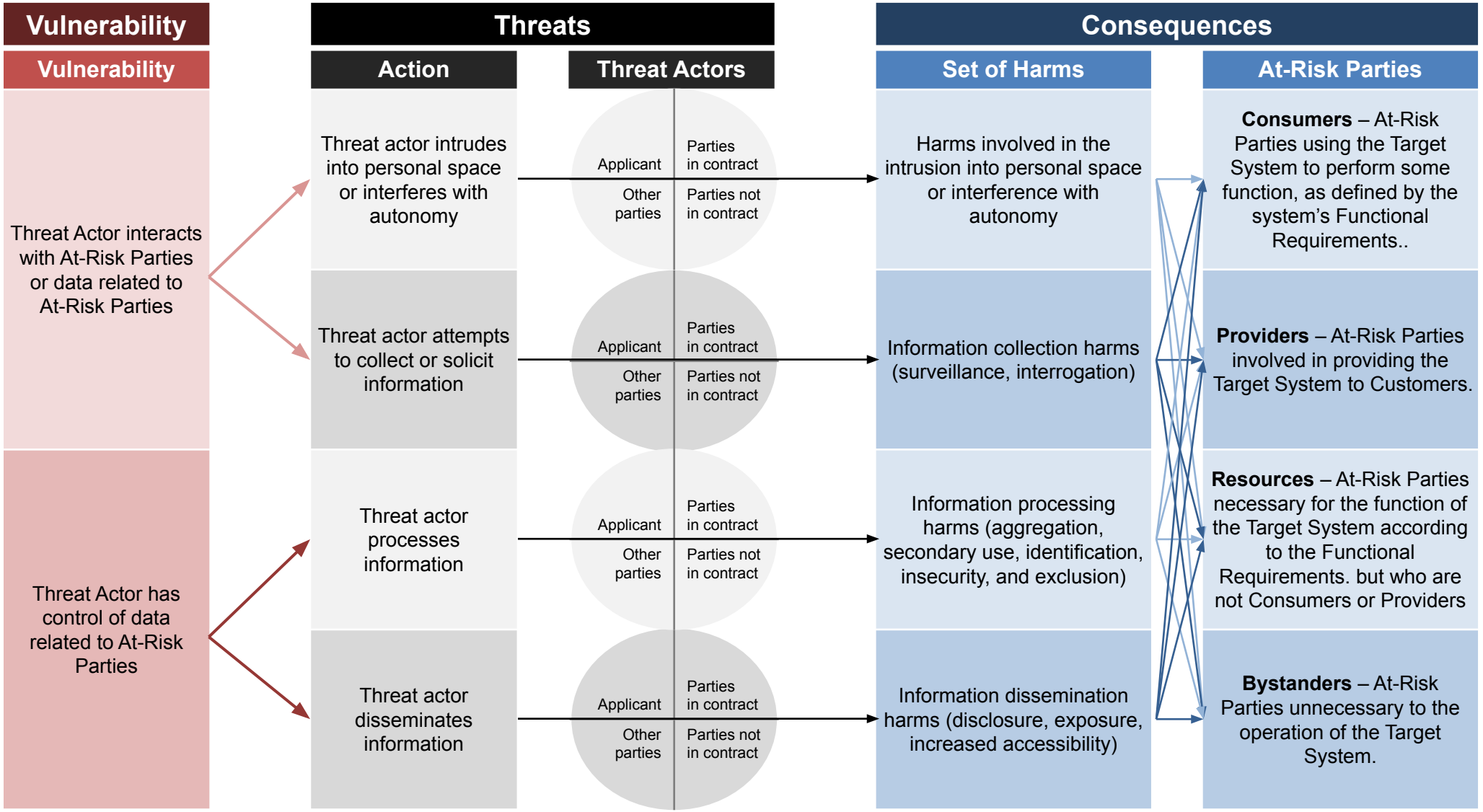
Threat Actors
Applicant
Parties in Contract
Parties Not in Contract
Others

At-Risk Parties
Consumers
Providers
Resources
Bystanders

Privacy Harms
Intrusion
Information Collection
Information Processing
Information Dissemination

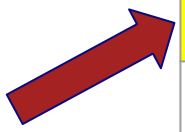
What can threat actors do to at-risk parties resulting in privacy harms?

Risk Model

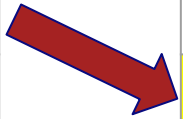

Vulnerability
Vulnerability
Threat Actor interacts with At-Risk Parties or data related to At-Risk Parties
Threat Actor has control of data related to At-Risk Parties
Threats
Action
Threat Actors
Threat actor intrudes into personal space or interferes with autonomy
Threat actor attempts to collect or solicit information
Threat actor processes information
Threat actor disseminates information
Applicant
Other parties
Parties in contract
Parties not in contract
Consequences
Set of Harms
At-Risk Parties
Harms involved in the intrusion into personal space or interference with autonomy
Information collection harms (surveillance, interrogation)
Information processing harms (aggregation, secondary use, identification, insecurity, and exclusion)
Information dissemination harms (disclosure, exposure, increased accessibility)
Consumers – At-Risk Parties using the Target System to perform some function, as defined by the system's Functional Requirements..
Providers – At-Risk Parties involved in providing the Target System to Customers.
Resources – At-Risk Parties necessary for the function of the Target System according to the Functional Requirements. but who are not Consumers or Providers
Bystanders – At-Risk Parties unnecessary to the operation of the Target System.

Risk Model

Threat Actors
Applicant
Parties in Contract
Parties Not in Contract
Others



At-Risk Parties
Consumers
Providers
Resources
Bystanders



Privacy Harms
Intrusion
Information Collection
Information Processing
Information Dissemination

64 Potential Risks

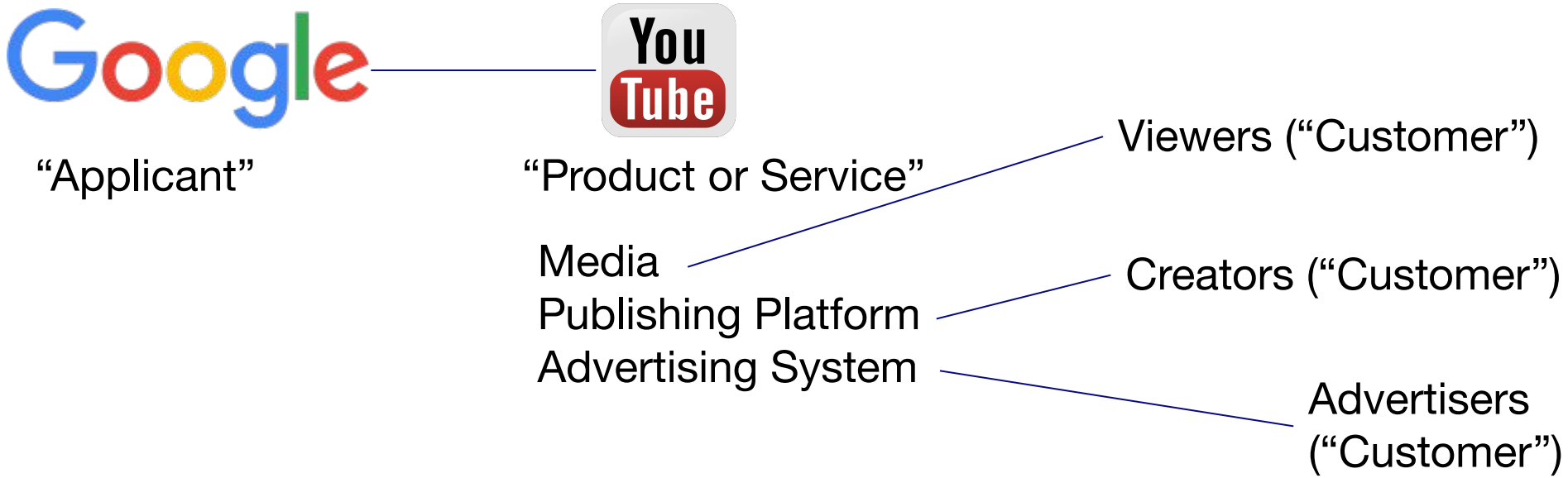
What information do parties in contract attempt to collect about consumers?

Quick Start Guide

Scoping	Target System	Controls	Residual Risk	Configurations
Identify the Applicant	Identify the product or service requirements	Specify how controls reduce risk	Justify residual risk	Documents configurations
Specify the product or service	Identify interactions	Show control verification process	Identify benefits	Show changes would increase risks or be undesirable
Specify the customers	Show interactions are necessary for the product or service	Show that controls were verified	Assure that benefits outweigh risks	
Select the risks		Show how to measure effectiveness of controls		
		Show controls are effective		

Importance of Perspective in Scoping

Scoping
Identify the Applicant
Specify the product or service
Specify the customers
Select the risks



3 Different Services with distinct risks

Importance of Perspective in Scoping

Scoping
Identify the Applicant
Specify the product or service
Specify the customers
Select the risks

Google

"Party in contract"

Media

Viewers ("Customer")

Creators ("Applicant")

Advertisers ("Parties not in contract")

Different Service = Different Risks

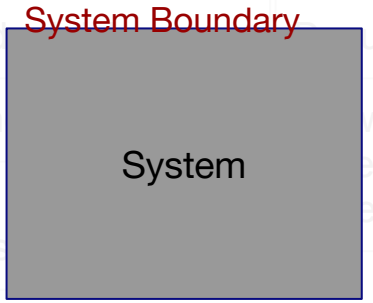
Quick Start Guide

Scoping	Target System	Controls	Residual Risk	Configurations
Identify the Applicant	Identify the product or service requirements	Specify how controls reduce risk	Justify residual risk	Document configurations
Specify the product or service	Identify interactions	Show control verification process	Identify benefits	Show changes would increase risks or be undesirable
Specify the customers	Show interactions are necessary for the product or service	Show that controls were verified	Assure that benefits outweigh risks	
Select the risks		Show how to measure effectiveness of controls		
		Show controls are effective		

System versus Environmental Controls

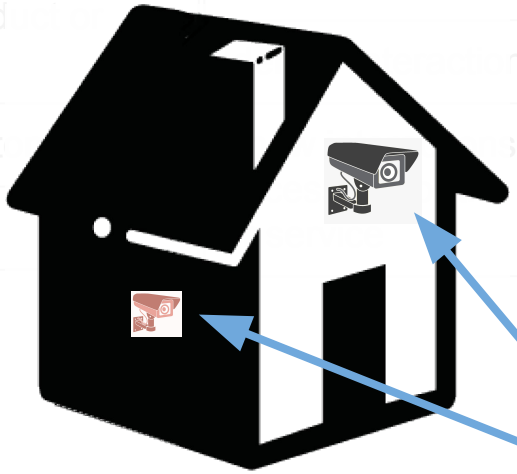
Common Control Divisions
Administrative, Technical & Physical
Technical & Organizational
Preventative, Detective and Corrective

Controls
Specify how controls reduce risk
Show control verification process
Show that controls were verified
Show how to measure effectiveness of controls
Show controls are effective



System versus Environmental Controls

Environment



Outside house or
Inside house?

System Boundary

System

NEXT STEPS

CURRENT WORK

Standards Committee

Controls Catalog

Article 42 Committee

Data Protection by Design and Default

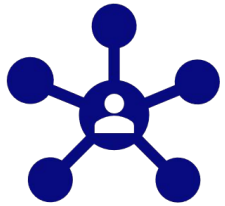
EU Certification

ISO/IEC DIS 17007

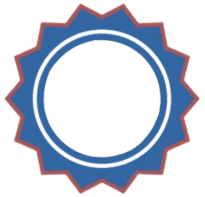
Conformity Assessment

CALL TO ACTION!

Review the Standard



Join the IOPD



Apply the Standard to your product or service

Open Volunteer Roles

Open to members and select* non-members

- Board of Directors - Treasurer
- Privacy Wiki Editors
- Standards Committee
  - Control experience
- Article 42 Committee
  - EU Regulatory Subject Matter Expertise

* Non-members, except Privacy Wiki Editors, must be approved by the Leadership Team

Thank You

Contact: admin22@instituteofprivacydesign.org

QUESTIONS?