# 0PN Decentralized Gov Framework

Trustworthy ID Architecture

The presentation of the 0PN[[1]](#endnote-2) System Architecture touches on all topics but first requires a description of governance and risk vectors, before introducing, the 0PN: eNotary, trustworthy ID eNotice system architecture, to address the governance and risk vectors highlighted with electronic consent. Addressed here from the human centric data control perspective on the premise that trustworthy ID is asserted with records the individual controls. Rather than records that are controlled for me by Controllers and Processors.

# Part 1: Governance & Risk (Data Control Assurance Framework)

In governance and risk discourse, research and legal instrument modelling, we identified that a fundamental vector of governance, personal data control, has been largely missing. As a result, the architecture presented prioritizes the human control vector of personal data control interoperability, then applies a privacy risk and security assurance model in accordance with security assurance requirements of this vector.

There are 3 vectors of digital identity governance with different privacy risks and security measures for trustworthy digital identifier management; each of those vectors has 3 tiers of digital identifier risk assurance

## 3 Vectors of Governance Risk

1. Personal Data Control: a reduced risk vector as data control and transparency is managed by the individual, and is indicative of decentralized digital identity transparency.

2. Co-Regulated Data Control – shared transparency and data control, identifier’s are distributed.

3. Data Protection – defined in regulation typically a centralized data control model with federated identity management system

## 3 Tiers of Risk Assurance

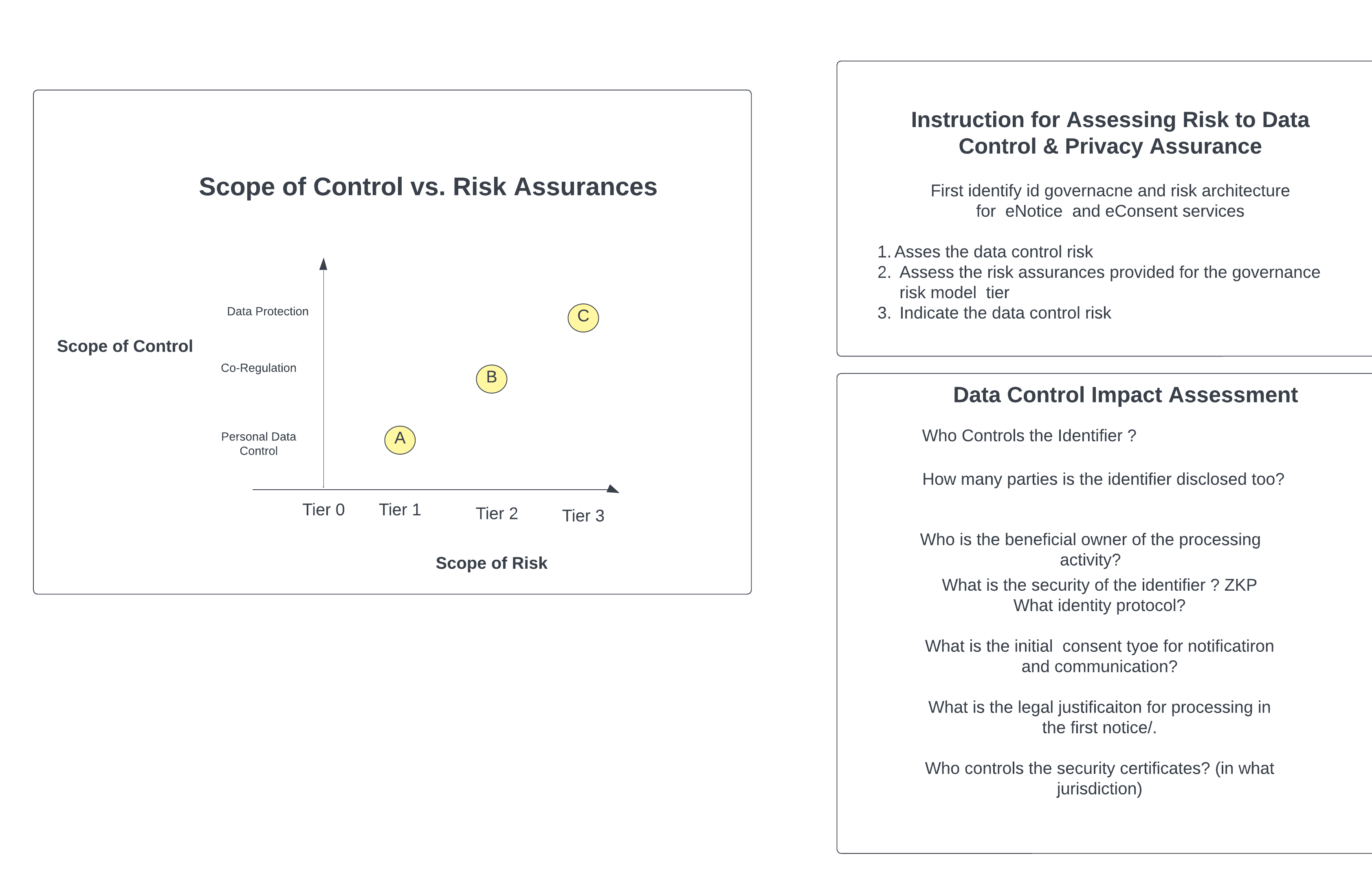
Each vector of the data control governance vectors has 3 tiers of digital identifier risk assurance

1.Self‑Asserted Assurance - Controller Credential usable for hyper‑ localized, - in‑ person privacy risk assessment and can be asserted by the individual (PII Principal)

2. Legal Assurance – a Data Controller Credential consists of a verified data controller and data protection officer, or company director, where privacy and security is enforced, and the controller credential is monitored by a in publicly accessible and standardized ledger.

3. Operationally Assured Controller Credential — Operator of a personal data control (eConsent) code of practice, which in addition to tier 2, is provided through certification and additional monitoring by a recognized provider/regulator for a specific set of data control and management practices.

The identifier vector and tiers can be determined by conducting a Data Control Impact Assessment, which entails the assessment of who controls a digital identifier, who is the beneficial owner of the data processing, how many parties the identifier is disclosed to, and what is the security/transparency when disclosed. The assessment can then identify the governance vector, level of assurance and the subsequent scope of data control based privacy risk for this trustworthy id system.



# Part 2: Trustworthy ID System Architecture (For A Consent Economy)

In this system architecture, trustworthiness is defined (in terms and definitions) from international privacy standard’s[[2]](#endnote-3) specifying the relative stakeholders.

This architecture defines how to wrap identifiers in electronic Notice records (micro-credentials) and to exchange identifiers in eConsent receipts.

This architecture is enabled by creating a Data Controller Credential (from public information in an international standard ISO/IEC record format[[3]](#endnote-4)), which is created by binding the organization identity with the organizations ‘accountable person’ into standardized record format. This architecture provides data controls that are governed by privacy laws and implemented with standards, not by (organizationally-imposed) contractual terms and conditions[[4]](#endnote-5).

When the individual interacts with a standardized notice (called a two‑ factor notice), a record and receipt is generated, thus producing proof of notice/knowledge record from this standardized controller credential. The eConsent receipt is generated to mirror this record and provide digital evidence of consent.

The anchored trust record once signed is called a micro-credential when stored in a digital wallet. This anchored trust record that the individual owns and controls; empowers the individual with their own relationship record, their own cookie/record of identifiers, meta-data and source of providence. This record which the individual controls and trust, is what provides a person with digital transparency over who processes and control’s personal data, which is what makes trustworthy digital id trustworthy.

When an individual provides consent, the electronic consent receipt is exchanged in the form of a micro-consent token, granting consent for a specific purpose, within which the digital identifiers are encrypted inside the purpose ‑specific specified token. Any third party that uses the token to gain access/control of personal identifiers is logged, captured with a record of processing is made transparent with the standardized record format.

Operationalizing digital identifier control with contextual privacy rights access is how this architecture proposed to scale data controls independently (autonomously) from a service provider. Controls which are specified, utilizing machine readable privacy law with the W3C Data Privacy Vocabulary[[5]](#endnote-6), machine readable privacy law. Revealing the Key to trustworthy digital id, which is consistent semantic transparency over who can see, process and control personal data and knowing when this control changes.

Central to this architecture is the Controller Credential[[6]](#endnote-7) which is used to generate records and receipt with a 2fN. A third-party receipt notary also signs receipts and is required to operate for the public-benefit. The notary signs eNotice records and receipts to validate the information in micro-credentials on behalf of the individual in order to mint micro-consent receipt tokens with digital trust.

This architecture is founded on international (non-national) standards for data governance that make it possible to automate and decentralize transparency, for the transparency signal for this architecture called “Differential Transparency”. The privacy as excepted,[[7]](#endnote-8) transparency signal / UI. The differential transparency signal is generated by comparing consent receipts token’s to see changes in the active privacy state. The consent token captures that initial state of privacy/purpose and consent. The controller’s operational policy is independently monitored for changes to this state, in addition to any relevant code of practice.

The core benefits, some content and references for this architecture have been cut from this abstract and can be found @ https://github.com/GPR-NGO/0PN-Framework/blob/main/Trustworthy-id-architecture

1. Zero Public Network (0PN), Identity Trust Public Registry [↑](#endnote-ref-2)
2. ISO/IEC 29100 – Privacy Framework [↑](#endnote-ref-3)
3. ISO/IEC 27560 -Consent Receipt [↑](#endnote-ref-4)
4. The Biggest Lie & Meaningful Consent [↑](#endnote-ref-5)
5. W3C Data Privacy Vocabulary [↑](#endnote-ref-6)
6. Controller Credential – ToiP – Task force [↑](#endnote-ref-7)
7. Privacy as Expected Consent Gateway – NGI Funded project [↑](#endnote-ref-8)