Working progress – for discussion only

The future is open
Peppol

Peppol Security Requirements Design Work Group

Peppol Cross Community Conference

3-4 November 2022

Official

Context and objectives

Background

- Security measures are like an insurance
- Recent major security breaches include
  - Telstra, Optus, Medibank and Mydeal in Australia[1]
  - three VPN providers that were hacked in May 2022 where 21 million users' personal data was posted publicly[1]

In order to be trusted, we must **demonstrate** trustworthiness

Generally

Specifically

[1] *https://termly.io/resources/articles/biggest-data-breaches/#biggest-data-breaches-in-2022*

Background

- **Security is important (crucial)**
    - To manage risks and maintain confidence in the Peppol network
        - Risks – protect against attacks, threats, abuse
        - Confidence – Peppol’s credibility and reputation running trusted and safe network

Generally

- **Security required by new Service Provider (SP) Agreement**
    - SPs must comply with minimum security requirements set out in the Internal Regulations (IR) and/or Operational Procedures (OP).

Specifically

- Working Group (WG)
    - Objective
        - Develop a proposal for Peppol Security Requirements to ensure there is a **consistent**, **minimum** level of security across the Peppol network.
        - MC decision that **End Users are out-of-scope**
    - Outcomes / Deliverables
        - Propose Security Requirements
        - Lodge a Request for Change (RFC)
            - RFC will be managed by the Agreements, Policies, and Procedures Change Management Board (APPCMB) in accordance with the Peppol change management process.

Gap Analysis

Where are we now?

- **Security in new Agreements (but no detail)** SPs
- **Different security requirements across regions**
  - Peppol Authorities (PAs) Specific Requirements
  - Differences makes it difficult for SPs PAs
- Inconsistent security verification
  - Some PAs verify security controls directly
  - Some PAs rely on Standards (e.g. ISO27001)
  - Some PAs have no verification End Users
- End User Identification (EUI)
  - In Agreements/IR Network
- Transport Security
  - TLS 1.2 between C2 and C3

Where do we want to be?

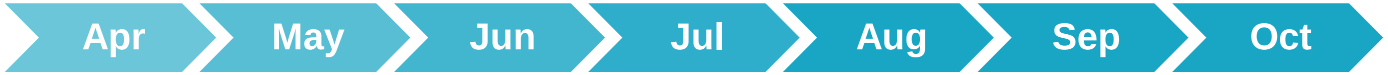
- Peppol security requirements "bar"
  - No need for local PA specific requirements (PASR)
  - Security is consistent across Peppol network
    - Security can be centrally managed and monitored
    - Peppol can respond to emerging risks and threats Easy to verify
- Consistent security verification
  - Verification can be easily done by all PAs
  - SPs can operate across jurisdictions
  - Enforcement in place to ensure compliance
- EUI
  - No change
- Transport Security
  - No change

WG – Bridge the Gap?

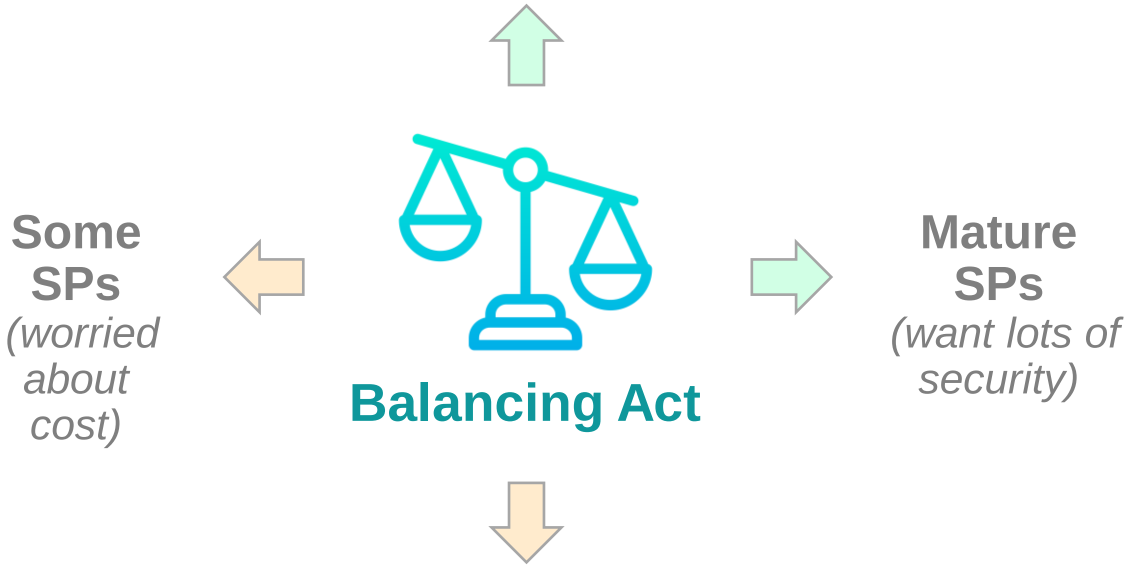
- Aspiration
  - Want a high security “bar”
    - Essential for future of Peppol
  - Want a level playing field
    - Uniform, thorough, provable
  - Want mandatory & enforceable
- Reality
  - Just set a minimum security “bar”
    - So that it is generally acceptable
  - Allow some choices
    - To meet legal, regional, industry requirements
  - Keep recommendations simple
    - Easy to understand and specify
  - Establish infrastructure to focus on security

14 Meetings
- SPs, PAs, technology providers, OO
- Europe, Singapore, AU, NZ

***Huge** topic, intense discussions*
100s of hours of out-of-hours work
Many trade-offs and compromises



Mature PAs
(want a strong security mandate, may have PA specific requirements)



Some SPs *(worried about cost)*

Balancing Act

Mature SPs *(want lots of security)*

Some PAs
(worried about time, cost, and lack of security expertise)

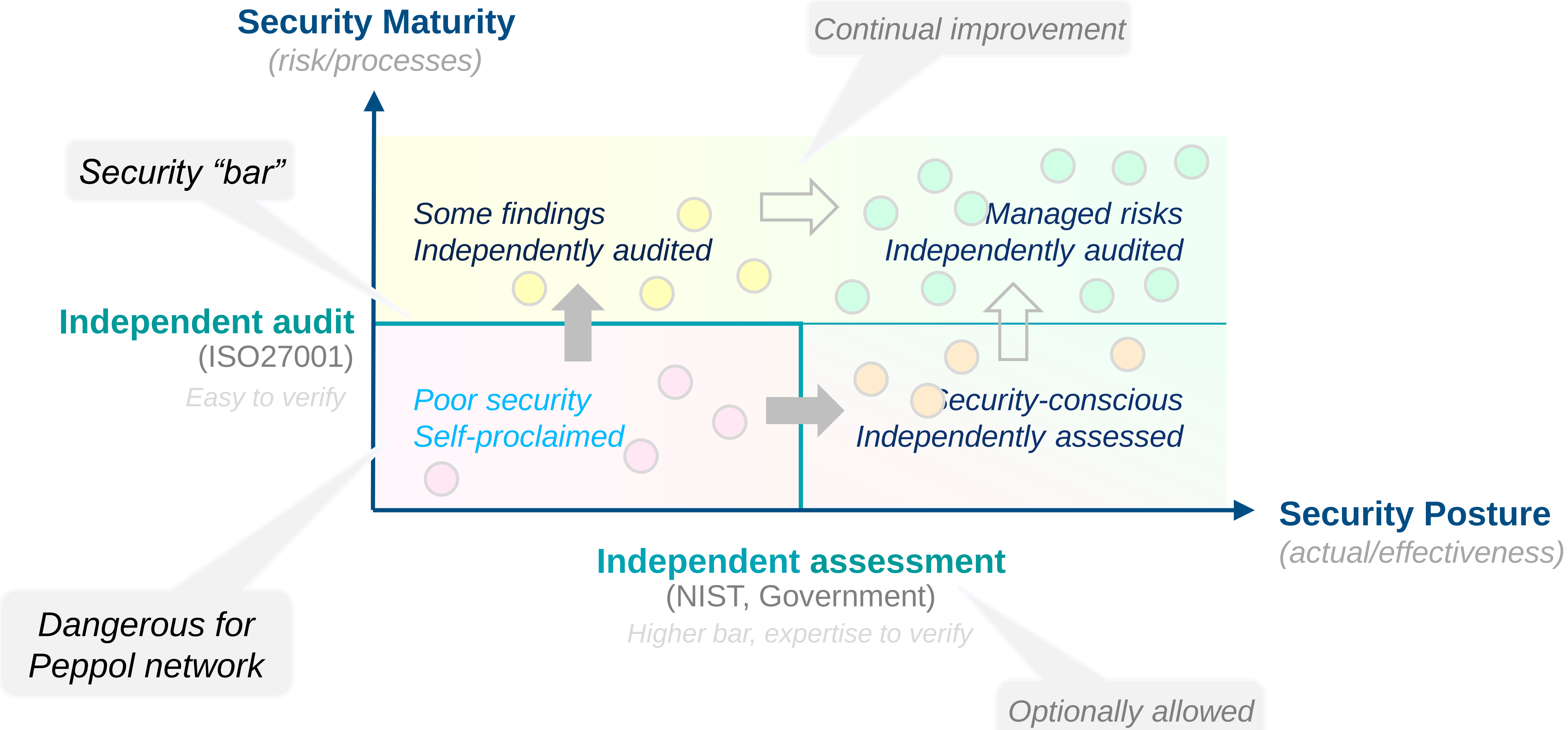
PA – Peppol Authority
SP – Service Provider
OO – OpenPeppol Operating Office
MC – OpenPeppol Managing Committee

Proposal

Problem – Provable Security

Conceptual scatter plot of Peppol SPs

Significant ISO27001 experience in AU



Security Maturity
(risk/processes)

Continual improvement

Security "bar"

Some findings
Independently audited

Managed risks
Independently audited

Independent audit
(ISO27001)
Easy to verify

Poor security
Self-proclaimed

Security-conscious
Independently assessed

Security Posture
(actual/effectiveness)

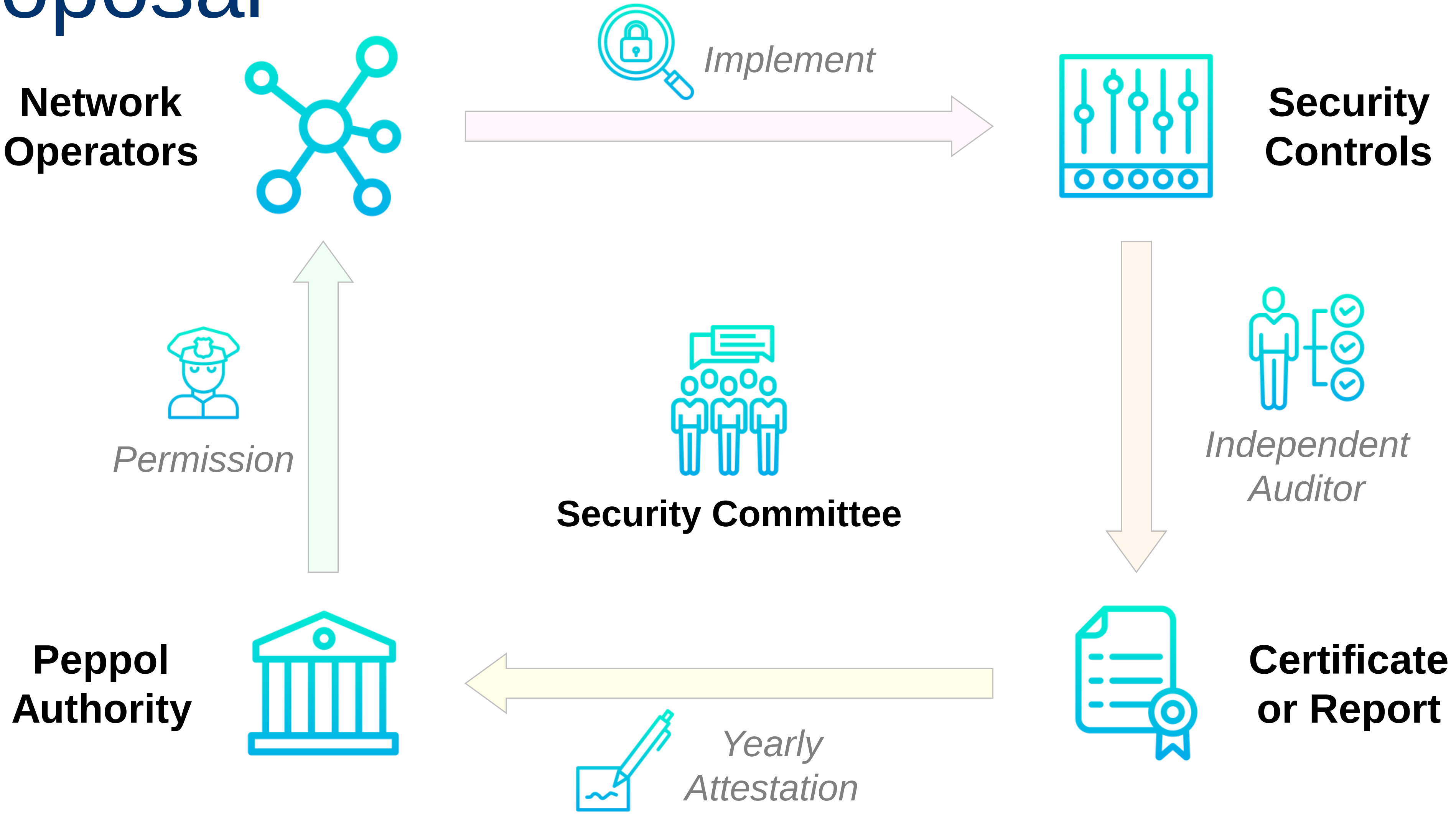
Independent assessment
(NIST, Government)
Higher bar, expertise to verify

Dangerous for
Peppol network

Optionally allowed
in a jurisdiction

c.f. unroadworthy car
(self-interest vs group-interest)

Proposal



Network
Operators

Implement

Security
Controls

Independent
Auditor

Certificate
or Report

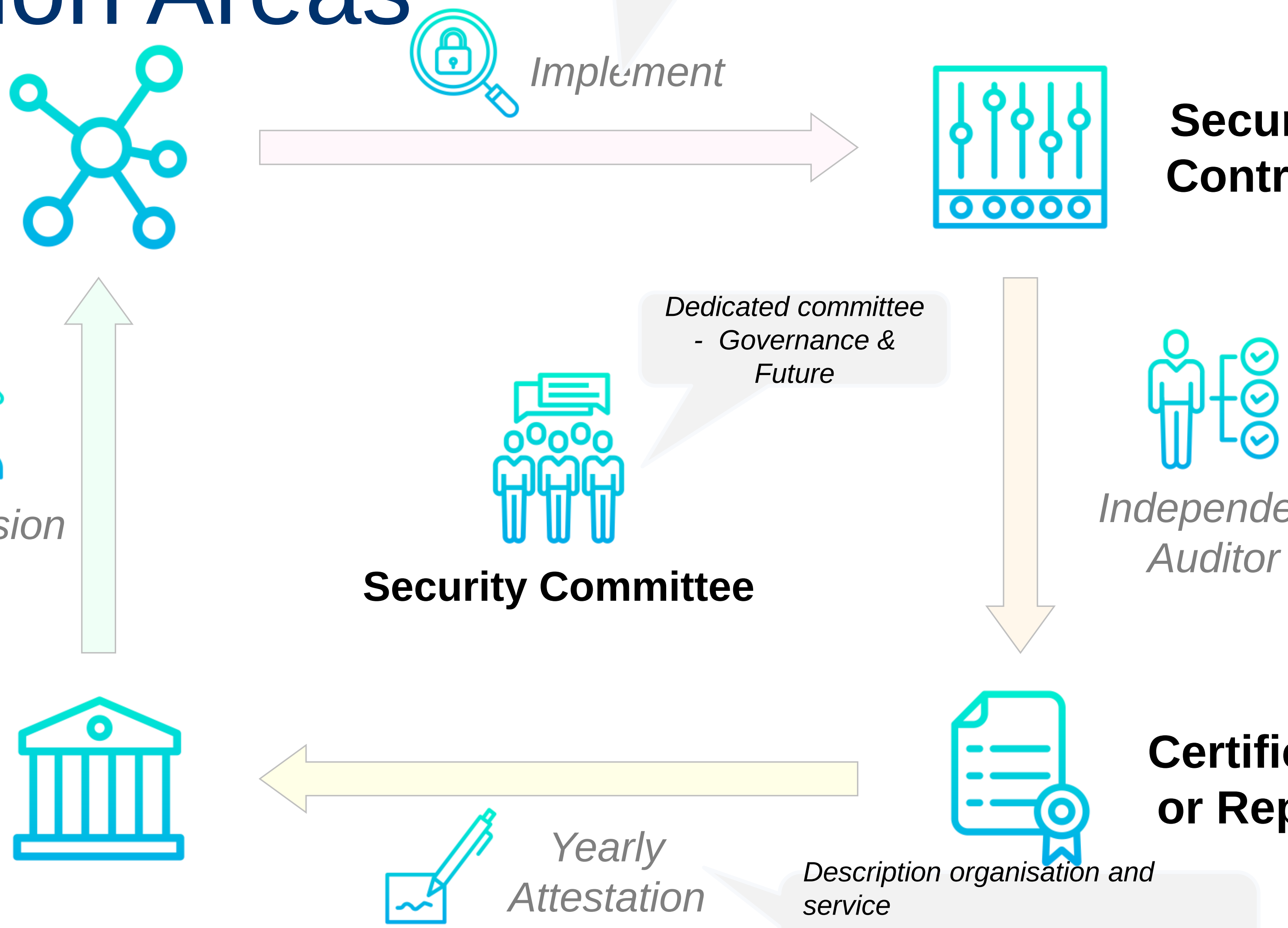
Yearly
Attestation

Peppol
Authority

Permission

Security Committee

ussion Areas



AP and SMP (incl. SPs and PAs) and OO technology & access services

Network Operators

Security controls

Implement

Approved Frameworks (ISO27001, NIST, Government)

Security Controls

PA report to OO Enforcement via existing non-compliance procedure (incl. avenue for escalation)

Permission

Dedicated committee
- Governance & Future

Security Committee

Auditor (ISO27001) or Assessor (NIST, Government)

Independent Auditor

ISO27001 (certificate) Report (NIST, Government)

PAs verify - can reject if SPs do not meet requirements

Peppol Authority

Certificate or Report

Yearly Attestation

Description organisation and service
Certificate/Report
Remediation & security improvements

Migration Plan

Migration Plan

Recommendation #10 – Migration Plan

Make high priority, allow transition, ensure ongoing security committee

Prepare
Approve
Transition
Mandate

Working Group (WG)	Formulate proposal Agree on recommendations	Submit RFC (doc req, changes to IR and OP, migration plan with dates)		Ongoing Security Committee Ongoing review
eDelivery Providers (SPs + OO)	Provide feedback to WG	Provide feedback to APPCMB	Submit “progress” reports Obtain assessment Submit attestation	Yearly attestations
Peppol Authorities (PAs)	Provide feedback to WG	Provide feedback to APPCMB	Evaluate Allow “working progress”	Collect yearly attestations Evaluate Enforce (SPs and OO)
Open Peppol Governance	Co-ordinating Committee - convene WG & set scope	APPCMB consultation APPCMB recommendation MC Approval	MC establish ongoing security committee	MC Escalation OO Enforcement (certs)
Timeframe	2022	Mid 2023	Late 2023 (“promise”)	Late 2024

Next Steps

Next Steps

- Finalise the proposal
  - Consider any feedback / input
- Request for Change (RFC)
  - Security Requirements
    - Changes to Internal Regulations
    - Description of security requirements
    - Migration Plan
  - Ongoing Security Committee
- **Agreements, Policies, and Procedures CMB**
  - Change management process includes consultation

Further information & Questions

- **Detailed presentation**
  - Rick Harvey presentation at the SPC on 25 October 2022
  - Recorded (uploaded to community page)

- Questions?