Working progress – for discussion only

The future is open Peppol

Peppol Security Requirements Design Work Group

Extraordinary Peppol SP Community Meeting

25 October 2022

Background

- **Management Committee (MC)**
  - 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
  - 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).

Generally

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?

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

Where do we want to be?

- **Clearly defined 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
- **Consistent security verification** *Easy to verify*
  - 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

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

Apr → May → Jun → Jul → Aug → Sep → Oct

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

Some SPs
(worried about cost)

Mature SPs
(want lots of security)

Balancing Act

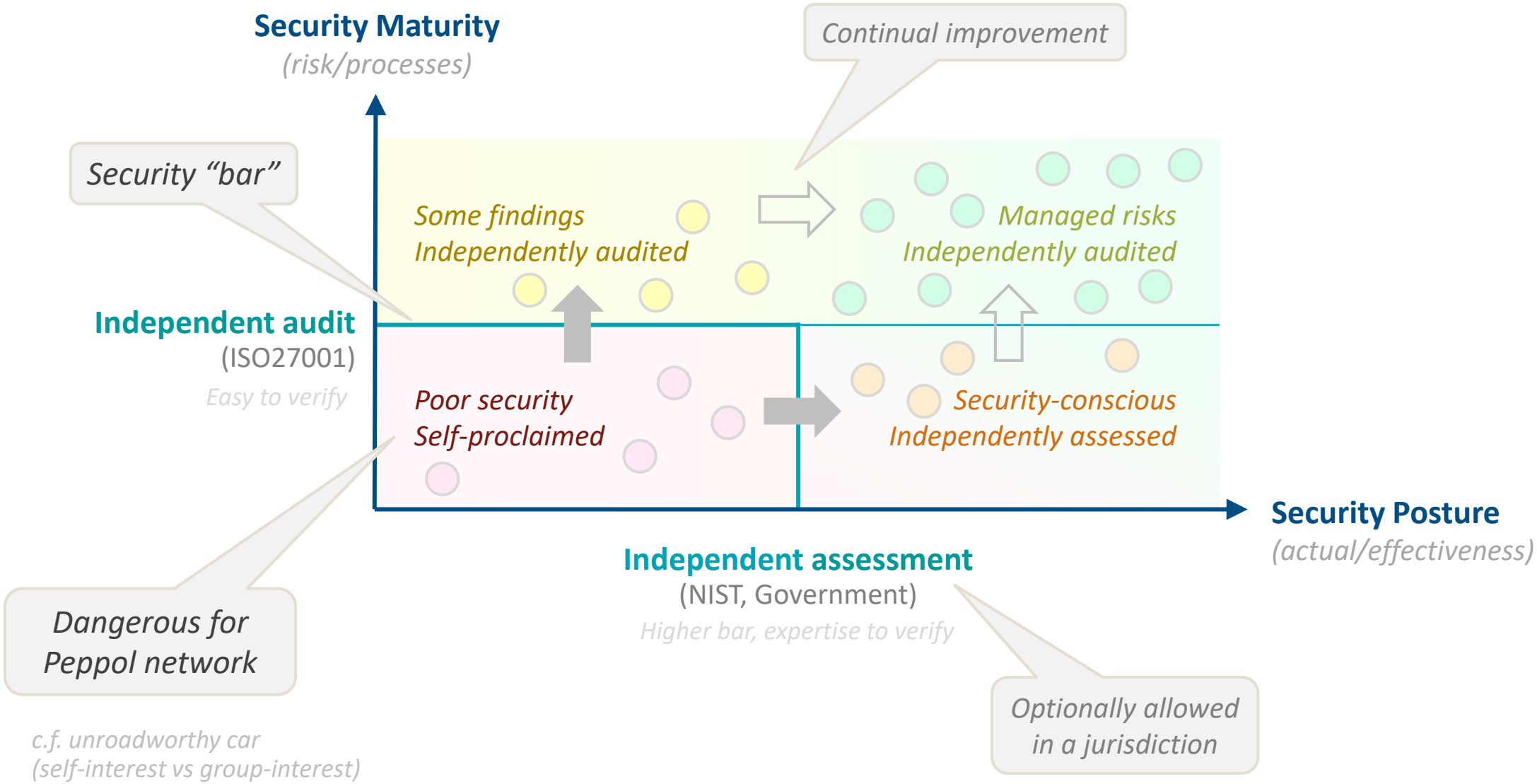
Some PAs
(worried about time, cost, and lack of security expertise)

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

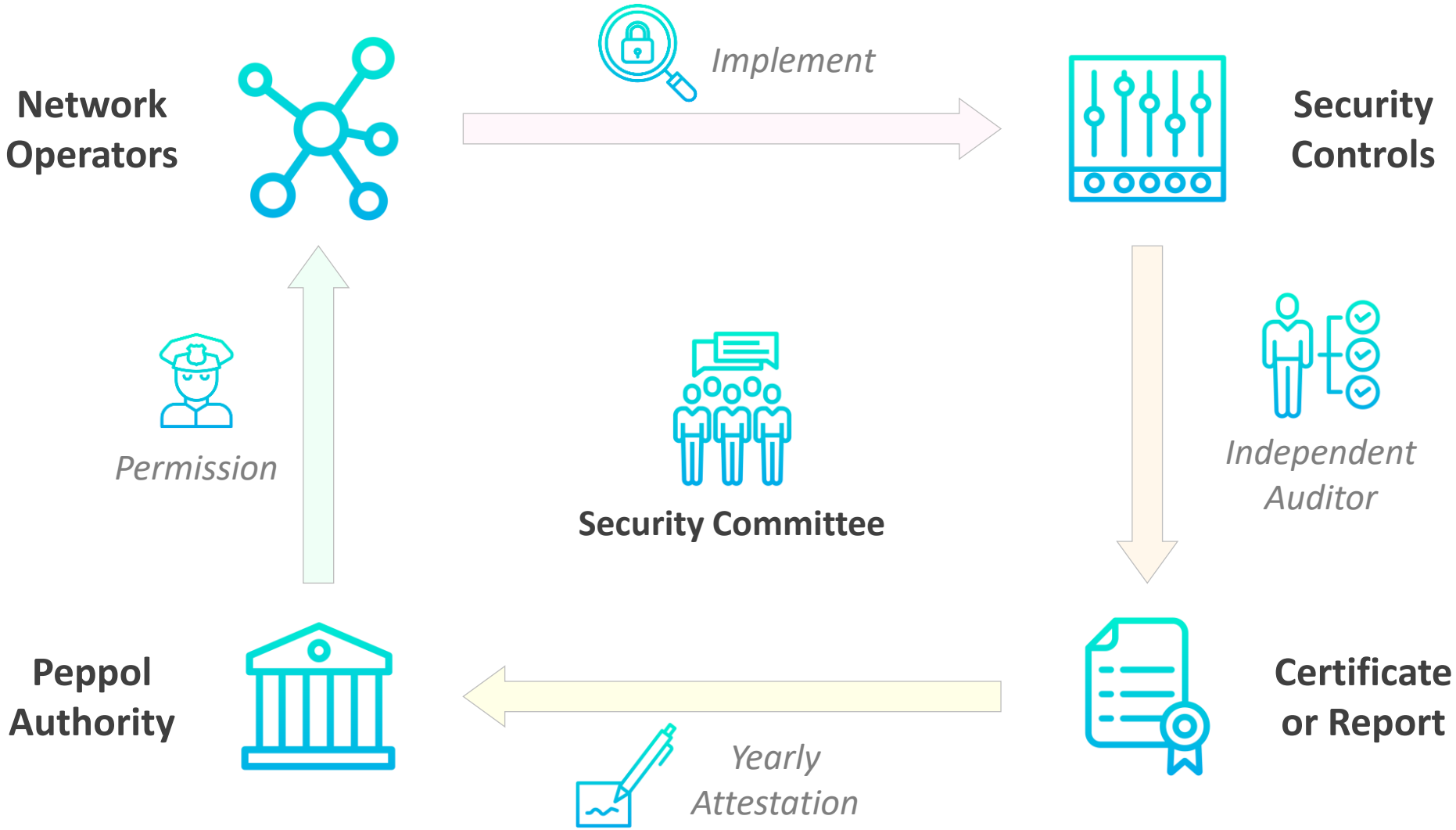
Problem – Provable Security

Conceptual scatter plot of Peppol SPs

Significant ISO27001 experience in AU



Proposal



Discussion Areas

1. Who?

Network Operators

2. Cost?

Implement

3. Frameworks?

Security Controls

4. Baseline controls?

Independent Auditor

5. Pass/fail?

Certificate or Report

6. Confidentiality?

Yearly Attestation

7. Verify?

Peppol Authority

8. Enforcement?

Permission

9. Future?

Security Committee

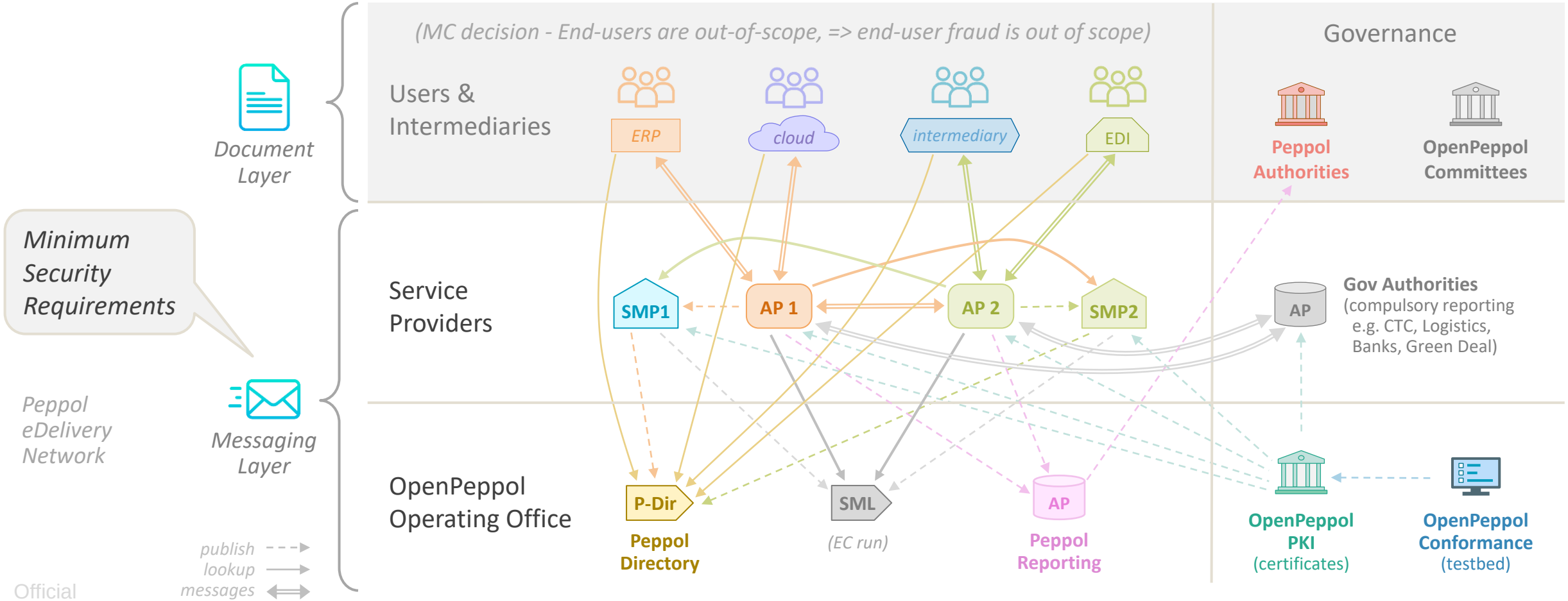
Discussion Areas (9)

More detail
Background Information
Recommendations

1. Network Operators (who?)

Recommendation #1 – Affected Entities

All SPs (run an AP or SMP) and OO services (internal or subcontracted) must meet the Peppol mandated minimum security requirements



2. Implementation (cost?)

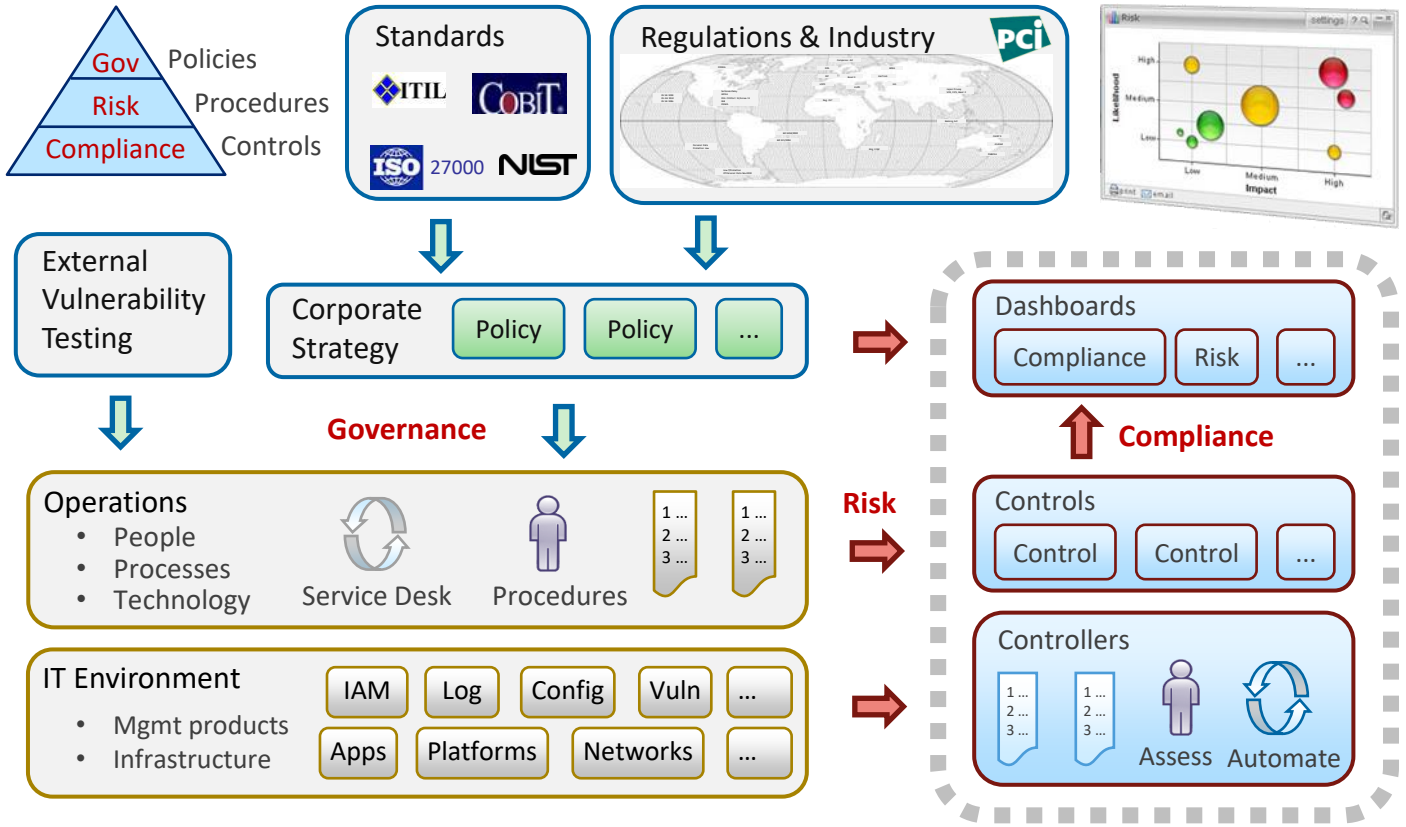
Recommendation #2 – Security Controls

All SPs and OO must implement security controls for their Peppol Services

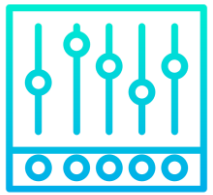
- **Security is Required**
  - Cost – security part of business
    - ISO27001 audits start from €5K p.a.
    - Certification is good for business
  - In Service Provider agreement

9.4.9. Ensure that it has sufficient resources for the readiness, testing, operation and maintenance of its services according to the minimum service level requirements …

10.3. The Parties shall use measures and procedures in accordance with accepted best industry practices to protect their own data systems used to perform this Agreement against illicit use, malicious code, viruses, computer intrusions, infringements and illegal tampering of data and other comparable actions by third parties.



3. Security Controls (frameworks?)



Recommendation #3 – Approved Information Security Frameworks

All SPs and OO must use an approved framework: ISO27001 or NIST or National Government

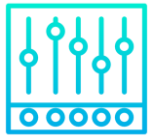
- **Acceptable Frameworks**
  - ISO27001 (dominant, 2022 is NIST harmonised)
  - Optional (PA decision)
    - NIST Cybersecurity Framework (NIST CSF)
    - National Government (e.g. AU IRAP)
- **Other Frameworks**
  - Complex, specialised, limited, country specific
    - Global – CIS, COBIT, COSO, CSA, ISF, MITR, PCI, SOC2…
    - Regional – ASD8, CMMC, ETSI, HITRUST, NCSC, PSR…

ISO27001

- International standard for Information Security
  - One of the ISO27000 family
- Requires an ISMS
  - InfoSec Management System
- Annex A – 93 Controls

Mandatory Requirements

- Scope [4.3]
- Risk assessment [6.12]
- Management
  - [5.2, 6.1, 6.2, 7.2, 9.1, 9.2, 9.3]
  - Risk, training, monitoring & measurement, internal audit, review, corrective actions



Service Controls

- Manage risk
- Implement
  - Policies & processes
- Collect evidence

Statement of Applicability (SoA)

- Which of 93 controls implemented
- Justify why others aren't implemented

4. Independent Auditor (baseline?)

Recommendation #4 – Evaluation by independent auditor/assessor

All SPs and OO must get their Peppol services and systems evaluated by an independent and accredited auditor or assessor

- **Acceptable**
  - Independent auditor (ISO27001)
  - Independent assessor (NIST, Gov)
- **Baseline controls?**
  - Not necessary, as auditor/assessor will review risk assessment and control coverage

Full Audit
- *0: Gap Analysis*
- *1: Readiness*
- *2: Examination*

Surveillance audits
- *Within 3 year cycle*

Auditor
- Independent
- Accredited

Meets minimum requirements

Examination
- Scope
- Controls verified
- List of findings
- Recommendation

No major findings

Certificate
- Scope
- Summary

Peer reviewed
Issued & published
Reviewed yearly

Findings
- *Major – no certificate*
- *Minor – 1 year to fix*
- *Needs improvement*

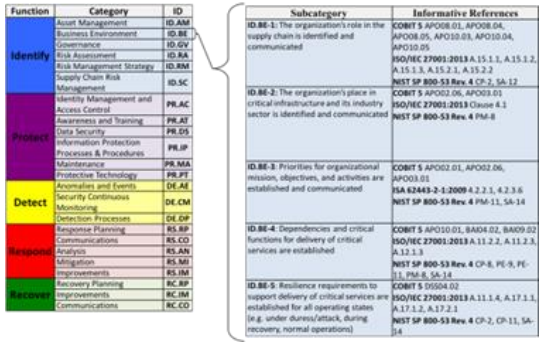
5. Certificate or Report (pass/fail?)

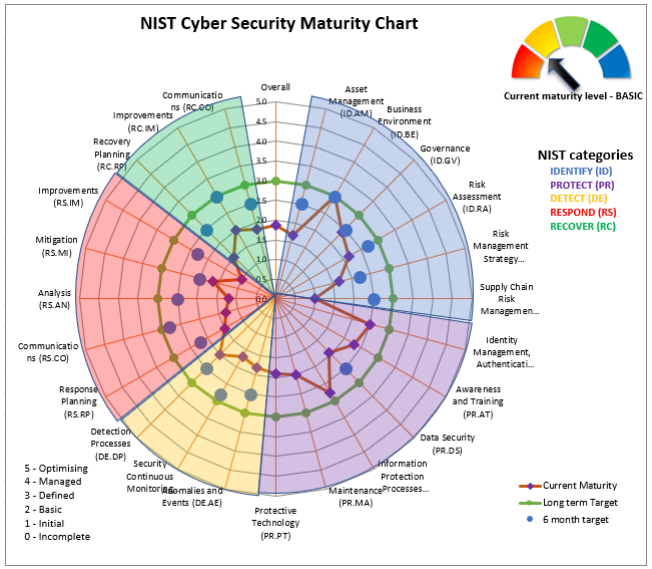
Recommendation #5 – Audit certificate or assessment report

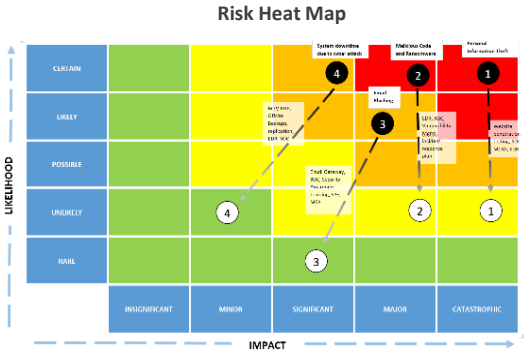
All SPs and OO must ensure the completion of an independent audit or security assessment

- **ISO27001 – Certificate**
  - Public, simple, “pass”
  - Renewed each year

- **NIST, Gov – Report**
  - Private, detailed, graded
  - Review needs security expertise
  - NIST maps onto ISO27001







6. Yearly Attestation (confidentiality?)

Recommendation #6 – Annual Attestation

All SPs and OO must provide a yearly attestation which includes the independent audit certificate or assessment report and commitments to remediation and ongoing security improvements.

- **Attestation**
  - Information about organisation and service
    - Includes changes in circumstances or environment
    - Includes associated dependencies e.g. supply chain
  - Provide independent audit/assessment
    - ISO27001 – certificate
    - NIST – independent assessor's security report
    - Gov – government security report
  - Declaration about ongoing remediation and security improvements
- **Process**
  - Provide yearly
    - SPs to their PA, OO to MC
  - Audit/assessment maybe an ongoing
    - SPs using ISO27001 over 3yrs
    - New SPs may show "in progress" and give timetable
- **Confidentiality**
  - SP's have a choice
    - ISO27001 certificate – just general certificate
    - NIST, Gov – need to provide report

7. Peppol Authority (verify?)

Recommendation #7 – Peppol Authority Evaluation

PA determines an SP attestation's acceptability. MC evaluates the OO attestation.
PA has the right to demand more information or reject an attestation.

- **Acceptability**
  - PAs may question an attestation
    - If the auditor/assessor is unacceptable
    - If scope of audit/assessment is unacceptable
  - PAs may ask for more info
    - E.g. if certification is "in progress"
    - E.g. if assessment is incomplete e.g. dashboards of coverage and effectiveness
  - PAs may reject an attestation
    - If SP refuses to meet requirements
- **Verification**
  - ISO27001 – evaluation is simple (yes/no)
  - NIST, Gov – optional for PA
    - Security expertise is required if PA chooses to accept NIST or Government security assessments
- **MC Role**
  - MC evaluates OO attestation
  - MC adjudicates if a PA operates an AP or SMP
  - MC needs to collect yearly report from PAs

8. Permission (enforcement?)

Recommendation #8 – Enforcement

PAs report to OpenPeppol. The SPs have the right to escalate. Failure to conform will result in revoking of Peppol certificate .

- **Pass**
  - PA's provide list of SPs to OpenPeppol
  - SPs or OO continue as usual

- **Escalation**
  - Non-compliance operational procedure
    - PA notifies OpenPeppol of a problem SP
    - SPs can appeal
  - MC intervenes if OO fails
- **Enforcement**
  - SP's AP or SMP certificate revoked
  - Or certificate won't be renewed (2-year cycle)

9. Security Committee (future?)

Recommendation #9 – Ongoing Security Committee

Establish an ongoing dedicated security committee to provide oversight, advice, review, planning and investigation of security related issues and concerns in the Peppol network

- **Ongoing Review**
  - Review security "bar" and process
    - Investigate program effectiveness
    - May need to produce guidelines
    - Look at specifying mandatory controls
- **Advice**
  - Provide expert opinion
    - Resource for MC, PAs, SPs
  - Investigate broader security topics
    - Security options for C1/C4
    - Security trends & emerging risks
    - Security differences between regions
- **Governance**
  - Provide oversight of Peppol operations
    - Security in eDelivery Standards (e.g. HTTPS for SMP)
    - Security of OO related services (e.g. central reporting)
    - Approval of particular national government framework
  - Provide input to planning
    - Security budget for OO needs increasing
    - Security implications of alliances (e.g. EESPA interconnection)
  - Provide input to strategy for Peppol's future
    - E.g. CTC is going to demand high levels of security
    - E.g. Interconnecting to other networks - higher security
    - E.g. Becoming international requires higher security

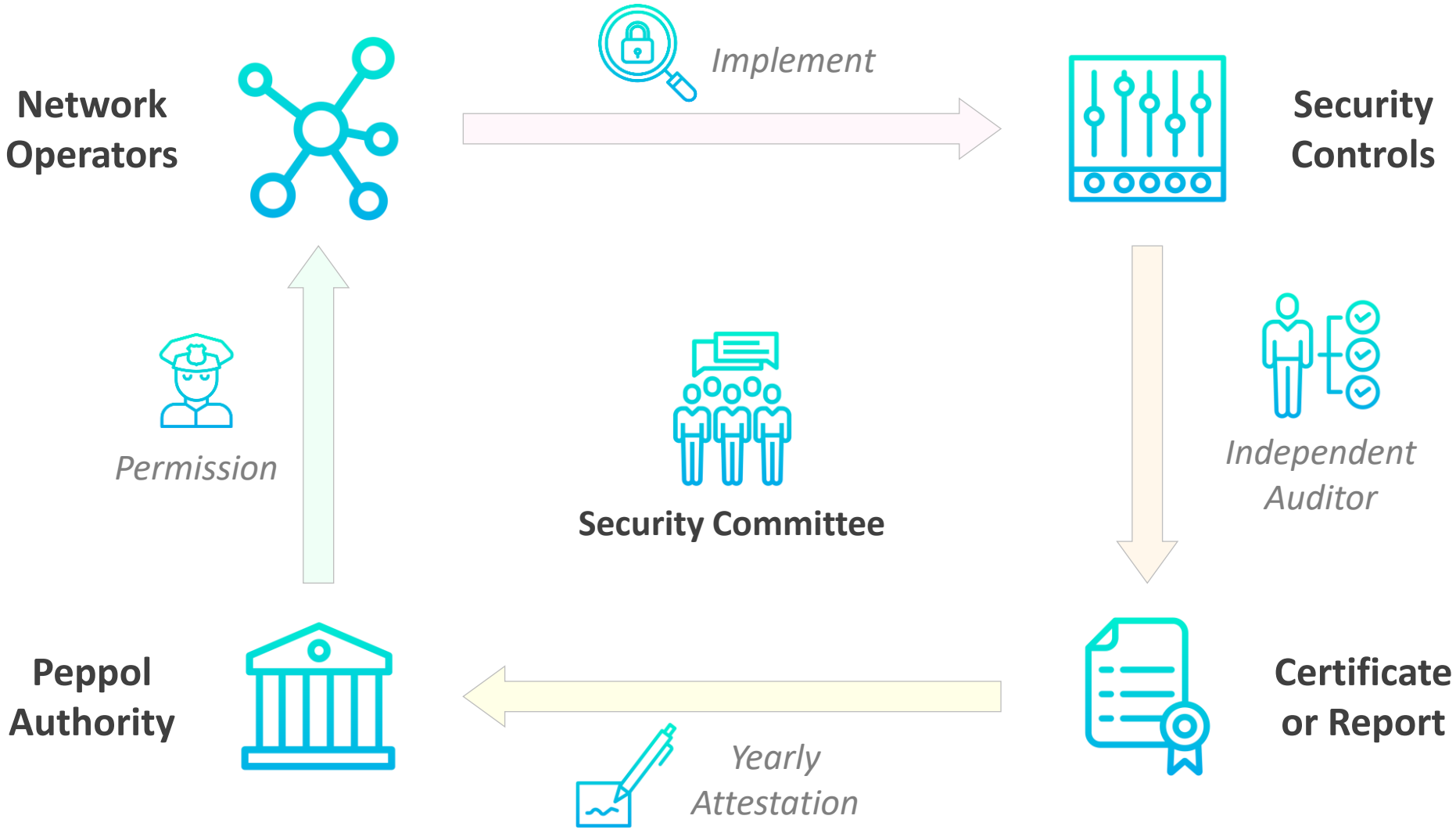
Summary and Next Steps

Proposal

Migration Plan

Questions

Proposal


Network Operators
Implement
Security Controls
Permission
Security Committee
Independent Auditor
Peppol Authority
Yearly Attestation
Certificate or Report

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

Summary

- **Next Step (RFC)**
  - Security Requirements
    - Entities – SPs (APs, SMPs) and OO (supporting eDelivery services)
    - Controls – ISO27001, NIST, Government
    - Audit – independently, accredited
    - Attestation – yearly
    - Enforcement – Peppol X.509 certificates
  - Migration Plan
    - Transition end of 2023 – allowing “in progress”
  - Ongoing Security Committee
    - Provide on-going review, updates, advice, and planning
- **Questions?**