eIAS Study on an electronic identification,
authentication and signature policy

Future Assessment Strategies for QTS(P)s

A European Scheme for Supervision of Qualified Trust Service Providers and Qualified Trust Services they provide – Conformity Assessment Guidance

in the context of
COM(2012) 238 Proposal for a
Regulation on electronic identification and trust services

DLA PIPER SEALED time.lex SGA PRICEWATERHOUSECOOPERS

Key principles

- **Trust services as key enablers in boosting use of online environment**
  - Qualified Trust Services (QTS) and their specific outputs being given a specific legal effect enhancing their legal certainty and admissibility over the EU
- **Supervision model: Maintaining national supervisory bodies but with stronger and harmonised rules** (process, mutual assistance, TSP security requirements, requirements for QTPs, trusted lists)
- **Monitoring of Trust Service Providers and their Trust Services to ensure information security risk management**
- **Supervision of QTS(P)s and Trusted Lists as essential building blocks for trust building** (claim vs confirmation)
- **Secondary legislation (D.A. / I.A.) “bridging” Primary legislation & Technical specifications (standards)**

Monitoring of Trust Services (Providers)

- **Supervisory Bodies to monitor TSPs for taking appropriate technical and operational risk management measures wrt. the security of their trust services**
  - TSPs may submit an audit security report carried out by an recognised independent body to confirm such measures
- **Possible next steps:**
  - **Clarify who exactly is to be considered as a TSP providing TS and who is not** (e.g. ISP's, free mailbox providers, etc.)
  - **Promote ISO/IEC 27001 certification to be carried out by an accredited certification body** as EU wide common minimum requirement for "Art15.1 security audit reports"
  - **Trusted List of "monitored" compliant TSP's**
  - **Evaluate impact on Supervisory Bodies, on TSP's, on effective security of monitored Trust Services**

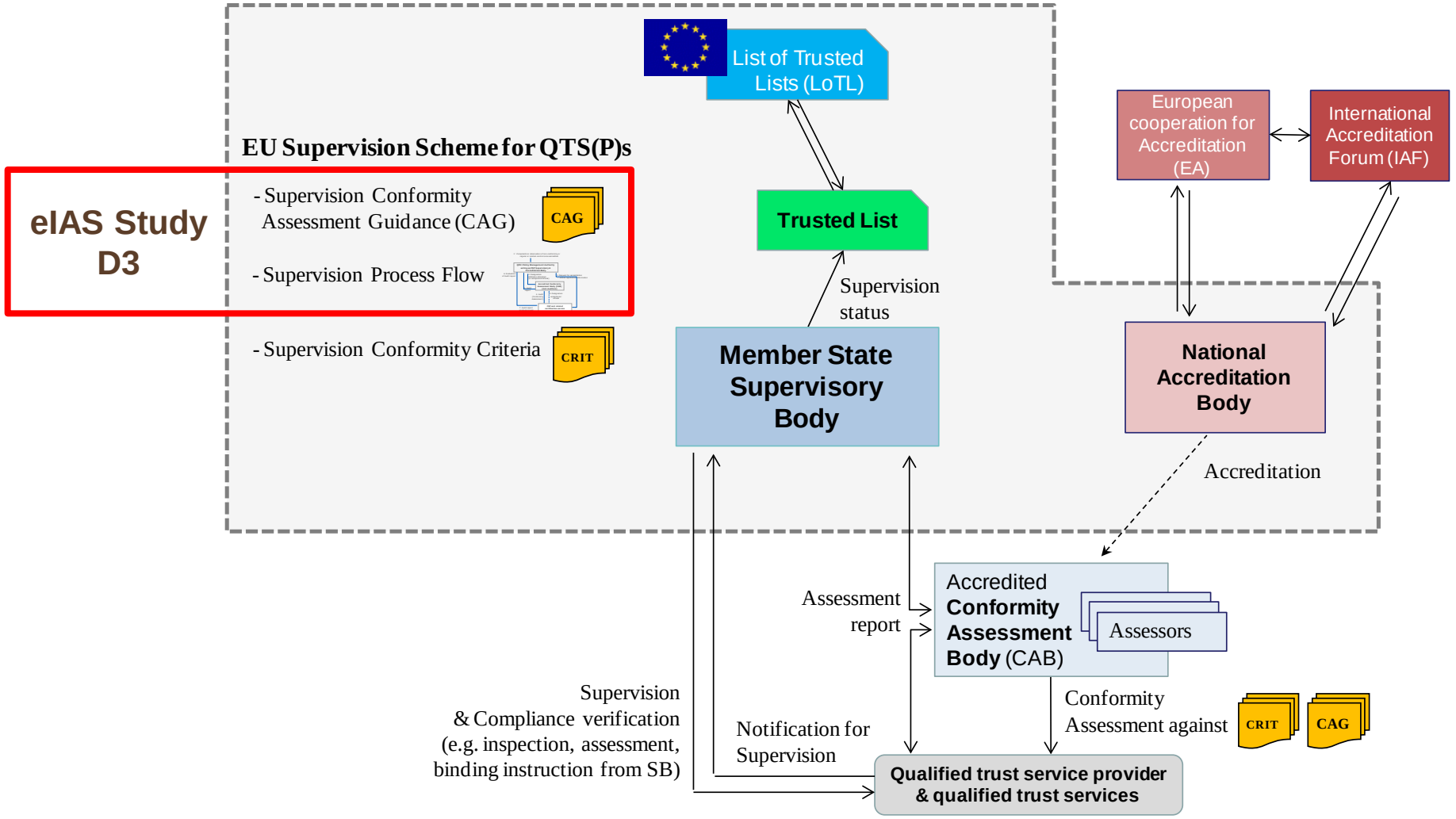
Supervision of QTS(P)s

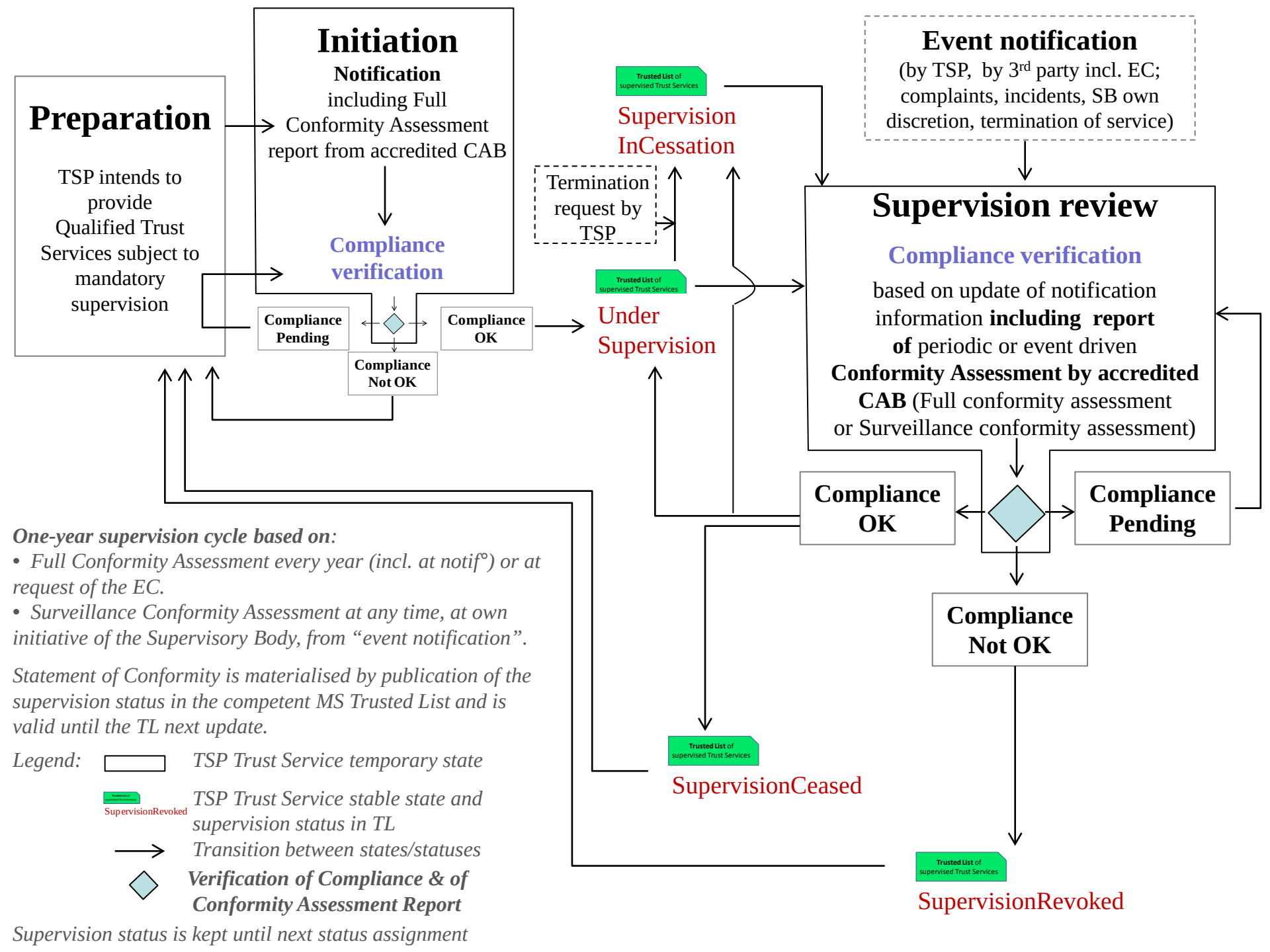
- **Supervisory Bodies to supervise Qualified Trust Service Providers and their Qualified Trust Services**
  - Chapter 2 - Art.13 to 19.
- **Possible next steps:**
  - **Consider a full prior authorisation model** (versus the hybrid model proposed in the Regulation that may lead to practical implementation / discriminatory issues)
  - **Establish a European Supervision Scheme for QTS(P)s based on**
    - **a Conformity Assessment Guidance – CAG** : including the description of the Supervision Process flow , taking into account the qualified status flow in Trusted Lists;
    - **Conformity Assessment Criteria – CRIT** : Mapping legal provisions to standards per type of qualified trust service
    - **Trusted List specifications** updated from CD 2009/767/EC as amended by CD 2010/425/EU.

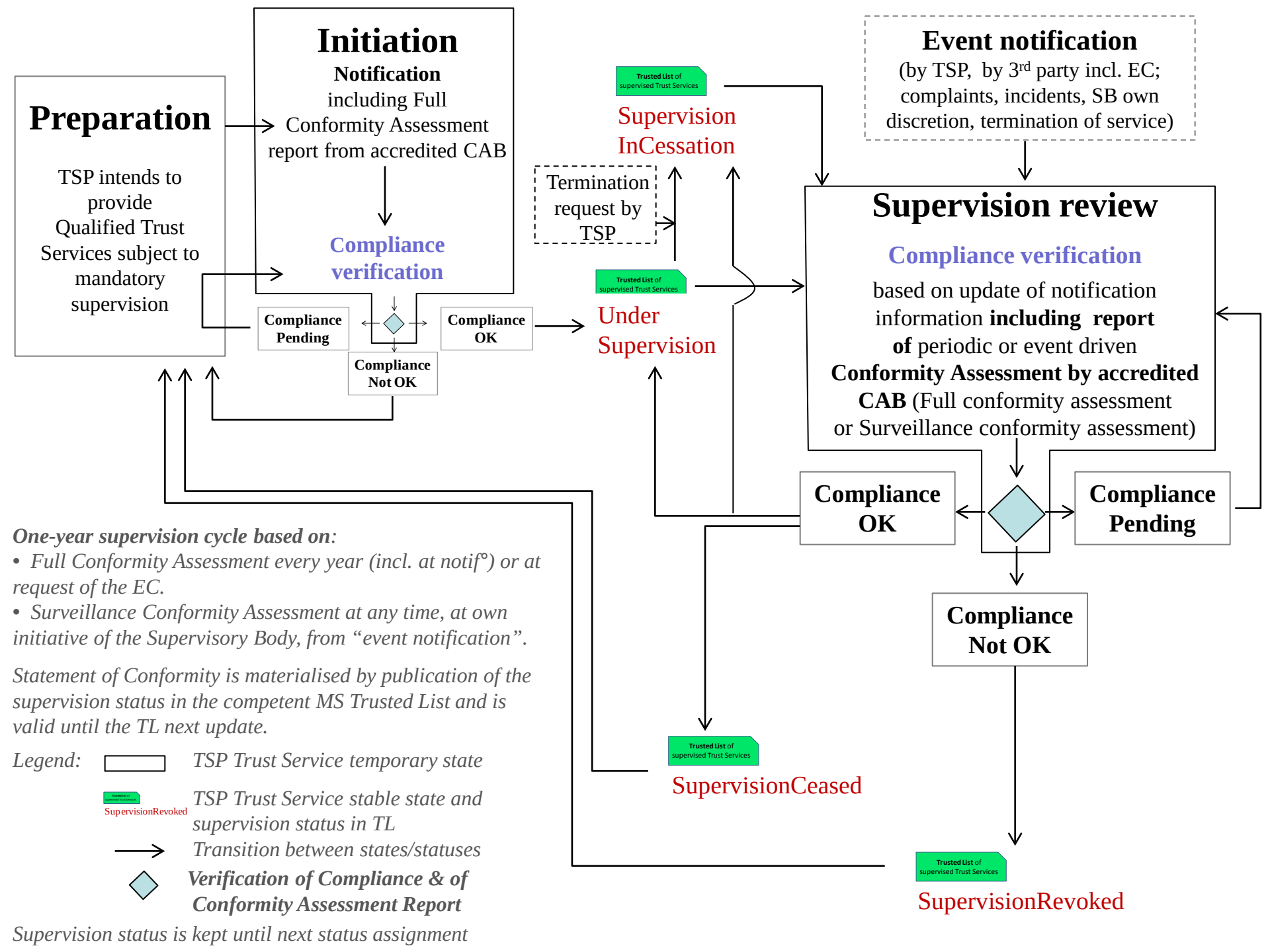
eIAS proposed model for EU Supervision Scheme

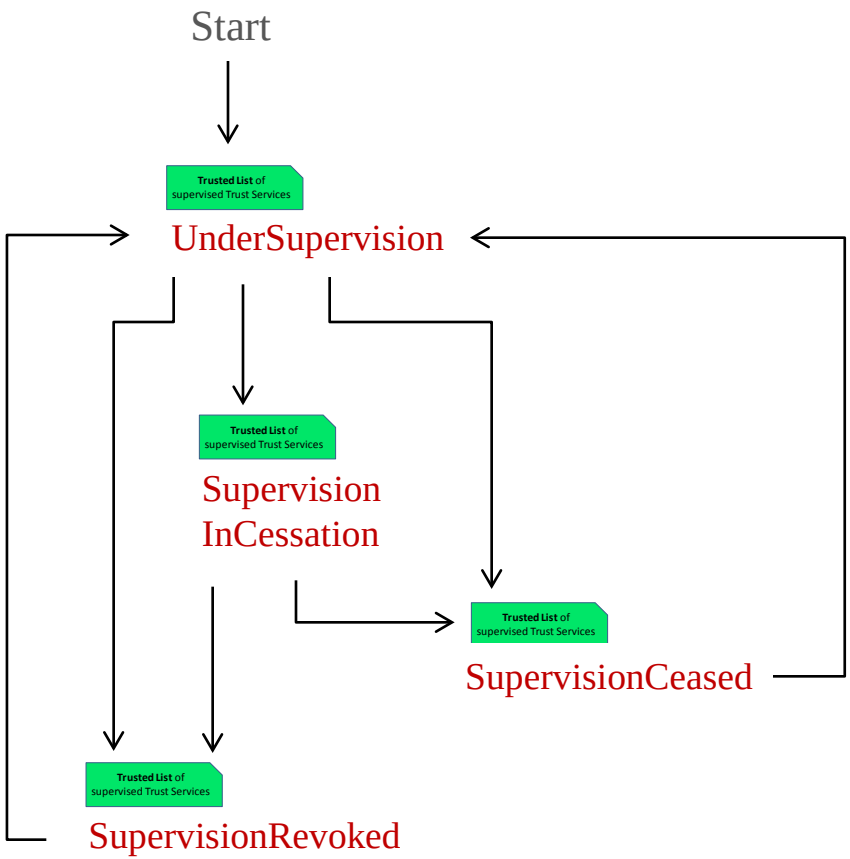
- ISO/CASCO based model (preferred to other models like ISAE 3000, AICPA, IFAC/IAASB/ISRS)
- Allow international recognition through EA and IAF
- Aligned with COM(2012) 238 proposal
- Conformity Assessment Guidance (CAG), Criteria (CRIT) and Trusted Lists specifications may be either part of such acts or standardised (e.g. ETSI EN 319403 drafted accordingly) & referenced in such acts.
- Backward compatible with Trusted Lists (CD 2009/767/EC amended by CD 2010/425/EU) – limited updates
- Allows monitoring of TSPs (based on ISO/IEC 27001 certification)
- EU Supervision Scheme common to all MS
  - Increase trust & confidence level of QTS(P)s in EU, transparency, equality, better preparation of QTSPs, harmonised and stronger rules
  - Trust recognition in EU and **beyond** as benchmarking reference for mutual recognition with 3rd countries and international organisations
- Delegated and implementing acts mechanism allow implementation of such a common EU Supervision Scheme

eIAS proposed model for EU Supervision Scheme

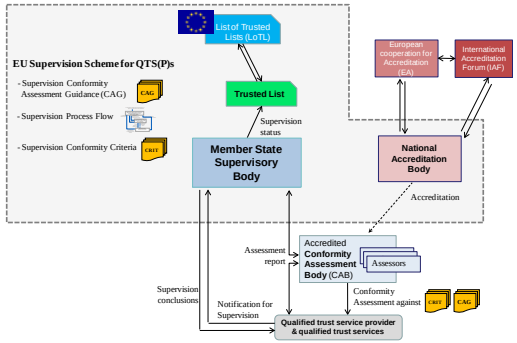



Preparation
TSP intends to provide Qualified Trust Services subject to mandatory supervision
Initiation
Notification including Full Conformity Assessment report from accredited CAB
Compliance verification
Compliance Pending
Compliance OK
Compliance Not OK
Trusted List of supervised Trust Services
Supervision InCessation
Termination request by TSP
Trusted List of supervised Trust Services
Under Supervision
Event notification
(by TSP, by 3rd party incl. EC; complaints, incidents, SB own discretion, termination of service)
Supervision review
Compliance verification
based on update of notification information including report of periodic or event driven Conformity Assessment by accredited CAB (Full conformity assessment or Surveillance conformity assessment)
Compliance OK
Compliance Pending
Compliance Not OK
Trusted List of supervised Trust Services
SupervisionCeased
Trusted List of supervised Trust Services
SupervisionRevoked
One-year supervision cycle based on:
• Full Conformity Assessment every year (incl. at notif°) or at request of the EC.
• Surveillance Conformity Assessment at any time, at own initiative of the Supervisory Body, from "event notification".
Statement of Conformity is materialised by publication of the supervision status in the competent MS Trusted List and is valid until the TL next update.
Legend:
TSP Trust Service temporary state
SupervisionRevoked
TSP Trust Service stable state and supervision status in TL
Transition between states/statuses
Verification of Compliance & of Conformity Assessment Report
Supervision status is kept until next status assignment


Preparation
TSP intends to provide Qualified Trust Services subject to mandatory supervision
Initiation
Notification including Full Conformity Assessment report from accredited CAB
Compliance verification
Compliance Pending
Compliance OK
Compliance Not OK
Trusted List of supervised Trust Services
Supervision InCessation
Termination request by TSP
Trusted List of supervised Trust Services
Under Supervision
Event notification
(by TSP, by 3rd party incl. EC; complaints, incidents, SB own discretion, termination of service)
Supervision review
Compliance verification
based on update of notification information including report of periodic or event driven Conformity Assessment by accredited CAB (Full conformity assessment or Surveillance conformity assessment)
Compliance OK
Compliance Pending
Compliance Not OK
Trusted List of supervised Trust Services
SupervisionCeased
Trusted List of supervised Trust Services
SupervisionRevoked
One-year supervision cycle based on:
• Full Conformity Assessment every year (incl. at notif°) or at request of the EC.
• Surveillance Conformity Assessment at any time, at own initiative of the Supervisory Body, from "event notification".
Statement of Conformity is materialised by publication of the supervision status in the competent MS Trusted List and is valid until the TL next update.
Legend:
TSP Trust Service temporary state
SupervisionRevoked
TSP Trust Service stable state and supervision status in TL
Transition between states/statuses
Verification of Compliance & of Conformity Assessment Report
Supervision status is kept until next status assignment


Start
Trusted List of supervised Trust Services
UnderSupervision
Trusted List of supervised Trust Services
Supervision InCessation
Trusted List of supervised Trust Services
SupervisionCeased
Trusted List of supervised Trust Services
SupervisionRevoked

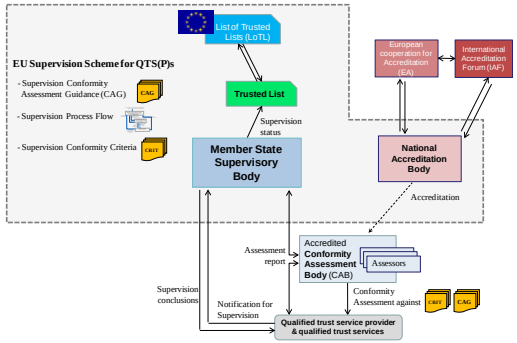
Comments received so far



NL, DE, ETSI, NO, UK

- *Accreditation requirements for CAB*
  - *(Full) management system: ISO 17021, 27006*
  - *Internal and external services: ISO 17065 / EN 45001*
  - *ISMS: ISO 27001*
  - *Security and QTSP services: Sector specific ISO 27006 with ability to perform assessments against CRIT*
- *Clarification: assessment scope*
  - *Assessment (FCA & SCA) are not limited to « management system » assessment but assessment against CRIT (that includes requirements on MS/ISMS&Security/provision of QTService/QTServiceProvider*
  - *Indeed one tool the Supervision Process can use but yearly occurrence requirement for FCA.*
- *CRIT ideally organised as "sector specific ISO 27001 certification" to include requirements on*
  - *Management system and **IS**MS (incl. Forensic Readyness/Damage Control)*
  - *Policy & Security requirements for the provision of QT**Services** and for QTSP*

Comments received so far

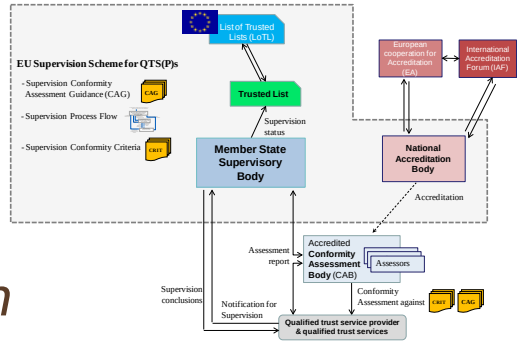


NL, DE, ETSI, NO, UK

- *SB evaluates assessments reports (stage1+2 report) and makes it own motivated decision (aligned or not with the report)*
- *[No] validation of stage 1 report by SB prior to stage 2*
- Clarify ability for SB immediate action from incidents:
  - In the event of severe incident, ability for SB to act without (F)CA or SCA is performed by SB and can be quick-to-action
  - TSP not collaborating with CAB, SB able to act without assessment (report) from CAB
  - etc.
- "Compliance pending/ok/Notok" are not "statuses" being reflected in Trusted List but outcomes of SB compliance verification process (supervision) that may lead to various status changes or not.

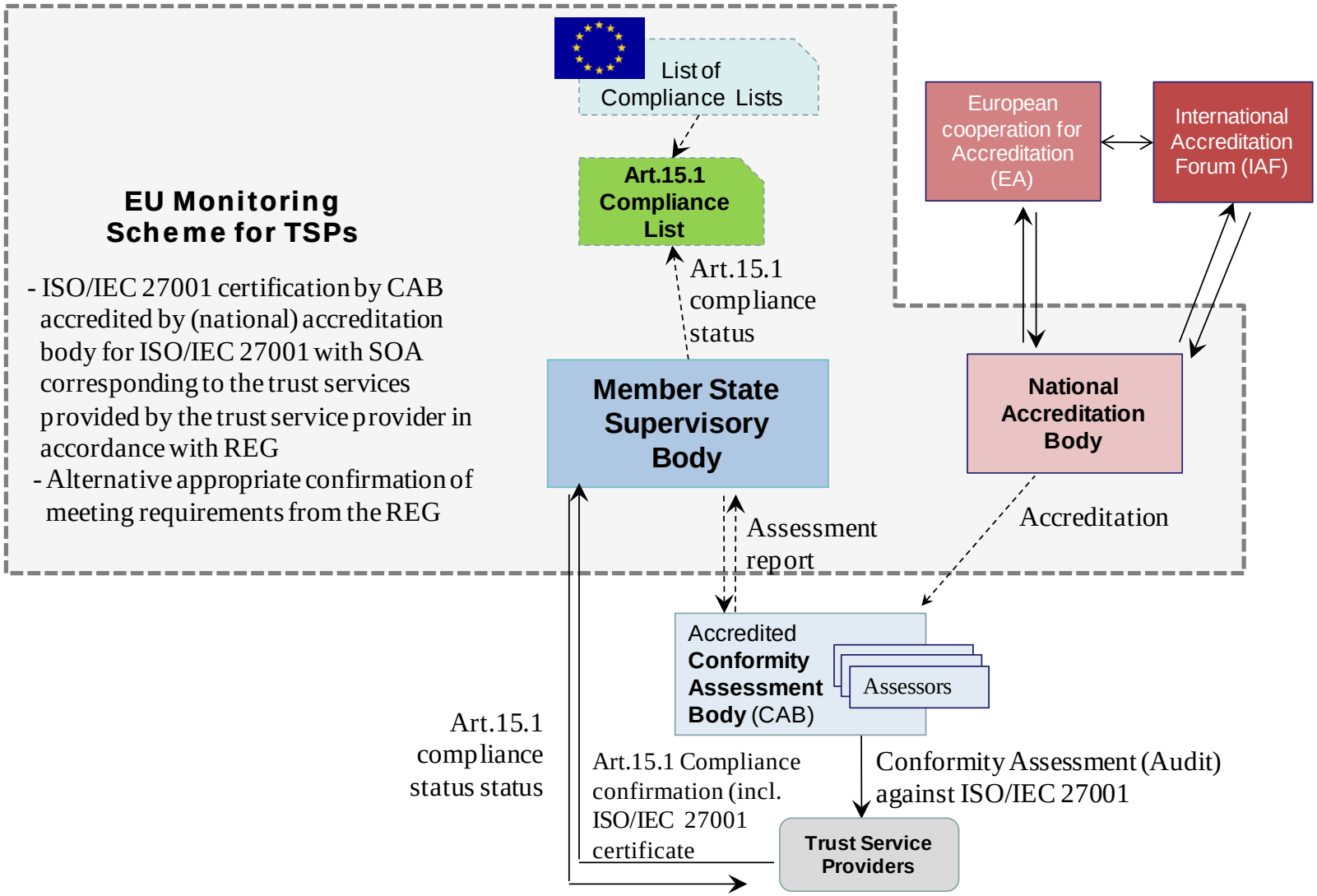
Comments received so far

NL, DE, ETSI, NO, UK



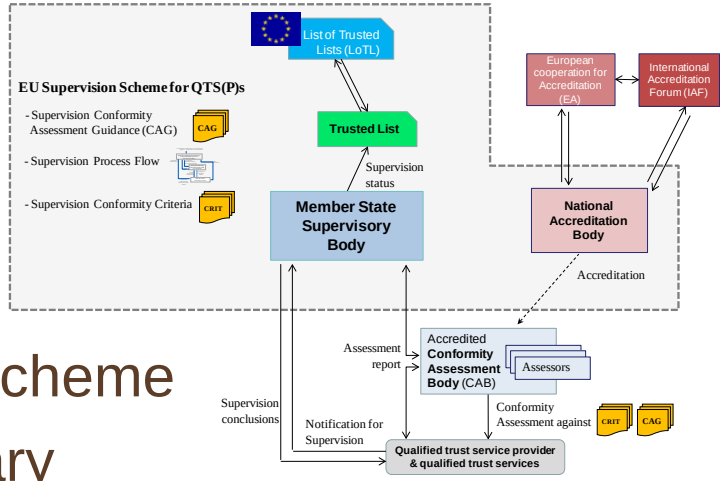
→ *Clarification: SB may undertakes the conduction of an assessment at any time at its sole discretion in addition to planned/scheduled assessments.*

Monitoring as part of the proposed Scheme



Conclusions

- EU Supervision Scheme common to all MS
  - Increase trust & confidence level of QTS(P)s in EU, transparency, equality, better preparation of QTSPs, harmonised and stronger rules
  - Trust recognition in EU and beyond as benchmarking reference for mutual recognition with 3rd countries and international organisations



- Delegated and implementing acts mechanism allow implementation of such a common EU Supervision Scheme and are key elements between primary legislation and technical standards