

PCI MPoC Certification Process

Pre & Post Certification Activities

4th February 2025

Chao QU - Senior Security Analyst
Alan MARZEC - CEO



Our Mission

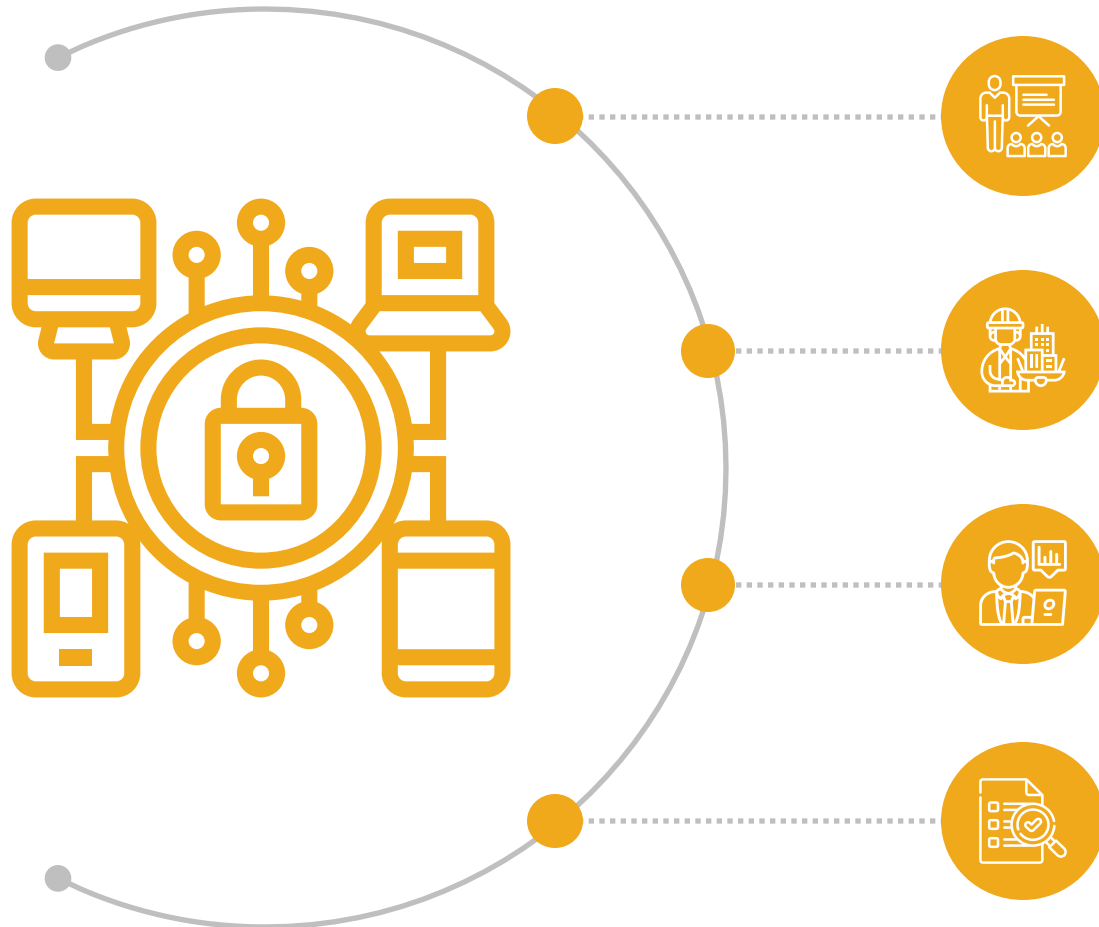
Products are now designed to be connected, all the time, everywhere. However, security is often not a primary consideration during the design phase. This creates a gap between industry standards and the actual product being deployed, hence presenting an important risk.

REEKON provides services to fill this gap by providing training, consulting, testing, and helping our partners reach certification for faster product launches.



Payment Security Services

How we help our clients



Training

- ▶ PCI / EMV / NFC

Design & Architecture

- ▶ Design Review
- ▶ Design Support

Consulting

- ▶ Documentation Support
- ▶ Technical Consulting

Testing (Pre/Post certif.)

- ▶ Penetration Testing
- ▶ Test Tools





PCI MPoC Certification Process



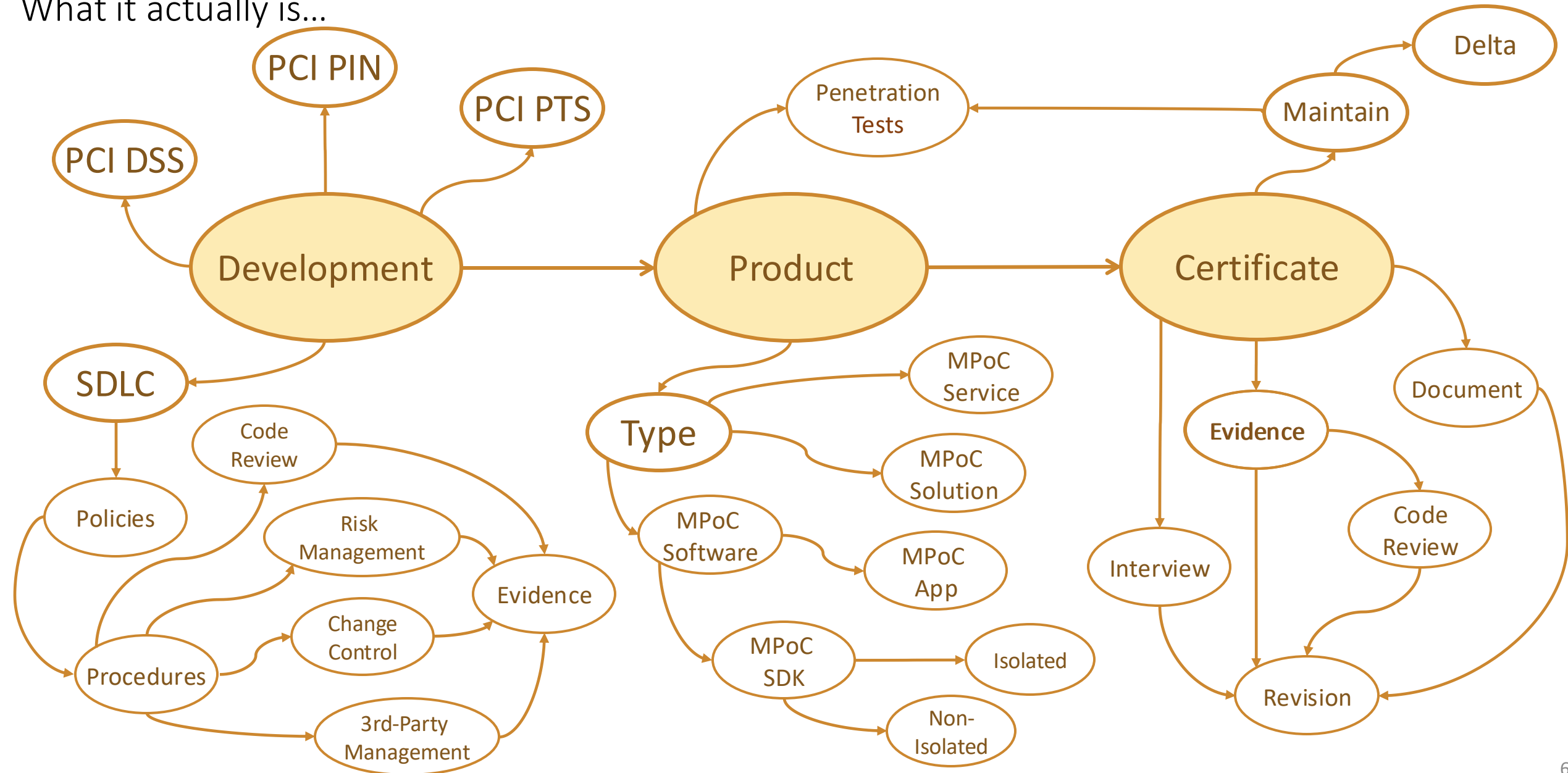
PCI MPoC Certification Process

What you might think...



PCI MPoC Certification Process

What it actually is...

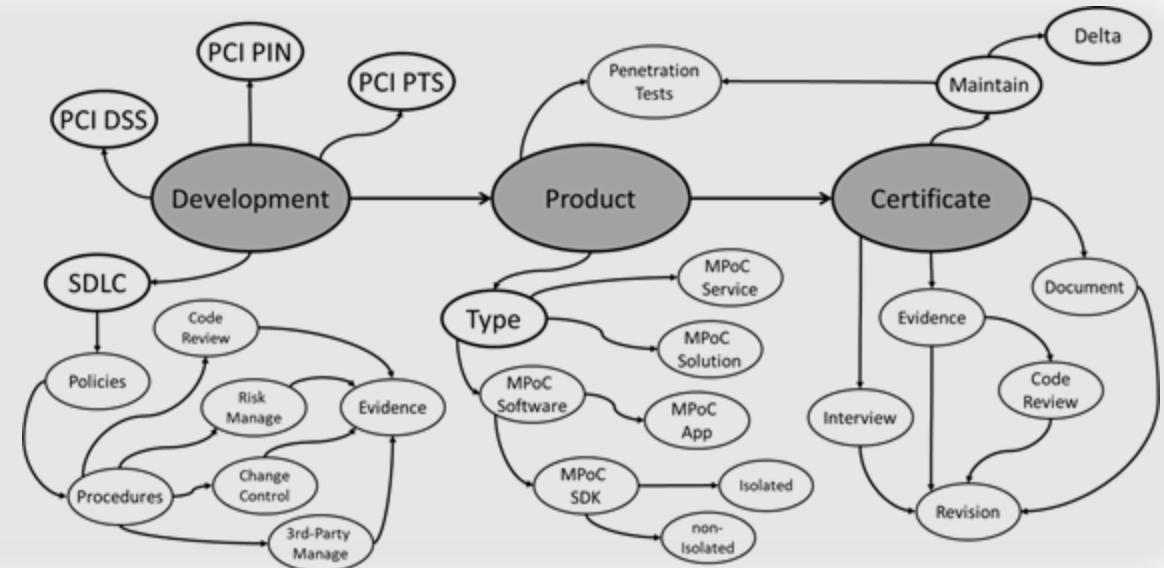


PCI MPoC Certification Process

Take away message

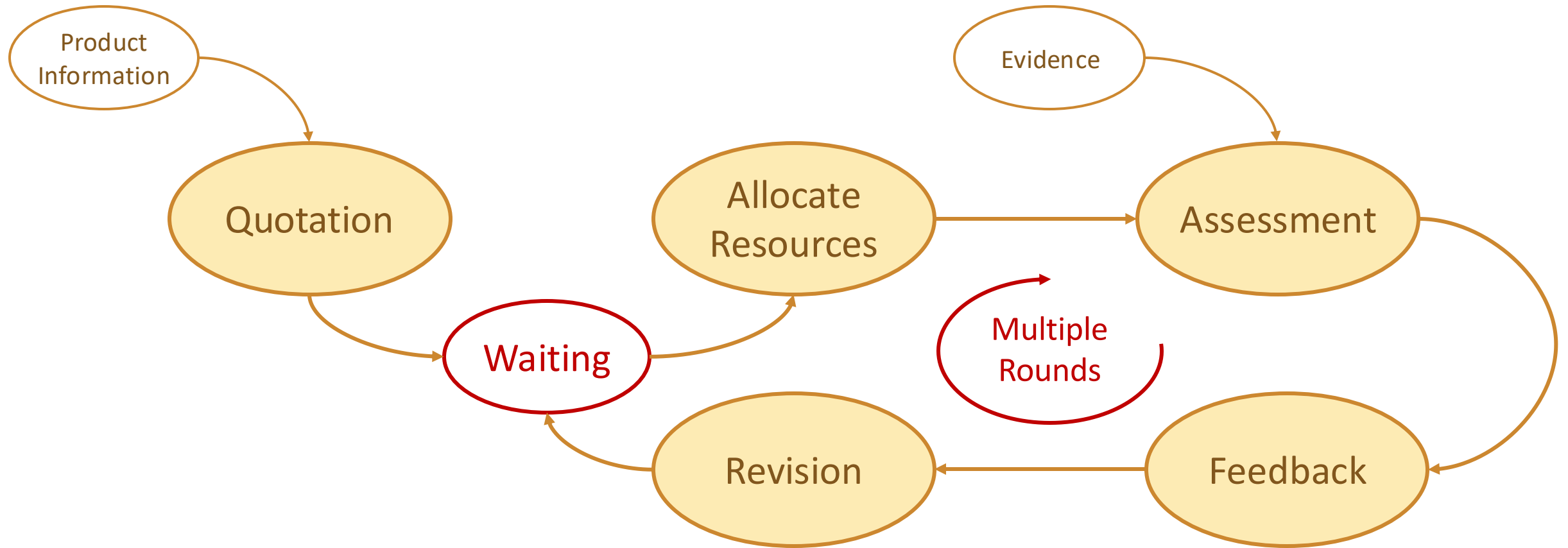
- PCI MPoC is not a requirement for the final product only
- PCI MPoC is a requirement for the entire life-cycle of the product, requiring certification activities and related processes to be continuous:
 - Develop
 - Certify
 - Maintain
 - Repeat

Every block is in scope of PCI MPoC



MPOC Accredited Laboratory

How it works and the status quo



MPOC Accredited Laboratory

Preparation and anticipation is key

- Laboratory availability differs from one to another at a certain time
- Multiple resources with different expertise are required for one MPoC project
- In case of major failure, project may enter a 'stop & go' phase during which fixes and solution updates might be necessary
- Evaluation timeline might be extended due to such iteration

- ✓ Time your evaluation well
- ✓ Anticipate laboratory review with internal checks and penetration testing
- ✓ Prepare a good evidence package and certification documentation

MPoC Requirement

Objective oriented

- The MPoC requirements are complicated and sometimes confusing

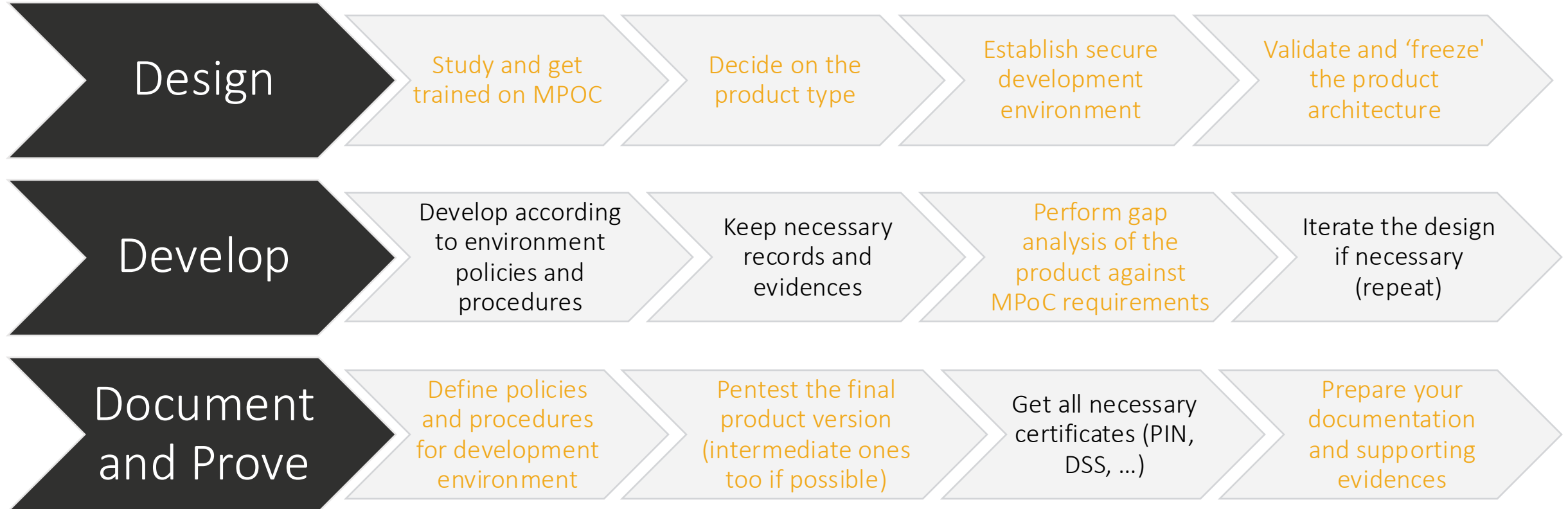


- Training is required to understand PCI's intention



Reekon's DOs and DON'Ts on Taking PCI MPoC Certification

Pre-evaluation phase



Ideal Process for PCI MPoC Certification

Evaluation phase



Submit the final product and evidence documents



Provide support to the security lab on their assessment



Take interview from the security lab



Address the feedback from the security lab



Revise the product when necessary



Security lab completes the evaluation report and submits to PCI



Help the security lab addressing PCI's inquiries



Get the PCI MPoC certificate

Key Parameters for PCI MPoC Certification

Post-evaluation phase

01

Perform regular vulnerability assessment

02

Perform annual penetration tests

03

Prepare for PCI MPoC annual check

04

Follow a change control policy for any modification

05

Request delta evaluation on security relevant changes

Common Issues

Architecture related

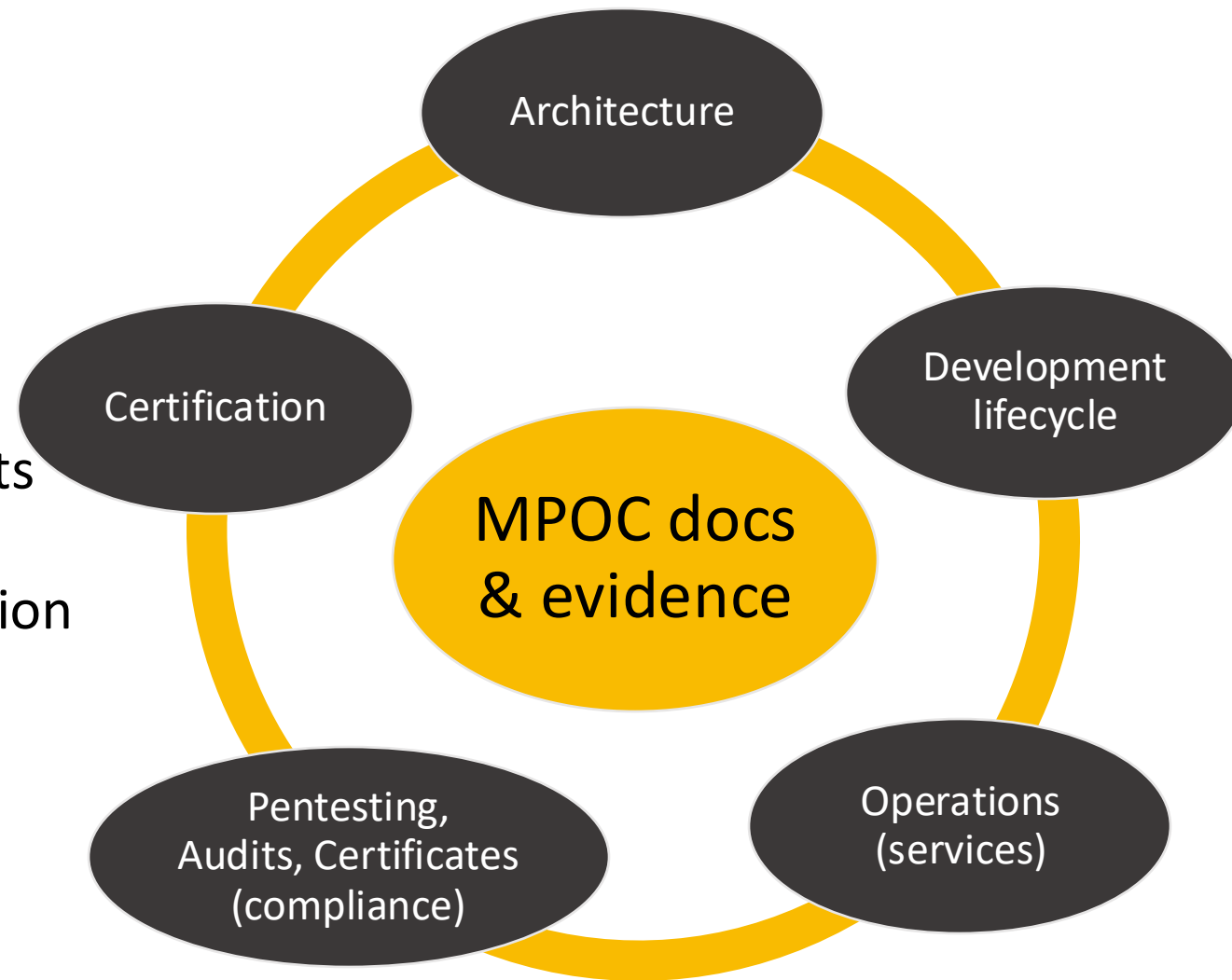
- Scope unclear
- SDK does not fully isolate the assets
- Missing mutual authentication for secure channel
- No real-time anti-tampering mechanism
- Bad key management
- Insufficient protection during transaction process



Common Issues

Evidence related

- Missing evidence
- Expired certificate
- Naming inconsistency between documents
- Inconsistency of implementation description between documents
- Policy and procedure not followed



Conclusion

Key takeaways

- Certification process can be confusing, thus planning in early stage of the project is crucial.
- Early engagement with security laboratory is essential for accurate planning.
- Timelines are usually longer than anticipated to complete the development and reach readiness for certification.
- While certification is the goal, pre- and post-certification continuity is also the reality.
- Finding right partners and stakeholders is the difference between success and failure.

