mojaloop

Mojaloop Quality & Security Workstream

PI-11 Mid-PI Progress Review Session – 11 September 2020

Presenter

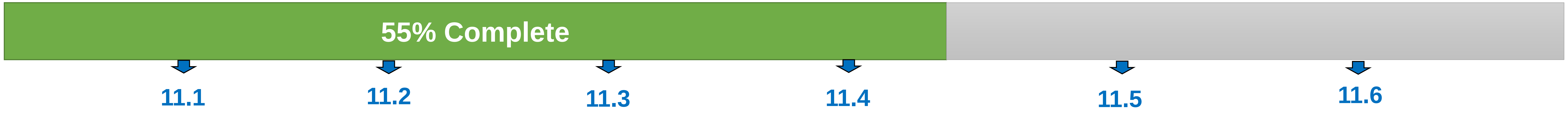
Godfrey Kutumela

Code Quality & Security (CQS) PI 11 Objectives

PI 11 objectives breakdown per epic

CQS Epic	Epic Objective (Multi-PI view)	PI 11 Objective
1. Functionality Support	Enhance security in new functionality additions	Review PISP and Portals security designs
2. Implementation Support	Support major implementations	Assist Mowali GDPR Compliance Initiative
3. Cryptographic Processing	Introduce a secure cryptographic processing	Deployment Planning – Low Level Designs
4. Data Protection	Improve data protection measures	Establish Data Protection Standards
5. Standard Baseline	Baselining of Mojaloop against industry standards	Finalize PCI DSS baseline recommendations
6. DevSecOps Integration	Maintain and enhance secure DevOps/CI CD practices	On going maintenance and enhancements
7. Community Engagement	Improve communication and community engagement	Restructure CQS documentation

Overall Progress



1. Functionality Support

PI objective – Security review of the PISP and Portals designs and ensure alignment with other CQS initiatives.

1. PISP - Core Functionality Support - PISP Initiation and Transfer Flows Security Review #1589

   Completed:

   - Detailed review and analysis of the PISP Linkage Flows (Tri-party Trust Model)
   - Identified areas of possible adjustments – Authentication and Consent Management process

   Outstanding Tasks:

   - On going review of all controls and measures - checking for any gaps in linking & transfer processes
   - How CPM can be leveraged – Current and future use cases.

2. Portals - Core Functionality Support - Mojaloop Portals for Hub Operations Design Review #1576

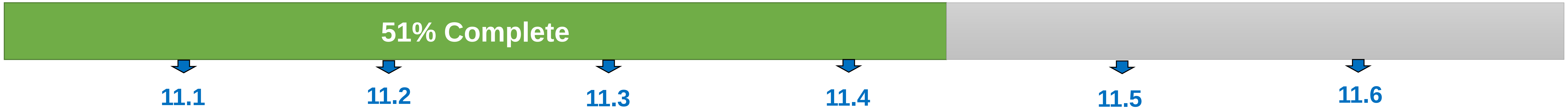
   Completed:

   - Risk and Threat Assessment Completed

   Outstanding Tasks:

   - Report analysis and documentation of gaps/requirements under way

Progress



2. Implementation Support

PI objective - Assist Mowali on the GDPR compliance initiative.

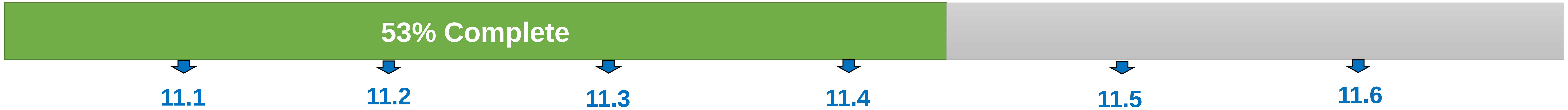
Completed:

1. Task 1 - Develop a Data Protection Impact Assessment framework and delivery model - Implementation Support - GDPR Data Protection Impact Assessment (DPIA) Guideline : Approach Note, Templates and Tools #1639

Outstanding Tasks:

1. Conduct DPIA using the below stories as examples – one each across all 4 key areas of GDPR DPIA:
    a) Implementation Support - Data Protection Impact Assessment (DPIA) : Establish Purpose for Processing PII in a P2P transfer (Same currency)# 1662 – On going now in sprint 11.4
    b) Implementation Support - Data Protection Impact Assessment (DPIA) : PII data assessment #1663 – On going now in sprint 11.4
    c) Implementation Support - Data Protection Impact Assessment (DPIA) : Establish a PII Access Management Framework #1664 – Planned for sprint 11.5
    d) Implementation Support - Data Protection Impact Assessment (DPIA) : Establish Data Retention and Deletion Rules #1667 – Planned for sprint 11.6

Progress



3. Cryptographic Processing

PI objective – Finalize the Cryptographic Processing Module (CPM) high-level design and plan deployment – Develop Low Level Designs.

Completed:

1) Updated the CPM High level Design (HLD) with a Key Update Adaptor to support any key management mechanism
2) DA approval granted on 12 August 2020 - Discuss the design approach of a standalone HSM capability for Mojaloop #62
3) Finalize and document CPM Use Cases - Cryptographic Processing Module (CPM) - Define supported use cases #1677
4) CPM LDD Framework - Cryptographic Processing Module (CPM) - Establish and approve a low-level design framework #1638

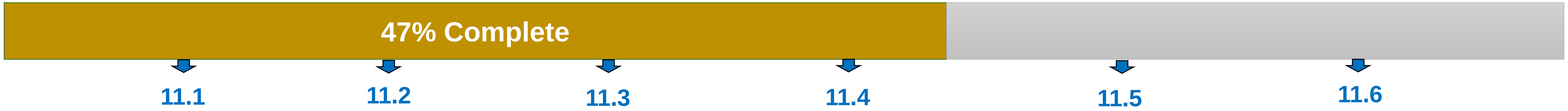
Outstanding tasks:

1) CPM LLD development - Cryptographic Processing Module (CPM) - Start with the low-level designs (LLD's) #1592 On going in sprint 11.4

CPM deployment supporting tasks:

1) CPM - Investigate design options and trust models for introducing CPM in the current P2P flow #1693 – Due to start in 11.5

Progress



4. Data Protection

PI objective – Provide data protection architectural improvements based on assessment findings from PI 10.

Completed:

1) Detailed analysis and documentation of Data Protection – PII and PCI DSS assessment findings from last PI - Data Protection - PII and PCI DSS Data Identification : Key Findings #1495

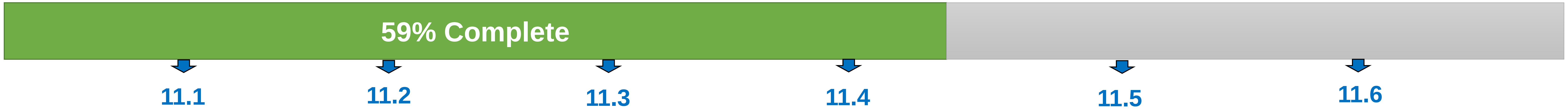
In Review/QA process:

1) Data Protection - Kafka/Zookeeper Security Standard and Guidelines #1359
2) Data Protection - Secure Logging Standard and Guidelines #1358

Outstanding Tasks:

1) Establish standard and guidelines for database protection – Target for sprint 11.4

Progress



5. Standard Baseline

PI objective – Propose additional controls and measures to improve our alignment to PCI DSS requirements.

Completed:

1) Standard Baseline - PCI DSS Section 1 : Build a Secure Network - Guidelines and Recommendations #1582
(Key Recommendations - Zoning and security groups, Web/API Gateway Protection and PIM for System Access Management)
1) Standard Baseline - PCI DSS Section 2: Protect Data - Guidelines and Recommendations #1583
(Key Recommendations – Alignment with data protection and cryptographic processing module epics outputs)

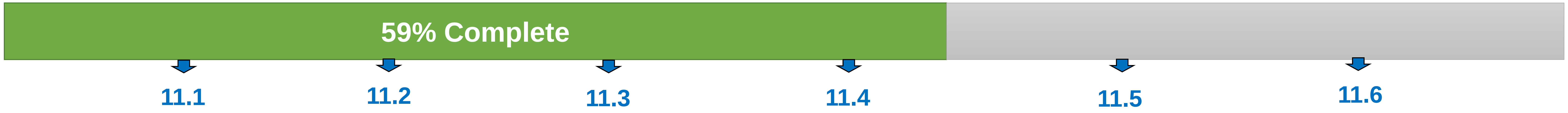
Review/QA:

1) Standard Baseline - PCI DSS Section 3 : Vulnerability Management – Guideline and Recommendations #1584
(Key Recommendations – Continuous maintenance and enhancement on the current vulnerability management measures at OSS level)

Outstanding tasks:

1) Standard Baseline - PCI DSS Section 4 : Strong Access Control - Guidelines and Recommendations #1585 – Target for sprint 11.4
2) Standard Baseline - PCI DSS Section 5 : Monitor Network - Guidelines and Recommendations #1586 – Target for sprint 11.5

Progress



7. DevSecOps Integration

PI objective – On going maintenance and enhancement of the DevSecOps processes, policies and tools and policies.

Completed:

1) Regular Security Patches + Updates – Regular Security Patches + Updates - August #1695
   - Addressing regular Dependabot alerts, running `npm audit` on flagged repos

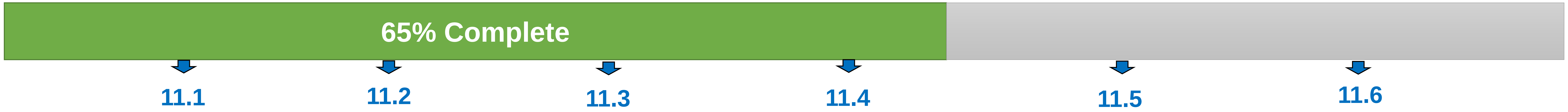
Planned Enhancements :

1) DevSecOps - Create a simple Security Alerts Dashboard #1398 - Simplify and summarize our security alerts into a single page.
   Investigating the possible use of Prometheus Github plug-in for data ingestion and Grafana for a monitoring dashboard

PI Backlog – Stretched Target:

1) DevSecOps - Investigate EFK SIEM capabilities for central logging and security reporting #1680
2) DevSecOps - Investigate Kubernetes security improvements (Alignment to security best practice) #1682
3) DevSecOps - Review current kurbenates audit logging setup and report on findings #1681

Progress



8. Community Engagement

PI objective – Review and restructure CQS related documentation across all information repositories for ease access

On going – Started in sprint 11.4

1) Review of all business and technical documentation

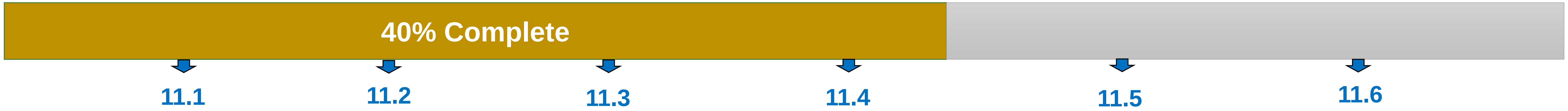
   a) Business information in the Scheme rules guidelines
      - Section 8 - Security, Risk Management, and Data Confidentiality
      - Appendix 16 - Risk Management, Security, Privacy, and Service Standards

   b) Technical
      - Issues – Review what info is created in the issues and how best approved items can be extracted and organized
      - Repos – Review repo specific reports from CI-CD CQS checks for security sensitive info

Targets for Sprint 11.5 & 6:

1) Propose a new documentation structure, views and taxonomy across all repositories (Mojaloop.io, Gitbooks, Github, Basecamps, Gdocs etc… – In line with the overall Mojaloop document taxonomy

Progress



muchas gracias

mojaloop

Thank you

Questions and Comments