RIPE NCC
RIPE NETWORK COORDINATION CENTRE

The RPKI Resiliency Project

Nathalie Trenaman | RIPE 81 | 29 October 2020

RPKI Resiliency Project

- Procedural and Operational Compliance
- RFC and Security Compliance
  - Future Work
- Certificate Practice Statement
- RPKI Repositories Resiliency
- Monitoring and Alerting
- Status Overview

Procedural and Operational Compliance

- Signed a contract with BSI to develop an RPKI audit framework
- SOC 2 Type II allows enough flexibility to tailor towards RPKI
- We will produce a SOC 3 report
- Goal is to have the framework finalised early 2021
- Another organisation will perform the actual audit

RPKI audit framework

Access control

Two-factor authentication

Network / application firewalls

Intrusion detection

Encryption

Access controls

Performance monitoring

Disaster recovery

Quality assurance

Processing monitoring

RFC and Security Compliance

- Goal is to gain insight into compliance with RPKI and cryptography RFCs as well as the security of the RPKI core, publication server and HSM interface module
- Radically Open Security performed an assessment between August and September 2020
- Report was delivered early October 2020

RFC and Security Compliance

- Result of the assessment was mostly positive, yet some issues have been found
  - “The implementation of RPKI-core complies with the RPKI RFCs to a high degree, although some issues are present.”
  - “The code bases of RPKI-core and the publication server are of high quality. The code bases have been nicely compartmentalized in discrete logic units, tied together in established design patterns. RPKI-core adheres to interface- based programming patterns, which allows for this compartmentalization. There is always a risk in over-engineering a program using the object oriented paradigm, but this hardly seems the case regarding this project. Methods generally do only one thing, and do it well.”

Future Work

- Crystal box penetration testing: performed on a system that is as close to the production system as possible
- Evaluation of the HSM: recommended to evaluate not only the physical device, but all security controls surrounding the HSM
- Red-team test: ask a security company to try to bypass physical defenses, gain entry to the facility, use social engineering to obtain key information, etc.
- Improvement of Unit Tests
- Improvement of Integration Tests

Certificate Practice Statement

- RIPE-549
- Last updated in 2012, needed an update
- Complete re-write, following RFC7382
- Current status: legal review
- Published before end 2020
- Special thanks to Legal, Ops and Tim Bruijnzeels

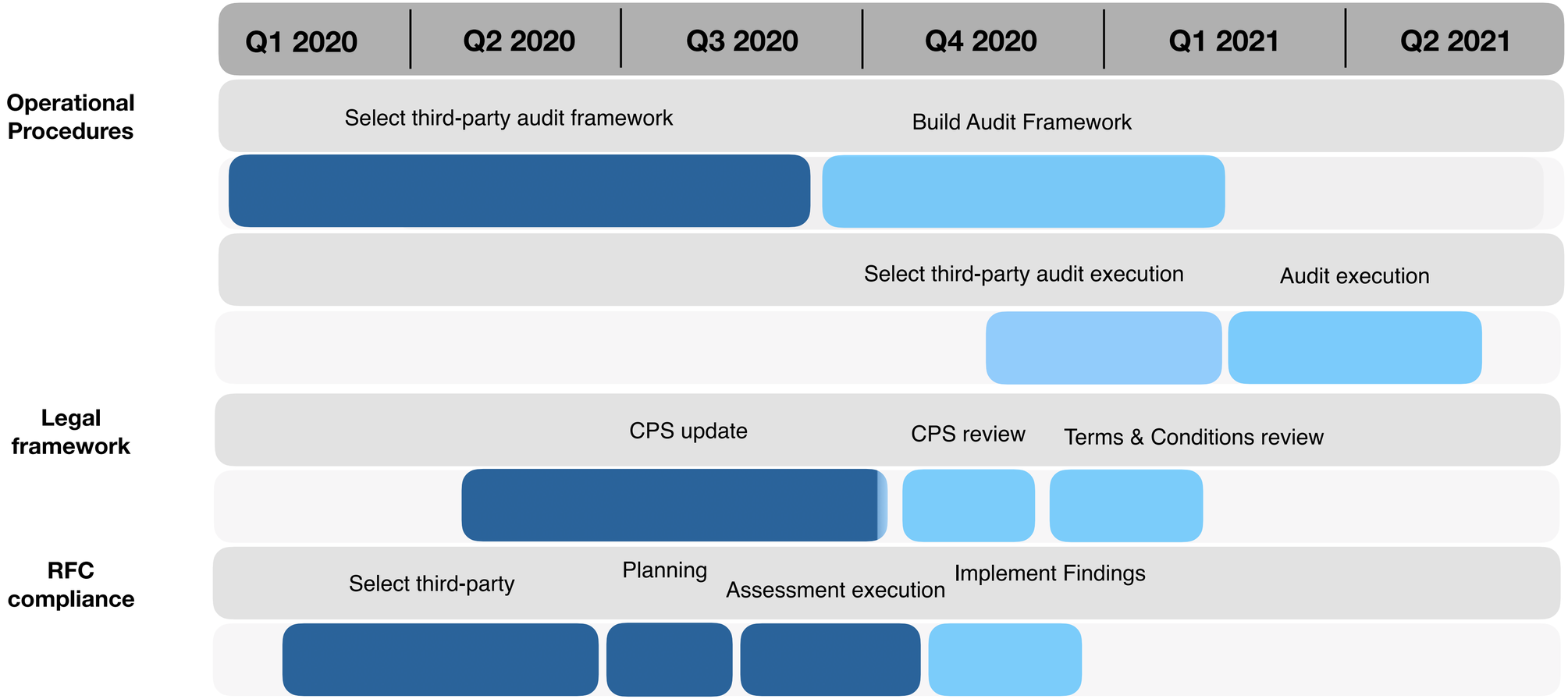
RPKI Repositories Resiliency

- Deployment of rsync into AWS in progress
  - Leveraging on multiple regions/availability zones, aiming for very high availability
- RRDP is already in AWS, but with a simpler architecture
  - Goal is to move RRDP to the same architecture as rsync
- Design and build back-up plan so we can fail over to our own infrastructure in case of catastrophic failure in AWS

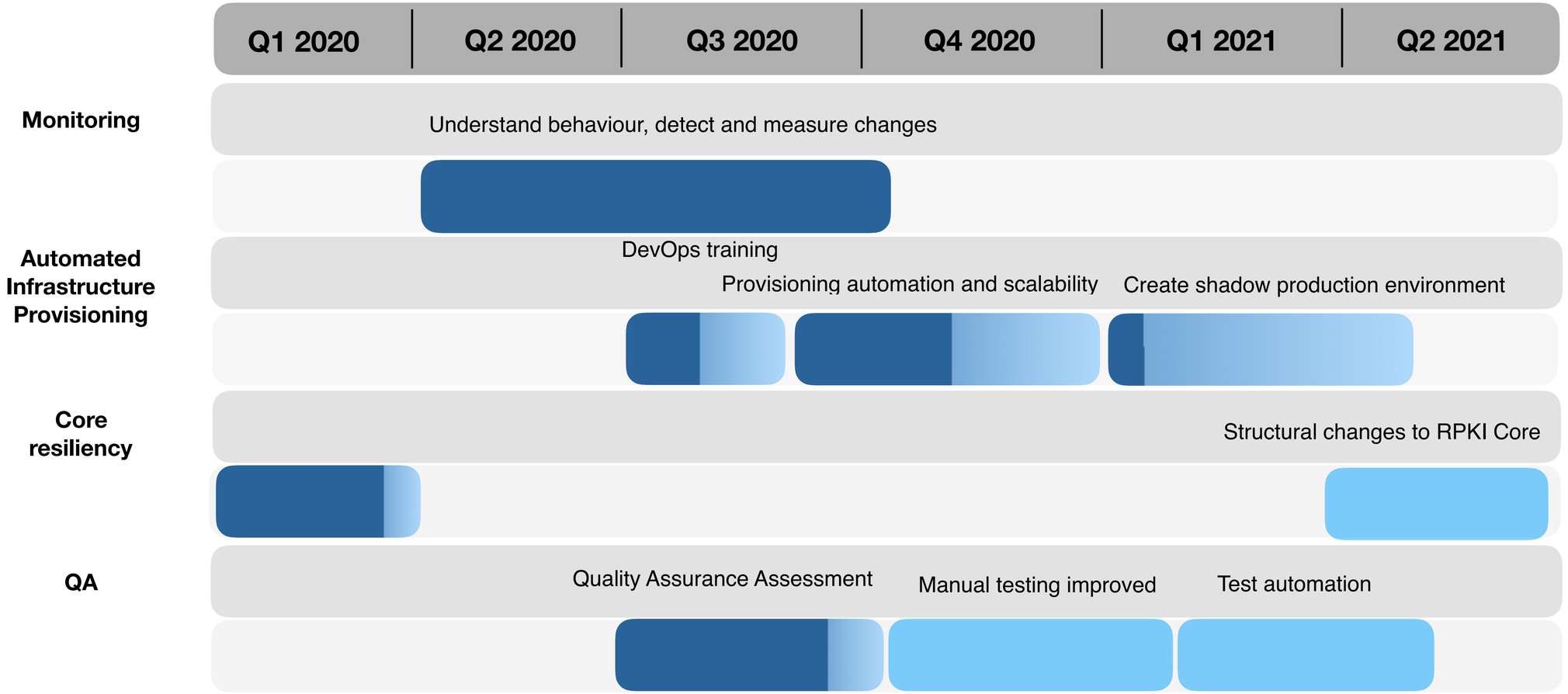
Monitoring and Alerting

- Following this years outages we have improved our monitoring and alerting
- Added and fine tuned many metrics
- Included a broader variety of validation tools
- This project is now finalised, but we keep fine tuning

Trust and Integrity



Technical Infrastructure



Questions

nathalie@ripe.net