

The Assessment Process



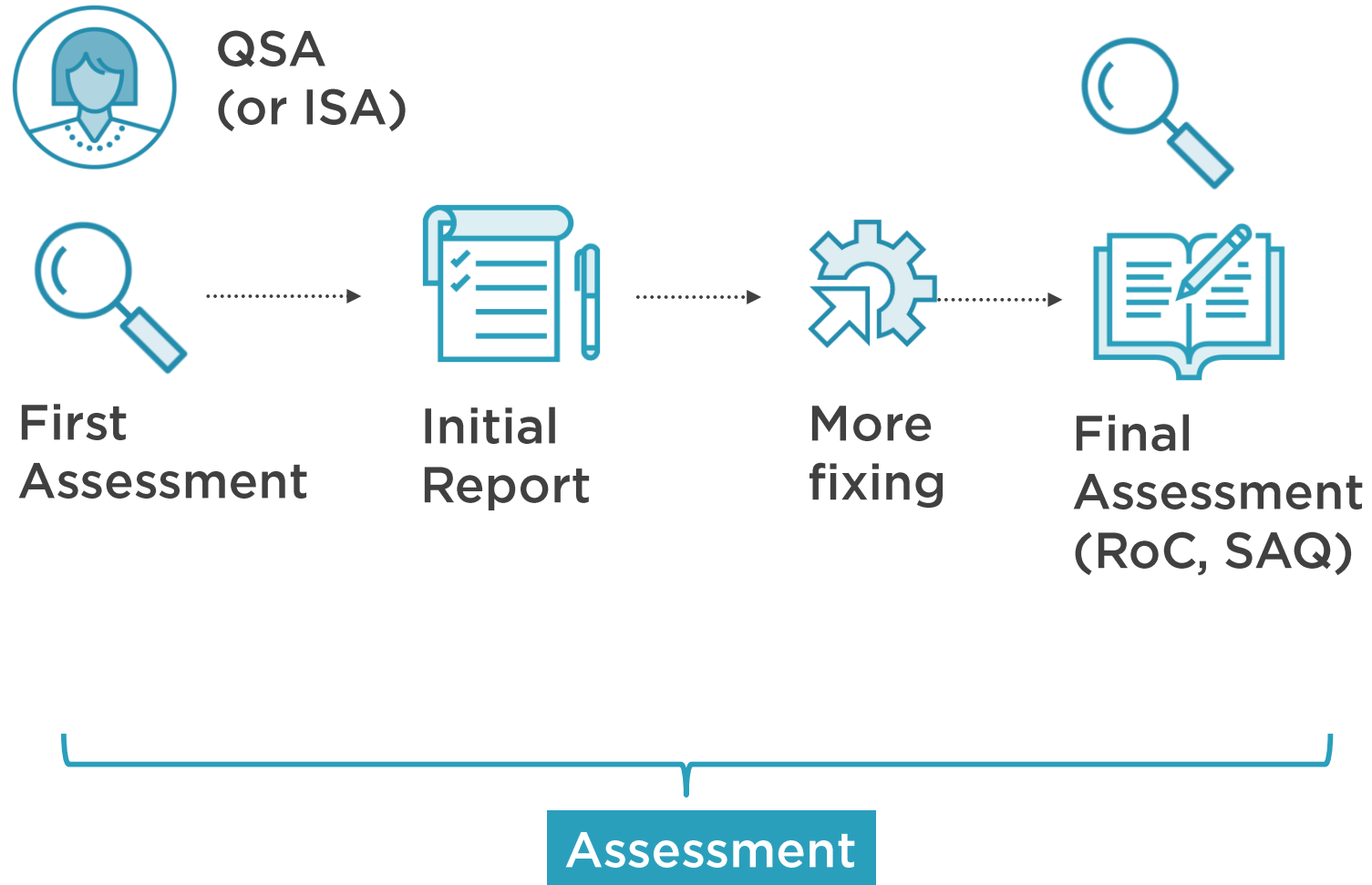
John Elliott

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire www.withoutfire.com



Almost There



QSA or ISA?



Based on brand (Mastercard, Visa etc) rules

ISA must generally be independent of the function specifying or managing controls

- E.g. Internal audit

Check with whoever is asking you to comply with PCI DSS



Prepare



Quiet space

Dual monitors

Somewhere to save screen captures

Printer

Which people on which days?

Send documents in advance

Agree schedule with the QSA

Think of the Poor Assessor



They will have X days allocated

- Some onsite, some for writing up

You are one of Y assessments in a month

Failure to prepare = prepare to fail

Make it easy for the assessor

They are people too ...

- You are equally responsible for their 'state'

Make sure your
people turn up

- on-time,
- engaged,
- cooperative



No
excuses



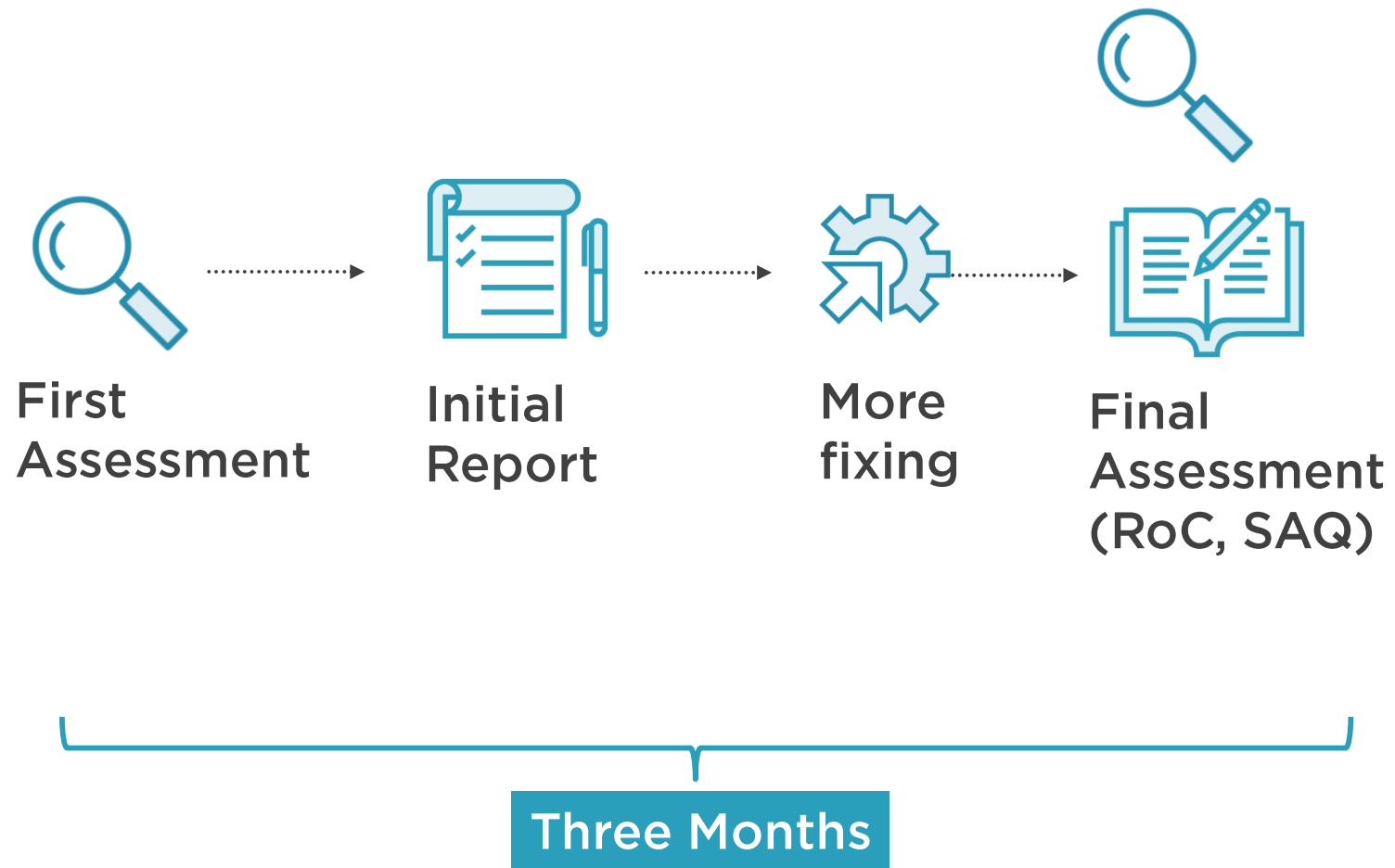


**First
Assessment**

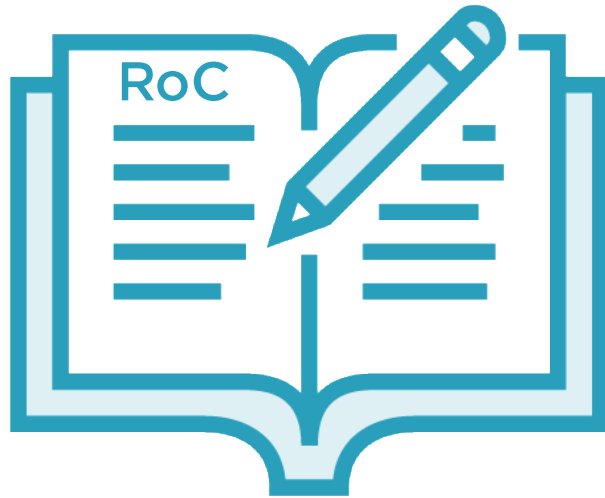


**Initial
Report**

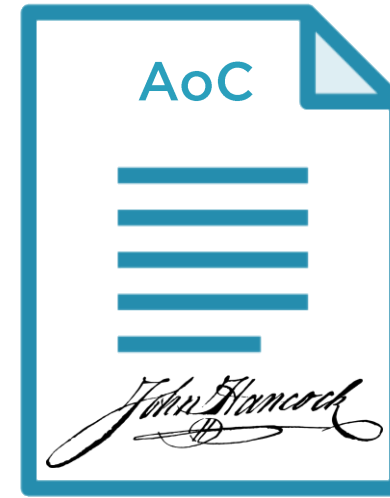




A Report and an Attestation



Report on Compliance
(RoC)



Attestation of Compliance
(AoC)

Assessments From a QSA



QSA Feedback



Next: Maintaining Compliance

