The 6 DORA Questions About Your Mobile App

A self-assessment for financial entities.

If you cannot answer these without calling your app team, your Register of Information has a gap.

A typical Nordics banking app contains around eleven third-party components, added by engineering over time to solve specific problems. Most arrived without a formal vendor assessment. Add the permissions the app requests, the servers it talks to and the data flows nobody mapped, and you have a live ICT environment your existing documentation simply doesn't describe.

THE 6 QUESTIONS

1. What third-party code is actually running inside our app this week?
2. Which components are new since last week's release?
3. Which permissions does the app really use, and which ones can we safely drop?
4. What data leaves the phone, where does it go, and is that consistent with what we've registered?
5. If a critical component in our app was compromised tonight, how fast could we disable it?
6. Which versions of our app are still available to customers, and when were they last risk-assessed?

HOW YOUR APP COMPLIANCE SOLUTION WOULD WORK

1 IT GETS THE APP FROM APP STORE

No source code. No work for your engineering team. Every new release triggers a fresh scan automatically.

2 IT TESTS IT LIKE A USER

Captures everything from third-party components, to data transfers and security weaknesses.

3 IT DELIVERS THE FACTS

You get an audit ready report. And the compliance bot makes it easy to fast forward the required ICT risk assessment paper work.

Want to check your mobile apps?

Or just talk more about DORA and your applications?
Reach out to me at regina@peakprivacy.eu

Product Lead | Security Compliance Specialist

PEAK PRIVACY