5G TACTIC Summer School on 5G Network Security

Scoring NordTel: questions to think with

Companion to the NIS2 Article 21 maturity self-assessment. Choose a level (0 to 3) for each measure and write your reasoning. Not a checklist with right answers.

Score NordTel as described, not an ideal operator. Pick the level you can defend from the scenario, then write why.

Separate what the scenario confirms from what it stays silent about. Some things are spelled out (the new RAN vendor, the open-source MANO); others say nothing (encryption, MFA). Where it is silent, you decide how to treat the missing evidence, and reasonable people land on different numbers. Defend yours.

One line per measure is enough. Name one concrete detail from the scenario and the first thing you would fix. A specific detail beats a paragraph, and writing it down is what makes you commit to a number instead of clicking on reflex.

0 · None	1 · Initial	2 · Defined	3 · Managed
Not in place. Topic not addressed.	Ad hoc. One person, by habit, nothing written.	Documented, applied consistently across the team.	Measured, reviewed, improved; audited regularly.

a Risk analysis & information security policies

- Is anything actually written down, or does it live in the IT team's heads?
- Has management signed anything off?
- Would one generic policy fit both a port and a hospital?

b Incident handling

- Is on-call for uptime the same thing as incident response for security?
- Is the 24h / 72h reporting path ready before something breaks?

c Business continuity & disaster recovery

- Does cloud resilience count, or only recovery objectives NordTel set and tested?
- What is the tested recovery time for the hospital telemetry?

d Supply chain security

- One vendor is covered, one is not. Is that a 1 or a 2?
- Is supplier risk in the contracts, or are you assuming it?
- Has the 5G Toolbox been applied to any vendor here?

e Security in acquisition, development & maintenance

- Who patches the open-source MANO, and how often?
- How does NordTel find out about a new vulnerability?

f Assessing the effectiveness of the measures

- Can NordTel be good at checking while weak everywhere else?
- Does anyone test the controls, or is it assumed?

g Cyber hygiene & security training

- Are you scoring the hygiene you can see, or the hygiene you assume?
- Does anyone outside the 8-person IT team get training?

h Cryptography & encryption

- Does cloud default encryption count, or do you need a policy and a key owner?
- The scenario says nothing about encryption. Is that a high score or a low one?

i HR security, access control & asset management

- Do you average the three parts, or does the weakest one set the score?
- Who can reach the MANO plane, and does the scenario tell you?

j MFA & secured communications

- Does the scenario confirm MFA on the admin accounts, or are you assuming it?
- Is there a secured channel to run an incident on?

Launch week

EVENT 1

- What did you take on trust when you first scored this?
- Does this change the evidence, or only your confidence in it?

EVENT 2

- What did you assume that you can no longer assume?
- What does this tell you that the scenario did not?

EVENT 3

- What were you giving NordTel the benefit of the doubt on?
- Which of your judgements does this put to the test?

TLP:GREEN