Overzicht van maatregelen in RTI v1.0 security awareness video:

- Zorg voor een directe verbinding tussen de beide endpoints. Omzetters (bijv. ethernet naar glasvezel) zijn toegestaan, wanneer deze uitsluitend voor het verbinden van de endpoints wordt gebruikt.
- Alle apparatuur van de netbeheerder die voor de RTI bij de klant geplaatst wordt, moet zich bevinden in een afgesloten ruimte die alleen toegankelijk is voor de netbeheerder. Dit kan dezelfde ruimte zijn waar de netbeheerder middenspanningsapparatuur heeft staan.
- Het endpoint aangeslotene mag via geen enkele interface rechtstreeks toegankelijk zijn vanaf het internet.
- Voor beheer op afstand van het endpoint aangeslotene moet een veilige oplossing worden gebruikt, welke is gebaseerd op extra maatregelen zoals VPN, jumpserver en multifactor authenticatie.
- Alle standaard wachtwoorden in het endpoint van de aangeslotene moeten worden vervangen voor unieke en sterke wachtwoorden.
- Minstens één keer per jaar moeten er security patches worden gedaan op de firmware van systemen van de aangeslotene en bekende kwetsbaarheden moeten worden verholpen.

Extra security maatregelen dienen geïmplementeerd te worden om het endpoint aangeslotene en achterliggende systemen voor andere risico's te beschermen. Denk hierbij aan standaarden zoals ISO 27001, IEC 62443 en IEC 62351.

Het is de verantwoordelijkheid van de aangeslotene om bovenstaande maatregelen te implementeren.

De aansluiting zal vanwege het verhoogde cyber security risico niet worden opgeleverd wanneer er aanwijzingen zijn dat niet aan de eisen of voorwaarden is voldaan.