

RAMBØLL

Bright ideas.
Sustainable change.

IT i praksis 2026

Er vi forberedt på det som kommer? Funn om sikkerhet og beredskap

NOKIOS 2026

TEK NORGE

Digdir

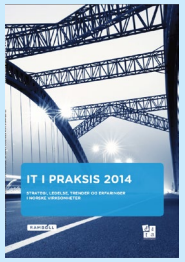
KS

NTNU

IT i praksis har fulgt utviklingen i offentlig digitaliseringsarbeid siste 20 år

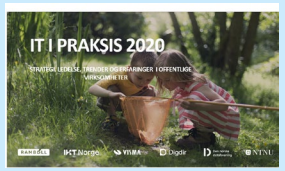


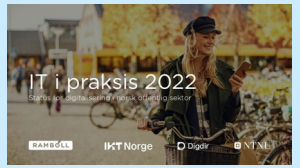






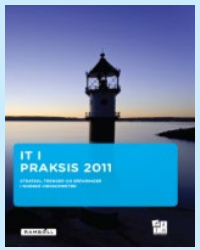




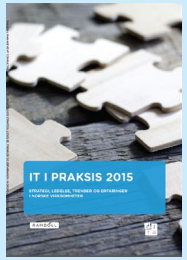






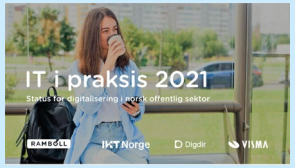


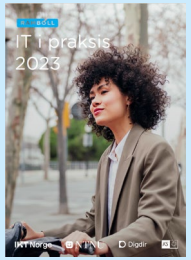














Norges største årlige undersøkelse om digitalisering i offentlig sektor



Utvikles av Rambøll, Digitaliseringsdirektoratet, KS, TEK Norge og NTNU



Gjennomført regelmessig de siste 20 årene



Virksomhetsundersøkelse til digitaliseringsansvarlige i statlige virksomheter og kommuner

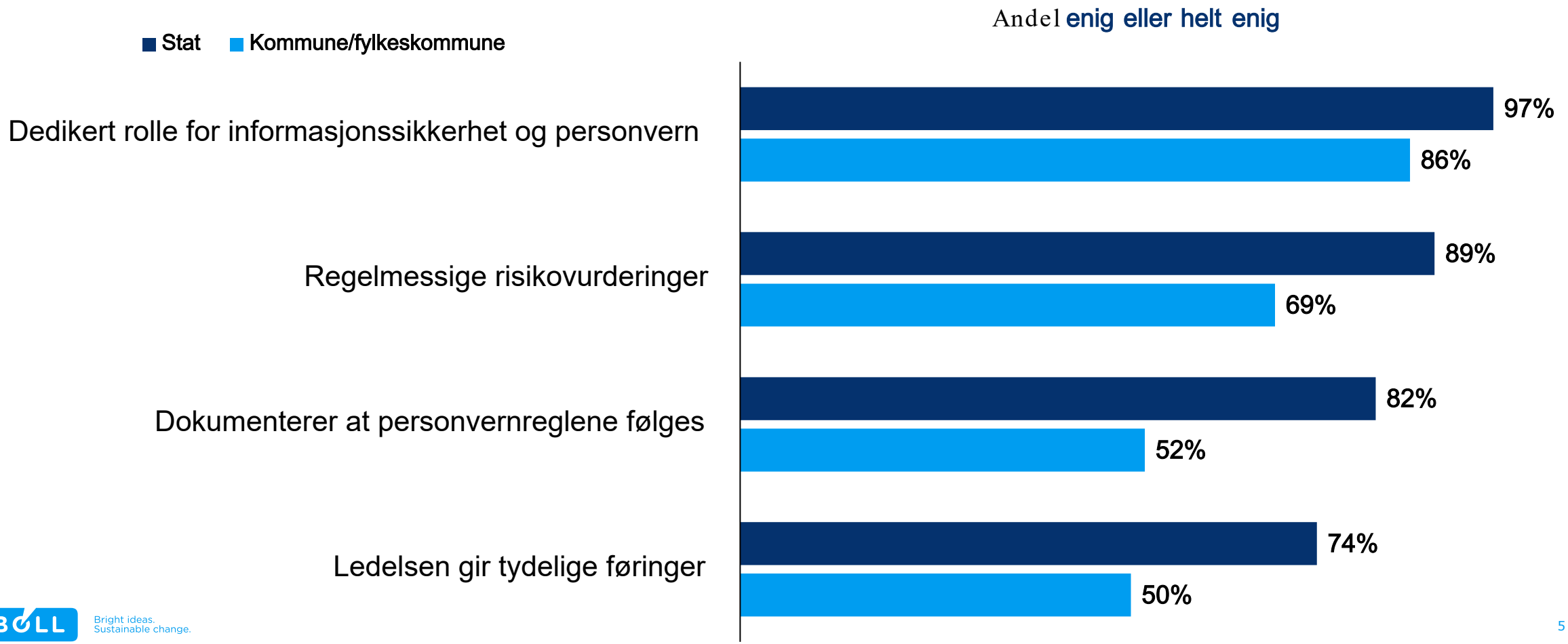


Innbyggerundersøkelse blant representativt utvalg av befolkningen

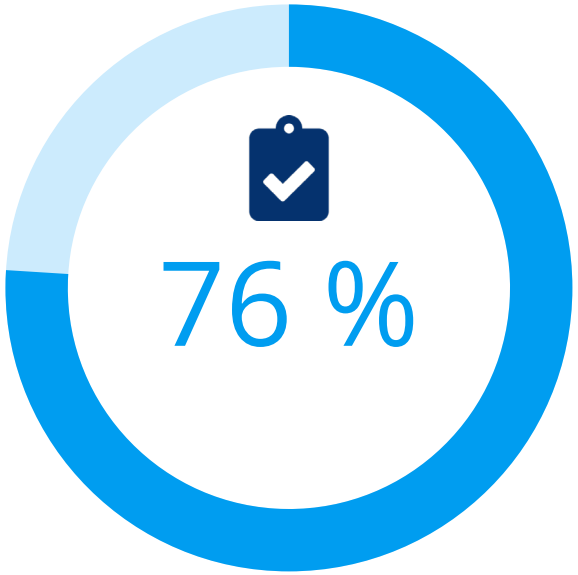
Fire hovedfunn

1. **Arbeidet med informasjonssikkerheten er i stor grad etablert**
2. **Et planverk om beredskap er ikke det samme som å være beredt**
3. **Styringssignalene er tydelige, men støtten oppleves som lav**
4. **Tillit fra befolkningen krever mer enn god forvaltning**

Sikkerhetsarbeidet er i stor grad etablert, kommunesektoren henger noe etter stat



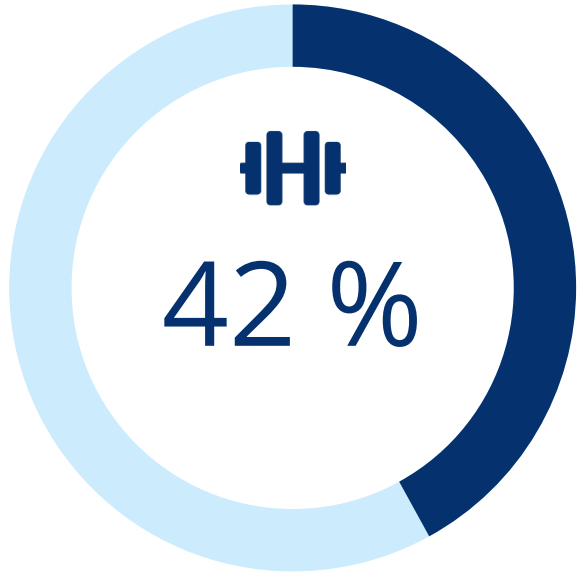
Å ha en plan er ikke det samme som å være beredt



har klare prosedyrer for å rapportere og håndtere cyberangrep

34

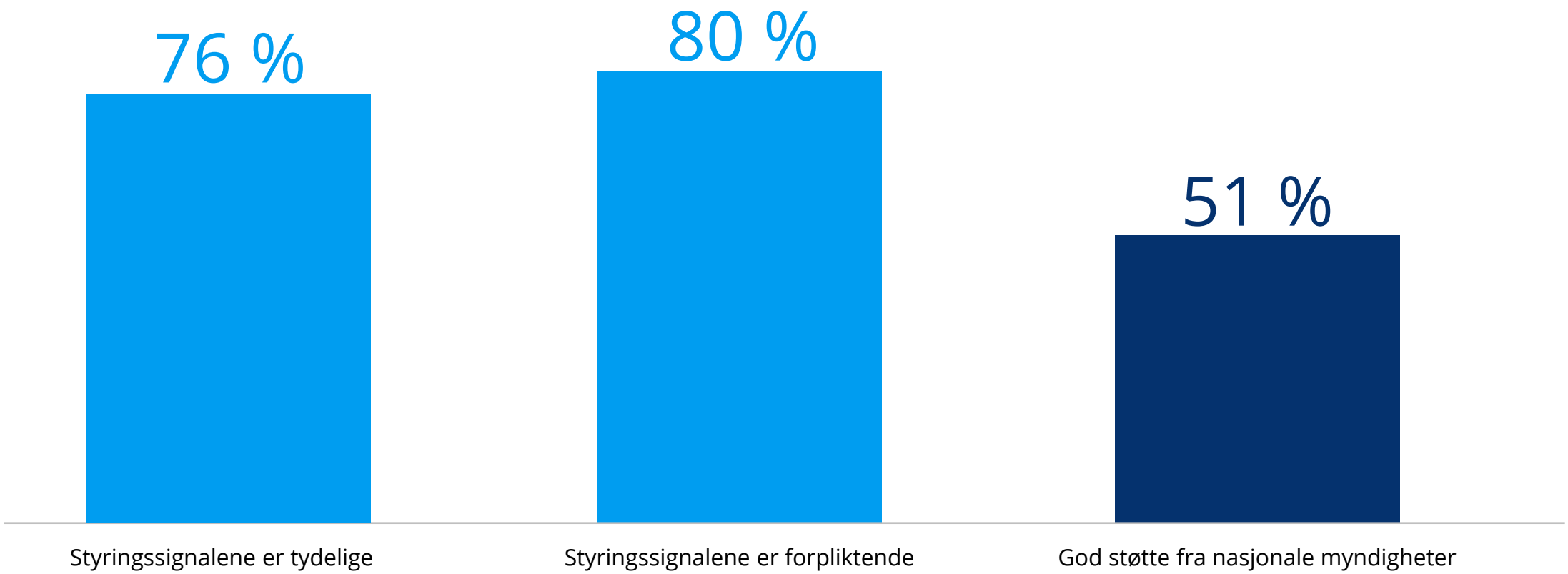
prosentpoeng fra plan til praksis



gjennomfører regelmessige øvelser for å håndtere cyberangrep

Signalene er tydelige, men må følges opp

Andel **enig eller helt enig** – informasjonssikkerhet

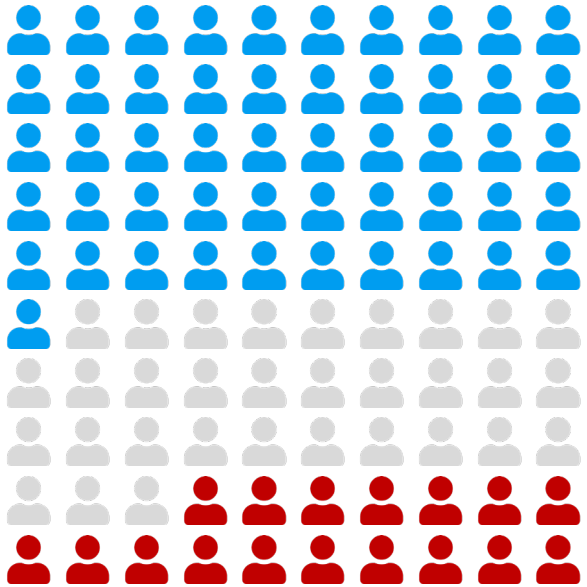


Tillit krever mer enn god forvaltning

Av **100 innbyggere** ...

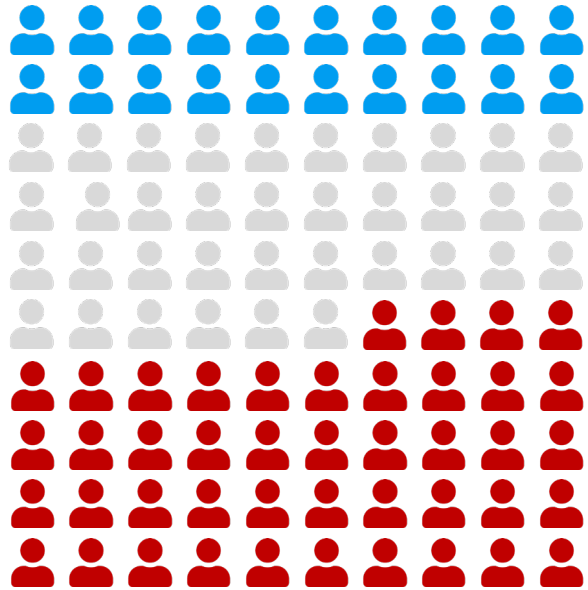
51

har tillit til at det offentlige ivaretar opplysningene deres trygt



44

har ikke tillit til at det offentlige er godt beskyttet mot cyberangrep



Det er bevissthet rundt hvor data lagres, men færre vurderer risikoer



har et bevisst forhold til hvilke data som lagres utenfor EU/EØS



har vurdert risikoen ved leverandøravhengighet og eierskap

CADA – Assurance levels



Cloud and AI Sovereignty Framework - consists of **4 assurance levels** cloud services shall meet to serve the public sector

All cloud services need to receive recognition by the national competent authorities on the basis of level specific assessment

Assurance level	Type of assessment
Level 1: Public sector data stays in Europe	Self-assessment
Level 2: Advanced measures to prevent 3rd country access to data and disruption of the service continuity	National authority based on 3rd party audit
Level 3: Providers must be owned and controlled from the EU. The Commission can recognise third-country providers	
Level 4: Full control over the software stack	

Strukturene er på plass.
Nå må de virke i praksis.



Thomas Nortvedt

Manager, Rambøll Management Consulting

thnr@ramboll.com

Les rapportene fra IT i praksis