Digital Transformation i Danmark 2026-2027

IT i praksis®



RAMBØLL

Bright ideas.
Sustainable change.

dansk•it

Indhold

Introduktion

04 Velkommen til Digital Transformation i Danmark 2026-2027, IT i praksis®

05 Om Digital Transformation i Danmark 2026-2027, IT i praksis®

06 Advisory Board

Strategiske udfordringer

10 Anvend containerisering som genvej til digital suverænitet

12 AI-modenhed kræver et bevidst valg af ambitionsniveau – ikke et kapløb mod fuld autonomi

14 Tag ansvar og styr risici, når AI rammer jeres virkelighed

16 Undgå at AI gør din it-organisation bedre til de forkerte opgaver

Digitale dagsordener

20 Geopolitisk uro bekymrer den offentlige sektor, men få handler på det

21 Fra skærpet trusselsbillede til reel handlekraft

22 Cyberangreb og værdi af AI-investeringer står øverst på risikodagsordenen

23 Øget modenhed i arbejdet med cybersikkerhed, men praksis følger ikke med

24 AI vinder frem internt i den offentlige sektor

25 Positive effekter ved kunstig intelligens, men besparelsen udebliver

26 Stigning i offentlige it-budgetter, men prioritering halter



Borgernes erfaringer og holdninger

30 Delte meninger om brug af kunstig intelligens i det offentlige

31 Kanalvalg afhænger af situationen – og borgerne ønsker valgmuligheder

32 Bred opbakning til digital suverænitet blandt borgerne

32 Utryghed ved det offentliges kriseberedskab

33 Usikkerhed om, hvordan data behandles af det offentlige

33 Tilfredshed med digitale services, men flere ønsker mere hjælp





Baggrund

34 Metode og datagrundlag

36 Om Rambøll Management Consulting og Dansk IT

37 Rambøll Management Consulting understøtter jeres digitale rejse

38 Kontakt og information

Velkommen til Digital Transformation i Danmark, IT i praksis®

2026-2027

For 31. år i træk har Rambøll Management Consulting, i samarbejde med Dansk IT, gennemført undersøgelsen Digital Transformation i Danmark, IT i praksis®, som belyser udviklinger, udfordringer og potentialer, som offentlige organisationer og private virksomheder står overfor i deres indsats for at opnå værdi gennem digitalisering.

It og digitalisering fylder mere og mere i mediebilledet, især når det handler om nøgletemaer som resiliens, digital suverænitet og cybersikkerhed. Danske offentlige organisationer og private virksomheder kæmper en vedholdende kamp for at være i spidsen, følge med og drage nytte af disse fremskridt. It- og digitale løsninger giver nemlig ikke kun udfordringer, men åbner også for samfundsmæssige muligheder inden for handlefrihed, effektivisering, værdi, sikkerhed og bæredygtighed.

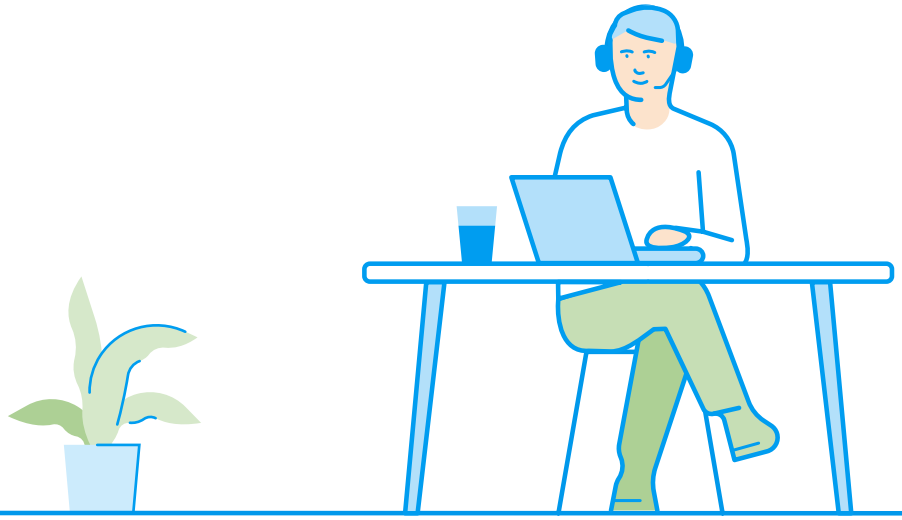
Disse emner er blandt de fokusområder, som fremhæves i denne udgave af IT i praksis®, hvor Rambøll og Dansk IT deler indsigter i digitale tendenser, udfordringer og muligheder i den digitale verden.

Gennem et dybdegående spørgeskema blandt it- og forretningsdirektører i den danske offentlige sektor bidrager IT i praksis® med værdifulde perspektiver på, hvordan organisationer kan forstå og håndtere digital suverænitet og strategi, cybersikkerhed, beredskab og resiliens, udvikling i digitale investeringer samt værdi og risici ved udnyttelsen af AI. På de følgende sider finder du inspiration baseret på rapportens nedslag i de strategiske udfordringer, som it- og forretningsdirektører står overfor, samt mulighed for at udforske digitale agendaer.

Ud over den danske rapport udkommer også en engelsksproget udgave, Digital Transformation in Denmark, IT in Practice, med fokus på den private sektor.

Vores Advisory Board er sammensat af en række topledere fra toneangivende myndigheder og virksomheder, som alle har bidraget til temaerne i årets udgave af IT i praksis®. En stor tak til alle Advisory Board-medlemmer for deres værdifulde indspil samt konstruktive respons.

Sidst, men ikke mindst, en stor tak til de topledere og it-direktører i offentlige organisationer og private virksomheder, som hvert år bidrager med viden og erfaringer gennem besvarelse af spørgeskemaer.



God læselyst!

Om Digital Transformation i Danmark 2026-2027, IT i praksis®

Digital Transformation i Danmark 2026-2027, IT i praksis® er anerkendt af førende CIO'er i Danmark. Årets CIO er en pris, der tildeles den CIO, som har været bedst til at lede teknologi som motor for vækst på en sikker, resilient og effektiv måde.

Claus Thomsen
CIO, Lundbeck
Årets CIO 2026

"AI udvikler sig hurtigt, og mulighederne er betydelige. Men én ting er blevet stadig mere klart for os: Den største udfordring er ikke selve teknologien. Det er, hvordan vi omlægger organisationen omkring den. Det ville være en fejl at behandle AI som endnu et it-projekt. Teknologien kan levere værktøjerne, men værdien skabes, når mennesker bruger dem til at arbejde anderledes, træffe bedre beslutninger og gentænke processer. Det kræver mere end platforme og data. Det kræver lederskab, nye kompetencer og en vilje til at udfordre eksisterende arbejdsmåder.

En af vores vigtigste erfaringer har været, at indførelsen af AI ikke kan drives af it alene. Vi har bevidst samlet kompetencer inden for teknologi, forretning og medarbejdere, fordi en vellykket indførelse i lige så høj grad handler om adfærd og organisatorisk forandring som om teknologi. AI er ikke et enmandsprojekt. Det betyder også, at vi skal gøre AI relevant for det daglige arbejde. Hvis det bliver for kompliceret, for kontrolleret eller for fjernt fra forretningen, vil indførelsen gå langsomt. Vi har brug for klare retningslinjer, enkle rammer og plads til, at medarbejderne kan eksperimentere, lære og dele, hvad der virker.

For mig er det her, den virkelige transformation finder sted. AI vil uden tvivl ændre vores teknologilandskab, men den største indvirkning vil måske være, hvordan vi organiserer os, samarbejder og leder. De virksomheder, der får succes med AI, vil ikke nødvendigvis være dem, der har adgang til den bedste teknologi. Det vil være dem, der er bedst til at forene teknologi, mennesker og forretning og omdanne nye muligheder til nye måder at arbejde på."

Claus Birkholm
CIO, NIRAS
Årets CIO 2025

"Det seneste år har vist os, at geopolitiske spændinger og usikkerhed ikke længere er noget, der kan ignoreres i danske it-afdelinger. Vi mærker konsekvenserne direkte, både i forhold til leverandørkæder, datasikkerhed og det øgede behov for agilitet i vores it-strategier. Parallelt hermed er der åbnet helt nye muligheder med GenAI, lettere adgang til ML og automatisering. De nye trusler og muligheder har gjort, at forretning og it aldrig har været tættere forbundet end nu, hvor evnen til at integrere og udnytte nye teknologier hurtigt kan gøre forskellen på at være på forkant eller blive hægtet af. Det stiller krav om, at vi som CIO'er tager hånd om resilience og griber de muligheder, som GenAI og automatisering giver – fra smartere dataanalyse til hurtigere beslutningsprocesser og mere effektive og sikre arbejdsgange. Transparens, fleksibilitet og evnen til at omstille sig er blevet nøgleord, og det kræver, at både ledelse og it-organisation tør tænke nyt og handle med omtanke. Jeg ser frem til at modtage dette års IT i praksis® med inspiration til, hvor vi sammen kan finde løsninger på de komplekse udfordringer, vi står overfor."

Martin Wood
CIO, Courts of Denmark
Årets CIO 2024

"Ingen organisation kan længere betvivle den strategiske vigtighed ved at mestre digitaliseringens muligheder, uanset om den leverer offentlige, borgervendte løsninger eller anvendes til at fremme nye forretningsmodeller og profit.
Forretning og it er konvergeret i et nødvendigt og ufravigeligt samspil, som er afgørende for succes. Men strategiske valg og kompetent ledelse af it er fyldt med dilemmaer og svære beslutninger om fremtiden. IT i praksis® tilbyder en nærværende og relevant afdækning af branchens trends og fokusområder og bidrager derigennem til at reducere usikkerheden og bedre navigere i dilemmaerne. Med erfaring og viden bliver det lettere at fatte mod til at søge nye veje til god digitalisering – noget jeg er stolt af, at vi har praktiseret."

Susanne Schustin
Global CIO, CEVA Logistics
Årets CIO 2023 (Blue Water Shipping)

"It's rolle i organisationen har længe været under udvikling væk fra blot at være en nødvendig omkostning til i dag at være det, der muliggør digitalisering, innovation og nye forretningsmodeller. Det stiller nye krav og kræver nye færdigheder af både it-medarbejderne og CIO'en selv. Vi går fra udelukkende at drifte og udvikle services til at skulle mestre at guide og rådgive vores organisation, ledelse og bestyrelse om, hvordan digital transformation kan muliggøre virksomhedens strategiske mål. I mit eget arbejde med at bygge it-forretningspartnerskaber har IT i praksis® været en værdifuld kilde til viden og kompetenceudvidelse, så mine teams har evnet at tage denne nye rolle på sig."

Advisory Board

Dette års bidragsydere og medlemmer af Advisory Board for Digital Transformation i Danmark, IT in praksis®.

Offentlig sektor

Anders Carlsen
Fagdirektør i Udviklings- og Forenklingsstyrelsen under Skatteministeriet

Klaus Larsen
Programdirektør
Sundhedsdatastyrelsen

Kristian Vengsgaard
CEO
KOMBIT

Lars Frelle-Petersen
Departementschef
Klima-, Energi- og Forsyningsministeriet

Lone Juric Sørensen
Chef for fælles it og digitalisering
Aarhus Kommune

Mette Lindstrøm Lage
Afdelingschef og chef for den digitale taskforce for kunstig intelligens
Digitaliseringsministeriet

Michael Ørnø
Direktør
Statens IT

Mikkel Hemmingsen
CEO
Sund & Bælt

Peter Bruun Nielsen
Vicedirektør for AU IT
Aarhus Universitet

Rikke Hougaard Zeberg
Direktør
Klimadatastyrelsen

Willy Kofoed
Kontorchef
Fødevareministeriets Departement

Privat sektor

Alan Jensen
CIO & Executive Vice President
Salling Group

Carl-Erik Vesterager
CIO
Nordic RCC

Charlotte Hersdorf
CIO
Nordea Finans

Daniel Skovsbo Erichsen
CDO
N1

Haktan Bulut
CITO
ATP

Jens Hartmann
CIO & Group Vice President
Grundfos

Kasper Sckerl
Vice President & Head of IT
Operations & Platforms
Danfoss

Nicolas Skovmand
CIO
Bestseller

Pernille Geneser
Professionelt bestyrelsesmedlem
& tidligere CIO

Rasmus Lundgaard Pedersen
CIO
OK a.m.b.a.

Ronni Cavling
Data, Automation & AI Lead
Andel

Steen Guldborg
Group IT Manager
Per Aarsleff

Søren Kofoed Weeke
Tidligere CIO & Executive
Vice President
SOS International

Torben Bonde
Professionelt bestyrelsesmedlem
& tidligere CIO

Torben Kjær
Professionelt bestyrelsesmedlem
& tidligere CIO



Strategiske udfordringer



Digital Transformation i Danmark, IT i praksis® perspektiverer de strategiske udfordringer, der kendetegner en tid med geopolitisk usikkerhed og konstant teknologisk udvikling. Og det kræver handling, hvis organisationer skal forblive konkurrencedygtige. Hertil kommer forpligtelsen til at efterleve rammeværker for ansvarlig brug af AI. I takt med stigende fokus på digital suverænitet og AI introducerer IT i praksis® værktøjer og handlepunkter til at imødekomme udfordringer.

Den digitale tidsalder medfører en række strategiske udfordringer, som succesfuldt skal håndteres af offentlige organisationer og private virksomheder for at kunne gennemføre deres kerneaktiviteter og øge værdiskabelsen.

Årets strategiske udfordringer inden for digitalisering er identificeret af Rambøll gennem kundeprojekter og i dialog med erhvervsledere. Her fremhæves de indsatsområder, som er væsentlige for ledelsen i såvel offentlige organisationer som private virksomheder at fokusere på. I denne sektion præsenterer IT i praksis® indsigt ind i de strategier og værktøjer, som kan understøtte offentlige organisationer og private virksomheder i mødet med disse udfordringer.

Det nuværende geopolitiske billede medfører yderligere krav til offentlige organisationer og private virksomheder. IT i praksis® fremhæver især udfordringer i målsætningen om digital suverænitet, hvor balancen mellem handlefrihed og integrerede løsninger kræver stærke strategiske prioriteringer og risikostyring.

Derudover vokser fokus på AI fortsat, hvilket giver en række udfordringer relateret til etik og ansvarlighed. Tæt koblet til dette, fokuserer IT i praksis® også på, hvordan AI-anvendelsesniveau måles i organisationen og et effektivt værktøj, der kan anvendes til dette.

På de følgende sider præsenteres et konceptuelt rammeværk og en række konkrete handlepunkter for hver af de strategiske udfordringer.

Strategiske udfordringer i Digital Transformation i Danmark, IT i praksis®

01 Anvend containerisering som genvej til digital suverænitet

02 AI-anvendelse kræver et bevidst valg af ambitionsniveau – ikke et kapløb mod fuld autonomi

03 Tag ansvar og styr risici, når AI rammer jeres virkelighed

04 Undgå at AI gør din it-organisation bedre til de forkerte opgaver

Anvend containerisering som genvej til digital suverænitet

Digital suverænitet er ikke noget, man har eller mangler – det er en skala, man bevæger sig på. Containerisering gør ikke en organisation suveræn i sig selv, men kan være den mest praktiske vej til at gøre exitplaner til reel handlefrihed og samtidig modernisere ældre fagsystemer.

Spørg en direktion, om organisationen kan flytte sine kritiske systemer til en anden leverandør, og svaret er som regel: "i teorien". I praksis kunne de færreste gøre det inden for få måneder. For en offentlig organisation handler det ikke kun om økonomi, men om forsyningssikkerhed, retssikkerhed og borgernes tillid.

Suverænitet er en skala, ikke en status

Digital suverænitet er ikke noget, man enten har eller mangler. Ingen organisation kommer til at operere udelukkende på teknologi, den selv kontrollerer, og det bør ikke forsøges. Det realistiske mål er en grad af leverandørafhængighed, som ledelsen kan acceptere: Hvor et skifte, hvis det bliver nødvendigt, er krævende, men muligt. Tjenester kan få ny pris, blive begrænset eller trukket tilbage fra dag til dag, og data om borgere kan blive omfattet af udenlandsk lovgivning. Værdien ligger i muligheden for at skifte. Den bruges måske aldrig, men styrker både forhandlingsposition og robusthed. Det er også et ledelsesansvar, da NIS2-loven placerer ansvaret for risici i leverandørkæden hos ledelsen, og i en udbudsverden skal exitmuligheder sikres, før kontrakten underskrives.

Hvad er containerisering?

Tænk på skibscontaineren. Før skibscontainerens udbredelse blev hver last pakket forskelligt. Med containere kan samme last flyttes fra skib til tog til lastbil uden at blive pakket om. Softwarecontainere gør det samme for applikationer. Hver applikation pakkes med alt, hvad den skal bruge, i en standardiseret enhed baseret på åbne branchestandarder og bygget med værktøjer som Podman eller Docker. En orkestreringsplatform – i dag næsten altid open source-løsningen Kubernetes – afvikler og styrer derefter de enkelte enheder. Fordi containeren er ligeglad med, hvad der ligger under den, kan samme løsning køre hos en global cloud-udbyder, en europæisk leverandør, i et fællesoffentligt driftscenter eller i eget datacenter.

Fleksibilitet er en form for suverænitetsvaluta

De fleste debatter om suverænitet handler om, hvor data ligger. Containerisering gør det muligt at stille et mere nyttigt spørgsmål: Hvor let kan vi flytte? Når løsninger er containeriserede og kører på standard Kubernetes, bliver cloud-udbyderen et udskifteligt lag frem for et fundament. Exitplaner bliver noget, man kan teste og ikke blot dokumentere. Hybride løsninger bliver realistiske, med følsomme borgerdata på suveræn eller egen infrastruktur og øvrige data, hvor det giver mest mening. Og leverandørdialogen ændrer sig, når begge parter ved, at man kan skifte – også til næste udbud.

Mere end en gevinst

Tre yderligere gevinster styrker argumentet for containerisering.

Modernisering og kompetencer. Med containerisering flyttes ældre fagsystemer over på teknologi, som nyuddannede allerede kender, mens ekspertisen i aldrende platforme går på pension. Forandringen forsvinder dog ikke – den flytter sig, da driften skal arbejde på en ny måde.

Sikkerhed. Softwarecontainere er ingen fæstning, da de deler det underliggende operativsystem. Til gengæld er standardiserede byggeprocesser, hurtigere opdateringer og tydeligere adskillelse mellem systemer med til at give bedre styring og overblik end et uoverskueligt, ældre systemlandskab.

Robusthed. Evnen til at genetablere løsninger et andet sted er en reel beredskabsevne. Når en leverandør, en region eller et datacenter svigter, bliver portabilitet til genopretning – netop den robusthed, som NIS2 og CER lægger op til.

Realitetskontrol

Softwarecontainere gør løsninger flytbare, men afhængigheden forsvinder ikke – den flytter sig. Den flytter ind i de databaser, identitetstjenester og proprietære funktioner, der omgiver containerne. Den flytter ind i leverandørspecifikke udgaver af Kubernetes. Og den flytter ind i data, som er tunge og dyre at flytte. Suverænitet er aldrig stærkere end den mindst flytbare afhængighed. Containerisering skal derfor kombineres med bevidste valg i alle lag af stakken: åbne standarder, flytbare datatjenester og identitetsstyring, man selv kontrollerer. Frigøres cloud-laget, mens man forbliver låst andre steder, er problemet blot flyttet – ikke løst.

Ikke alt bør containeriseres. Mainframe-løsninger, store monolitiske fagsystemer og standardsoftware uden leverandørsupport bør ofte forblive, som de er – eller udskiftes. Og Kubernetes er komplekst. Uden et dedikeret platformteam, der leverer containere as-a-service, kan kompleksiteten hurtigt overstige gevinsterne.

Bundlinjen

Containerisering er ikke en suverænitetsløsning i sig selv. Det er et greb. Brugt rigtigt, er containerisering med til at bringe exitstrategier fra papirløfter til reel handlefrihed, samtidig med at systemlandskabet moderniseres, og sikkerheden styrkes.

Brugt ukritisk bytter man blot en afhængighed ud med en anden. For den offentlige sektor handler det i sidste ende om at kunne levere til borgerne, uanset hvad der sker i verden. Hvor data ligger, betyder noget – men hvor let man kan flytte, betyder mere.

Hvordan containerisering ændrer afhængigheden

Containerisering har størst effekt midt i teknologistakken. Organisationens samlede suverænitet afgøres af lag med højest afhængighed. Derfor kræver hvert lag et bevidst valg.

TEKNOLOGISTAK	AFHÆNGIGHED	ÆNDRING OG GEVINST
SaaS og slutbrugerværktøjer	**Høj**	Ingen direkte effekt, men frigør kapacitet til at håndtere disse separat.
Applikationer	**Lav**	Pakkes som flytbare, standardiserede enheder, hvilket giver mulighed for modernisering samt tilpasning til nyuddannedes kompetencer.
Identitet og sikkerhed	**Middel** Identitet ofte bundet til leverandør	Ingen direkte effekt på identitet; tydeligere adskillelse af systemer samt potentiale for hurtigere patchning.
Orkestrering (Kubernetes)	**Lav** ved standardudgave; høj ved proprietær udgave	Et fælles styringslag på tværs af miljøer, hvilket medvirker til samme driftsform overalt.
Cloud-platform (IaaS)	**Lav**	Udbyderen bliver et udskifteligt lag, medfører exitmuligheder, hybride løsninger og øget forhandlingsstyrke.
Data	**Høj** Datatyngde og omkostninger ved flytning	Databaser kan køre i containere, men data skal stadig migreres. Til gengæld bliver åbne alternativer som PostgreSQL mere realistiske.
Fysisk infrastruktur	**Middel** Forsyningskæde for hardware	Samme løsninger kan køre i eget, fællesoffentligt eller eksternt datacenter, og hjemtagning og egen drift bliver muligheder.

Handlepunkter

- Mål exitparathed, ikke intentioner. Identificer kritiske løsninger og vurder, hvor lang tid, hvor dyrt og hvor forstyrrende et skifte vil være. Lad ledelsen beslutte, hvilken afhængighed der er acceptabel.
- Standardiser på åbne fundamenter. Åbne containerstandarder og certificeret, leverandøruafhængig Kubernetes. Behandl proprietære udgaver og tillægstjenester som bevidste kompromiser, ikke standardvalg.
- Se ud over cloud-laget. Kortlæg afhængigheder i alle lag af stakken – data, identitet, sikkerhed og SaaS. Suverænitet er aldrig stærkere end den mindst flytbare afhængighed.
- Byg et platformteam, der leverer containere as-a-service – gerne i fællesskab med andre myndigheder. Omskol driftsmedarbejdere, så forandringen styres og ikke blot flyttes.
- Sikr leverandørkæden og test exitplanen. Skriv krav om portabilitet ind i udbud, hent software fra betroede kilder og bevis jævnligt portabiliteten ved faktisk at flytte en løsning.

AI-anvendelse kræver et bevidst valg af ambitionsniveau – ikke et kapløb mod fuld autonomi

De fleste organisationer arbejder allerede med AI på flere anvendelsesniveauer parallelt – fra medarbejderens prompts til de første workflows udført af AI-agenter. Rambølls model for AI-anvendelsesniveau gør det muligt at fastlægge organisationens nuværende niveau, mål og forudsætninger.

De fleste organisationer har i stor stil taget AI til sig og afprøver løbende, hvordan organisationen får bedst værdi af AI. IT i praksis® viser eksempelvis, at 47 pct. af offentlige organisationer i dag anvender AI til analyse af dokumenter og udarbejdelse af referater. Da erfaringen er begrænset, og den teknologiske udvikling er høj, sker ibrugtagning på en måde, så anvendelse er meget varierende på tværs af organisationen: Nogle medarbejdere prompter dagligt, andre har bygget AI ind i deres værktøjer, og enkle afdelinger eksperimenterer med delvist autonome agenter til at løse simple opgaver.

Når AI-anvendelse skal bevæge sig fra pilotinitiativer til drift, og når anvendelsen ofte samtidig bliver mere avanceret, stiller det øgede krav til både, hvilke AI-løsninger der skal være til rådighed for medarbejderne, og hvilken implementering og hvilke styringsmodeller der skal være til stede i organisationen for at lykkes.

For at kunne definere, hvad der kræves af organisationen, er det vigtigt, at man har defineret sine mål for anvendelse af AI i organisationen generelt eller inden for de enkelte forretnings-områder og støttefunktioner. Rambølls model for AI-anvendelsesniveau kan bruges som grundlag for dette arbejde og giver mulighed for at styre dialogen om projekter, forudsætninger og forventninger. Med en fælles ramme undgår man, at AI-indsatsen bliver styret af enkelte initiativer og leverandørløfter frem for organisationens egne mål.

Tre grupper – seks niveauer

Modellen samler seks anvendelsesniveauer i tre grupper, og hvert niveau beskriver AI's og brugerens rolle, udbredelsesmodel og tekniske forudsætninger.

På prompt-niveau 1 og 2 forbedrer AI enkelte trin i en arbejdsopgave, og hver opgave igangsættes af en slutbruger. På dette niveau styrer og gennemgår brugeren alle trin i arbejdet, og ofte kan det blot være et enkelt trin i en arbejdsproces, som udføres med hjælp fra AI. Udbredelsen sker lokalt gennem inspiration til prompts og konkrete use cases og baseres på en AI-understøttelse med godkendte standardværktøjer med let eller ingen integration til organisationens øvrige it-systemer.

På workflow-niveau 3 og 4 udfører en AI-agent en arbejdsproces med menneskelig kontrol ved hvert betydende trin. Det er entydigt fastlagt, hvordan workflowet igangsættes, fx en defineret handling som modtagelse af en e-mail eller en alarm, og agenten stopper igen, når workflowet er gennemført. Med automatisering i opgaveløsningen er det nødvendigt, at organisationen har den nødvendige styring af teknologien. Dette kræver typisk, at agenter udvikles koordineret og standardiseret, før de rulles ud til lokale teams. Det stiller samtidigt krav til it-platformen i organisationen, som skal etablere en it-arkitektur med bl.a. agentplatform og integrationer til nødvendige systemer.

På de autonome niveau 5 og 6 varetager AI-agenter en arbejdsopgave eller et helt serviceområde med kontrol over egne arbejdsprocesser. Når AI-agenter er idriftsat, vil de varetage opgaverne, indtil de afbrydes eller selv afbryder opgaven, fordi indbyggede principper kræver det. Organisationens rolle er at fastsætte politikker for området og have kontrol over systemet. Dette niveau kræver tæt governance og monitorering, og agenterne udvikles og styres typisk centralt via en fælles agentplatform, der er fuldt integreret i organisationens it-platform, blandt andet via en identitetsmodel, der sætter de rette rammer for den enkle agents muligheder for at agere.

Set på tværs, flytter udførelsen fra medarbejderen til systemet, udbredelsen går fra lokalt til centralt placeret, og kravene vokser fra et værktøj til en platform. Hvert niveau kræver derfor mere af organisationen – ikke kun af teknologien.

Find tyngdepunktet

Første skridt er at forstå, hvor organisationen befinder sig i dag. Det gøres ved at placere de konkrete AI-anvendelser på modellen: Hvor bruges AI som personligt værktøj? Hvor er AI bygget ind i et workflow? Og findes der områder, hvor agenter allerede arbejder selvstændigt? Billedet viser, hvor og hvordan hovedparten af værdien skabes i dag. Kortlægningen kan fx afsløre, at enkelte initiativer ligger højere, end fundamentet kan bære. En agent, der operer uden fælles platform og uden tilstrækkelig styring, er et typisk eksempel.

Ikke alle skal nå niveau 6

Det er fristende at se modellen som en trappe, hvor målet er toppen. Men målet er at finde det rette niveau. Dermed kan både teknologiens udvikling og organisationens forbedrede evner over

tid gøre, at målet ændres. Fx hvis en stor del af organisationens opgaver er regelbaserede og afgrænsede. Kræver de menneskelig vurdering ved væsentlige beslutninger, kan workflow-niveauerne være det naturlige tyngdepunkt for AI-ambitionerne – også på lang sigt. Gevinsten ligger i at få processerne til at køre sikkert og effektivt, ikke i at fjerne den menneskelige indflydelse helt.

Dertil kommer en ydre grænse. Autonome agenter, der arbejder kontinuerligt og i stor skala, kræver betydelig regnekraft. Med den nuværende datacenterkapacitet vil det ikke være muligt for alle organisationer at have tyngden på niveau 6, selvom løsningerne findes.

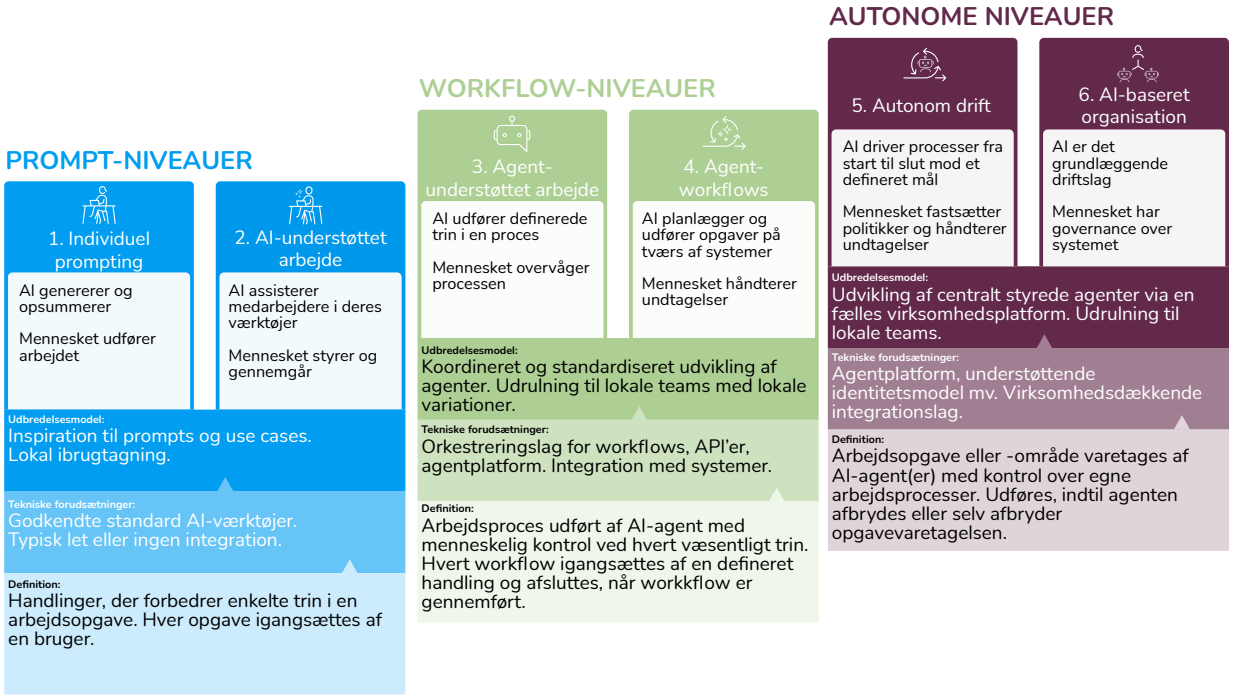
Fra mål til initiativer

Når målet er kendt: Hvad vil organisationen for nuværende opnå med AI? Dernæst sætter modellen kursen: Hvilket niveau kræver målene? Hvad kræver niveauet af teknologi og organisation, og hvilke initiativer skal realiseres for, at organisationen kan udføre det, der kræves? På den måde sikres det, at investeringer kan begrundes i konkrete mål, og at der hverken opbygges mere eller mindre fundament, end ambitionen kræver.

AI-anvendelse handler om at nå det rette niveau og vide, hvad det kræver at komme dertil.

Niveauer for AI-anvendelse

AI-anvendelse kan udføres fra den basale anvendelse til den avancerede fuldt autonome anvendelse. Hvert niveau er egnet til egne typer af arbejdsopgaver og stiller stigende krav til teknisk understøttelse og styring af AI-løsninger.



Handlepunkter

- Kortlæg nuværende AI-anvendelser og identificer tyngdepunktet – det niveau, hvor hovedparten af værdien skabes i dag.
- Fastlæg målsætninger for AI på kort og lang sigt og afgør, hvilket niveau målene reelt kræver.
- Afdæk, hvad det ønskede niveau kræver af organisationen – både organisatorisk og teknisk.
- Prioriter initiativer, der tilsammen skaber de nødvendige tekniske og organisatoriske forudsætninger. Sørg for, at fundamentet er på plads, før autonomien øges.

Tag ansvar og styr risici, når AI rammer jeres virkelighed

AI er begyndt at transformere den globale økonomi, og alle vil blive påvirket. Det stiller nye krav til, hvordan organisationer skal håndtere risici ved anvendelse af AI – ikke kun internt, men også i forhold til miljø, mennesker og samfund. Begrebet 'ansvarlig AI' er en guideline til, hvordan risici og muligheder gribes ansvarligt an.

Ingen går fri

Uanset hvor i AI-værdikæden en organisation indgår – som leverandør af data og AI-modeller eller som bruger af færdige AI-løsninger – skal den forholde sig til konsekvenserne af de beslutninger, der træffes. Eller af mangel på konkret handling. Ansvarlig AI er en ramme for, hvordan organisationer kan håndtere dette ansvar systematisk og struktureret, hvor navnlig OECD har været retningsgivende for ansvarlig virksomhedsadfærd, globale AI-principper og senest med sin vejledning om ansvarlig AI.

De organisationer, der er kommet længst med adoption af AI, oplever ansvarlig AI som en katalysator snarere end en stopklods. Alligevel er det Rambølls erfaring, at danske organisationer generelt stadig er på et tidligt modenhedsniveau. Hastig udrulning af AI uden moden risikohåndtering udfordrer organisationens egen robusthed, lige såvel som miljø, mennesker og samfund kan blive påvirket.

Fra princip til praksis

Rambølls model for ansvarlig AI er baseret på OECD's rammeværk for due diligence, illustreret i figuren, som giver et praktisk svar med seks trin: Fra forankring af ansvarlig AI i politikker og ledelsessystemer til håndtering af negative konsekvenser, når de opstår. Disse trin kan også genkendes i blandt andet ISO/IEC 42001's krav til ledelsesforankring og risikovurdering eller EU's direktiv for Corporate Sustainability Due Diligence. Organisationer, der bruger modellen, kan få en mere effektiv og systematisk håndtering af aktuelle indvirkninger og risici, tilpasset deres organisation og tilhørende krav – uanset hvilken lovgivning eller standard de i øvrigt navigerer efter. Det betyder også, at modellen kan bruges til at vurdere og dokumentere, hvor moden organisationen er i sit arbejde med ansvarlig AI.

Ansvarlig AI skal forstås bredt

Selvom de seks trin i OECD's rammeværk for due diligence også skaber et grundlag for at håndtere risici i forhold til organisationen selv, er det grundlæggende formål, hvordan organisationen effektivt kan håndtere mulige negative konsekvenser af AI i forhold til miljø, mennesker og samfund. Jo bedre og rettidig håndtering, desto mere fair og legitim vil AI-transitionen opleves, ligesom de positive konsekvenser af AI kan optimeres. Overgangen til AI, herunder også udvikling og anvendelse, rækker videre end det rent tekniske eller spørgsmålet om it-sikkerhed. Det kræver, at man er på forkant og vurderer indvirkningerne heraf så tidligt som muligt.

Modenhed er mere end en politik

En moden og robust organisation kendetegnes ikke af enkeltstående AI-politikker, men af forankring og ejerskab af ansvarlig AI i øverste ledelseslag. Samtidig skal det gennemsyre hele organisationen og ikke fungere som et separat spor ved siden af forretningen, som illustreret i modellens trin 1.

Der skal være klare roller, og ansvarlig AI skal integreres i eksisterende governance, politikker, processer, systemer, KPI'er, driftskontrol og risikohåndtering. Afhængigheder på tværs af organisationen eller i forhold til eksterne samarbejdspartnere bør afdækkes for at forstå, hvor risici og indvirkninger af AI kan opstå og håndteres. AI-relaterede hændelser kan være alvorlige for såvel organisationen selv, men også i forhold til levering af ydelser til samarbejdspartnere og kunder. En moden og robust organisation skabes ved, at medarbejderne bliver klædt på til udfordringerne og dermed kan agere effektivt med et klart mandat. Og det er vigtigt, at de nødvendige ressourcer samt incitamentsstrukturer, der kan understøtte dette, er til stede.

Risikovurderinger, som er en integreret del af trin 2 i modellen, skal ske så tidligt som muligt – i designfasen eller før nye AI-løsninger bliver taget i brug – og bør opdateres løbende i takt med teknologiens udvikling. Det gælder ikke mindst Agentic AI, hvor autonome agenter selv træffer og eksekverer beslutninger. Vi ser et stigende antal eksempler på AI-agenter, der er sat i drift med indbyggede sårbarheder eller uden klare grænser for, hvad agenten må disponere over, og hvornår menneskelig involvering er påkrævet. Det kan få store konsekvenser; fra svækket leveringsevne til utilsigtede negative indvirkninger på mennesker eller samfund, eksempelvis tillid til samfundsbærende institutioner. Her rækker den periodiske og output-baserede kontrol, som mange organisationer i dag bruger i deres governancemodeller, ikke længere. I stedet er der behov for en kontinuerlig governancemodel, der er teknisk forankret gennem agentens livscyklus, for eksempel ved at kontrollen er indbygget i agenten fra start til slut. Det indebærer autoritetsgrænser (hvad agenten selv må beslutte), eskaleringstærskler (hvornår menneskelig involvering er påkrævet) og logning (sporbarhed af beslutninger), understøttet af værktøjer som automatiseret 'red teaming', hvilket vil sige en systematisk, gentagen afprøvning af systemets svagheder og AI-værktøjer, der holder styr på og har overblik over organisationens teknologi. Disse processer skal være til stede som del af modellens trin 3 og 4, for at håndtere negative konsekvenser og risici.

En del af den organisatoriske modenhed er at kunne se risikobilledet i sin fulde bredde. Det rækker langt ud over teknologien selv og omfatter miljø (så som øget energi- og vandforbrug), mennesker – herunder egne medarbejdere, der kan opleve overvågning eller eksklusion – og samfund, for eksempel gennem bias eller misinformation.

Dette bredere risikobillede er samtidig grundlaget for at forstå, hvor organisationen er mest sårbar, og hvor man kan sætte ind for at styrke organisatorisk robusthed, fx over for regulatoriske sanktioner, tab af tillid, operationel kontinuitet eller svækket leveringsevne.

Inddragelse er ikke en eftertanke

Rettidig og løbende involvering af interessenter (medarbejdere, kunder og berørte grupper) er indlejret i alle seks trin i modellen. Det minimerer risici, gør brugen af AI-løsninger mere transparent og styrker organisationens legitimitet og konkurrenceevne.

Konkret handler det om reelle feedback-kanaler – fra medarbejdere, der bruger AI-løsninger i praksis, til kunder og borgere, der påvirkes af beslutningerne bag.

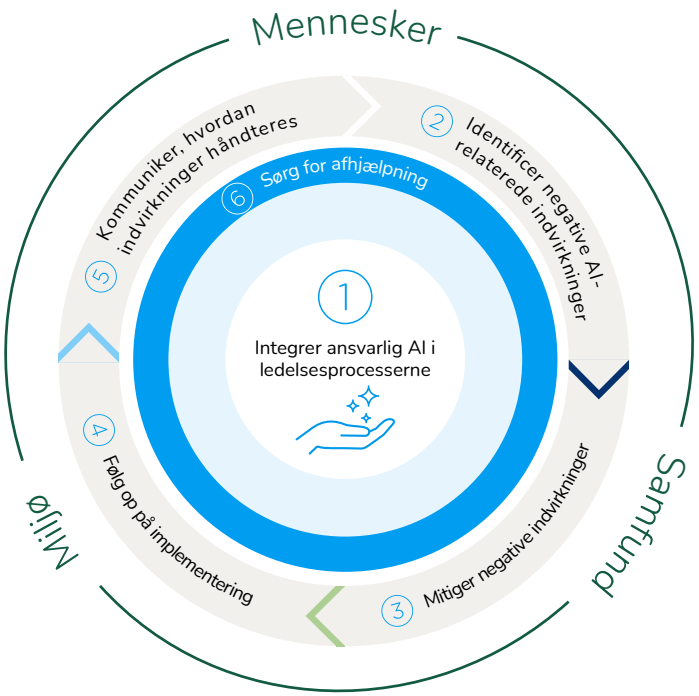
Vi ser generelt, at organisationer med klare klageordninger tidligt får indsigt i risici og svagheder, før de eskalerer og potentielt bliver dyrere at korrigere, ligesom kommunikation til interessenter kan medvirke til at styrke tilliden, adressere utryghed og skabe et rum for drøftelse af, hvordan AI kan anvendes bedst muligt.

Ansvarlighed betaler sig

Ansvarlig AI adresserer ikke kun negative indvirkninger på miljø, mennesker og samfund samt efterlevelse af lovgivning som EU's AI-forordning, men rækker i virkeligheden langt dybere. Ved at arbejde systematisk med ansvarlig AI vil man kunne opleve, at det bidrager til værdiskabelse for hele organisationen. Det kan være større intern og ekstern tillid, et mere troværdigt brand samt konkurrencefordele, ligesom det også kan betyde bedre forsikringsvilkår til dem, der kan dokumentere reel AI-governance og præventive tiltag. Ansvarlig AI er således fundamentet for at skalere AI sikkert for såvel organisationen som for omverdenen.

OECD's rammeværk for due diligence

OECD's rammeværk for due diligence understøtter efterlevelsen af lovkrav, herunder EU AI Act. Trinnene er samtidige og gentagne – ikke en lineær tjekliste.



1. Integrer ansvarlig AI ind i politiker, ledelsessystemer og processer.
2. Identificer og vurder negative AI-relaterede indvirkninger inden for drift, værdikæder og forretningsrelationer, fx ved at kortlægge AI-værdikæder som første skridt.
3. Mitiger negative indvirkninger, fx ved at introducere redskaber til at understøtte håndtering af risici i AI-løsningens livscyklus.
4. Følg op på implementering, fx ved løbende at undersøge, om AI-løsningen i praksis fungerer som tilsigtet.
5. Kommuniker, hvordan indvirkninger håndteres, fx om brugen af 'red teaming' eller hvad AI-systemet kan, ikke kan og bør bruges til.
6. Sørg for eller samarbejd om afhjælpning, når det er passende, fx ved at sikre at klagemekanismer er designet til at behandle klager ved brug af AI-løsninger og -værdikæder som første skridt.

Handlepunkter

- Forankr ansvarlig AI i en politik, der reflekterer OECD's AI-principper og er godkendt af topledelsen. Integrer i eksisterende governance, beslutningsprocesser og managementsystemer – ikke som en isoleret compliance-funktion.
- Kortlæg risici bredt for hver enkel AI-løsning op mod miljø, mennesker (inkl. egne medarbejdere) og samfund og vurder samtidig, hvor robust organisationen er.
- Etabler monitorering og rapportering. Hav et løbende overblik over AI-anvendelser, hændelser, kontroller og performance.
- Byg en kontinuerlig governancemodel til Agentic AI med klare autoritetsgrænser, eskaleringstærskler og logning gennem hele agentens livscyklus.
- Involver interessenter tidligt og løbende – det imødegår risici og styrker både AI-løsningens og organisationens legitimitet.

Undgå at AI gør din it-organisation bedre til de forkerte opgaver

AI ændrer leverandørers løsninger, fagområders handlemuligheder og it's rolle. It-ledere bør genoverveje arbejdsdeling mellem aktører, investeringer og strategisk kontrol – ellers risikerer de at optimere en Operating Model, hvor forudsætningerne er ændret.

Den største AI-drevne forandring af din it-organisation kan komme udefra

Systemleverandører bygger AI ind i deres løsninger. Drifts- og serviceleverandører ændrer måden, de leverer på og deres prismodeller. Fagområder får nye muligheder for selv at konfigurere løsninger, automatisere arbejdsgange og understøtte beslutninger. Samtidig bruger it-organisationen AI til at blive hurtigere og mere effektiv.

Alligevel giver forbedringer af den digitale værdikæde imidlertid ikke nødvendigvis bedre opgaveløsning. AI ændrer også, hvem der med fordel kan udføre opgaverne, hvor nye investeringer gør størst forskel, og hvilken kontrol myndigheden fortsat skal have.

Risikoen er ikke blot, at it ikke får taget AI i brug, men at it bliver stadig bedre til at levere ydelser, som organisationen fremover har brug for på en anden måde – eller slet ikke behøver it til at levere.

To forskydninger ændrer spillereglerne

AI forandrer leverandører, it og fagområder i forskellige tempi. To forskydninger udfordrer derfor grundlaget for den måde, IT Operating Models er indrettet på i organisationen.

For det første ændrer AI de relative leverancefordele. Det vil sige, hvilken aktør kan levere en digital service bedst, hurtigst og mest omkostningseffektivt. En opgave, der tidligere bedst kunne udføres internt, kan nu blive en standardfunktion i en leverandørs fagsystem. Omvendt kan AI gøre det mere attraktivt at løse udvalgte opgaver internt. Mere outsourcing er derfor ikke nødvendigvis svaret – og det er mere hjemtagning heller ikke.

Tag applikationsforvaltning. Hvis leverandøren kan udføre den samme opgave ved brug af AI med en væsentligt mindre indsats, hvem får så gevinsten? Myndigheden kan fortsat risikere at betale efter en prismodel, der afspejler gårsdagens omkostninger. Og hvis egne medarbejdere nu kan gennemføre bestemte ændringer hurtigere, bør den eksisterende arbejdsdeling mellem aktører så fastholdes? AI gør det nødvendigt at gentænke både kontrakter og leverancevalg.

For det andet ændrer AI, hvor øget kapacitet og kompetencer skaber størst værdi for opgaveløsningen. Når en aktivitet gennemføres hurtigere, betyder det ikke, at den samlede opgave løses bedre. Hvis AI accelererer systemudvikling, mens integration, implementering eller ændringer i arbejdsgange fortsat tager lige så lang tid, kan flere udviklingsressourcer stadigt resultere i begrænset effekt. Den vigtigste investering kan ligge et helt andet sted – også uden for it-organisationen.

Forskellen er afgørende: Der hvor en opgave bedst udføres lige nu, er ikke nødvendigvis der, hvor den næste investering skaber størst værdi. Det kan være fornuftigt at overlade mere opgavevaretagelse til leverandører og samtidig styrke egne integrationskompetencer. Eller at hjemtage bestemte udviklingsopgaver uden at udvide udviklingsorganisationen.

Gentænk it's rolle – ikke kun effektiviteten

De to forskydninger kalder på mere end et program for AI-produktivitet. It-ledelsen må genoverveje grænserne mellem leverandører, it og fagområder og flytte investeringer til de kapabiliteter, der nu begrænser en bedre opgaveløsning.

Samtidig må CIO'en gentænke sin strategiske kontrol. Når leverandører og fagområder får større handlekraft gennem AI, kan udførelse, beslutningskompetence og ansvar komme til at ligge forskellige steder. Formelle beføjelser er ikke tilstrækkelige, hvis myndigheden mangler indsigt i kritiske afhængigheder eller muligheder for at ændre kurs og gribe ind.

Strategisk kontrol betyder ikke, at it-organisationen skal godkende enhver AI-løsning. Det betyder, at beslutninger skal placeres hensigtsmæssigt, så myndigheden bevarer den faktiske mulighed for at forstå, ændre, standse eller genetablere kritiske digitale aktiviteter.

Forestil dig AI indbygget i et fagsystem. Fagområdet kan være bedst til at anvende og tilpasse løsningen, alt imens datagrundlag, automatiserede handlinger og afhængigheder kan række langt ud over det enkelte fagområde. Her handler det hverken om at bremse lokale initiativer eller at overlade hvert område til sig selv, men derimod at kombinere lokal handlekraft med fælles dataforudsætninger, integration, transparens og tydeligt ansvar.

Det gælder også leverandører: At overlade opgavevaretagelsen til andre må ikke betyde, at myndigheden mister den viden, de aftalerettigheder eller de alternativer, der er nødvendige for at kunne ændre retning.

It kan derfor få større strategisk betydning, selvom organisationen udfører færre opgaver. Her bliver bidraget i stigende grad at få egne, leverandørers og fagområders digitale kapabiliteter til at fungere sammen – uden at alle beslutninger skal gå gennem it.

Omkostningen ved at lade stå til

En Operating Model kan have været velbegrundet, da den blev etableret, og alligevel blive uhensigtsmæssig, når AI ændrer forudsætningerne. Risiciene er:

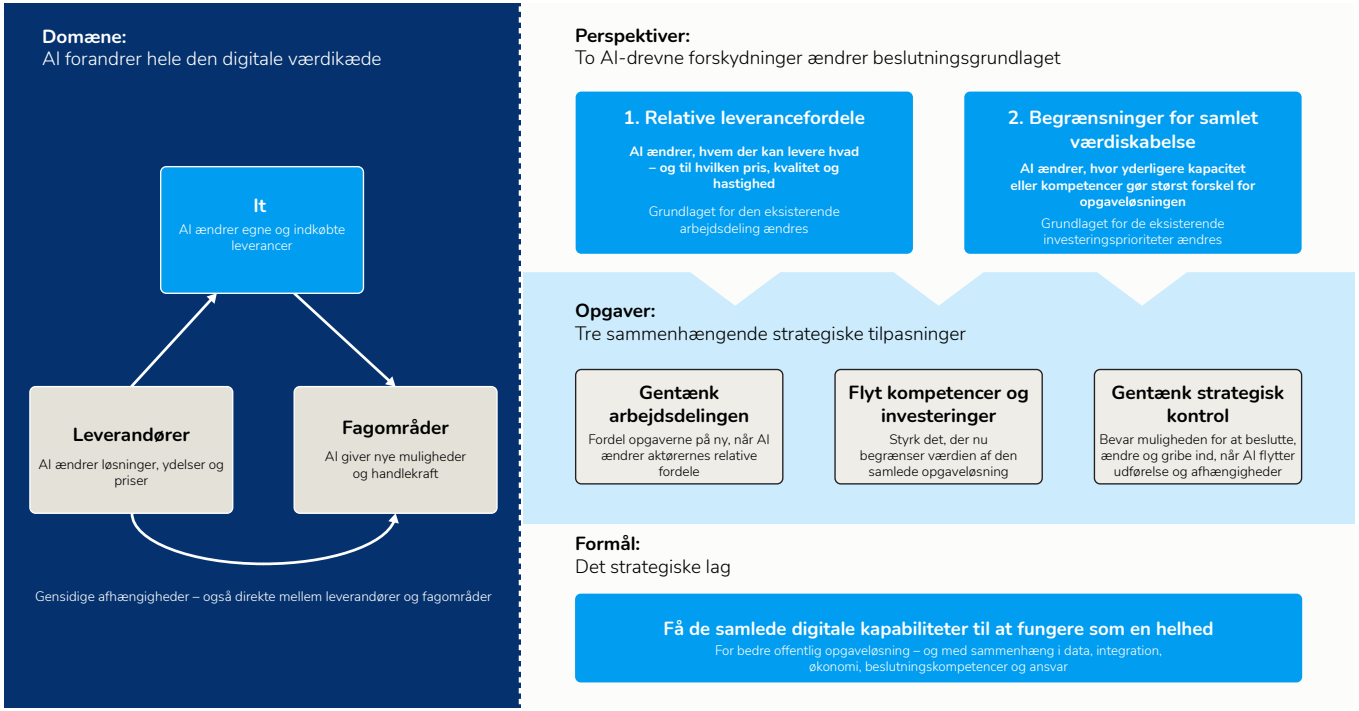
- *Forkerte opgaver:* at fastholde givent arbejde og aktiviteter, andre nu kan løse bedre.
- *Forkert kapacitet:* at investere i resultater, som ikke fjerner de væsentligste hindringer for værdiskabelse.
- *Forkert kontrol:* at stå med ansvaret uden reel mulighed for at påvirke kritiske forhold.

Alle tre risici kan vokse, også på trods af en mere effektiv it-organisation.

Gevinsten ved AI handler derfor ikke blot om en mere produktiv it-organisation. Det er understøttelsen af en samlet digital værdikæde, der samlet gør opgaveløsningen hensigtsmæssig – og en it-organisation, der er indrettet til at understøtte netop det behov.

AI forskyder, hvor it skaber værdi

AI forandrer, hvem der bedst kan levere digitale ydelser, og hvor nye investeringer skaber størst værdi. It-organisationen må tilpasse arbejdsdelingen mellem aktører, kompetencer og strategisk kontrol, så den samlede digitale værdikæde understøtter opgaveløsningen.



Handlepunkter

- Gentænk arbejdsdelingen mellem aktører. Sammenlign leverandører, it og fagområder med AI-justerede omkostninger, kvalitet og hastighed. Udfordr både eksisterende sourcing begge veje samt muligheder for selektiv hjemtagning.
- Invester der, hvor værdien begrænses. Undersøg, hvad der står i vejen for bedre og hurtigere opgaveløsning. Flyt ressourcer fra isolerede produktivitetsgevinster til de kapabiliteter og løsninger, der styrker helheden.
- Udfordr leverandørøkonomien. Undersøg, om leverandørers AI-gevinster giver bedre priser eller vilkår. Genbesøg aftaler og bevar reelle alternativer, hvor gevinster ikke kommer myndigheden til gode.
- Bevar strategisk kontrol. Afklar, hvem der må beslutte og handle, og hvad myndigheden skal kunne gennemskue, ændre eller standse. Giv fagområder handlefrihed uden at miste fælles styring og ansvar.

Digitale dagsordener



Digital Transformation i Danmark, IT i praksis® undersøger de digitale dagsordener, der aktuelt påvirker den offentlige sektor. Årets undersøgelse uddyber blandt andet digital suverænitet, det digitale beredskab, progression i og værdiskabelse af AI, cybersikkerhed, udviklinger i it-investeringer samt mitigering af digitale forretningsrisici.

Digital transformation samt it- og digitale færdigheder er fortsat en vigtig del af den offentlige organisations fokus. It- og digitale løsninger er drivende for både værdiskabelse og effektivisering, og kommer med en stærk sikkerhedsvinkel.

IT i praksis® sætter fokus på, hvordan it-ledelsen rykker endnu tættere på forretningen, herunder digitaliseringens vigtige rolle i offentlige organisationer. Derudover undersøges, hvilke former for AI der anvendes i offentlige organisationer, og hvordan det skaber værdi for borgere og samfund. Cybersikkerhed og det digitale beredskab kræver fortsat stort fokus fra it- og forretningsledelsen, men nu understreges også betydningen af digital suverænitet, hvilket skaber yderligere udfordringer. Endelig ses der fortsat generelt stigende omkostninger til it-investeringer og drift.

IT i praksis® adresserer de emner, der står øverst på de offentlige organisationers digitale dagsorden, baseret på input fra topledere og it-direktører.

På de kommende sider introduceres de vigtigste digitale dagsordener, understøttet af kvantitative indsigter fra undersøgelsen.

Digitale dagsordener i Digital Transformation i Danmark, IT i praksis®

01 Geopolitisk uro bekymrer den offentlige sektor, men få handler på det

02 Fra skærpet trusselsbillede til reel handlekraft

03 Cyberangreb og værdi af AI-investeringer står øverst på risikodagsordenen

04 Øget modenhed i arbejdet med cybersikkerhed, men praksis følger ikke med

05 AI vinder frem internt i den offentlige sektor

06 Positive effekter ved kunstig intelligens, men besparelsen udebliver

07 Stigning i offentlige it-budgetter, men prioritering halter

Geopolitisk uro bekymrer den offentlige sektor, men få handler på det

Risikoen ved afhængighed af leverandører uden for EU/EØS og de facto-monopoler er bredt erkendt. Erkendelsen omsættes imidlertid sjældent til handling: Kun få organisationer har konkrete mitigeringsplaner, og endnu færre har en it-arkitektur, der muliggør et reelt skifte fra dominerende platforme.

Langt fra erkendelse til aktiv handling for at reducere risiko

Geopolitisk uro og skærpet regulering har sat digital suverænitet på dagsordenen. IT i praksis® viser, at tre ud af fem offentlige organisationer vurderer afhængighed af leverandører uden for EU/EØS som en høj risiko. Tilsvarende ser to ud af tre risici ved leverandører, der reelt fungerer som monopoler.

Til trods for denne vurdering er der lang vej til handling: Kun knap en tiendedel har i høj grad planer om at mitigere leverandørrisikoen, og endnu færre har skiftet til leverandører indenfor EU/EØS som følge af geopolitisk uro.

Til gengæld vurderes placeringen af kritiske data på datacentre, underlagt lovgivning uden for EU/EØS, som mindre kritisk med knap to ud af tre, der enten i mindre grad eller slet ikke ser det som en risiko. Dette kan enten skyldes, at data aldrig har ligget på datacentre, underlagt lovgivning uden for EU/EØS, at data allerede er blevet flyttet, eller at de offentlige organisationer ikke er bevidste om, at datacentre kan være underlagt anden lovgivning.

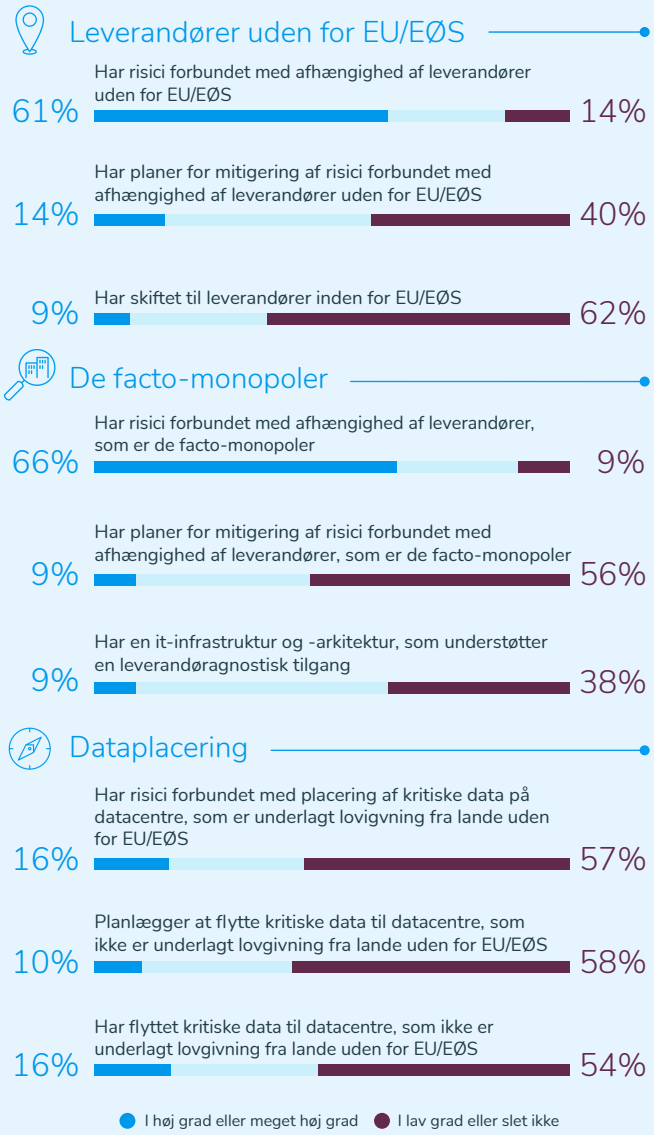
Lukket it-arkitektur begrænser offentlige organisationers suverænitet

Når det gælder it-arkitektur i den offentlige sektor, vurderer tre ud af fire organisationer, at deres it-infrastruktur i mindre grad eller slet ikke understøtter en leverandøragnostisk tilgang. Dette står i skarp kontrast til, at mere end tre ud af fem organisationer vurderer, at der er risici forbundet med afhængighed af leverandører som er de facto-monopoler.

Resultaterne af årets undersøgelse indikerer dermed, at det er kompliceret at realisere et højere niveau af digital suverænitet, fordi den nuværende it-arkitektur ikke understøtter reel handlefrihed mellem teknologier og platforme. Derfor kræver det tydelig ledelsesmæssig prioritering, hvis organisationen reelt vil ændre position. Øget handlefrihed og suverænitet er indgribende i alle digitaliseringsbeslutninger, hvis der skal skabes reel forandring.

Risikolandskabet i den offentlige sektor

Figuren viser, hvordan offentlige organisationer forholder sig til risici ved leverandører uden for EU/EØS, de facto-monopoler og placering af kritiske data i datacentre underlagt lovgivning uden for EU/EØS.



Fra skærpet trusselsbillede til reel handlekraft

Den offentlige sektor har for alvor taget et skærpet trusselsbillede til sig, og digitalt beredskab er rykket op på ledelsens dagsorden. Risikoforståelsen er modnet hurtigere end det operationelle beredskab, og der er stadig et markant spring fra dokumenterede planer til afprøvet handlekraft – især i kommunerne.

Et skærpet trusselsbillede fylder i den offentlige sektor

IT i praksis® viser, at et skærpet trusselsbillede sætter digitalt beredskab øverst på ledelsens dagsorden. Knap hver sjette af de adspurgte organisationer har udarbejdet egentlige sårbarhedsvurderinger og indtænker i høj grad scenarier om hybridkrig og cyberspionage i deres beredskab. Bevidstheden om, hvad der kan ramme organisationen, er i høj grad i fokus hos flertallet i den offentlige sektor. Der tegner sig dermed et billede af, at risikoforståelsen er modnet i takt med det skærpede trusselsbillede, men også at mere end hver tredje organisation endnu ikke har inkorporeret disse trusler i deres beredskab.

Det operationelle beredskab halter bagefter

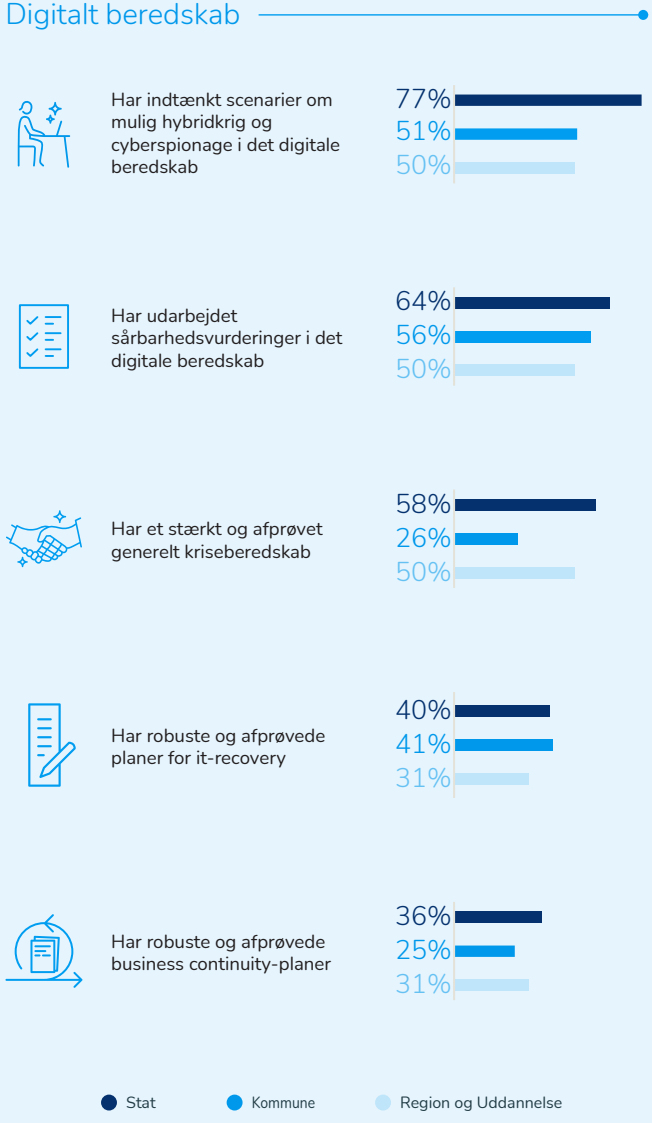
Når blikket flyttes fra risikoforståelse til operationelle planer, tegner der sig imidlertid et anderledes billede. Kun hver tredje har i høj grad robuste og afprøvede business continuity-planer, og under halvdelen vurderer, at deres generelle kriseberedskab er stærkt og afprøves løbende. Der er dermed et spring fra risikoforståelse til reel handlekraft. Et spring, der er særligt tydeligt i kommunerne, hvor kun godt en fjerdedel har et stærkt afprøvet kriseberedskab.

Balance mellem risikoforståelse og reel resiliens

Der tegner sig et billede af en offentlig sektor, hvor risikoforståelsen er modnet hurtigere end reel resiliens. Planer er i højere grad dokumenteret end indøvet. Sårbarhedsvurderinger og trusselsscenarier har begrænset værdi, hvis de ikke omsættes til afprøvede planer, klare roller og gentagne øvelser. Her ses et klart forbedringspotentiale i den offentlige sektor for at sikre, at digital resiliens når helt ud i det operationelle beredskab. Især den kommunale sektor har en markant opgave foran sig.

Risikoforståelse og beredskab i den offentlige sektor

Figuren viser, i hvilken grad offentlige organisationer indtænker og tester scenarier i deres kriseberedskab for at styrke organisationens digitale beredskab og resiliens.



Cyberangreb og værdi af AI-investeringer står øverst på risikodagsordenen

Cyberangreb topper suverænt den strategiske risikodagsorden i offentlige organisationer. Samtidig fremstår manglende udnyttelse af digitale værktøjer og AI også som en højt prioriteret risiko, mens geopolitiske forhold og eksterne compliancekrav også fylder i risikobilledet.

Cybersikkerhed som grundpræmis

Cybersikkerhed indtager førstepladsen på den strategiske risikoagenda med næsten alle respondenter, som vurderer, at håndtering af cyberangreb og utilstrækkelig sikkerhed er vigtig eller meget vigtig. Og i både stat og region er tilslutningen tæt på 100 pct. Mere bemærkelsesværdigt er det, at fire ud af fem samtidig peger på utilstrækkelig viden om og opmærksomhed på cyber- og digitale risici i topledelsen som et strategisk vigtigt risikoscenarie. Det afspejler en stigende digital kompleksitet, hvor topledelsen skal forholde sig til risici, governance og regulering i en hastig udvikling. Konklusionen er klar: Selvom cybersikkerhed er anerkendt som en generel ledelsesdisciplin og ikke kun et it-anliggende, mangler der fortsat viden om og prioritering af området i de øverste beslutningslag.

AI og digitale værktøjer ligger højt på risikodagsordenen

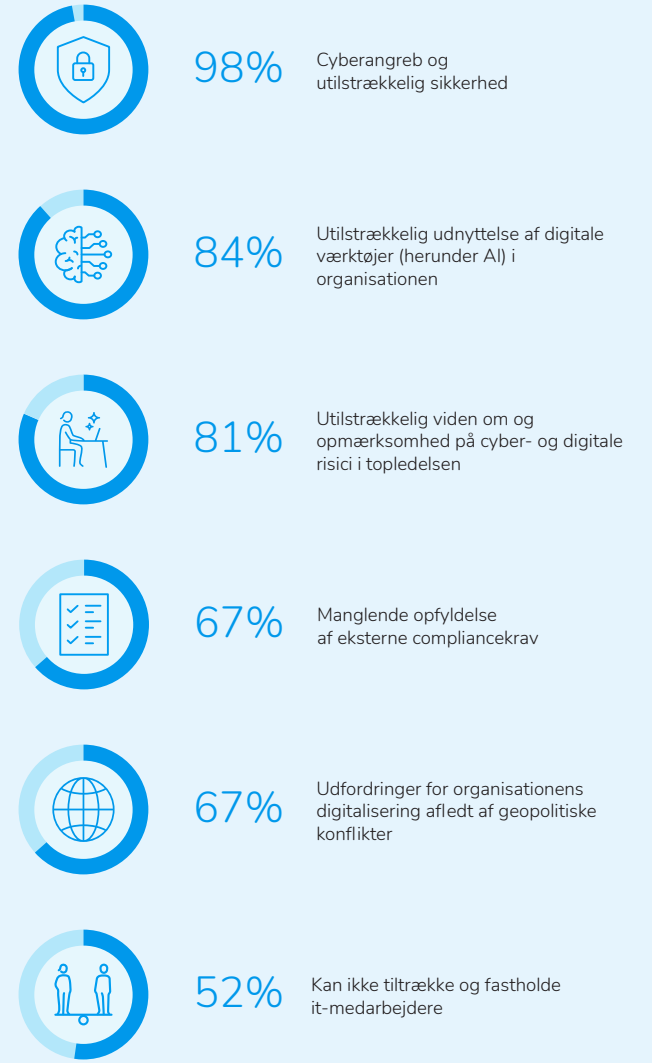
I takt med udbredelse af AI bliver anvendelse af AI og digitale værktøjer en central strategisk faktor. Mere end fire ud af fem offentlige organisationer vurderer, at manglende udnyttelse af digitale værktøjer og AI er en strategisk vigtig risiko. Dette understreger, at AI ikke længere blot er et digitalt anliggende, men bliver et spørgsmål om at opnå effekter af at anvende digitale værktøjer, der kan have direkte betydning for opgaveløsning og effektivitet.

Geopolitik står tydeligt i risikobilledet

Udfordringer i det geopolitiske billede er ved at etablere sig som en selvstændig dagsorden. To ud af tre respondenter vurderer, at digitaliseringsudfordringer afledt af geopolitiske konflikter er strategisk vigtige at mitigere. Konklusionen er, at det ikke længere blot handler om at udvikle it-landskabet, men om at agere strategisk i en digital virkelighed, der er blevet både mere sårbar og politiseret.

Den offentlige sektors vurdering af aktuelle digitale forretningsrisici

Figuren viser, i hvilken grad offentlige organisationer vurderer aktuelle digitale forretningsrisici som strategisk vigtige for deres organisation.



Øget modenhed i arbejdet med cybersikkerhed, men praksis følger ikke med

Cybersikkerhed er fortsat i fokus i den offentlige sektor, og den generelle modenhed er øget. Involvering af topledelse, risikovurderinger og procedurer ved cyberangreb står stærkest, mens medarbejderadfærd og øvelser fremstår som udviklingspotentialer. Mere end halvdelen af de offentlige organisationer har selv oplevet driftsforstyrrende cyberangreb.

Øget modenhed i cybersikkerhed, men også flere vellykkede cyberangreb

Organisationers modenhed i arbejdet med cybersikkerhed er forbedret det seneste år. IT i praksis® viser, at knap hver anden offentlig organisation vurderer, de er modne i arbejdet med cybersikkerhed. De handlinger i organisationen, der traditionelt indikerer modenhed, ligger endda markant højere. Godt syv ud af ti udarbejder således risikovurderinger og har klare procedurer for håndtering af cyberangreb.

Cyberangreb er ikke blot en risiko, som den offentlige sektor skal forholde sig til, men udgør en konkret og synlig driftsforstyrrelse. Mere end seks ud af ti har inden for det seneste år været udsat for angreb, der har forstyrret driften. De mange driftsforstyrrende angreb understreger, at truslen materialiserer sig bredt og med mærkbare konsekvenser, som kræver stærke mitigerende foranstaltninger.

Governance på papir og som proces kan ikke stå alene

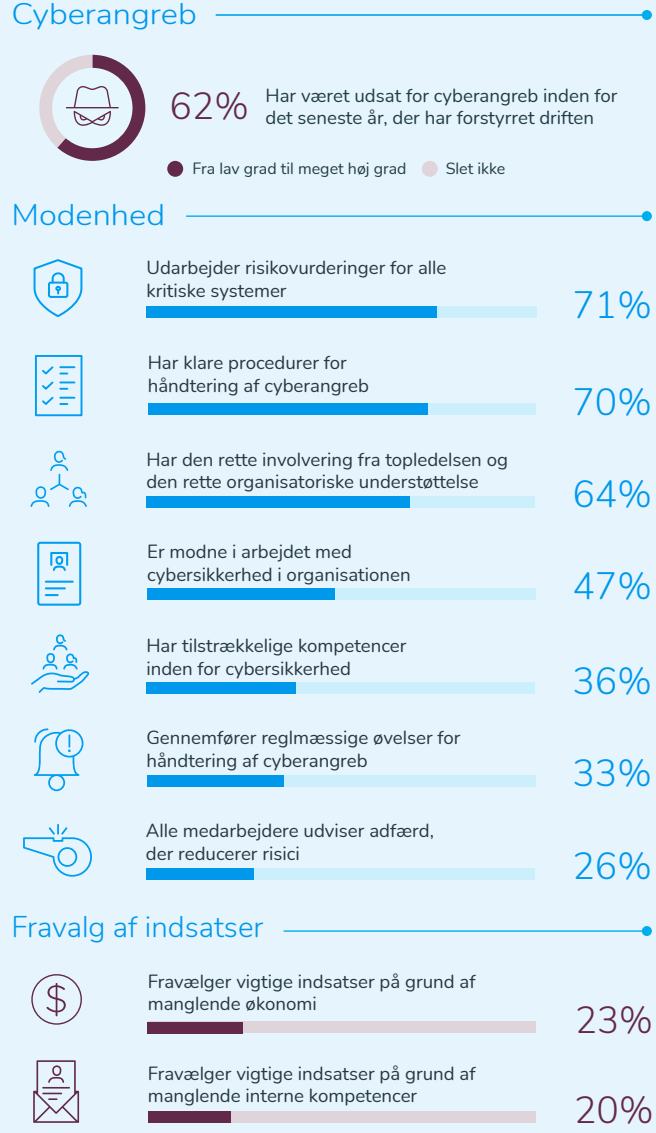
En del af forklaringen på højere modenhed samtidig med flere vellykkede cyberangreb synes at ligge i, at det formelle og det operationelle er opdelt. Governance står stærkt organisatorisk funderet med knap to tredjedele, som oplever den rette involvering fra topledelsen og den nødvendige organisatoriske understøttelse. Her er de statslige organisationer i front med knap tre fjerdedele, mens kommunerne er mindre modne.

Når blikket flyttes fra det formelle lag til adfærd i praksis, ændrer billedet sig markant. Her vurderer blot hver fjerde af de offentlige organisationer, at medarbejderne i høj grad udviser risikoreducerende adfærd, mens kun godt tre ud af ti i høj grad gennemfører regelmæssige øvelser.

Barriererne peger tilbage mod ressourcer, hvor knap hver fjerde i høj grad må fravælge vigtige sikkerhedsindsatser af økonomiske årsager. Næste bølge peger derfor i retning af at investere i adfærd, træning og kompetencer for at løfte cybersikkerhed yderligere i den offentlige sektor.

Cyberangreb og modenhed

Figuren viser, hvordan offentlige organisationer vurderer deres nuværende arbejde med cybersikkerhed på en skala fra i meget høj grad til slet ikke.



AI vinder frem internt i den offentlige sektor

Sammenlignet med sidste års undersøgelse, viser IT i praksis® i år, at anvendelse af kunstig intelligens (AI) i den daglige drift er steget betydeligt i de offentlige organisationer. Det mest udbredte anvendelsesområde er fortsat som informationsassistent.

Chatbots er fortsat det mest udbredte AI-værktøj

AI vinder for alvor indpas i den offentlige sektor, som i årets undersøgelse viser betydelige stigninger i anvendelsen af AI. Chatbots som informationsassistent er fortsat det mest udbredte AI-værktøj, hvor godt to tredjedele af organisationerne benytter disse i den daglige drift. Endnu tydeligere er stigningen i specialiserede interne opgaver. Her er andelen, der bruger AI internt til at afklare lovgivning og regler, mere end fordoblet i forhold til sidste år. Et klart tegn på, at AI for alvor er ved at blive en del af den daglige drift.

Dokumentanalyse og fagsystemer i markant vækst

Den samme udvikling ses inden for dokument- og dataanalyse. Knap halvdelen af organisationerne anvender i dag AI i den daglige drift til at analysere dokumenter, næsten en fordobling i forhold til sidste år, og mere end halvdelen oplever betydeligt positive erfaringer hermed. Også integration af AI i fagsystemer er steget markant fra blot 6 pct. sidste år til 24 pct., der i dag anvender AI i den daglige opgaveløsning.

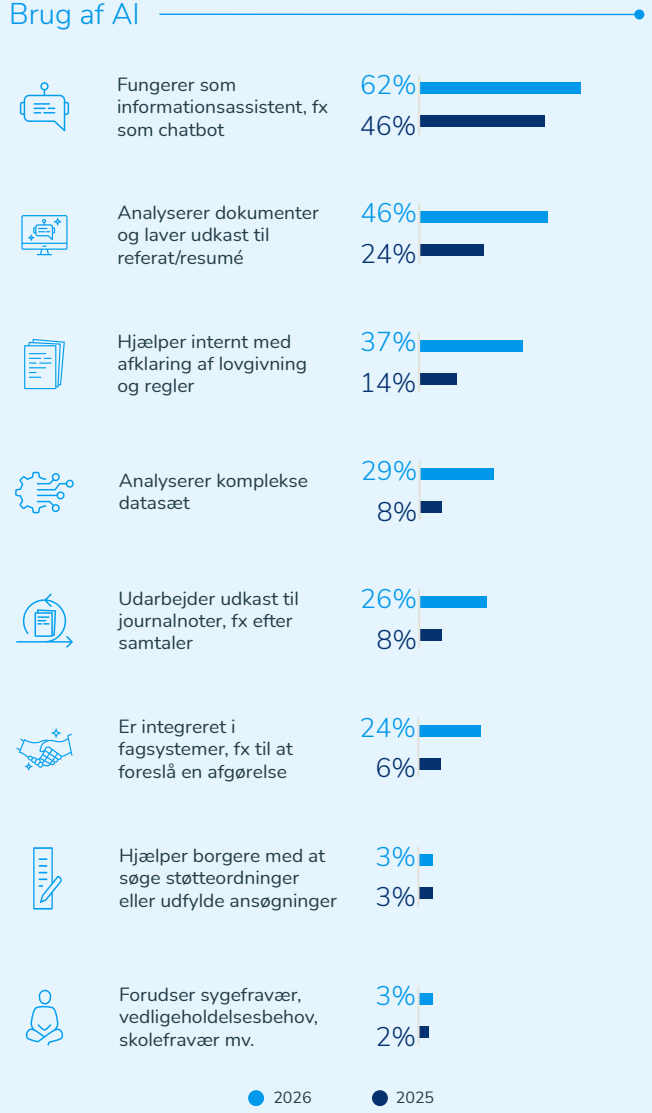
Borgerrettede løsninger halter fortsat efter

Kun 3 pct. af organisationerne bruger i dag AI til at hjælpe borgere med at skrive ansøgninger, og knap tre fjerdedele har ingen planer om at implementere det på nuværende tidspunkt. Det tegner et billede af, at det er langt mere komplekst at udvikle borgerrettede AI-værktøjer end værktøjer, der udelukkende anvendes internt. En kløft mellem intern og ekstern anvendelse, som ikke har flyttet sig nævneværdigt siden sidste års undersøgelse.

Samlet set viser IT i praksis® en offentlig sektor, hvor AI for alvor er blevet en del af hverdagen internt, mens borgernære løsninger fortsat ligger på et bundniveau.

Konkret implementering af AI i den offentlige sektor

Figuren viser, hvor udbredt anvendelsen af AI er i den offentlige sektor målt på, om de offentlige organisationer har implementeret AI til forskellige formål.



Positive effekter ved kunstig intelligens, men besparelsen udebliver

Anvendelse af kunstig intelligens (AI) i den offentlige sektor modnes, og teknologien leverer især værdi gennem hurtigere opgaveløsning, højere kvalitet i processer og frigjort tid til andre opgaver. Det står klart, at AI indtil videre ikke har udløst store besparelser eller reduktioner i medarbejdergruppen i den offentlige sektor.

Bedre kvalitet og mere effektive processer i fokus

AI er ved at finde sit fodfæste i den offentlige sektor. IT i praksis® viser, at mange organisationer har opnået gevinster i forhold til øget kvalitet, men få organisationer har opnået besparelser i personale eller omkostninger.

AI-anvendelse har især bidraget til forbedret kvalitet i opgaveløsning. Hurtigere eksekvering er i høj grad konstateret hos fire ud af ti organisationer. Bedre kvalitet i processer og services samt frigjort tid til andre opgaver ses i høj grad hos knap hver tredje organisation.

På trods af stor udbredelse af AI har få offentlige organisationer reduceret antallet af medarbejdere eller reduceret omkostninger. Effekterne af AI-anvendelse materialiserer sig dermed primært som forbedringer i arbejdsprocesser, ikke som direkte besparelser på bundlinjen. Når gevinsterne af AI ikke omsættes til direkte besparelser, kan det skyldes, at frigjort tid og højere kvalitet ikke kan konverteres på en let og enkel måde. Det forudsætter større omlægninger, som kan være vanskelige at gennemføre uden et større erfaringsgrundlag i organisationen.

IT i praksis® viser, at AI-anvendelsen i dag primært ses som et hjælpeværktøj og ikke som en egentlig erstatning for ansatte.

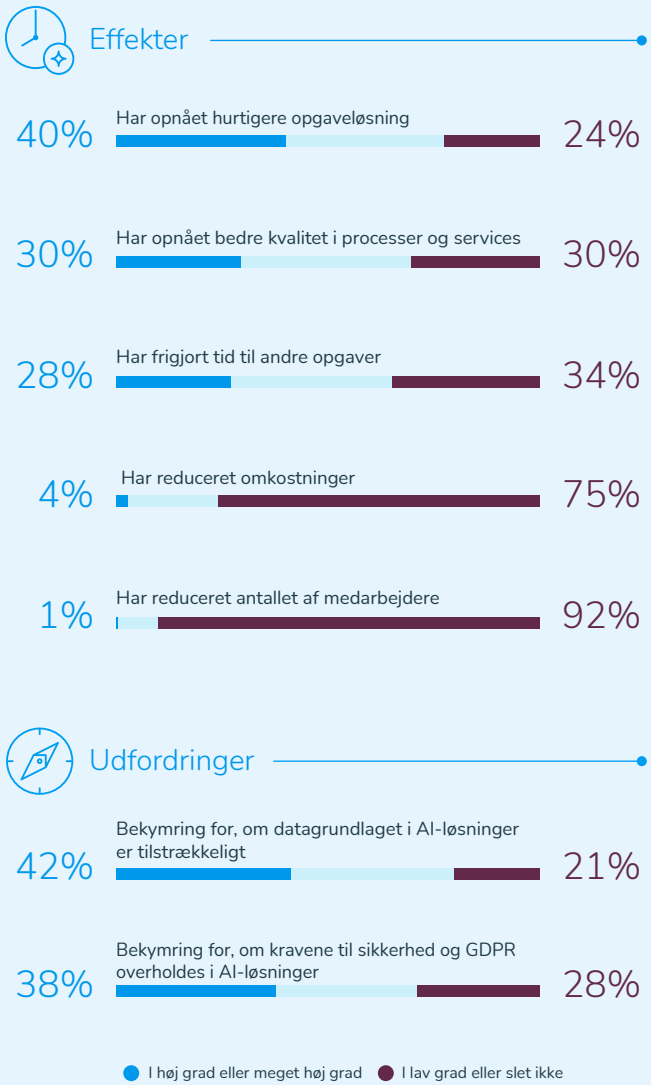
Usikkerhed i forhold til AI-governance

Selvom effekterne af AI viser sig i den offentlige sektor, fylder bekymringer om datagrundlaget. Fire ud af ti organisationer er usikre på, om datagrundlaget bag AI-løsninger er tilstrækkeligt, og næsten lige så mange tvivler på, at kravene til sikkerhed og GDPR overholdes.

Uagtet at usikkerheden forventeligt vokser i takt med anvendelsen af AI, står det klart, at governance skal følge den teknologiske udvikling for at sikre, at krav og risici imødekommes. Dette understreger, at behovet for ansvarlig brug af AI vokser med omfanget, hvorfor det bliver afgørende for de offentlige organisationer at have styr på deres risikobillede. Ellers risikerer den offentlige sektor, at gevinster på procesniveau ender med at koste dyrt på tillid.

AI-effekter og -udfordringer i den offentlige sektor

Figuren viser, hvilke effekter den offentlige sektor oplever af AI, og i hvilket omfang organisationen ser udfordringer ved anvendelse.



Stigning i offentlige it-budgetter, men prioritering halter

De offentlige it-budgetter vokser markant, drevet af investeringer i AI og cybersikkerhed samt udgifter til softwarelicenser. Mens teknologien får tilført ressourcer, er kompetenceudvikling og den økonomiske styring imidlertid ikke fulgt med – og risikerer dermed at underminere værdien af de stigende investeringer.

De offentlige it-budgetter stiger fortsat

Den offentlige sektor skruer igen i år op for it-budgetterne. Godt halvdelen af de offentlige organisationer har øget it-investeringernes andel af det samlede investeringsbudget, og tre ud af fem af har inden for det seneste år hævet budgettet til drift, forvaltning og vedligeholdelse af it og digitalisering. Bag totalen tegner der sig dog et differentieret billede: I staten oplever mere end hver syvende et fald i driftsbudgettet, mens næsten alle uddannelsesinstitutioner har opjusteret.

Cybersikkerhed og AI har topprioritet

Ny teknologi og et skærpet trusselsbillede driver udviklingen i de offentlige it-budgetter. Tre ud af fire organisationer har øget investeringerne i AI-løsninger og i it- og cybersikkerhed, mens omkostninger til softwarelicenser følger tæt efter. Kommunerne trækker det tungeste læs på sikkerhedsområdet, hvor knap ni ud af ti har hævet budgettet. Cybertrusler og anvendelse af AI bliver dermed ikke længere set som valgfrie strategiske spor, men grundlæggende driftsvilkår.

Kompetencer og styring halter bagefter

Den økonomiske styring af it-omkostninger og investering i organisationens kompetencer følger imidlertid ikke med. Kun godt hver tredje organisation har hævet budgettet til kompetenceudvikling, mens flertallet fastholder niveauet. Samtidig har blot en tredjedel i høj grad etableret et aktivt program for reduktion af it-omkostninger. Uden sideløbende kompetenceudvikling og økonomisk disciplin risikerer de stigende it-budgetter blot at blive til stigende udgifter i den offentlige sektor frem for reel værdiskabelse.

Udviklingen i den offentlige sektors it-budgetter gennem det seneste år

Figuren viser den procentvise udvikling i den offentlige sektors it-budgetter gennem det seneste år, angivet som stigende og faldende it-budgetter.





Borgernes erfaringer og holdninger



Digital Transformation i Danmark, IT i praksis® sætter fokus på borgernes erfaringer med og holdninger til digitalisering i den offentlige sektor. I år belyses aktuelle emner såsom udviklingen i brugen af kontaktkanaler, tilfredshed med offentlige digitale services, anvendelse af AI, digital suverænitet samt beredskab ved krisesituationer.

Interaktionen mellem borgere, offentlige myndigheder og private virksomheder er præget af stigende digitalisering, men også øget usikkerhed. I takt med teknologiske fremskridt skal borgerne tage stilling til muligheder såvel som udfordringer relateret til digitale interaktioner.

IT i praksis® er igen i år optaget af, hvornår borgerne foretrækker digital selvbetjening eller personlig betjening, hvilket følger tendenser fra tidligere år. Årets undersøgelse vender også blikket mod emner som borgernes holdninger til det offentliges brug af teknologi inden for og uden for EU/EØS, det offentliges kriseberedskab, behandling af borgernes data, tilfredshed med offentlige digitale services samt det offentliges brug af AI.

Borgernes holdninger giver undersøgelsen en ekstra vinkel, som sætter perspektiv på de offentlige organisationers egne vurderinger af dem selv og aktuelle emner. Dette kan enten vise hvor der findes en dissonans, og at det offentlige bør kigge på målrettet kommunikation i forhold til aktuelle temaer, eller om der reelt findes forbedringspotentialer.

Årets mest markante erfaringer med og holdninger til digitalisering

01 Delte meninger om brug af kunstig intelligens i det offentlige

02 Kanalvalg afhænger af situationen – og borgerne ønsker valgmuligheder

03 Bred opbakning til digital suverænitet blandt borgerne

04 Utryghed ved det offentliges kriseberedskab

05 Usikkerhed om, hvordan data behandles af det offentlige

06 Tilfredshed med digitale services, men flere ønsker mere hjælp

Delte meninger om brug af kunstig intelligens i det offentlige

Kunstig intelligens (AI) anvendes mere og mere i den offentlige sektor. En stor andel af borgerne er helt trygge ved det offentliges anvendelse af AI, men en endnu større gruppe er utrygge ved udviklingen. Særligt hvis AI støtter beslutninger om borgeren. Flertallet mener dog, at det offentlige bør bruge mere AI.

IT i praksis® viser, at borgerne har meget forskellige holdninger til brugen af AI i det offentlige, herunder hvordan det anvendes til sagsbehandling og borgerkontakt.

Flertallet syntes, at det offentlige bør bruge AI alle steder, hvor det kan give fordele. Tre ud af ti borgere er meget trygge ved AI, når det fx bruges til at give hjælp til at søge støtteordninger eller udfylde ansøgninger, foreslå behandlinger, forudse fremtidige behov til støtte samt understøtte tidlig indsats. Til gengæld forventer størstedelen af borgerne ikke, at kontakten med det offentlige bliver nemmere.

To ud af fem borgere er generelt utrygge ved, at offentlige organisationer bruger AI i deres it-løsninger. Borgernes utryghed knytter sig særligt til situationer, hvor det offentlige bruger AI til at træffe beslutninger om borgeren og det offentliges eventuelle brug af borgerens data til at udvikle deres AI-services. Når det gælder chatbots, foretrækker halvdelen af borgerne igen i år, at det offentlige ikke anvender disse.

Rambøll vurderer derfor, at borgernes opmærksomhed er på både potentialer og bekymringer for det offentliges brug af AI. Hvor borgerne er mere positive over for brug af AI til at løfte borgerrettet service, har offentlige organisationer endnu ikke udnyttet AI til at hjælpe borgere med fx at skrive ansøgninger. Og flertallet har ingen planer om at implementere det på nuværende tidspunkt. Læs mere om dette i den digitale dagsorden om kunstig intelligens.

Den offentlige sektor rammer dermed skævt på borgernes ønsker til AI, hvorfor der fremadrettet ligger et potentiale i at realisere øget støtte til borgerne, sikre tilstrækkelig transparens i forhold til, hvordan AI og data anvendes, og tage hånd om borgernes muligheder for at komme til orde, hvis de oplever fejlagtig behandling pga. AI.

Forskellige holdninger til AI blandt borgerne

Figuren viser, i hvilken grad borgerne er enige i forskellige udsagn om brug af AI i det offentlige.



Kanalvalg afhænger af situationen – og borgerne ønsker valgmuligheder

IT i praksis® viser, at borgernes foretrukne kontaktkanal afhænger af, hvad henvendelsen omhandler. Til rutineprægede og informationssøgende opgaver er den digitale kanal klart førstevalget, mens dialog, tvivl og alvor igen i 2026 trækker borgerne mod personlig kontakt. Uanset hvad, står et ønske stærkt; muligheden for selv at vælge kanal.

Den digitale kanal er førstevalget, når opgaven er konkret

Skal borgerne ansøge om eller indberette noget, foretrækker mere end fire ud af fem en digital kanal. Næsten lige så mange vælger også den digitale vej, når de skal fremsøge faktuel information. Selv klager bør håndteres digitalt, synes to ud af tre borgere. Det er afgrænsede, transaktionsprægede opgaver, hvor det digitale er blevet hverdag. Spørger man udelukkende til kontaktfladen i almindelighed, har knap tre ud af fem en digital kanal som førstevalg.

Behov for dialog og sagens karakter trækker mod den personlige kanal

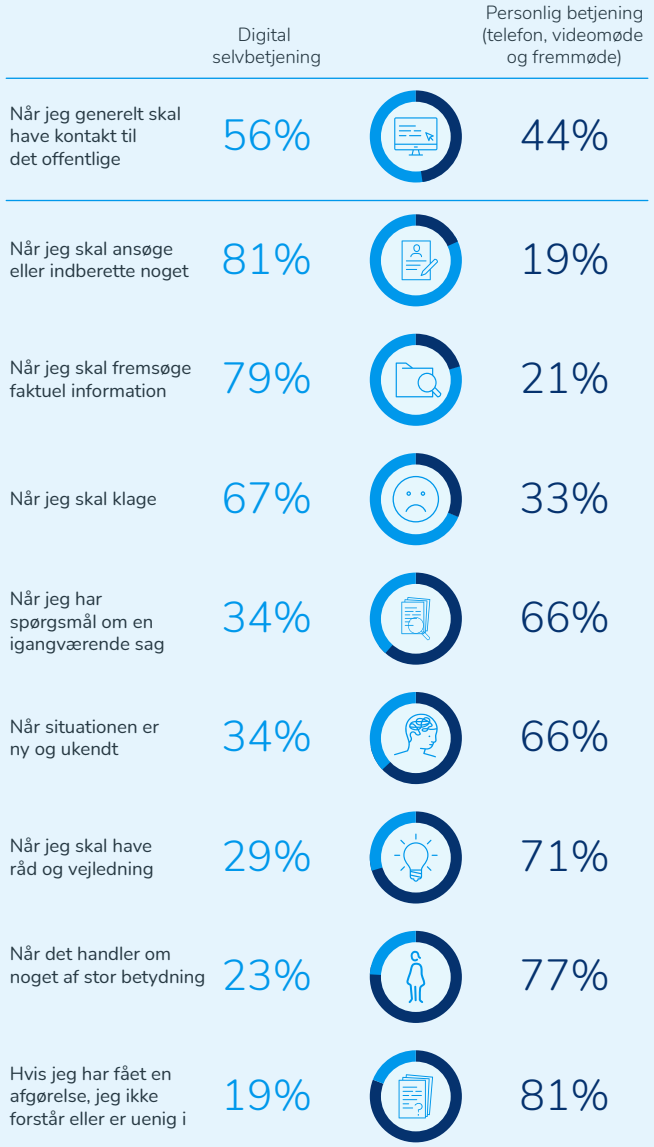
Kræver henvendelsen særlig forståelse eller vurdering, vender billedet. Har borgeren fået en afgørelse, som vedkommende ikke forstår eller er uenig i, foretrækker hele fire ud af fem en personlig kanal – den mindst digitale form i undersøgelsen. Det samme gælder, hvis noget har stor betydning for borgeren, man har brug for råd og vejledning eller information om igangværende og nye sager. Borgerne fravælger her ikke blot det digitale: Over halvdelen vil ringe, når de står med en afgørelse, de ikke forstår. Behovet er ikke en teknologi, men en stemme i den anden ende.

Valgfrihed er nærmest ufravigelig

Bag valgene ligger et gennemgående ønske: Næsten ni ud af ti mener, det er vigtigt selv at kunne vælge kanal. Godt halvdelen bakker op om, at digital selvbetjening bør være udgangspunktet, mens godt hver femte er direkte uenig. Rambøll vurderer, at afstanden mellem de to tal er den egentlige pointe: Borgerne har taget det digitale til sig, hvad angår rutineprægede opgaver. Et digitalt førstevalg har kun mandat, så længe det ikke bliver det eneste. Kanalstrategien bør derfor følge henvendelsens karakter: En 'hovedvej' med selvbetjening til rutineopgaver og en 'bemandet vej' til dialog, når det bliver komplekst.

Borgernes foretrukne kanal afhænger af situationen

Figuren viser, hvor stor en andel af borgerne som foretrækker en digital henholdsvis personlig kanal i de anførte situationer.



Bred opbakning til digital suverænitet blandt borgerne

Digital suverænitet er de senere år formuleret som en offentlig ambition. IT i praksis® har undersøgt, hvordan borgerne ser på den offentlige sektors afhængighed af data og digitale løsninger, som er forankret og ejet af virksomheder uden for EU.

Årets undersøgelse viser, at der er stor enighed blandt borgerne om, at udvikling af digitale løsninger hos det offentlige bør være baseret på dansk eller europæisk teknologi. På tværs af alle aldersgrupper ønsker fire ud af fem den europæiske tilknytning prioriteret i den fremtidige udvikling, hvilket er samme høje andel som i sidste års undersøgelse. Tilsvarende mener fire ud af fem borgere, at det offentlige bør undgå afhængighed af digitale løsninger, der er placeret uden for EU.

I forhold til placering af data er der et stort gab mellem borgernes ønsker og de offentlige organisationers faktiske handlinger. Mere end fire ud af fem borgere mener, at det offentlige bør undgå, at data bliver gemt på servere uden for EU. Handling halter imidlertid bagefter hos de offentlige organisationer. Mindre end hver femte organisation har således planlagt eller ageret på at flytte data til datacentre, der opererer inden for EU-lovgivning. Læs mere om dette i den digitale dagsorden om digital suverænitet.



88% Mener, at det offentlige skal undgå, at offentlige data gemmes på servere uden for EU

86% Mener, at det offentlige skal prioritere at udvikle digitale løsninger baseret på dansk eller europæisk teknologi

85% Mener, at det offentlige skal undgå afhængighed af digitale løsninger placeret uden for EU

Utryghed ved det offentliges krise-beredskab

Geopolitiske konflikter og mange cyberangreb sætter det offentliges beredskab i fokus. IT i praksis® viser, at flertallet af borgerne er bekymrede for, om det offentlige er i stand til at håndtere fremtidige krisesituationer.

Næsten hver tredje borger er meget utryg ved det offentliges kriseberedskab, herunder evnen til at opretholde kritiske services (fx vand, el og sundhed) under en krisesituation og evnen til at reagere hurtigt nok på nye trusler.

Borgernes tiltro til, at det offentlige digitale Danmark er tilstrækkeligt sikret i en krisesituation, er endnu mindre. Hver anden borger angiver at være meget utryg og kun en ud af fem er tryg. Den største bekymring er cyberangreb, hvor mere end halvdelen er utrygge ved, om det offentlige er nok beskyttet.

Den generelle utryghed, som IT i praksis® afdækker, er ikke nødvendigvis udtryk for faktiske forhold, som den enkelte borger næppe har indsigt i. Alene det, at så mange borgere ikke er trygge, kan påvirke den offentlige debat og tilliden til myndighederne og kalder på tydelige initiativer, der kan betrygge borgerne.

22%
Er tryg ved, at det offentlige digitale Danmark er tilstrækkelig sikret i en krisesituation



19%
Er tryg ved, at det offentlige er godt beskyttet mod cyberangreb

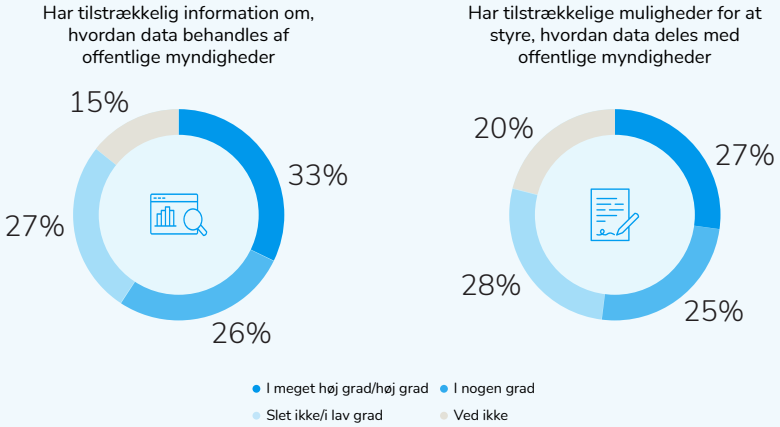
Usikkerhed om, hvordan data behandles af det offentlige

Tryghed ved brug af borgernes data er afgørende for tilliden til den offentlige digitalisering. IT i praksis® dokumenterer, at borgerne har meget forskellige vurderinger af graden af information og samtykke ved behandling af deres data.

Hver tredje borger oplever, at de i høj grad har tilstrækkelig information om, hvordan deres data behandles af offentlige myndigheder. Det er særligt de ældre borgere (over 57 år), som vurderer, de har tilstrækkelig information. Modsat angiver hver fjerde borger ikke at have tilstrækkelig information, mest udbredt i den yngre aldersgruppe.

Kun en ud af fire borgere oplever, at de har tilstrækkelige muligheder for at styre, hvordan deres data deles med offentlige myndigheder. Nogle data må deles uden borgerens samtykke, mens andre kræver samtykke. Det er derfor vanskeligt for borgeren at vide, hvornår forskellige regler gælder. Hver femte borger har dog svaret 'ved ikke', som indikerer, at de måske slet ikke er bekendt med problemstillingen.

På begge områder er bedre information fra myndigheder om databrug og deling af data nødvendig og udgør en vigtig indsats for at sikre tryghed og opbakning til den generelle digitalisering.



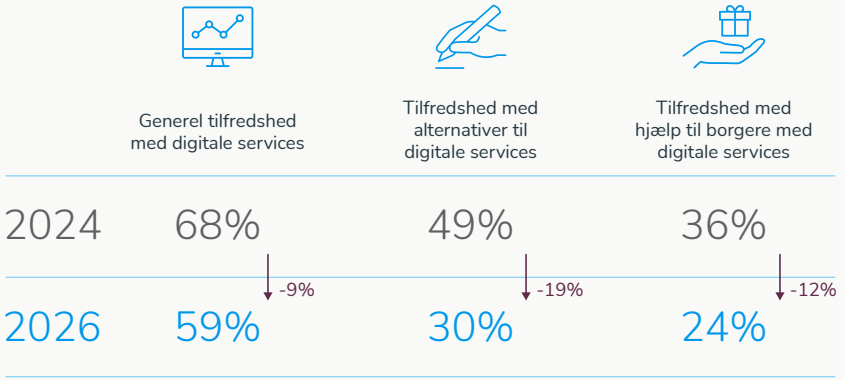
Tilfredshed med digitale services, men flere ønsker mere hjælp

IT i praksis® har spurgt borgerne om deres generelle tilfredshed med de offentlige digitale services, de har interageret med (hjemmesider, selvbetjeningsløsninger, Digital Post osv.).

Tre ud af fem borgere er generelt meget tilfredse med de digitale services, de har benyttet. Det er en høj positiv score, særligt da mange af disse services er obligatoriske at anvende for mange borgere. Det er kun hver ottende borger, der ikke er tilfreds.

Det offentlige gør dog ikke nok for at hjælpe borgerne med at anvende de digitale services. Kun hver tredje er enig i, at det offentlige hjælper nok, mens en lige så stor andel er uenig. Nogle borgere har brug for alternativer til de digitale services. Hver tredje borger er enig i, at det offentlige generelt tilbyder gode alternativer til digitale services, og at disse passer til borgerens behov. Hver femte borger er imidlertid uenig heri og oplever ikke, at alternativerne passer til borgerens behov. Det gælder i alle aldersgrupper.

Generelt er tilfredsheden dog dalende. Rambøll vurderer, at det offentlige bør lægge en større indsats i at kommunikere relevante alternativer til digitale services og øge indsatsen for at hjælpe borgerne med at anvende digitale servicetilbud.



Metode og datagrundlag



Digital Transformation i Danmark, IT i praksis® er baseret på en undersøgelse foretaget blandt samtlige kommuner, regioner og myndigheder samt de største private virksomheder i Danmark.

I perioden fra april til august 2026 er der gennemført en spørgeskemaundersøgelse, målrettet forretningsansvarlige og it-ansvarlige i både den offentlige og private sektor. På udvalgte områder bygger undersøgelsen videre på tidligere års erfaringer, men er revideret for at afspejle Rambølls nyeste viden om relevante udviklinger inden for digitale strategier, tendenser og erfaringer. Derudover har et Advisory Board, bestående af topledere og it-direktører fra både den offentlige og private sektor, bidraget med værdifulde input til yderligere skærpelse af temaer og prioritering af indhold.

Der skelnes mellem den offentlige og den private sektor for derved at kunne levere et fyldestgørende og nuanceret billede af både holdninger, udfordringer og tendenser.

Offentlig sektor

Den offentlige sektor inddeles i fire niveauer: stat, videregående uddannelse, kommune og region, hvor stat både omfatter ministeriernes departementer, statslige styrelser og institutioner. Spørgeskemaet er formidlet til samtlige statslige myndigheder og institutioner samt de 98 kommuner og fem regioner.

Digital Transformation i Danmark 2026-2027, IT i praksis® rapporterer på baggrund af besvarelser fra 130 it- og forretningsansvarlige, fordelt på de førnævnte fire kategoriseringer af den offentlige sektor. Den danske udgave af rapporten præsenterer resultaterne af undersøgelsen i den offentlige sektor.

Privat sektor

Resultaterne af undersøgelsen i den private sektor præsenteres i den engelske udgave af rapporten, Digital Transformation in Denmark 2026-2027, IT in Practice. I den private sektor er spørgeskemaet distribueret til Danmarks største virksomheder, der indgår i Børsens seneste top-1000 virksomhedsoversigt. Her rapporterer undersøgelsen på baggrund af besvarelser fra 130 it- og forretningsansvarlige.

Meningsmåling blandt borgere om digitalisering af den offentlige sektor

I forbindelse med Digital Transformation i Danmark 2026-2027, IT i praksis® er der gennemført en meningsmåling blandt et repræsentativt udsnit af 1.032 danske borgere i et online webpanel. Respondenterne har besvaret en række spørgsmål om digitalisering i den offentlige sektor, herunder myndighedernes brug af skabende kunstig intelligens i afgørelser, borgernes beredskab i en eventuel krisesituation, samt hvordan de forholder sig til digital suverænitet.





Om Rambøll Management Consulting og Dansk IT

Rambøll Management Consulting er et af Nordens førende konsulenthuse og en integreret del af Rambøll Gruppen, som i alt beskæftiger 18.000 medarbejdere, fordelt på 35 lande.

Rambøll Management Consulting agerer som en betroet partner for private virksomheder og som en aktiv aktør i udviklingen af kernevelfærden i den offentlige sektor.

Vores rådgivning hviler på et strategisk og analytisk fundament, datadrevet indsigt og et stærkt blik for nødvendige, bæredygtige og forandringsrelaterede processer. For at sikre den bedst mulige løsning for vores kunder benytter vi muligheden for at håndplukke eksperter og sammensætte teams fra hele Rambøll Gruppen, på tværs af fagområder og lande.

Digital Transformation i Danmark 2026-2027, IT i praksis® er udarbejdet af Rambøll Management Consultings konsulenter med speciale i Digital Transformation, der yder rådgivning om forretningsmæssig værdi gennem digitalisering og brug af teknologi inden for områderne strategi, analyse, bæredygtighed, organisering og eksekvering.

Dansk IT er en uafhængig forening og et fællesskab for it-professionelle. Her sættes fokus på karriereforløb gennem kompetenceudvikling og deltagelse i Danmarks største it-faglige netværk. Dansk IT arbejder for at fremme og understøtte it, hvor dette skaber værdi for samfundet og den enkelte. At samle, styrke og udvikle it-brugeres og it-professionelles kompetencer og faglighed og på et uafhængigt grundlag varetage samfundets og medlemmernes it-interesser. Du kan læse mere om Dansk IT på www.dit.dk.

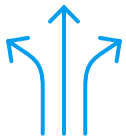
Dansk IT udbyder året rundt konferencer, kurser, faglige medlemsmøder og certificeringer. Foreningen faciliterer samtidig en række politiske udvalg, fagråd og netværksgrupper.

På https://akademi.dit.dk har medlemmer af Dansk IT adgang til webinarer, e-learning, podcasts og artikler, der styrker deres viden og kompetencer på det digitale område

Rambøll Management Consulting understøtter jeres digitale rejse

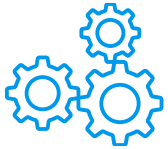
Rambøll Management Consulting er en uafhængig rådgiver inden for digital transformation. Vi tilbyder teknologiuafhængig rådgivning og hjælper vores kunder med at opnå succes gennem strategi, analyse og implementering

Strategi for digitalisering og AI



Vi hjælper vores kunder med at udvikle strategier for digitalisering og AI, så de kan realisere de potentialer, der ligger i den digitale verden.

Digital Operating Model



Vi hjælper vores kunder med at udvikle digitale driftsmodeller og it-organisationer, sikre digital kapacitet og afbalancere grænseflader mellem interne og eksterne partnere og processer.

Indkøb af digitale produkter og tjenester



Vi hjælper vores kunder med at indkøbe digitale tjenester. Lige fra den indledende analyse gennem forhandlings- og udbudsprocesser til etablering af et effektivt leverandørsamarbejde.

Digitaliseringsprogrammer



Vi hjælper vores kunder med at implementere og realisere de forretningsmæssige fordele ved ændringer i processer, digitale tjenester og produkter.

Kontakt og information

Digital Transformation i Danmark 2026-2027, IT i praksis®

Redaktion

Steen Christensen, Lorenzo Courir, Asger Højen Danielsen, Jacob Fink, Thomas Fjeldberg, Maja Levin, Nikolaj Vad Schou, Cathrine Lind, Thomas Trier Larsen, Nils Roien og Morten Damgaard

Udgivet af

Rambøll Management Consulting A/S
Hannemanns Allé 53
2300 Copenhagen S
Denmark

Telefon +45 5161 1000
www.ramboll.com/management-consulting

31. årgang, Version 1.0
ISSN: 2596-3821

Gengivelse af undersøgelsen er tilladt, når Rambøll Management Consulting angives som kilde.



Steen Christensen
Director
STEC@ramboll.com

Ansvarlig for
Digital Transformation i Danmark,
IT i praksis®



Lorenzo Courir
Consultant
LZCR@ramboll.com

Projektleder og kontaktperson for
Digital Transformation i Danmark,
IT i praksis®

Læs mere om, hvordan vi muliggør samfundets omstilling til en bærdygtig fremtid.
www.ramboll.com/management-consulting

Bright
ideas.
Sustainable
change.

RAMBØLL