CIO kredsens fælles indsats i forhold til digital suverænitet

DeiC konferencen 2026

v/ Tina Skriver Didriksen, vicedirektør i Digital, Roskilde Universitet



Indhold

- Hvad handler digital suverænitet om?
- Strategisk styring af digital suverænitet i en dansk universitetskontekst
- Fælles tilgang på tværs af alle danske universiteter
- Hvordan gør vi i praksis? Eksempel fra Roskilde Universitet

Hvad handler digital suverænitet om?

For at kunne tale om, hvordan vi som universiteter skal forholde os til digital suverænitet, er vi nødt til at starte med at have en fælles forståelse af begrebet og sætte det ind i en universitetskontekst.

Hvad handler digital suverænitet om?

Digital suverænitet handler om evnen til selvstændigt at styre, beskytte og fastholde vores kritiske, digitale teknologier, data og infrastrukturer, samt at kunne træffe og gennemføre egne teknologivalg uden at være bundet af enkeltleverandører, eksterne jurisdiktioner eller geopolitiske forhold.

= Digital robusthed

Det handler <u>ikke</u> om:

- At afskære sig fra globale teknologier og leverandører.
  De er centrale for innovation, drift og effektivitet. Og på nogle områder er der ikke et alternativ.
- At bygge alt selv. Det ville være dyrt, langsomt og ineffektivt.
- At øge IT-sikkerheden og beskytte universiteterne mod cyberangreb. I nogle tilfælde vil IT-sikkerheden blive forringet og sværere at håndtere.

- Vores grad af og håndtering af afhængighed til tech-giganter
- Vores evner til at beskytte og kontrollere vores data
- Vores muligheder for at kunne vælge leverandører til og fra

Digital suverænitet er i dag blevet en strategisk ledelsesdagsorden

Europa er i dag stærkt afhængig af få globale teknologileverandører.

Når teknologi, data og platforme bliver forretningskritiske, bliver afhængighed også en strategisk risiko.

Leverandørafhængighed

Cloud, data og produktivitetsplatforme domineres af få aktører

Geopolitik & regulering

Internationale konflikter og lovgivning kan påvirke adgang til data og services

Stigende sårbarhed

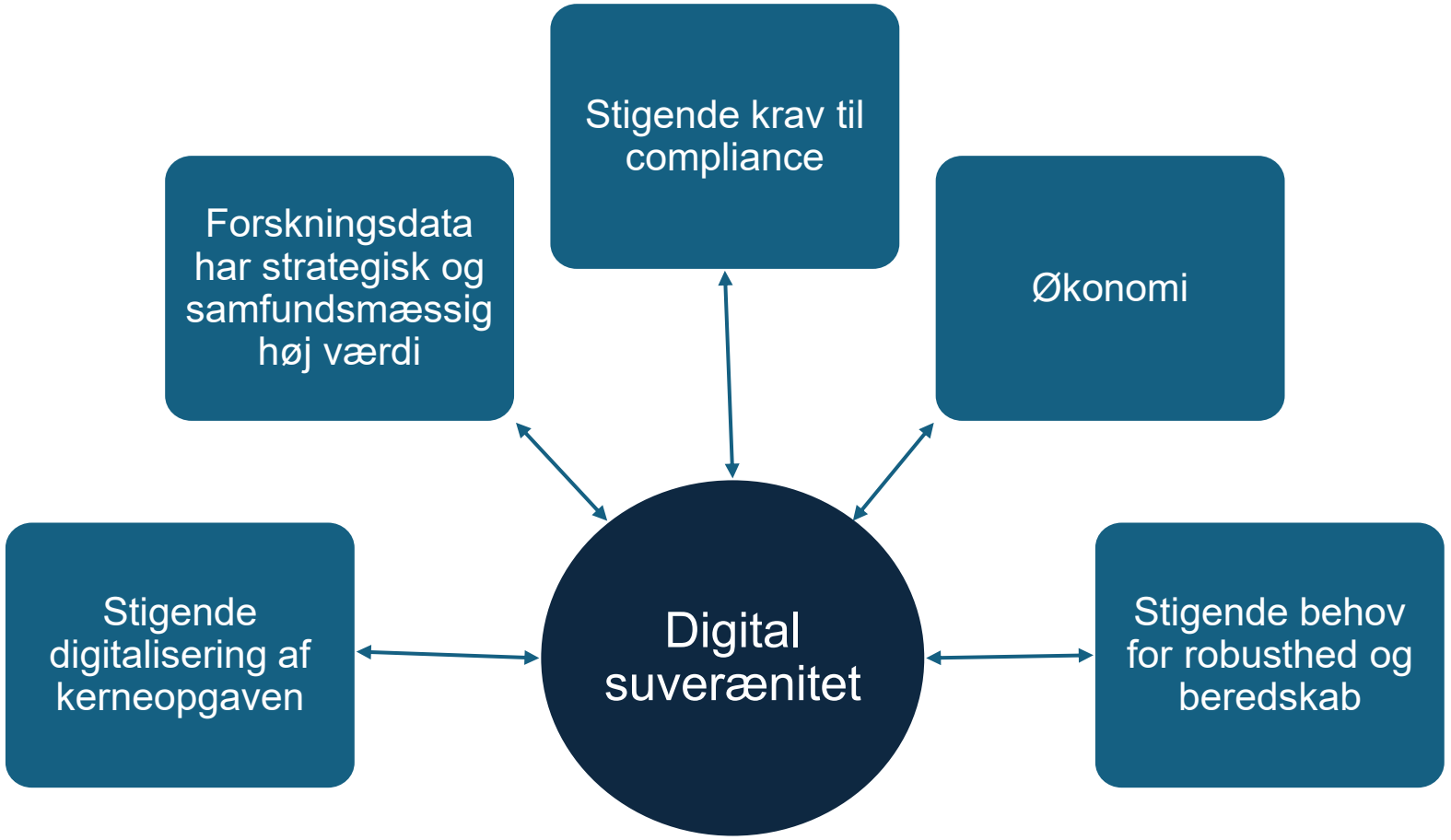
Driftsstop eller ændrede vilkår kan få direkte konsekvenser

Hvad betyder det for universiteterne

Digital suverænitet er ikke primært et IT-spørgsmål.

Det er et spørgsmål om:

- Strategisk styring af risici
- Digital robusthed
- Strategisk handlefrihed
- Forretningskontinuitet



Hvad betyder det set fra et ledelsesperspektiv?

Vi skal kunne drive vores kerneopgaver
– også når omverdenen ændrer sig

Digitale platforme er forretningskritiske.

Vi skal have reel valgfrihed

– og kunne sige nej, forhandle priser
og ændre retning

Data er strategiske ressourcer

Vi skal kunne kontrollere vores mest
værdifulde aktiver: data og viden

Vide hvor de ligger, hvem der har adgang
og sikre dem

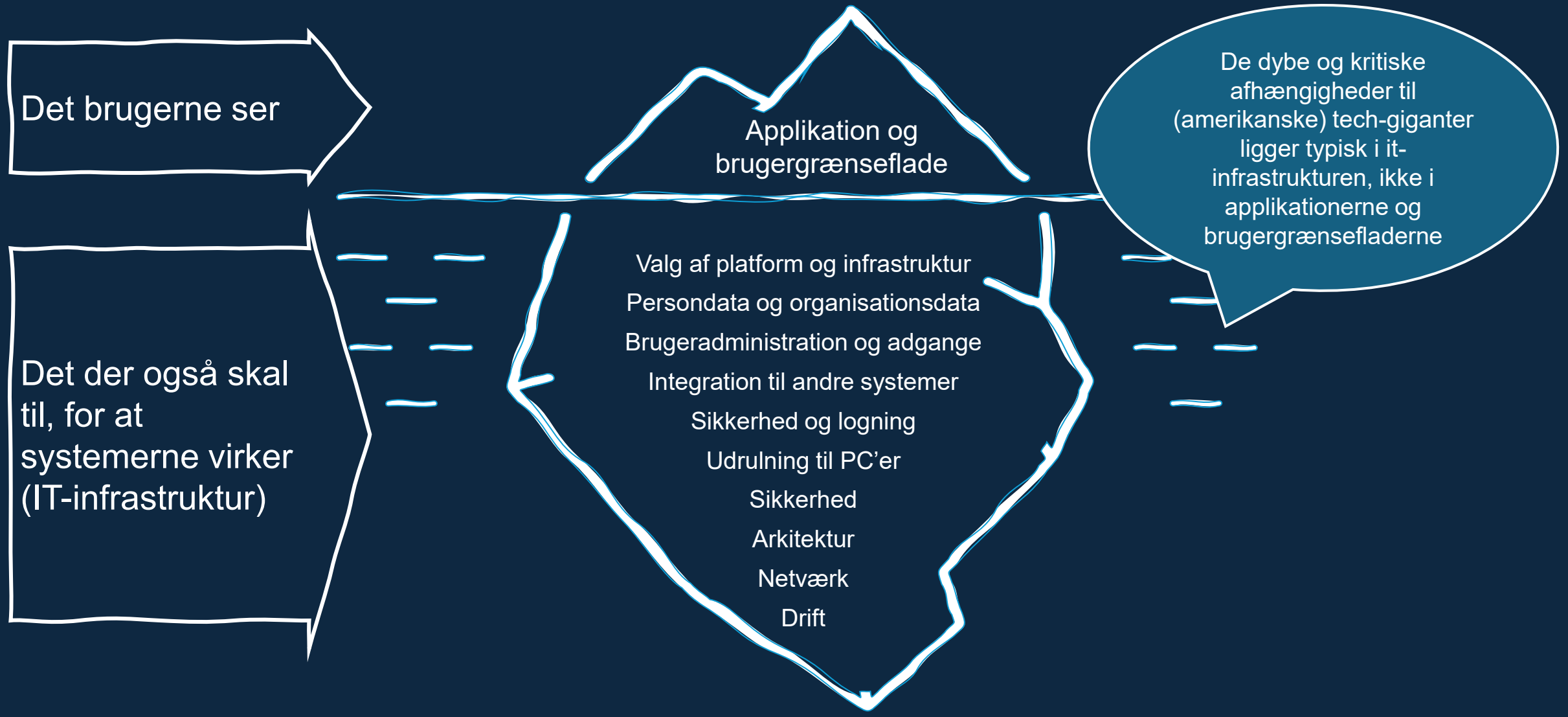
Robusthed er et ledelsesansvar

Vi skal være forberedte på kriser
og have en fungerende “Plan B”,
der gør det muligt at fortsætte driften i kriser

Strategisk styring af digital suverænitet i en dansk universitetskontekst

… kræver en fælles forståelse for, hvordan IT-infrastrukturen er opbygget, og hvad der bliver påvirket af de valg, vi tager omkring teknologivalg og grad af suverænitet.

Digitale systemer kræver, at den underliggende IT-infrastruktur virker



Afhængigheder ne findes i alle IT-lagene

Det handler ikke kun om vores IT-systemer, mail, telefoner og computere, men om alle lagene i infrastrukturen.

Fra computer og systemer til databaser, servere, netværk og ikke mindst sikkerhedsløsninger.

LAG	BESKRIVELSE
Applikations- og brugergrænselaget *Systemer og programmer*	ERP, CRM, specialudviklede systemer og SaaS-løsninger. AI, RPA mv.
Computere og andre devices	IT-udstyr, AV og telefoni
Brugerstyring	Identitetsstyring og adgangskontrol
Sikkerhed	Compliance og beskyttelse på tværs af hele IT-stacken.
Platformlaget	Operativsystemer, databaser, middleware, integrationsplatforme og DevOps-værktøjer.
Infrastrukturlaget	Servere, storage, netværk, cloud-infrastruktur og virtualisering.

Universiteternes mest kritiske afhængigheder

Her med amerikanske tech-leverandører som eksempel

- Microsoft
- Oracle
- Salesforce
- Cisco









Mulige veje at gå: Vi skal starte med et tydeligt formål

Er digital suverænitet et endemål for os eller ej – og i så fald hvorfor?

Vi bør starte med at definere, i hvilken grad vi ønsker suverænitet og hvorfor.

Og vi skal forholde os til både de fordele og ulemper, der følger med beslutningen, og hvad det vil kræve.

OBS!
Den store afhængighed til ikke-europæiske leverandører er ikke kun relevant for universitetssektoren.

Det er en generel situation for hele Danmark og hele Europa.

Vi bør derfor også forholde os til, i hvilken grad universiteterne skal gå forrest med denne dagsorden, eller om vi skal afvente en tydelig politisk retning.

Dilemma: Både fordele og ulemper

Begrænset suverænitet og høj afhængighed

Fordelene ved vores nuværende IT-infrastruktur, som bygger på høj grad af afhængighed til tech-giganter er:

- Modne, stabile og velafprøvede løsninger
- Høj innovationshastighed og adgang til ny teknologi
- Stærk cybersikkerhed og compliance-apparat
- Integrerede økosystemer, der reducerer kompleksitet
- Tilgængelighed af kompetencer og support
- Bedre mulighed for skalering og standardisering

Ulemper:

- Geopolitisk og strategisk sårbarhed
- Økonomisk afhængighed og manglende konkurrence
- Manglende kontrol over data og kritisk infrastruktur
- Lock-in og meget svære udskiftningsmuligheder
- Juridiske konflikter og compliance-usikkerhed
- Svækket innovationskraft i Europa
- Forsyningssikkerhedsrisici ved globale nedbrud



Høj suverænitet og lav afhængighed

Fordele ved høj digital suverænitet og lav afhængighed til tech-giganter er:

- Mindre sammenhængende/fragmenteret system-landskab
- Mindre sårbarhed i en urolig geopolitisk verden
- Mindre leverandørafhængighed
- Øget fleksibilitet og handlefrihed
- Øget gennemsigtighed og kontrol over data
- Bedre konkurrence i markedet
- Lavere licensudgifter

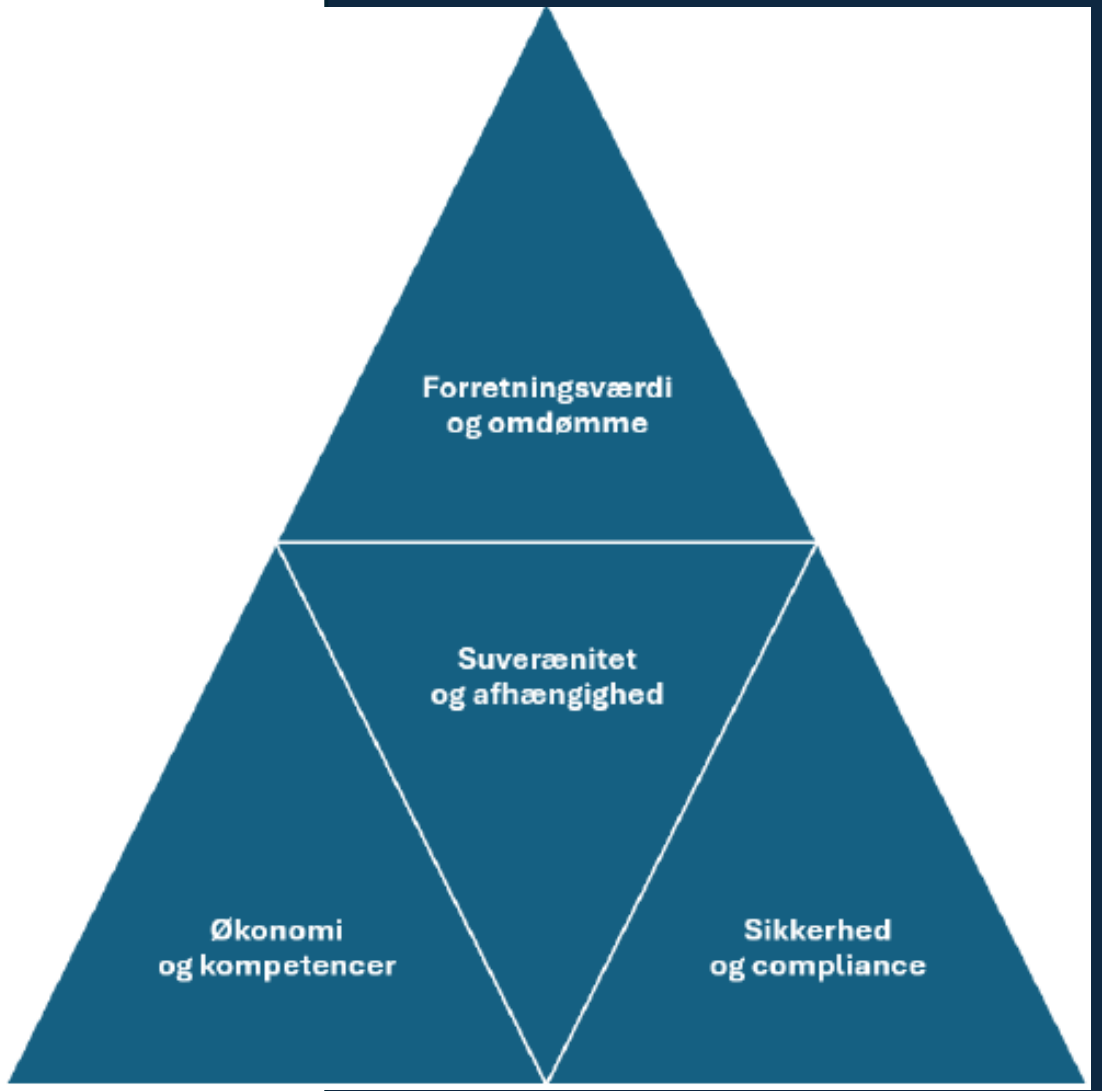
Ulemper:

- Omlægningen kræver store investeringer og ny type IT-organisation
- Lavere innovationshastighed
- Øget kompleksitet
- Nye kompetencekrav og rekrutteringsbehov
- Begrænsede eller ikke-eksisterende alternativer
- Fragmentering og lavere standardisering
- Risiko ved migrering
- Potentielt lavere cybersikkerhed på kort sigt

Vurderingskriterier som strategisk værktøj

Beslutninger om suverænitet og afhængigheder bør altid vurderes ud fra:

- **Forretningsværdi og omdømme:**
  Hvilken effekt ønsker vi at opnå?
- **Økonomi og kompetencer:**
  Hvor meget vil og kan vi investere – både i drift, omstilling og kompetenceopbygning?
- **Sikkerhed og compliance:**
  Hvilken lovgivning skal vi leve op til?
  Hvilket risikoniveau kan vi acceptere, og hvor kræver vi fuld kontrol?
  Hvordan skaber vi det nødvendige IT-sikkerheds set-up?



Mulige handlinger kræver forskellige indsatser



FÆLLES TILGANG PÅ TVÆRS AF ALLE DANSKE UNIVERSITETER

Suverænitetsdebatten i medierne bør ikke være styrende for universiteternes teknologivalg.

En balanceret tilgang med fokus på evnen til risikostyring og strategisk kontrol,
som er forankret i øverste ledelse.

Med henblik på at reducere sårbarhed og øge handlefrihed
– uden at afskære adgang til kritiske teknologier.

Behov for fælles tilgang, sprog, samarbejde og videndeling.

En balanceret tilgang til digital suverænitet på Roskilde Universitet

Fra strategisk beslutning til udmøntning i praksis…



Balanceret tilgang: Fra beslutning til praktisk udmøntning

Strategisk styring

Balanceret tilgang til digital suverænitet
Risikostyring
Datasikkerhed
Roller og ansvar

Differentieret datahåndtering

Fælles principper, fx

Risikobaseret tilgang
Aktive valg omkring afhængigheder
Plan B for kritiske systemer
Data som strategisk aktiv

Praktisk udmøntning

Ny infrastrukturstrategi
Fra ”Cloud first” til ”Hybrid og fleksibel sourcingmodel”

Opdaterede og sammenhængende politikker og styringsrammer

Vejledninger og awareness

Digital understøttelse

Øget dialog om behov og risici

<u>Fælles værktøjer:</u>

Dataklassifikation

Vurderingsmodel

Arkitekturprincipper

Risikovurderinger

Hvad betyder det i praksis for Digital

En balanceret tilgang til digital suverænitet handler ikke om at vælge fra – men om at vælge bevidst, styre aktivt og bevare handlefriheden.

Det kræver en anden og ny form for IT-understøttelse fra Digital og en anden form for ledelsesophæng og –styring – og ikke mindst strategisk forankring.

I 2026-2027 bygger vi det nye fundament, vi skal stå på for at kunne arbejde med en balanceret tilgang til digital suverænitet.

2026 mål ✓

Revidering og tilpasning af **fælles politikker** for IT-, informationssikkerhed og datamanagement

2026 mål ✓

Dataklassifikation som grundlag for beslutninger og services

2026 mål ✓

Strategisk funderet hybrid og fleksibel sourcingmodel for storage og compute og øget dialog med brugerne om muligheder og risici

2026 mål ✓

Øget fokus på organisatoriske og IT-tekniske risikovurderinger og handleplaner

2026 mål ✓

Gradvis stillingtagen, når noget skal fornys eller udskiftes og ved nye behov

2027 mål ✓

Strategiske principper for styringen og praktisk udmøntning i værktøjer og processer

2027 mål ✓

Tydelige og brugerrettede **IT-services**

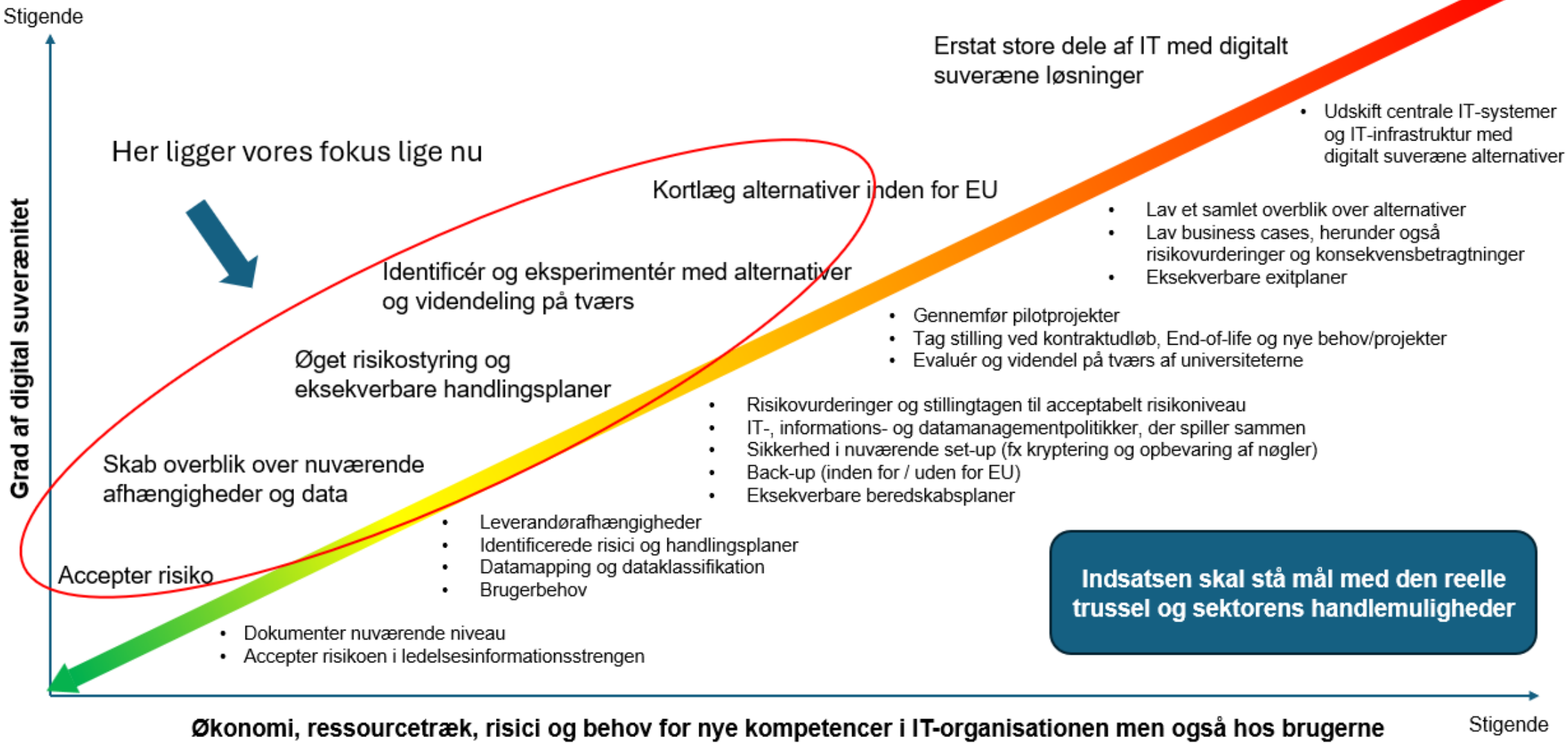
2027 mål ✓

Reviderede **IT-arkitektur-principper**

2027 mål ✓

Indarbejdes i processerne omkring **projektmodel, processer og systemgovernance**

Handlingstrappen og prioriteret fokus på Roskilde Universitet lige nu



Tak for opmærksomheden…