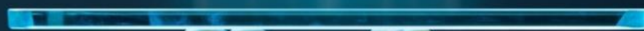


Cloud computing

10 dilemmaer

- og anbefalinger til løsninger



Mange danske virksomheder og organisationer arbejder med cloud-løsninger. Dansk IT's fagråd for Business & IT Alignment har erfaret, at der rejser sig en række centrale spørgsmål om hvor meget, hvordan og i hvilken takt, at cloud-løsninger strategisk og taktisk kan blive bragt i anvendelse.

Af Fagrådet for Business & IT Alignment

Fagrådet for Business & IT Alignment i Dansk IT har evalueret 10 konkrete dilemmaer ved brugen af cloud computing - og har en række anbefalinger til, hvordan man kan håndtere dilemmaerne. Der er tale om cloud-dilemmaer, som rådets medlemmer har mødt i deres arbejde med enterprise arkitektur og cloud i danske virksomheder og organisationer.

De 10 dilemmaer er beskrevet nedenfor under disse overskrifter:

1. Ja – selvfølgelig ved jeg, hvad cloud er
2. Stor omstilling i arbejdsopgaver og roller og behov for nye kvalifikationer
3. Vendor lock-in
4. (De-)centralisering af indkøb af cloud-ydelser
5. Er der udfordringer på Governance og integrationer til SaaS-løsninger?
6. Når Ops bliver glemt i DevOps
7. Hvordan sikres et økonomisk overblik samt samlet budget for brug af it i en organisation
8. Ejerskab af data
9. Legacy-systemet kan flyttes i cloud, men opnår virksomheden fordelene?
10. Enterprise arkitekt versus cloud arkitekt

Baggrund

Det kan være fristende for en virksomhed at overlade designet af transitionen til cloud eller valget af cloud-services til sin leverandør. Argumenterne kunne være, at leverandøren er mere vidende og bedre kan lave designet, og at leverandøren også er *ansvarlig* for den tekniske løsning. Det er en sandhed med modifikationer.

På engelsk skelnes mellem *accountable*, som er overordnede ansvarlige part, og *responsible* som er ansvarlig for udførelsen. Mens leverandørerne godt kan gøres *responsible* for at tage design-beslutninger om cloud, så kan *accountability* ikke udliciteres til leverandøren. For det er virksomheden, der kommer til at leve med resultatet af et dårligt design.

“All architecture is design but not all design is architecture. Architecture represents the significant design decisions that shape a system, where significant is measured by cost of change”

- Grady Booch

Den ansvarlige virksomhed sørger for at stå på mål for de cloud-designs, som vil være sværest og dyrest at lave om. Med andre ord arkitektur-beslutningerne om cloud. Dilemmaerne i denne artikel handler om, hvorvidt de svære og dyre beslutninger, som virksomheden er *accountable* for, er de rigtige. At hjemtage virksomhedens ansvar for de beslutninger vil være god, rettidig it-ledelse.

Hjemtagning af ansvaret kræver viden og indsigt. Det er Dansk IT's håb med denne udgivelse at give en hjælpende hånd til kunne at løfte det ansvar.

10 dilemmaer om cloud computing

De 10 beskrevne dilemmaer sætter fokus på, at cloud som teknologi og strategi stiller krav til virksomhederne. Der er også behov for nye kompetencer, et opdateret syn på sikkerhed i forbindelse med cloud-løsninger og en opdateret og tilrettet governance og økonomisyn, som it-afdelingen skal stå på mål for.

1. Ja – selvfølgelig ved jeg, hvad cloud er

Det er efterhånden sjældent, at vi drøfter hvad cloud egentlig er. Betyder det så, at vi har løst udfordringen og har et fælles sprog omkring cloud? Er vi organiseret, så vi effektivt kan arbejde med de nye metoder og værktøjer? Har vi en uniform model for cloud og integrationer mellem clouds og on-premise-løsningerne?

Nej, det tænkte vi nok.

Prøv at kig på nedenstående definitioner fra det amerikanske NIST (National Institute of Standards and Technology). De er frit fortolket af fagrådet.

Essential Characteristics

- *On-demand self-service*: Det er en løsning, som brugeren (consumer) selv kan købe og tage i brug umiddelbart.
- *Broad network access*: Løsningen er tilgængelig fra internettet eller inden for et stort firmas domæne.
- *Resource pooling*: Regnekraft, lager og andre ressourcer deles med andre og er ikke en fast størrelse.
- *Rapid elasticity*: Løsningen kan skalere til peak perioder og være helt på nul - både for antal brugere, regnekraft og datamængder.
- *Measured service*: Det kan måles hvem, som bruger hvad. I mange tilfælde danner det grundlag for en betaling / omkostning.

Hvor mange af de fem essentielle karakteristika har du overvejet, sidst du drøftede en cloud-løsning med dine kollegaer?

Essential Characteristics	Service Models	Deployment Models
On-demand self-service	Infrastructure as a Service (IaaS)	Private cloud
Broad network access	Platform as a Service (PaaS)	Public cloud
Resource pooling	Software as a Service (SaaS)	Community cloud
Rapid elasticity		Hybrid cloud
Measured service		

Kilde: [NIST](#)

Anbefaling: Når du arbejder med cloud-dilemmaerne (både i dagligdagen og i artiklen) og har dine egne drøftelser, bør du forholde dig til de fem cloud-karakteristika, de tre service modeller og hvordan deployment-modellen ser ud.

2. Stor omstilling i arbejdsopgaver og roller og behov for nye kvalifikationer

Er din virksomhed klar til at sige farvel til visse, gamle kompetencer ved en omstilling, er der stadig kritisk masse ift. opgaver der stadig skal laves - især i transition? Når driftsmodellen skifter fra outsourced til cloud, bliver ansvaret i virksomhedens "driftsafdeling" ændret fra at være teknikere, der sikrer, at virksomheden som kunde har fået den rette ydelse for outsourcing, til at afdelingen skal være i stand til at forvalte IaaS og PaaS på fx Azure og være specialister på det område.

Der kommer et arbejde med at omstille sine medarbejdere til at få tillid til en anden form for teknologi og håndtering, end man er vant til. Myter har det med at hænge ved - f. eks. at skyen er mere usikker.

Anbefaling: Du skal som enterprise arkitekt (EA) sikre, at virksomheden har en aktiv cloud-arkitekt - eller at du selv påtager dig denne rolle. Der skal være viden om hvilke tekniske løsninger, der skal beholdes,

også når der outsources, så de rigtige krav og evalueringer af leverandører kan foretages. De kvalifikationer kombineret med viden om virksomheden giver værdien.

3. Vendor lock-in

For de it-værktøjer, man som virksomhed anvender i sin kerneforretning og sine ydelser/produkter til kunderne, har der altid været en større eller mindre risiko i forhold til den afhængighed, man har fået til leverandører, medarbejdere, partnere osv.

I support processerne sigtes ofte på, at værktøjerne standardiseres evt. med en konfigurerings. Og har man behov for at skifte disse værktøjer, så kan det pga. konkurrence i markedet og netop standardiseringen ofte gøres mere eller mindre smidigt. Men i relation til kerneprocesserne hvor meget kommer man så ud af kontrol ved at bero på en leverandør og dennes softwareprodukter? Det er altid en god ide at gøre sig det klart, hvordan exit-strategien ser ud for det indkøbte produkt, inden man indgår kontrakten.

Er det blevet anderledes for cloud-produkter? Ser man på SaaS-løsninger, så er det stadig vigtigt at overveje, hvor meget afhængighed ens forretningsudvikling har af netop det produkt. Produkt-roadmap fra leverandøren skal tilfredsstille ens egne behov, såsom udbygges og vedligeholdes produktet, som man gerne vil ønske og ajourføres roadmappet stabilt?

Leverandørens fokus kan også ændre sig og give helt andre forudsætninger som kunde til produktet. Her skal exit-strategien derfor ikke glemmes, og måske skal man qua lethed i at få produktet løbende udfordre sig selv med afhængigheden.

Anvender man IaaS i en public cloud vil man have en langt større uafhængighed i forhold til leverandøren - der venter dog også et større arbejde i opbygningen af ens forretningsløsning. Udarbejder man selv sin applikation i et PaaS miljø fx hos en public cloud-leverandør, får man mere uafhængighed fra leverandører generelt. Dog hvis man bygger sin løsning op i dennes 'native' komponenter, så får man igen en større vendor lock-in til den specifikke cloud-leverandør. Det koster på den ene side at have en arkitektur, som understøtter standard, og på den anden side betaler man for fordelene i en proprietær løsning med lock-in.

Anbefaling: Under ikke-funktionelle krav bør man derfor have overvejelser om portering af løsningen. De tanker, man gør sig der, vil være en anden måde at se ens risiko på. En applikationsstrategi, der bygger på native-komponenter, kan have et utilsigtet vendor lock-in, og det kan være omfattende at skulle bygge om på et senere tidspunkt, hvis man ønsker at portere (dele af) løsningen.

Generelt skal man være bevidst om, hvad konsekvenserne er for de strategier, der træffes valg om i retning af leverandører. Valg af cloud-leverandør bør have en samlet forretning og teknisk vurdering med væsentlige leverandør-scenarier og reaktionsmuligheder. Byg det evt. ind i et *cloud vendor assessment*.

4. (De-)centralisering af indkøb af cloud-ydelser

Indkøb af it-ydelser i form af SaaS-produkter kan gøres meget nemt af fx medarbejdere i de enkelte forretningsfunktioner, der kan supplere eller sammensætte deres it-understøttelse af selvstændige komponenter på SaaS-markedet. De enkelte komponenter skal håndteres på samme måde som de store enterprise-systemer, når det kommer til sikkerhed, GDPR, business continuity, it-support mv. Det stiller krav til den enkelte medarbejder der laver et indkøb, som skal sikre, at intet "smutter" mht. sikkerhed, GDPR mv. Og betyder, at de enkelte medarbejdere, der varetager købene, skal sikre tilpas høj kvalitet på disse parametre.

Da støtte til indkøb er mere nødvendige support-kompetencer end kerneforretning i de fleste virksomheder, og der ofte støttes med eksterne specialister - fx fra cloud-leverandørerne - så kan det være en fordel at centralisere støtten til decentralt valg af it-løsning. Derudover skal virksomhedens it governance også bygges til denne slags overleveringer fra mange kilder - den enkelte medarbejder - til decentral support.

Anbefaling: Man kan med fordel etablere et virtuelt cloud assessment forum, der inddrages i leverandør- og løsningsevaluering samt sikre, at governance og evt. 'hvidlister' kan lette arbejdet. Forummet skal have særligt fokus på at være hurtigt arbejdende, beslutningstagende, og kompetent, samt en besluttet del af governance. Det kan fx skabe et cloud vendor assessment til organisationen, som kan bruges som kommunikationsværktøj og i sig selv vil give en større bevidsthed om cloud.

5. Er der udfordringer på Governance og integrationer til SaaS-løsninger?

"A service is a means of delivering value to customers by facilitating outcomes customers want to achieve, but without the ownership of specific costs and risks."

- ITIL v/3

I den ultimative tolkning af Software as a Service ligger ansvaret (responsibility) hos leverandøren af den valgte service, men der er stadig et ansvar for virksomheden omkring sammenhænge i data-klassifikation og -integration, brugeradgange og roller, samt business continuity og risk management.

Som firma/organisation skal du ikke selv optimere sikkerhed, performance og sikre tilgængelighed – det er leverandørens ansvar (og også interesse). Men er det så ikke bare at bruge løs? Som firma og organisation har du stadig ansvaret for at sikre, hvad der er acceptabel sikkerhed, performance og tilgængelighed i forhold til virksomhedens risikoappetit. Dertil kommer, at softwaren, der leveres, ofte er en del af en større sammenhæng. Men du får kun, hvad du betaler for.

Den første udfordring kommer allerede, når løsningen er købt, uden at sammenhængen til de øvrige systemer er gennemtænkt. "Vi skal bare bruge løsningen standalone". Det er så lige ud over integration af bruger og adgange via AD og så selvfølgelig lidt master data fra SAP, der også ret hurtigt dukker op som behov. For en del SaaS-løsninger – små værktøjer og niche løsninger, så afgrænser det

udfordringen. Men der er også løsninger, som skal integreres i to-vejs data og proces flows – og hvor backup af såvel data som konfiguration heller ikke er uden betydning.

Ikke alle udfordringer er kendte i on-premise verden. Et eksempel er "Governor limits" på SaaS løsningen. Fordi man deler ressourcerne med andre, så kan man ikke gøre, som man vil med ressourcerne. I og for sig en pendant til den fysiske verdens bæredygtighed, og noget man måske har glemt/ikke fået lært, fordi vi skal 20-30 år tilbage i tiden for at se på, hvornår man talte clockcykler og bits. Ressourcerne har i en periode umiddelbart været rigeligt, men aldrig nok til dårlige algoritmer, og sjuskede queries.

Derudover kan en manglende teknisk-, data- og compliance-indsigt give en glorificeret forståelse af, hvad det kræver at lave integration mellem systemer. Det er fx ikke nødvendigvis så trivielt, som det kan tegnes på en Powerpoint.

Anbefaling: Som EA kan du være med til at fremme fokus på governance omkring SaaS-løsningerne og sikre, at både brugerne (forretningen) og IT tager del i ejerskabet af løsningerne og sammenhænge til det øvrige systemlandskab, herunder sikring af data, brugerroller og ansvar, og sidst men ikke mindst økonomi og driftsomkostninger, som løbende skal overvåges for, at SaaS- løsningerne ikke løber løbsk økonomisk og uden for kontrol i forhold til governance på virksomhedens it-portefølje og anvendelse. Følg konceptualiseringen af SaaS-anvendelsen op med en afdækning af kompleksitet, risici, afhængigheder og evt. økonomi både ifht. forretning og teknik.

6. Når Ops bliver glemt i DevOps

Lad os slå muren ned mellem udvikling og drift og lad vores udviklere arbejde agilt med DevOps. Det er en god og tillukkende tanke, og der er rigtig meget hjælp at hente i agile teorier og hos leverandører af specielt PaaS/IaaS – fx Microsoft Azure.

DevOps er skabt i et cloud-fundament af bestemte virksomheder med bestemte scenarier, og bliver nu hyldet som "det rigtige", men er det også noget, der overhovedet kan bruges i alle de scenarier, som man tror, at det skal? De store leverandører og deres økosystem er det, vi som virksomheder/brugere skal rette ind efter. Det skal harmonere med, at vi ønsker at opnå essentielle cloud-karakteristika for vores løsninger (fx rapid release, elasticity, scalability) - for er det ellers besværet værd?

Det hele bliver bare lidt udfordret af, at vi ikke ændrer beslutningsmodel og måden, it organiseres og tildeles midler på. Vi arbejder stadig med projekter, og det er også sådan, vores it-organisation får midler.

Det er her, interessen for Ops inkl. sikkerhed og andre gode drift-dyder glider lidt i baggrunden, når vi løber for stærkt med DevOps.

Modsat er det også svært at tage springet til et DevOps- og produkt-fokus – uden projekter og milestones – så vi skal finde en model, der skaber balancen. Ellers bliver skyen bare en tåge af dårlige løsninger uden klart ejerskab.

Anbefaling: Som EA eller EA-funktion kan du bidrage to steder:

- Først og fremmest kan du hjælpe med at modne et produkt fokus – vel at mærke på områder, som egner sig. Det er typisk områder, der kan defineres og afgrænses uden mange afhængigheder og uden behovet for et helt fastlagt forløb.
- Hvis ikke der er modenhed og vilje til at organisere sig efter DevOps-organisationens mange nye roller og ansvarsdelinger, så kan du som EA fokusere på, hvordan Ops- organisationen inddrages i rette tid, uddannes og også automatiserer deres arbejde.

7. Hvordan sikres et økonomisk overblik samt samlet budget for brug af it i en organisation

Med den voksende anvendelse af cloud-løsninger i organisationerne og virksomhederne og den lette tilgang for nye brugere til at kunne benytte cloud-løsninger, er der et voksende behov for at kunne følge op på anvendelse af cloud-løsninger i virksomhederne og den økonomisk udgift, som det påfører virksomhederne og organisationerne.

Mulighederne for at tilgå SaaS-løsningerne er ofte lette og uden umiddelbare forhindringer for, at brugerne kan oprette og tilgå disse løsninger, så den lette tilgang er en umiddelbar fordel for brugerne.

Den prismæssige konsekvens af cloud-anvendelse er ofte uigennemskuelig, fordi man i forvejen ikke har et 100 procent overblik over, hvad der er ens nuværende og kommende forbrug. Hvordan er omkostningsbilledet skruet sammen i forhold til forventet forbrug? Betales for en ydelse efter forbrug, kan det være et større arbejde at holde øje med forbrug, som måske er ved at overstige budgettet? Skal man ligefrem hindre ressourceanvendelse, hvis man overhovedet kan det?

Ved en migrering fra on-premise til cloud kommer der nemt en periode, hvor virksomheden stadig har den fulde on-premise konfiguration kørende, mens man omstiller sig til det rette niveau af cloud-anvendelse.

Og det er er ikke sikkert, at alt kommer med i cloud, så afvikling af denne del, som går i cloud i forhold til det eksisterende systemlandskab, skal også gennemføres for at opnå besparelser.

Det kan være et komplekst arbejde at få indsigt i den præcise omkostningsstigning eller fald. Udfordringerne for it-afdelingen og den øvrige organisation er at kunne få et overblik over anvendelsen og sikre, at der ikke indkøbes parallelle løsninger på ensartet krav, og at man kan overholde både

sikkerhed og data compliance på de data, som lægges i skyen, og hvilke exit-kriterier, som er aftalt med SaaS-leverandøren i tilfælde af konkurs, eller at virksomheden ønsker at tage løsningen tilbage.

Med EA-øjne er der et fortsat ønske om at kunne se cloud-løsningerne som en del af applikationsporteføljen, så den samlede anvendelse på tværs af virksomheden kan opgøres, så forretningsmæssige ønsker og også non-funktionelle krav og support bliver tilgodeset på tværs af cloud og on premise drift.

Mange bække små gør en stor å, og med it service som tidsregistrering, skabeloner til Office, digitale underskriftsløsninger, projektoversigter med mere, kan it-omkostningerne vokse eksponentielt, og der skal gøres en indsats for at bevare overblikket over udgiften.

Anbefaling: Få etableret en proces i virksomheden for at anskaffe cloud-løsninger, hvor it fortsat er en aktiv partner, således at hver cloud-anskaffelse kan ske ud fra et centralt virksomheds- og sikkerheds-syn, og at it-indkøb får en aktiv rolle ved at vurdere udgiften og de løbende omkostningerne ved cloud-anvendelserne. Sidst men ikke mindst skal virksomhedens sikkerhedsafdeling ind over for at sikre, at der ikke bliver eksponeret interne data, og hvordan compliance med gældende regler kan sikres.

8. Ejerskab af data

"Data som det nye guld" er et gennemgående tema, men hvordan forholder det sig med ejerskab og adgang til data, når man lagrer det hos en cloud-leverandør? Grundlæggende ved man ikke helt, hvor det bliver af, men det bliver jo lagret på et fysisk sted. Og data kan i princippet replikeres i det uendelige, og hvem har ret til at tilgå dine data? Det gælder for data som for processer, funktionalitet, SLA osv. at *accountability* ikke kan outsources til leverandøren.

Som virksomhed - hvad enten man betegner data som et ædelmetal af den ene eller anden kaliber eller ej - så skal man selv sørge for at have eller købe kompetencerne for at kunne imødegå risici ved placering af data. Det er heller ikke alt data, der er guld - noget er ligefrem kronjuveler, og andet er meget ordinært. Klassificering af data kan sikre det rette fokus på det rigtige data - lad interne roller være ansvarlige for og tage ejerskab af alt data.

Lovgivning for lande er bestemt ikke ens. Som dansk virksomhed af en vis størrelse er man typisk godt afklaret i den danske og EU-lovgivningen - eller kan få assistance til det. Lagrer man data i lande uden for EU, bør man have særlig opmærksomhed på ejerskabet, og om man overhovedet må sende data ud af landet, hvis man får behov for det. Adgang til data kan være usikkert - har myndighederne i det pågældende land adgang til data; og hvis ja, kunne man så være nervøs for at det bliver udnyttet?

En virksomhed kan fx også kryptere egne data - enten via cloud-udbyderens service; som er til for at beskytte mod utilsigtet adgang, men også mod en regeringsadgang? Alternativt kan man også udvikle og kryptere data (eller væsentlige dele af det), hvilket dog kan komme til at koste mere forbrug ved ud- og indpakning.

Anbefaling: Vær klar på hvor cloud-leverandøren lagrer (og replikerer) dine data, og vær klar på hvad lovgivningen er i det pågældende land. Afdæk strategien i tilfælde af exit, opkøb, konkurs og lignende.

Lad interne medarbejdere tage ansvar for sikkerheden og tilgængeligheden af data inden for rammerne af, hvad der er muligt - herunder muligheden for almindelig funktionalitet som at hente, redigere, slette - også i relation til GDPR. Lad det være en del af jeres leverandørvurdering inden valg af cloud.

9. Legacy systemet kan flyttes i cloud, men opnår virksomheden fordelene?

Der er set flere eksempler på ønsker om at flytte fra et specialudviklet, on-premise system til skyen. Begrundelserne har været flere på samme tid: At spare penge, øge udviklingshastigheden eller øge fleksibiliteten. Teknisk set er det da også ofte muligt - og til tider endda simpelt - at flytte systemet i hvad, leverandørerne kaldet et "lift-and-shift": Systemet flyttes ved virtualisering af de servere, systemet ligger på i dag eller efter kodekonvertering af fx COBOL til Java, som så efterfølgende bliver driftet i skyen.

Spørgsmålet er dog, om en lift-and-shift flytning til skyen vil opnå de ønskede fordele? Lift-and-shift kan virke tiltalende i sit enkle koncept. Simpel og hurtig provisionering af ekstra servere kan - ideelt set - hurtigt få bugt med overbelastning og lange svartider. Men realiteterne er ofte mere brogede.

Legacy-systemer er sjældent bygget til at kunne udnytte mulighederne i cloud, som on-demand horisontal skalering og automatisk neddrøsling uden for peak-perioder. I praksis opstår ofte performance-flaskehalse og besvær med at adskille lagerplads i dyre og billige partitioner. Derfor kan driftsomkostningerne ved at gå i skyen risikere at blive overraskende høje uden at fordelene materialiserer sig.

Ud fra en EA-synsvinkel er spørgsmålet om flytning af et legacy-system til skyen et spørgsmål om, hvilke fordele virksomheden ønsker. En god enterprise arkitektur kræver ikke nødvendigvis anvendelse af cloud. Den rigtige enterprise arkitektur er den, som understøtter virksomhedens behov, og en flytning til skyen er da heller ikke altid en god idé.

Anbefaling: Få en dialog med forretningen og leverandøren ved at stille de gode spørgsmål og få belyst de sammensatte bevæggrunde bag ønsket om at flytte til cloud.

- Øget udviklingshastighed er ofte ikke afhængigt af, om systemet driftes i cloud eller ej. Hvis øget udviklingshastighed er ønsket, så fokusér i stedet på at få etableret automatisk test og automatisk deployment (CI/CD). Cloud-teknologi kan hjælpe, men er ikke en forudsætning for at lykkes med det.
- Omkostningsreduktion *kan* opnås, men kun hvis systemets arkitektur tillader det. Der kan være gevinster, hvis system-ressourcerne i dag er overdimensionerede og i stedet kan erstattes af få

og små cloud-ressourcer uden for peak-tidsrum, eller hvis virksomheden står foran investering i nye system-ressourcer, som på den måde kan undgås.

- Legacy-systemer kan være af en teknisk dårlig kvalitet og have høj teknisk gæld. At flytte det til skyen i den stand, det er i, løser ikke de problemer, som er kendetegnet for legacy-it. Hvis det er tilfældet, så overvej alternativer til at flytte legacy-systemer til skyen som "lift & shift":
 - Omkodning af systemet med forskellige velafprøvede, moderne værktøjer og teknikker,
 - Erstatning af systemet med en kombination af standardsystemer, som evt. kan være cloud-baserede,
 - Indkapsling af systemet og i stedet udstille dets data og funktionalitet som API'er, som tillader andre systemer gradvist at overtage it-understøttelsen, samt
 - Etablering af en "digital platform", som kan fjerne noget af forandrings-preset fra legacy-systemet.

10. Enterprise arkitekt versus cloud arkitekt

Der er forskellige holdninger til, om EA-arkitekten og cloud-arkitekten er den samme person eller rolle. Ofte ses et stillingsopslag, hvor man efterspørger en enterprise arkitekt, men hvor første bulletpunkt under arbejdsopgaver er en transformation af virksomhedens it-anvendelse til skyen.

Enterprise arkitekten skal kende nok til cloud-fordele og de mulige service modeller for cloud- løsningers (IaaS, PaaS og SaaS) fordele og den mulige anvendelse i virksomheden.

Der vil være behov for at involvere både infrastruktur-arkitekter og løsningsarkitekter (applikationer), såfremt virksomheden satser på et udpræget mix af IaaS, PaaS og SaaS, da der er brug for detaljeviden til at kunne sikre cloudløsningernes samarbejde og dataudveksling med on premise-løsningerne. Ligeledes vil sikkerhedsarkitekterne have stor interesse i at risikovurdere cloud-løsningerne i forhold til compliance og mitigering af risici.

Der vil være brug for at kunne dokumentere de valgte løsninger, som er foretaget for at sikre virksomhedens anvendelse af cloud-løsninger.

Anbefaling: Få styrket samarbejdet mellem enterprise-arkitekterne, løsnings-arkitekterne, infrastruktur-arkitekterne samt sikkerheds-arkitekterne, således der kan skabes en proces for hvordan cloud-løsningerne evalueres, risikovurderes og mitigeres, samtidigt med at viden om cloud-anvendelse i virksomheden udbygges, og arkitekturkompetencerne opbygges, således at cloud arkitekt-rollen kan deles/understøttes i fællesskab.

Medlemmer af Fagrådet for IT & Business Alignment

Jan Staack

Allan Baungaard Jakobsen

Jesper Platz Helles

Michael Folkmann

Peter Nørregaard

[Mere om fagrådet](#)

