

IT-STRATEGI FOR FOLKEKIRKENS IT 2020-2022

Den 1. januar 2020
Akt nr. 95028



Baggrund

Digitalisering i folkekirken sker et samspil mellem overordnede målsætninger, teknologiske muligheder og konkrete beslutninger. Digitaliseringsstrategien 2020-2025 for folkekirken og Kirkeministeriet udstikker generelle pejlemærker og principper for digitalisering i folkekirken i et 5-årigt perspektiv.

Digitaliseringsstrategien understøttes af en it-strategi, som med en 3-årig tidshorisont beskriver, hvilke teknologier, it-politikker og styringsmodeller Folkekirkens It vil anvende som grundlag for at levere og udvikle it-ydelser til folkekirken og Kirkeministeriet.

It-strategien lægger sig endvidere op af de rammer, der er fastlagt i gældende It-arkitekturprincipper for Folkekirkens It og Informationssikkerhedspolitik for Kirkeministeriet og Den danske folkekirke.

Folkekirkens It er den enhed i Kirkeministeriet, som varetager drift og udvikling af folkekirkens og Kirkeministeriets fælles digitale løsninger. Som en del af Kirkeministeriet er Folkekirkens It underlagt de almindelige forvaltningsmæssige og statslige regler samt revision.

Kirkeministeren har nedsat en It-Følgegruppe, som rådgiver Kirkeministeriet om it-strategiske overvejelser, forretningsudvikling, økonomisk styring og prioritering. It-Følgegruppen arrangerer desuden en årlig digitaliseringskonference med bred deltagelse fra hele folkekirken. Folkekirkens It er sekretariat for It-Følgegruppen.

It-budgettet fastsættes af Kirkeministeren efter indstilling fra It-Følgegruppen henholdsvis Budgetfølgegruppen.

It-Følgegruppen rådgiver om fælles og centrale digitaliseringsinitiativer, inden der træffes beslutning om iværksættelse. Den enkelte myndighed og institution tager aktivt stilling til og beslutter, hvordan man ønsker at bruge digitaliseringen lokalt inden for de gældende regler og rammer.

It-strategien indeholder bl.a. rammer for valg af teknologi, anskaffelse af nye it-løsninger, hvilken infrastruktur og arkitektur der arbejdes ud fra m.v. It-strategien skal således sikre, at konkrete digitaliseringsinitiativer kan gennemføres med de mest hensigtsmæssige tekniske midler og procedurer.

It-strategien bidrager til optimal udnyttelse af de midler, der anvendes på it via en sammenhængende og veltilrettelagt styring, herunder effektiv anvendelse af eksterne leverandører samt rettidig vedligeholdelse og fornyelse af it-infrastrukturen.

It-strategien er dermed Folkekirkens It's værktøj til at sikre fælles forståelse og konsistens i arbejdet vedrørende følgende temaer:

- Den anvendte it-arkitektur (afsnit 4)
- Den anvendte it-infrastruktur (afsnit 4)
- Den valgte teknologi (afsnit 5)
- Den fastlagte informationssikkerhed (afsnit 6)
- Den valgte placering af opgaveløsningen, hhv. internt eller ved eksterne leverandører (afsnit 7)
- Den vedtagne styringsmodel for it og leverandører (afsnit 8)



Indholdsfortegnelse

1	It-målsætninger	5
1.1	Hvilken it-arkitektur er der brug for?	5
1.1.1	Behov afledt af digitaliseringsstrategien.....	5
1.2	Teknologier der understøtter arkitekturen.....	6
1.2.1	Miljøer/platforme, herunder versioner.....	6
1.2.2	Påvirkning af it-infrastrukturen.....	7
1.3	Arbejdspladsudstyr.....	7
2	Teknologivalg	8
2.1	Krav til udvikling.....	8
2.2	Brugerstyring.....	8
2.2.1	Ansatte	8
2.2.2	Menighedsrådsmedlemmer og frivillige.....	8
2.2.3	it-medarbejdere og it-administratorer	8
2.3	Integrationsteknologier	9
2.4	Applikationer og forretningsprogrammel.....	9
2.4.1	Applikationer med integration i Folkekirkens It's brugerstyring....	10
2.4.2	Applikationer, der primært retter sig mod offentligt tilgængelige hjemmesider.....	10
3	Informationssikkerhed og databeskyttelse.....	11
3.1	Organisering	11
3.2	Sikkerhedsniveau – målsætninger	11
3.3	Styring – realisering af målsætning	12
3.4	Beredskab og kontrol.....	12
4	Hvilke opgaver løses internt – hvilke eksternt?.....	13
4.1	Principper for anvendelse af interne og eksterne it-kompetencer i Folkekirkens It.....	13
5	It-Governance	14
5.1	Gennemførelse af it-projekter	14
5.2	Leverandørstyring.....	15



Hvordan efterleves it-strategien?

It-strategien er Folkekirken's It's værktøj til fastlæggelse af rammerne for, hvordan it-ydelser skal tilvejebringes, udvikles og styres.

På baggrund af it-strategien udarbejder og vedligeholder Folkekirken's It et teknologisk roadmap, der tydeliggør de nødvendige driftsmæssige initiativer, eksempelvis ved udløb af teknologier og sikkerhedsstandarder.

Desuden – i et værktøj til arkitekturunderstøttelse – et roadmap som omfatter standardapplikationer og andet forretningsprogrammel. Dette roadmap giver et overblik over applikationsporteføljen (systemer i drift), herunder indgåede kontrakter vedr. applikationer og teknologiunderstøttelse.

Formålet med de 2 roadmaps er desuden at sikre en kontinuerlig styring af teknologierne i Kirkenettet og give et overblik over arkitektur og aftaler vedrørende applikationer og forretningsprogrammel.

Roadmaps er til tjenstligt brug og indgår ikke i den offentliggjorte It-Strategi

Herudover vedligeholdes i forhold til digitaliseringsstrategien et overblik over igangværende projekter i forretningsudvikling og projekt – projektporteføljen.

Applikationsporteføljen og projektporteføljen er sammenhængende, da færdige projektløsninger indgår i applikationsporteføljen ved projektafslutning. Omvendt kan idriftsatte applikationer afføde et behov for fornyelse eller større justeringer, der foranlediger igangsættelse af nyt projekt.

It-strategien godkendes af Folkekirken's It's ledelse, og revideres som hovedregel årligt.



1 It-målsætninger

1.1 Hvilken it-arkitektur er der brug for?

1.1.1 Behov afledt af digitaliseringsstrategien

1.1.1.1 Grundlæggende it-arkitektur

Der arbejdes mod en platformsuafhængighed på Kirkenettet, og at der leveres it som understøtter en 'brug dit eget udstyr'-tilgang ('BYOD'¹). Det vil også ofte være det krav til it-løsninger, at de fungerer responsivt og kan afvikles på både pc og mobile platforme, jf. afsnit 5 om teknologivalg.

For at kunne opfylde dette skal Folkekirkens It kunne tilpasse arkitekturen og derfor konstant være opmærksom på alt, hvad der rører sig, og i hvilken retning udviklingen går. I forbindelse med anskaffelse af enhver ny løsning skal der være en åben dialog således, at systemerne ikke risikerer uforvarende at blive afhængige af en bestemt teknologi eller udelukkende kan interagere med én type udstyr.

Med henblik på at kunne levere den rette arkitektur skal der være enighed om, hvilke services og systemer der skal være til rådighed, herunder ressourcer m.m.

Der anvendes adskilte udviklings-, test- og produktionsmiljøer, og udvikling må ikke ske i test- og produktionsmiljøer. Test af nye systemer på testmiljøet skal sikre, at de nye systemer er kompatible med allerede eksisterende systemer inden idriftsættelse. Samtidig sikrer Folkekirkens It, at de nødvendige standarder er korrekt anvendte, at dokumentation er til stede, samt at løsningen kan afvikles i et stabilt driftsmiljø.

1.1.1.2 Fleksibel it-infrastruktur

Folkekirkens It skal levere en it-infrastruktur, der hurtigt og sikkert kan tilføjes ressourcer, når der opstår behov herfor. Ligeledes skal der sikkert og hensigtsmæssigt kunne lukkes for systemer, der ikke længere er i brug, eller skrues ned for systemer, der lægger beslag på for mange ressourcer, som reelt ikke anvendes.

For at sikre, at Kirkenettet har en fleksibel it-infrastruktur, anvendes der ydelser fra flere leverandører.

Det er vigtigt løbende at overveje, hvilke fleksibilitetsbehov ved nye systemer der kan og skal tilgodeses med den bagvedliggende it-infrastruktur.

1.1.1.3 Økonomi og effektivitet

Ved valg af it-arkitektur anvendes en totaløkonomisk betragtning. Det analyseres, hvilken arkitektur og med hvilken fleksibilitet der skal udbydes services og til hvilke produkter. Analysen beror på parametre for tilgængelighed, sikkerhed, brugervenlighed samt hastighed, hvilket er grundelementerne i valget af teknologi og leverandør.

¹ Bring your own device



På denne baggrund vælges den arkitektur, som samlet set vurderes billigst, når der tages højde for ovennævnte parametre samt de medarbejderressourcer, der skal anvendes til udvikling, implementering, drift og vedligehold af arkitekturen.

1.2 Teknologier der understøtter arkitekturen

På baggrund af ovenstående mål for it-arkitekturen anvender Folkekirkens It følgende it-infrastruktur.

1.2.1 Miljøer/platforme, herunder versioner

For at sikre en stabil og ikke-administrativ tung drift af it på Kirkenettet leverer Folkekirkens It it på både fysiske servere og virtuelle servere (VMware og HyperV).

1.2.1.1 Netværk/datalinjer

Kirkenet-pc'er, der kobler op på Kirkenettet, bliver godkendt via de på pc'en aktiverede sikkerhedspolitikker. Denne godkendelse skal leveres fra servere, der skal være placeret på to fysisk adskilte lokationer. Endvidere placeres strømmettet også på to fysisk adskilte lokationer med henblik på at sikre høj opetid for Kirkenettets systemer.

Folkekirkens it-leverer datalinjer til institutionerne, men det er også muligt for de enkelte institutioner frit at kunne vælge, hvilken leverandør der ønskes til dataforbindelse.

Folkekirkens It skal kunne levere ydelser og systemer ud til alle brugere i folkekirken og Kirkeministeriet.

1.2.1.2 Azure

På Kirkenettet anvendes Azure, der er Microsofts cloudcomputing platform, og hvor der kan vælges mellem Platform som en service (PaaS), Infrastruktur som en service (IaaS) og Software som en service (SaaS)².

Azure anvendes primært til testmiljøer, da Azure giver mulighed for at skalere disse op og ned efter behov samt lukke, når miljøerne ikke anvendes. Endvidere benyttes Azure til produktion i det omfang, at det er nødvendigt i forhold til anvendelse og administration af Office365.

Microsoft Azure Active Directory (Azure AD)-tjenesten anvendes til styring af trust mellem Kirkenettets on premise AD-løsning og AD i Azure. Dette omfatter almindeligt logon og/eller multifaktorgodkendelse, som beskytter Kirkenettets brugere.

1.2.1.3 Operativsystemer på servere

Operativsystemer (OS) på servere anvendes i to versioner bagud. En ny version af et OS anvendes først, når den første samlede opdatering foreligger (update 1). Der vil derfor være en kontinuerlig proces med opgradering af servere, der sikrer, at gamle versioner løftes til den seneste godkendte version. Dette vil i perioder medføre, at der kan eksistere op til tre samtidige OS-versioner.

² De forskellige services er nærmere beskrevet i Digitaliseringsstyrelsens Vejledning i anvendelse af cloudservices (november 2019). Vejledningen ses [her](#).



Der anvendes Windows som OS på alle servere i Kirkenettet på nær til hjemmesideserverne (AWS), hvor der anvendes en LAMP-konfiguration.

1.2.1.4 Amazon Web Services

I Amazon Web Services (AWS) findes den Linux-baserede cloud-løsning, hvor de eksternt rettede hjemmesider er placeret. Der benyttes hovedsageligt IAAS-løsninger (EC2 og S3) i AWS.

De eksternt rettede hjemmesider er med placeringen i AWS adskilt fra den øvrige del af Kirkenettet. Dermed minimeres skaden, såfremt hjemmesiderne rammes af vellykkede angreb.

Den daglige drift af AWS-løsningen varetages af en ekstern part, der sørger for patching af de dele, som AWS ikke varetager. Herudover er den eksterne part ansvarlig for backup og overvågning samt den tekniske dialog med AWS.

1.2.2 Påvirkning af it-infrastrukturen

For at sikre et stabilt og sikkert miljø på Kirkenettet vedligeholder Folkekirkens It et overblik over tidspunkter (servicevinduer) for, hvornår hardware og software (OS, Office-pakke m.v.) skal udskiftes.

Dette overblik fremgår af et teknologiske roadmap som løbende vedligeholdes.

1.3 Arbejdspladsudstyr

It-strategien fastlægger en politik i forhold til arbejdspladsudstyr, der betyder, at det udstyr, som anvendes, skal ses i sammenhæng med, hvad det skal bruges til.

Pc'er og særligt udstyr, som printere der skal kunne printe attester, og som skal tilkobles Kirkenettet, skal anskaffes gennem Folkekirkens It. Øvrigt udstyr kan i nogle tilfælde anskaffes gennem Folkekirkens It, men også købes hos andre leverandører, eks. multifunktionsprintere.

I udgangspunktet tilbyder Folkekirkens It følgende typer af udstyr:

- Stationære og bærbare pc'er
- Printere
- Andet tilbehør til en it-arbejdsplads, eks. skærme, mus/tastatur, udstyr til videomøder m.v.

Udstyr købes via Kirkenettets bestillingsside. Inden køb kan foretages, skal institutionen have indgået en drifts- og indkøbsaftale med Folkekirkens It og have tilmeldt sig til PBS-betalingsaftale.

Smartphones og tablets skal institutionerne selv anskaffe uden om Folkekirkens It.



2 Teknologivalg

2.1 Krav til udvikling

Ved udviklingen af applikationer til Kirkenettet skal gældende standarder for tilgængelighed, sikkerhed, brugervenlighed samt hastighed og grafisk konsistens i forhold til brugerfladen overholdes.

Som udgangspunkt skal applikationer kunne anvendes på den type udstyr, som brugeren foretrækker i den givne situation. Dvs. at løsningerne i videst muligt omfang skal være responsive og derved kunne tilpasse sig brugerinteraktionen, så de kan benyttes både på en mobil, en tablet eller en pc. Således sikres den maksimale brugervenlighed i brugen af applikationen.

Udvikling skal ske efter principper, som sikrer god databeskyttelse, hvilket vil sige databeskyttelse gennem design (privacy by design) og databeskyttelse gennem standardindstillinger (privacy by default). Dette skal sikre bl.a. minimering af data med personoplysninger, pseudonymisering, kryptering af data, korte opbevaringsperioder og begrænset adgang til data, jf. Vejledning om Behandlingssikkerhed Databeskyttelse gennem design og standardindstillinger (Juni 2018).³

2.2 Brugerstyring

2.2.1 Ansatte

Brugeradministration i Kirkenettet (AD og MIM) er baseret på informationer fra Kirkenettets Informationssystem (KIS), som indeholder masterdata (stamoplysninger) på sogne, menighedsråd, folkekirkens og Kirkeministeriets personale m.v. Den aktive styring af rettigheder (adgang) til informationer, portaler, filer m.m. sker gennem Microsofts Active Directory (AD).

Oven på AD ligger der en brugeradministration således, at Kirkenettets sikkerhedsansvarlige selv kan håndtere administrationen af deres egne Kirkenetbrugere. Denne brugeradministration er baseret på Microsoft Identity Manager (MIM).

2.2.2 Menighedsrådsmedlemmer og frivillige

Derudover er der på Kirkeministeriets og folkekirkens intranet – Den Digitale Arbejdsplads (DAP) – en løsning til administration af udvalgsbrugeres rettigheder og adgange. Udvalgsbrugere er menighedsrådsmedlemmer, frivillige og ansatte, som ikke er på Kirkenettet, eks. en kirkegårdsmedarbejder.

2.2.3 it-medarbejdere og it-administratorer

Styring af leverandørers og Folkekirkens It's adgang til servere på Kirkenettet sker med Microsoft-værktøjet Privileged Access Management (PAM). Der tillades

³ Vejledningen ses på Datatilsynets hjemmeside. Vejledningen ses [her](#).



kun adgang med unikke brugere, og al adgang logges. Brugere skal være oprettet i MIM, før de kan få adgang via PAM.

En bruger fra en leverandør skal forespørge om adgang på forhånd, og i forespørgslen anføres begrundelse for adgangen, tidspunkt for adgangen, samt hvor lang tid adgangen skal være åben med et maksimum på 8 timer. Adgangen opnås først, når den er godkendt af Folkekirkens It.

Enkelte brugere hos Kirkenettets driftsleverandør har direkte adgang via PAM for at kunne opretholde den løbende drift, men også her skal adgangen begrundes.

Brugerstyringen skal ske via ovennævnte systemer, hvilket skaber den fornødne adgangssikkerhed og desuden nedsætter ekspeditionstiden samt minimerer risikoen for menneskelige fejl.

Som udgangspunkt skal systemer i Kirkenettet kunne implementeres med AD. På den måde sikres det, at administration af adgangen til systemerne sker via de dertil oprettede brugergrupper. Dette skal ske inden for krav til single-sign-on, som er fastlagt i it-arkitekturprincipperne.

2.3 Integrationsteknologier

Som udgangspunkt benyttes der altid en standard til udveksling af data mellem de forskellige systemer, interne som eksterne. Det betyder bl.a., at de systemer, som Folkekirkens It stiller til rådighed, i muligt omfang skal udstille relevante brugergrænseflader (api'er) efter alment anerkendte it-standarder. Læs yderligere om integration i it-arkitekturprincipperne.

2.4 Applikationer og forretningsprogrammel

Applikationer og forretningsprogrammel til Kirkenettet skal af hensyn videreudvikling, vedligeholdelse og kvalitet, så vidt det er muligt, være standard- og/eller rammesystemer. Det vil som hovedregel også sikre det bedste forhold mellem pris og kvalitet. Det betyder, at særligt systemudvikling, som omfatter mere end konfiguration, begrænses.

I visse tilfælde vil folkekirkens særlige struktur og opgaver tilsige løsninger, som designs og udvikles specifikt til folkekirken. I de tilfælde vil digital innovation indimellem udfordre, at folkekirken er villig til at afprøve mindre udbredte teknologier og metoder. Udvikling af den slags helt nye systemer for folkekirken forudsætter i givet fald en nærmere afgrænsning af projektet, samt at systemet afprøves under kontrollerede forhold og i øvrigt ikke kompromitterer hverken sikkerhed eller databeskyttelse.

Applikationer og forretningsprogrammel anskaffes som hovedregel med tilhørende vedligeholdelses og opgraderingsaftaler. Overblik over applikationer og forretningsprogrammel fremgår af et applikationsroadmap, som løbende vedligeholdes.

Når der foretages systemudvikling, skal nedenstående krav overholdes.



2.4.1 Applikationer med integration i Folkekirkens It's brugerstyring

Applikationer, der har behov for at integrere med Folkekirkens It's brugerstyring, udvikles på Microsoft-teknologier. Til dette benyttes MS SQL som database, og IIS benyttes som webserver.

Folkekirkens digitale løsninger skal være robuste, stabile i drift, brugervenlige og velfungerende. Derfor baseres digitalisering i folkekirken som hovedregel på teknologier, der har en vis udbredelse, og på metoder, som er velafprøvede. Det gælder især for administrative systemer på områder, hvor folkekirkens behov er sammenlignelige med andre offentlige institutioners.

Folkekirken skal med andre ord ikke være 'first-mover' med hensyn til ny teknologi – men gerne dem der følger lige efter, hvor det giver teknologisk mening i forhold til den øvrige infrastruktur og it-strategi. Og hvor det bærende element er, at der direkte eller indirekte er en brugermæssig værdi at hente.

2.4.2 Applikationer, der primært retter sig mod offentligt tilgængelige hjemmesider

De offentligt tilgængelige hjemmesider udvikles i open source Content Management Systemerne TYPO3 eller i NEOS. Disse programmer implementeres på en server konfigureret med Linux/MySQL/PHP.

Disse hjemmesider skal være placeret i et cloud-miljø leveret af en anden leverandør end leverandøren til Kirkenettets øvrige cloud-løsninger og er derfor placeret i AWS. Denne opsplитning er begrundet i et ønske om at minimere risici, såfremt et cloud-miljø bliver utilgængeligt eller udsat for angreb, jf. også afsnit 1.2.1.4.



3 Informationssikkerhed og databeskyttelse

De specifikke retningslinjer, der skal sikre fortrolighed, integritet, tilgængelighed og autenticitet gældende for applikationer og data, er fastlagt i og reguleret af Informationssikkerhedspolitik for Kirkeministeriet og Den danske folkekirke samt Cirkulære om informationssikkerhed, herunder sikkerhedsforanstaltninger i Kirkenettet.

Såvel politikken som cirkulæret er udarbejdet i henhold til den gældende statslige sikkerhedsstandard, ISO 2700, samt databeskyttelseslovgivningen⁴ og gældende vejledninger om informationssikkerhed og databeskyttelse.

3.1 Organisering

Informationssikkerhedsorganisationen består af et informationssikkerhedsudvalg, en it-sikkerhedskoordinator, en databeskyttelsesrådgiver, de forretningsmæssigt forankrede systemejere og dataansvarlige samt Folkekirkens It's systemansvarlige.

Informationssikkerhedsudvalget er nedsat som et permanent udvalg til at sikre, at informationssikkerhedsmæssigt relevante emner løbende behandles. Det består af repræsentanter fra Kirkeministeriet, Folkekirkens It, stifterne og de faglige organisationer samt it-sikkerhedskoordinatoren.

I det daglige træffer Folkekirkens It's ledelse dispositioner og afgørelser vedrørende Kirkenettets drift og sikkerhed i overensstemmelse med de fastlagte retningslinjer, og disse effektueres umiddelbart.

Endvidere er der nedsat et forum for databeskyttelse, som består af medlemmer fra de faglige foreninger og organisationer, der er repræsenteret i Folkekirkens Samarbejdsudvalg.

3.2 Sikkerhedsniveau – målsætninger

Folkekirkens brug af digitale løsninger skal ske på en tryk og sikker måde, som fastholder den høje tillid, som samfundet har til folkekirken. Folkekirkens mange myndigheder og institutioner skal overholde databeskyttelseslovgivningen og øvrige relevante it-sikkerhedsstandarder.

Et højt digitalt sikkerhedsniveau opnås med en kombination af sikre systemer og sikker adfærd. Folkekirkens It sikrer løbende, at Kirkenettets systemer overholder de gældende sikkerheds- og databeskyttelsesstandarder. Det er samtidig et væsentligt hensyn ved udvikling af nye digitale løsninger, at sikkerhed tænkes ind fra starten, således at brugervenlighed og sikker adfærd indgår i løsningsdesignet.

⁴ Databeskyttelsesforordningen (Europa-parlamentet og rådets forordning (EU) 2016/679 af 27. april 2016) samt Databeskyttelsesloven (LOV nr. 502 af 23/05/2018).



Sikkerhedsniveauet på Kirkenettet er fastlagt ud fra en risikobaseret tilgang og er beskrevet nærmere i informationssikkerhedspolitikken. Den risikobaserede tilgang betyder, at der er fokus på driften af de mest forretningskritiske processer og it-aktiver, men samtidig med at der også er den nødvendige sikkerhed for øvrige processer og aktiver. Der skal implementeres de sikringsforanstaltninger på Kirkenettet, der er nødvendige for at opretholde sikkerhedsniveauet i forhold til det aktuelle trusselsbillede.

Viser en risikovurdering, at sandsynligheden for en sikkerhedshændelse er højere end middel, skal Folkekirkens It – under hensyntagen til de økonomiske forhold – implementere sikringsforanstaltninger til at nedbringe sandsynligheden og dermed den samlede risiko. Såfremt konsekvensen ved en forretningskritisk proces er høj eller meget høj, skal sandsynligheden søges bragt ned på lav.

3.3 Styring – realisering af målsætning

Til styring af arbejdet med informationssikkerhed og databeskyttelse, herunder gennemførelse af risikoanalyser, anvendes værktøjer anbefalet af Statens It-sikkerhedsforum samt Digitaliseringsstyrelsen.

Folkekirkens It, særligt it-sikkerhedskoordinatoren, deltager i relevante fora, uddannelser, konferencer mv. for at sikre, at den fornødne sikkerhedsmæssige viden er til stede for at kunne opretholde et højt sikkerhedsniveau på Kirkenettet.

Ved anskaffelse af nye it-systemer samt ved væsentlige ændringer foretages der en risikovurdering.

En systematisk risikovurdering af alle forretningskritiske processer og de tilhørende it-aktiver foretages årligt, og på baggrund heraf fastlægges behovet for evt. yderligere sikringsforanstaltninger.

Folkekirkens It gennemfører jævnligt informationskampagner og lignende aktiviteter for at øge bevidstheden om informationssikkerhed og databeskyttelse på Kirkenettet og gældende retningslinjer samt for at skærpe bevidstheden omkring eget ansvar for opretholdelse heraf.

3.4 Beredskab og kontrol

Beredskabs- og retableringsplaner skal altid foreligge i et sådant omfang, at forretningskritiske processer kan udføres i videst mulig udstrækning uden sikkerhedsmæssig påvirkning. Planerne skal afprøves løbende for at sikre disses aktualitet.

Gennemførelse af tilbagevendende it-sikkerhedsreviews og kontroller skal sikre den fortsatte overholdelse af gældende standarder og regler.



4 Hvilke opgaver løses internt – hvilke eksternt?

It-ydelser til Kirkenettets brugere leveres af såvel interne medarbejdere i Folkekirken It som eksterne it-leverandører.

I det følgende beskrives de principper, der fastlægger hvilke it-kompetencer og hvilken opgaveløsning, der er nødvendige internt i Folkekirken It, samt hvilke kompetencer og hvilke typer opgaver der vil blive indkøbt efter behov.

4.1 Principper for anvendelse af interne og eksterne it-kompetencer i Folkekirken It

Valget af, hvorvidt en given opgave ved Folkekirken It skal varetages internt eller eksternt, baseres på følgende overordnede princip:

- Opgaver skal løses, hvor det sker med lavest mulige totalomkostninger, samtidig med at Folkekirken It sikres leverancesikkerhed samt reel mulighed for styre og kontrollere de it-ydelser, der leveres til slutbrugerne.

De følgende principper er formuleret for i praksis at støtte realiseringen af det overordnede princip:

- Folkekirken It vil internt opretholde kompetencer til opgaver hvor:
 - Der kræves stort kendskab til Kirkenettets brugere og dyb viden om arbejdsprocesser.
 - Der forudsættes intern varetagelse for at sikre nødvendig styring og kontrol med de leverede it-ydelser, f.eks. projekt- og leverandørstyring samt sikring af persondata.
- Opgaver, der primært løses internt, er arbejdet med strategi og governance vedrørende Kirkenettet, sikkerhed og databeskyttelser, herunder opfølgning på compliancestatus, supporthåndtering med tilhørende vejledning og uddannelse m.fl.
- Folkekirken It vil indkøbe ekstern bistand til opgaver kendetegnet ved:
 - Specialistopgaver, hvor Folkekirken It's størrelse ikke giver kritisk masse til at opretholde den nødvendige kompetence.
 - Standardopgaver, som kan indkøbes billigere, set i forhold til intern produktion, herunder ved behov for døgnovervågning/-service.
 - Adgang til skalerbare ressourcer, hvor der kun periodisk er behov for bistand.
- Opgaver, der typisk søges ekstern bistand til, er vurdering af sikkerheds- og driftsmæssige problemstillinger, juridisk og ledelsesmæssig rådgivning samt udvikling af applikationer. Dertil kommer de forretningskritiske ydelser, der leveres af eksterne it-leverandører inden for flerårige aftaler, herunder drift af store it-systemer som ESDH og løn samt drift af servere.

Efter behov suppleres den interne opgavevaretagelse med ekstern bistand.



5 It-Governance

It-governance handler om tilrettelæggelsen af arbejdet med it og digitalisering, særligt når det gælder ansvar, ledelse og organisering. De grundlæggende retningslinjer for it-governance i folkekirken er fastlagt af kirkeministeren i 2017, og omfatter fem hovedprincipper⁵:

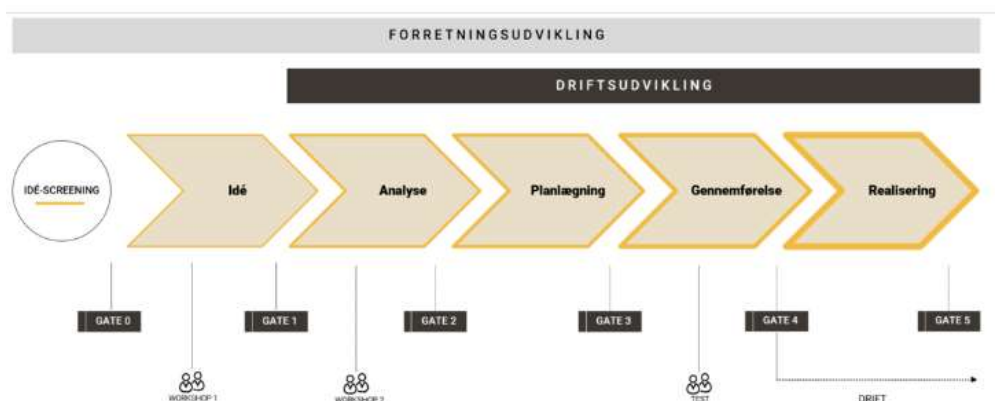
1. Kirkeministeriet har ansvaret for Folkekirkens It
2. It-Følgegruppen rådgiver om strategiske it-spørgsmål
3. Brugere inddrages fra først til sidst
4. Folkekirken tager ejerskab for de digitale løsninger
5. Digitale løsninger skal kunne betale sig.

Dette udmønter sig i forhold til Folkekirkens It's daglige arbejde i den tilbagevendende gennemførelse af konkrete styringsaktiviteter, eks. vedrørende sikkerhed og databeskyttelse, hvilket er nærmere beskrevet i afsnit 6, men også vedrørende gennemførelse af projekter og leverandørstyring.

5.1 Gennemførelse af it-projekter

Alle it-projekter gennemføres efter en tilpasset udgave af den statslige model for it-projektledelse, og de følger Folkekirkens It's model for projekt- og porteføljestyring, hvor et projekt gennemløber fem faser.

Projektmodellens faser er; Idé, Analyse, Planlægning, Gennemførelse og Realisering, hvor sidstnævnte ligger i Forretningen.



Forretningsudviklingsprojekter og driftsudviklingsprojekter følger samme projektforløb. Forretningsudviklingsprojekter forelægges It-Følgegruppen, mens driftsudviklingsprojekter som hovedregel ikke forelægges for It-Følgegruppen, men derimod for Folkekirkens It's ledelse.

⁵ De fem hovedprincipper er nærmere beskrevet på Folkekirkens It's [hjemmeside](#).



I *Idé- og Analysefasen* er et projekt forankret i Forretningsudvikling, mens Projektafdelingen er ansvarlig for projektet i *Planlægnings- og Gennemførelsesfasen*. I *Realiseringsfasen* overdrages projektet, som nu er en idriftsat applikation, til forretningen, der har ansvaret for at realisere gevinsterne.

For hvert projekt vurderes det, hvilken udviklingsmetode der skal anvendes. Vandfaldsmetoden med forholdsvis få og faste projektfaser kan med fordel anvendes, når det fra start er meget veldefineret, hvad den ønskede løsning er. Agil udvikling med mange og korte udviklingsforløb (sprints) anvendes typisk, hvor det i højere grad er ønskeligt, at have fleksibilitet ift., hvordan den endelige løsning skal være. Uanset valg af vandfald eller agil udvikling anvendes traditionel projektledelse som styringsredskab for tid, kvalitet, økonomi samt varetagelse af interessenter og styring af risici. I praksis vil Folkekirkens It typisk anvende en blanding af vandfald og agil udviklingsmetode, jf. også scenarier i Statens It-projektmodel.

I projektarbejdet sikres løbende brugerinddragelse samt evt. inddragelse af en referencegruppe. Til større idriftsatte applikationer sikres også brugernes indflydelse på den løbende forvaltning af applikationen ved nedsættelse af et forum eller tilsvarende for forvaltning af applikationen, eks. er der for ESDH-systemet F2 nedsat F2 Forum.

Det tilstræbes, at initiativet og ansvaret for nye digitale løsninger og videreudvikling af eksisterende systemer i videst muligt omfang skal forankres det sted i folkekirken, som skal drage nytte af et system.

Derfor sidder den relevante enhed i folkekirken med som systemejer, når der skal formuleres krav og specifikationer for en digitale løsning, når den konkrete løsning skal vælges, og når fordele, ulemper og gevinster skal vurderes.

Folkekirkens It understøtter både udvikling og drift med it-faglig bistand på grundlag af tydelige projekt- og leveranceaftaler med den ansvarlige enhed i folkekirken. Folkekirkens It vil således almindeligvis stille en projektleder til rådighed for projekterne.

5.2 Leverandørstyring

Folkekirkens It har et koncept for leverandørstyring, der omfatter følgende:

- Governancemodel for leverandørstyring, herunder rollebeskrivelser (RACI)
- Etablering af leverandørstyringssite (samling af relevant dokumentation og information)
- Formalisering af centrale driftsprocesser (processer for incident, problem og change management baseres på ITIL best practise)
- Systemunderstøttelse af drift, support, vedligeholdelse og videreudvikling
- Standardisering af leverandørkrav (bidrage til sammenlignelighed og forenkling af leverandørstyringen).

Leverandørstyringen understøttes af processerne for håndtering af kald, fejl og fejlrettelse, som er baseret på ITIL.

