IT Governance-anbefalinger 2012

Fagrådet for IT Governance og Management
DIT - DANSK IT

dansk•it

Indhold

IT Governance-anbefalinger

IT Governance er en integreret del af Corporate Governance[1].

Med IT Governance kan virksomhedens ledelse sikre sig, at it på den ene side understøtter virksomhedens effektivitet og på den anden side medvirker til at udvikle virksomheden.

Fagrådet for IT Governance og Management arbejder for at fremme udviklingen af effektiv og værdiskabende it-anvendelse i såvel privat som offentlig virksomhed. Som et led i dette arbejde har Fagrådet udarbejdet disse anbefalinger, der henvender sig til virksomhedens topledelse, forretningsledelse og it-ledelse.

Fagrådet har taget afsæt i det arbejde, der er gennemført af IT Governance Institute[2] og fremsætter en række anbefalinger, der tager udgangspunkt i de vilkår, der er gældende for danske virksomheder.

Anbefalingerne er bevidst lagt på et forholdsvis højt ambitionsniveau. Anbefalingerne vil således for de fleste virksomheder være et ambitionsniveau, man bør arbejde hen imod. Specielt større og internationale virksomheder vil typisk leve op til alle eller de fleste af anbefalingerne. For mange små virksomheder og virksomheder, hvor it har ringe betydning for forretningen, er anbefalingerne mindre relevante.

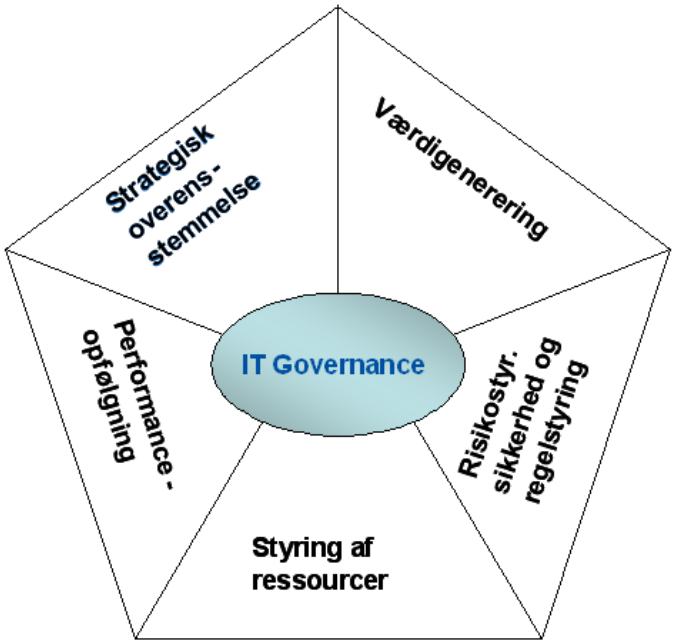
Nogle virksomheder vil af den ene eller den anden grund bevidst fravælge at opfylde bestemte anbefalinger. Disse bør klart kunne redegøre for, hvorfor man ikke følger disse anbefalinger i overensstemmelse med princippet om ”comply or explain”, som også anvendes inden for Corporate Governance.

Fagrådet inviterer interessenter til at give deres kommentarer til anbefalingerne. De kommentarer, Fagrådet modtager, vil indgå i vurderingen af, hvorledes anbefalingerne om IT Governance skal udformes og løbende tilpasses.

---

[1] Corporate Governance eller god virksomhedsledelse som begreb opstod som reaktion på en række erhvervsskandaler i England og USA i 1990'erne og ind i dette årti. Debatten har bredt sig til andre lande, og op gennem 1990'erne fik en række lande et Corporate Governance-kodeks. I Danmark blev resultatet af de første arbejder med et kodeks udgivet i 2001 ved en rapport om god selskabsledelse i Danmark fra Nørby-udvalget. I maj 2005 kom en revideret udgave fra Københavns Fondsbørs' komite for god selskabsledelse "Rapport om god selskabsledelse i Danmark 2005". Efter flere opdateringer udkom de endelige anbefalinger 8. april 2010. www.corporategovernance.dk

[2] IT Governance Institute, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL, USA 60008. www.itgi.org



Anbefalingerne omfatter fem fokusområder som vist i figuren ovenfor:

1 Strategisk overensstemmelse mellem forretningsstrategien og it-strategien

2 Værdigenerering

3 Styring af ressourcer

4 Risikostyring, sikkerhed og regelstyring

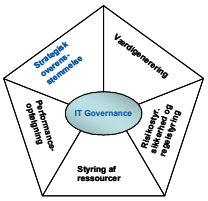
5 Performanceopfølgning.

Det førstnævnte fokusområde vedrører strategiske overvejelser om it og forretningen. De efterfølgende områder vedrører den nærmere fokusering, styring og opfølgning.

IT Governance betyder balance mellem værdi og effektivitet af it på den ene side og risici og regelstyring på den anden side. Ved de forskellige IT Governance-aktiviteter, som iværksættes, skal omkostningerne stå i rimeligt forhold til konsekvenserne ved risici, der tages, ved ikke at sikre IT Governance.

Alle fem fokusområder bidrager til, at virksomheden kan opnå omkostningseffektiv og effektfuld it-anvendelse.

1. Strategiske overensstemmelser mellem forretningsstrategien og it-strategien



Det er afgørende, at der er overensstemmelse mellem forretningsstrategien og it-strategien. It skal understøtte virksomhedens forretningsfunktioner og aktivt påvirke og eventuelt indgå i kerneaktiviteterne ved virksomhedens udvikling.

IT Governance fordrer drøftelse på øverste ledelsesniveau af it's muligheder for forretningen, typisk med udgangspunkt i overvejelser om forretningsstrategien. Den øverste ledelse fastlægger rammer, organisation og styring af it.

IT Governance indebærer derfor et tæt samspil mellem virksomhedens øverste ledelse og ledelsen af it-aktiviteterne. Dette for at sikre, at virksomhedens it-aktiviteter udvikler sig i overensstemmelse med forretningen, og at it aktivt bidrager til at udvikle forretningen.

Det anbefales at sikre, at it-strategien er i overensstemmelse med forretningsstrategien, og at der er en plan for realisering af strategien. Overensstemmelse skabes, ved at repræsentanter fra forretning og it-funktion arbejder sammen om at "tænke it ind i forretningen" og afklarer forretningsmæssige mål og it-mål ved udarbejdelse af forretningsstrategi og it-strategi. It-funktionen skal tilføre forretningen viden om it, og forretningen skal tilføre it-funktionen viden om forretningen.

Det anbefales, at it-strategien med jævne mellemrum revurderes, sædvanligvis hvert andet år, men i øvrigt afpasset ændringerne i forretningsstrategien.

Det anbefales, at den øverste ledelse fastlægger rammer for anvendelse og styring af it. Rammerne fastlægges i form af prioriteringer, planer og budgetter for it-anvendelsen, herunder tages der stilling til sourcing. Opgaver, roller og ansvar for it-aktiviteterne fastlægges på overordnet niveau, herunder fastlægges ansvaret for elementerne i IT Governance. It-ledelsen er ansvarlig for den konkrete organisering af it-funktionen.

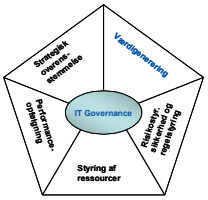
I virksomheder, hvor it spiller en central rolle for forretningen, er det væsentligt, at der tages stilling til, om sådanne drøftelser hensigtsmæssigt foretages i virksomhedens almindelige ledelsesstruktur eller foretages i et permanent it-forum (strategikomite, strategiudvalg eller lignende) og konfirmeres i den øverste ledelse.

Virksomheden er på den ene side drevet af at skabe værdi og være effektiv. På den anden side stilles der krav om minimering af risici og overholdelse af lovgivning, myndighedskrav og god forretningsskik. Fokuseres der for meget på værdi og effektivitet, kan dette ske på bekostning af sikkerhed og overholdelse af regler. Omvendt, såfremt der fokuseres unødvendigt på sik-

kerhed og overholdelse af interne regler, kan resultatet være, at virksomhedens evne til at skabe værdi og være effektiv formindskes.

Det anbefales, at der etableres balance mellem værdi og effektivitet af it på den ene side og risici og regelstyring på den anden side, bl.a. gennem udarbejdelse og risikovurdering af it-understøttelsen.

2. Værdigenerering



Mulighederne ved it-anvendelse kan og bliver – med rette – opfattet meget bredt og forskelligt. Dels som et område, hvor omkostningerne på traditionel vis bør optimeres i forhold til behovene, dels som et område, der er en central driver for løbende værdiskabelse gennem innovation, nye produkter/services og optimering af virksomhedens interne processer.

It kan derfor ikke entydigt opfattes som enten et omkostningsområde eller et værdigenererende område. Virksomheden bør derfor nøje overveje, hvilken betydning it har – og fremadrettet skal have – ved formulering af IT Governance-principperne.

IT Governance indebærer, at forretningen og it-specialister arbejder sammen i projekter og ved anvendelsen af it med henblik på optimering af forretningsprocesserne og udnyttelse af it's muligheder.

IT Governance skal også – med udgangspunkt i virksomhedens samlede strategier og styringsprocesser – afbalancere sammenhængen mellem koncernen og de enkelte forretningsområder inden for koncernen.

Denne problemstilling aktualiseres af, at de fleste større virksomheder i dag orienterer sig mod en sammenhængende og lagdelt it-arkitektur på virksomhedsniveau. Denne udvikling udfordrer i høj grad mulighederne, for at de enkelte forretningsenheder selv kontrollerer og styrer, hvordan it skal indgå eller understøtte deres produktudvikling og produktion.

Valget mellem central kontra decentral styring på it-området – eller en kombination heraf - er dermed et meget vigtigt og afgørende element i afklaring og etablering af IT Governance.

Det anbefales, at repræsentanter fra den øverste forretningsledelse og fra it-ledelsen porteføljestyrer og overvåger projekter og forvaltning af it. Det er væsentligt, at der tages stilling til, om disse aktiviteter skal foretages gennem virksomhedens almindelige ledelsesstruktur eller skal foretages i et permanent it-forum. Strukturen skal sikre, at der sker aktiv projektstyring og en koordinering af parallelle projekter. Endvidere skal det sikres, at serviceniveauet er fastlagt, og at it-services leveres som aftalt.

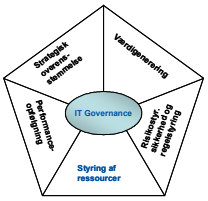
Det anbefales, at der etableres systemer til vurdering af værdien af it og til prioritering af indsatsen på it-området.

Porteføljestyring af projekter bør gennemføres på basis af opgørelse af ROI og/eller cost-benefit for projekterne.

Det anbefales, at projekter styres efter en fast projektstruktur og med en aktiv styregruppe. Projekterne gennemføres i et samarbejde mellem forretningen og it-funktionen. De forretningsansvarlige har ansvaret for projekter, som vedrører forretningsprocesserne. Projekterne styres efter en egnet projektstyringsmetode.

Det anbefales, at der indgås aftaler om serviceniveauet på alle væsentlige områder for de services, der leveres til brugerne (Service Level Agreements, SLA), herunder med de leverandører, der leverer services til virksomheden. Det bør i tilknytning hertil tydeliggøres, hvilke omkostninger der er knyttet til de valgte serviceniveauer.

3. Styring af ressourcer



Effektiv styring af ressourcerne er en forudsætning for, at it kan bidrage til forbedring af virksomhedens effektivitet og udvikling. IT Governance indebærer, at it udnyttes og drives efter forretningsmæssige principper. Mål, strategier og aktiviteter på it-området kommunikeres, så det kan forstås af alle interessenter. It-ressourcerne, herunder menneskelige ressourcer og it-infrastruktur i hele virksomheden, anvendes og udvikles gennem anvendelse af standardiserede processer. Virksomheden bør tilstræbe best practices, herunder sikkerhed for effektiv levering af outsourcede services.

Inden for overordnede rammer for it-anvendelsen skal den it-ansvarlige gennemføre it-strategien og varetage den daglige ledelse af it-funktionen. Den it-ansvarlige fastlægger opgaver og organisering af it-funktionen. Det anbefales, at der dedikeres ressourcer til stadig udvikling af IT Governance i virksomheden.

Der bør tages stilling til, om aktiviteter med henblik på overvågning og vurdering af, hvorvidt ny teknologi eller arkitekturer er relevant for forretningen, skal foregå i virksomhedens almindelige ledelsesstruktur eller foretages i et teknologiråd/arkitekturråd eller lignende.

Det anbefales, at der etableres og vedligeholdes politikker, procedurer, metoder og standarder for:

- Udvikling
- Drift
- Vedligehold
- Support
- Sourcing
- Opgørelse af omkostninger, besparelser og værdi/fordeling/afregning af ydelser
- Porteføljestyring
- Projektstyring
- Kvalitetsstyring

- It-arkitektur
- Teknologi
- It-sikkerhed.

Etableringen og vedligeholdelsen af politikker, procedurer, metoder og standarder på områderne kan ske med inspiration i en række standardmetoder og -værktøjer[3].

Virksomheden bør tage stilling til anvendelsen af metoder og værktøjer, herunder på hvilket ambitionsniveau disse skal anvendes.

Det anbefales, at der etableres og vedligeholdes processer, som sikrer en it-platform, der understøtter forretningens behov.

Omkostningsniveau, udviklingshastighed og performance er stærkt afhængigt af platform og arkitektur. Disse bør derfor fastlægges centralt, eksempelvis i en styrekomite.

Der bør endvidere etableres og vedligeholdes processer, som sikrer optimering af viden om it-anvendelse i virksomheden, herunder at der arbejdes systematisk med udvikling af medarbejdere.

Det anbefales, at virksomheden udarbejder og opdaterer rammer og strategi for sourcing. Sourcing af henholdsvis udvikling, drift, support og vedligehold bør vurderes i sammenhæng med henblik på at fastlægge, hvilke it-opgaver der skal løses i virksomheden, og hvilke opgaver der skal løses uden for virksomheden.

Inden for fastsatte rammer og fastsat strategi bør de daglige leveranceprocesser over for brugerne styres.

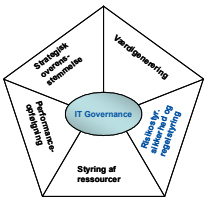
---

[3] Blandt disse kan nævnes:

- COBIT (Control Objectives for Information and related Technology). COBIT er et rammesystem, som giver vejledning for styring af virksomhedens it. Stærk i interne kontroller og målinger. www.itgi.org
- Val IT. Supplerende rammesystem til COBIT som fokuserer på it-understøttede forretningsinvesteringer, realisering af fordele og værdigenerering. www.itgi.org
- ITIL (Information Technology Infrastructure Library). ITIL angiver best practice for it-servicefunktioner. Stærk i processer for drift og service. www.itil-officialsite.com
- CMMI (Capability Maturity Model Integration). CMMI er en modenhedsstandard primært anvendt af it-virksomheder, som udvikler systemer, men efterhånden udvidet til at dække bredere. www.sei.cmu.edu/cmmi/.
- ISO27001. International anerkendt standard for organisering af it-sikkerhedsarbejdet. www.27000.org/iso-27001.htm
- EA (Enterprise Architecture). TOGAF: Et rammesystem, som kan anvendes frit ved arbejde med it-arkitektur: www.opengroup.org/architecture/togaf/
- ISO/IEC 38500. ISO-standarden giver principper for Governance of IT, udarbejdet for det øverste ledelsesniveau. www.iso.org/iso/catalogue_detail.htm?csnumber=51639

Over for leverandørerne bør der udøves kontraktstyring, som omfatter overvågning af leverandørernes performance, implementering af ændringer i ydelser og kontrakter, dag-til-dag-administration, indgåelse af aftaler om nye ydelser og projekter og udvikling af nye ydelser.

4. Risikostyring, sikkerhed og regelstyring



Risikostyring og regelstyring, herunder overholdelse af lovkrav, er væsentlige elementer i den øverste ledelses ansvar. IT Governance indebærer, at der foretages en hensigtsmæssig styring af it-relaterede risici, og at it-anvendelsen omfattes af og understøtter virksomhedens interne kontrolsystemer og overholdelse af lovgivning, myndighedskrav og god skik.

Det anbefales, at der etableres hensigtsmæssige systemer til opgørelse af risici og virkningen af hændelser. Sådanne systemer omfatter en klarlæggelse af risikovilligheden, samt hvordan risici styres ved henholdsvis at undgå, acceptere og/eller reducere virkningen og/eller ved at afdække risici hos andre. Det anbefales, at risikovurderingen tages op til revurdering med jævne mellemrum, f.eks. i forbindelse med den periodiske revurdering af it-strategien.

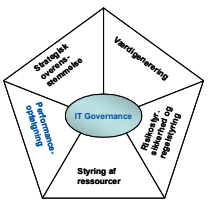
Der bør etableres beredskab for at undgå eller reducere risici og begrænse skaden ved uheld. Omkostningerne ved kontroller og forebyggende arbejde bør være i rimelig balance i forhold til at dele eller acceptere risici. Der bør foretages realistisk afprøvning af katastrofeplaner og risikostyring af alle væsentlige projekter.

Det anbefales, at der ved implementering af nye systemer og vedligeholdelse af eksisterende systemer fokuseres på introduktion af it-kontroller, som understøtter virksomhedens interne kontrolsystemer, og som sikrer datas integritet og hindrer tab af data.

It skal bidrage til, at lovgivning og myndighedskrav overholdes gennem etablering og anvendelse af hensigtsmæssige systemer, ligesom generelle anbefalinger vurderes og efterleves, såfremt de er relevante for virksomheden.

Rammerne for sikkerhedsarbejdet skal fastlægges, herunder skal ansvaret for formidling af regler og holdning fastlægges. Det skal sikres, at den generelle adfærd er i overensstemmelse med reglerne. Det bør overvejes, om sikkerhedsspørgsmål skal varetages i virksomhedens almindelige ledelsesstruktur, eller om det tidligere omtalte teknologiråd/arkitekturråd, -udvalg, -gruppe eller lignende tillige skal varetage sikkerhedsspørgsmål.

5. Performanceopfølgning



Det er afgørende for styring af it-anvendelsen, at der følges op på it-projekter og serviceydelser, herunder nytteværdien, som skabes i forretningsenhederne. Målinger af performance er nødvendige for styring. IT Governance indebærer, at der etableres systematisk opfølgning på it-performance.

Det anbefales, at der etableres et performanceopfølgningssystem indeholdende:

- Bruger-/kundeundersøgelse
- Opfølgning på strategien: Er strategi, teknologi og arkitektur i overensstemmelse med markedets udvikling, følger applikationsstrategien virksomhedens udvikling, og implementeres it-strategien som besluttet?
- Produktivitet og effektivitet
- Opfølgning på projekter
- Opfølgning på serviceydelser.

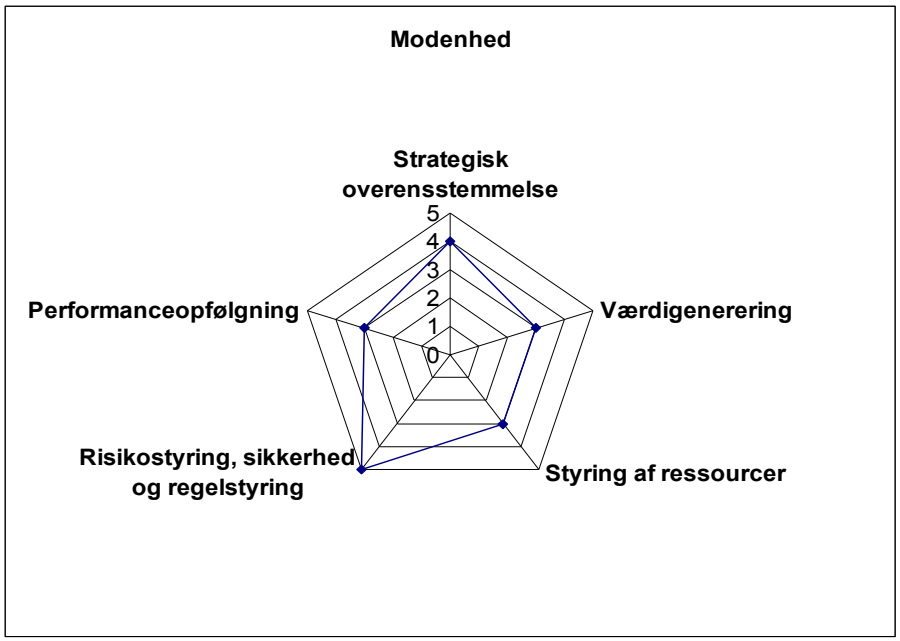
Udfordringen er her at fastlægge objektive mål og afklare, om niveauet er det rigtige.

Det anbefales, at den øverste ledelse løbende følger udviklingen på udvalgte måleområder og sikrer, at der foretages benchmarking mod andre virksomheder.

Det anbefales endvidere, at den øverste ledelse løbende foretager en vurdering af egen indsats på IT Governance-området.

Analyserne bør omfatte afdækning af årsags-/virkningssammenhænge for processer, som kommer ud af kontrol, eller som fører til uhensigtsmæssige resultater. Analyserne bør give anledning til iværksættelse af forbedringsprogrammer for it-anvendelsen.

En analyse af en konkret virksomheds profil på de fem IT Governance-dimensioner behandlet ovenfor kan afbildes som vist i nedenstående figur. Denne kan danne baggrund for en drøftelse med virksomhedens øverste ledelse om IT Governance-initiativer.



Arbejdet med udarbejdelse af Anbefalingerne om IT Governance 2006 blev gennemført af det daværende Fagråd for IT Governance. Arbejdet med 2012 - udgaven er gennemført af Fagrådet for IT Governance og Management, som består af:

Niels Bjørn-Andersen
Professor, Copenhagen Business School

Per Buchwaldt
Senior Manager, Deloitte Business Consulting

Knud Fiil-Nielsen
Managementkonsulent, eget firma

Lars Fruergaard Jørgensen
Senior Vice President, Novo Nordisk

Bo Lind
CIO, Vestforbrænding I/S

Allan S. Bager
Digitaliseringschef, Odense Kommune

René Munk-Nissen (formand)
It-direktør, DSB

Peter Trier Schleidt
Vicedirektør, Danske Bank.