

WHITEPAPER

# It-revision kan skabe store forretningsværdier – hvis det gøres rigtigt

# It-revision kan skabe værdi



## God it-revision er guld værd for din forretning

I en moderne digital forretningsverden kan man ikke overvurdere, hvor stor en rolle en god it-revision spiller for en forretnings resultater. God it-revision skaber robuste processer, sikkerhed og compliance. Det skaber også et årshjul for driften, der sikrer, at dine systemer, processer og din organisation løbende bliver bedre.

### ER JERES IT-REVISION ET AKTIV ELLER ET PASSIV FOR FORRETNINGEN? TEST JER SELV.

Følgende syv spørgsmål kan måske hjælpe dig til at blive skarp på om, jeres tilgang til it-revision kan blive mere værdiskabende:

1. Har I en metodisk tilgang til revision, og har I høstet erfaringer med, hvordan I gennemfører revision uden at løbe ind i problemer?
2. Kan I hurtigt lukke anmærkninger fra revisoren i én iteration og uden, at omkostninger stikker af?
3. Følger I løbende op på revisionen fra sidste år, kan I finde dokumentation og har I styr på omkostninger forbundet med revision?
4. Har I kontrol over aktiviteter i it-revisionen?
5. Er du og organisationen trænet til at styre revisionen på en effektiv måde?
6. Har jeres organisation fokus på it-revision, og har I etableret et driftshjul, der er indarbejdet i organisationen?
7. Har I organiseret it revisionen, så det er en løbende driftsopgave, der skaber plads til at udvikle?

### HVEM ER DET RELEVANT FOR?

It-revision er relevant og værdiskabende for alle typer virksomheder. GDPR er den aktuelle murbrækker, der sort på hvidt synliggør for rigtig mange virksomheder, at de skal arbejde systematisk og struktureret med deres it-systemer og data. Et andet eksternt incitament er, at mange virksomheder stiller krav til deres leverandører om, at de kan dokumentere, at de har gennemgået en grundig it-revision. I den finansielle sektor er der en lang række lov- og myndighedskrav, der skal overholdes. I den farmaceutiske branche stiller de nationale sundhedsmyndigheder strenge krav til sporbarhed og dokumenterede it-processer, og det samme gør sig gældende for fødevarer virksomheder. Offentlige virksomheder skal være ISO 27001

# It-revision kan skabe værdi

## Hvad er it-revision for en størrelse?

*It-revision er en integreret del af den traditionelle årlige regnskabsrevision, hvor virksomheden skal redegøre for og dokumentere, at virksomhedens driver en fornuftig forretning, der lever op til de krav og love, som gælder generelt og for virksomhedens specifikke branche. Det er en årlig eksamen, hvor en ekstern revisor fungerer som censor. It-delen af revisionen fylder i dag langt mere end den gjorde for 10 og 20 år siden, fordi ingen virksomheder i dag kan drive nogen form for forretning uden it-systemer. It-systemer bliver en mere og mere fundamental og integreret del af forretninger, og der er i dag en række eksterne og interne krav til it-infrastruktur og -drift, som er livsnødvendige for virksomheder at leve op til.*

certificerede, fordi en it-revision giver en ledelsesgaranti for, at der er styr på it-systemer og -processer, og at der er gjort en seriøs indsats for it-sikkerheden.

Men der i dag også mange virksomheder, som ikke nødvendigvis skal leve op til eksterne myndighedskrav, som alligevel investerer i en grundig it-revision. Det gør de fordi, de har erkendt, at en it-revision repræsenterer en arbejdsmåde og et mind-set, som skaber store forretningsværdier for virksomheden. Det er forretningsværdier som for eksempel stærkere processer, mere effektiv drift, højere sikkerhed, bedre compliance, mere salg og skarpere fokus på løbende forbedringer.

## HVAD ER UDFORDRINGERNE DERUDE?

Mange virksomheder undervurderer opgaven med at gennemføre it revision, som derfor bliver præget af hovsa-løsninger og panik få dage før den årlige finansielle revision.

Der er mange udfordringer, som alle sammen peger på, at der er god mening i at tage it revisionen seriøst. Lad os bare nævne fem forskelligartede udfordringer:

1. Organisationer bevæger sig fra centraliseret til decentraliseret kontrol og styring. Når ledelseshierarkier bliver fladere, kan én leder ikke overskue alle processer, og det bliver derfor nødvendigt at indføre en række it-forankrede tjekpunkter som en slags ramme om kaos eller den øgede kompleksitet.
2. Mængden af medarbejdere, der skifter roller eller har flere roller i virksomhederne stiger. Det samme gør deres adgangsrettigheder til it-systemerne. Mængden af adgangsrettigheder vokser markant, og i mange virksomheder er der begrænset overblik over, hvem der har adgang til hvad, ligesom der ikke løbende bliver fulgt op og justeret på rettighederne i systemerne.
3. It-afdelingen er begravet i nyudviklinger og daglig drift. De har svært ved at finde ressourcer til compliance, processer, sikkerhed, nødvendige opdateringer af systemer, udskiftning af udstyr og hardware og den slags rutineprægede men fundamentalt vigtige opgaver.
4. Topledelsen har i de fleste virksomheder fokus på salg og udvikling. Topledelsen bruger ikke mange timer på at sikre, at it-fundamentet løbende er på plads. Det er ikke sexet, og det er ikke den slags faglighed, den administrerende direktør selv kommer fra endsige bliver direkte målt på af bestyrelsen og omverdenen.
5. Det er for mange CIO'er og it-chefer vanskeligt at løfte dialogen om it revisionens forretningsfordele over for topledelse og kollegaer. I nogle sektorer er it revision en license to operate, og her er det naturligvis nemmere at få ørenlyd og få bevilliget budget. Men i mange andre sektorer er det et strategisk valg om, virksomheden vælger at bruge ressourcer på it-revision, og mange it-ledere har svært ved at opbygge og kommunikere en businesscase for en grundig it-revision.

# It-revision kan skabe værdi

## GDPR kræver styr på it

*EUs persondataforordning GDPR er et godt og aktuelt eksempel på, hvor vitalt det er at have styr på it-systemer og de processer, systemerne understøtter. Hvor bliver hvilke data gemt? Hvordan bliver de anvendt, og hvem har adgang til dem? Statslige virksomheder skal være ISO 27001 certificerede, men også mange private virksomheder har i dag stor gevinst af at blive ISO 27001 certificeret eller lignende certificering – både fordi det giver et stærkere forretningssystem, og fordi det giver konkurrencefordele, fordi kunder og leverandører foretrækker at samarbejde med virksomheder, der kan dokumentere, at de har styr på processer, kvalitet, data og systemer.*

## HVORDAN SER DEN GODE OPSKRIFT UD?

Den første overvejelse er: Er formålet med min it-revision blot at bestå "eksamen" og så slippe den der - eller er det at gribe det proaktivt an, finde hullerne i osten og forstærke hele det it-baserede forretningssystem?

Vi mener, at it-revisionen er en glimrende anledning og løftestang til at blive bedre. It-revisoren er en uvildig, ekstern og professionel sparringspartner, der kan hjælpe med at finde frem til, hvor det kan betale sig at sætte ind baseret på en risikovurdering – og derved også hvor det ikke betaler sig at sætte ind.

Men det forudsætter, at ledelsens indstilling er: "vi er ikke perfekte. Vi kan altid blive bedre, og vi ønsker altid at blive bedre". Eller formuleret på en anden måde: Anser I it revision for en trussel eller en mulighed?

Når det er sagt, handler vores opskrift på den gode it-revision om struktur, prioritering, risikostyring, genbrug og et gennemtænkt årshjul baseret på værktøjer. Lad os uddybe det en smule:

- **Struktur:** Det vigtigste ved en it-revision er at anlægge en struktureret tilgang. De fleste virksomheders it-landskab er præget af mangel på strukturerede tilgange og mangel på overblik. It-afdelingerne løber afsted for at følge med behovet for udvikling af nye apps og løsninger samt for at lappe huller, der løbende opstår. Der er sjældent tid til at skabe sig et overblik over helheden og lægge en plan. Et godt eksempel er dokumentstrukturen, som i mange virksomheder er kaotisk.
- **Prioritering og risikostyring:** Udgangspunktet for en it-revision bør være en grundig risikovurdering, hvor man vurderer og dernæst prioriterer risikoen/værdiskabelsen på de enkelte forretningsområder, processer og tilhørende it-understøttelse. Vores råd er på pragmatisk vis at prioritere de områder, der skaber de største risici/værdier og sætte ind der først. Brug ressourcerne på de 20 procent, der skaber mest forretningsværdi. Det handler også om ikke at sætte barren for højt og bruge for mange ressourcer på de 80 procent, der skaber mindre værdi.
- **Genbrug:** I mange større virksomheder vil der være mange former for it-revisioner i løbet af et år. Vi har set eksempler på op til 25 revisioner på et år. Mange af revisionerne trækker på de samme dokumenter. En ISAE 3402 SOC2 erklæring og en ISO 27001:2013 compliance rapport har begge op mod 150 kontrolpunkter, hvoraf mange omhandler de samme kontroller. Ved at samordne principper kan man benytte de samme strukturer og dokumenter. Herved spares der betydeligt tid, ressourcer og omkostninger. Når en virksomhed således opbygger en velordnet dokumentstruktur, hvor det er nemt at finde dokumentation for et konkret sæt processer frem, så er der hurtigt sparet masser af tid.
- **Årshjul og værktøjer:** En god proces for it-revision i en virksomhed, der ikke har haft tradition for systematiseret it-revision, kræver en hård indsats de første to-tre år. Det kræver design af årshjul, hvor opgaver og aktiviteter bliver fordelt på årets 12 måneder, så organisationen ikke endnu engang bliver fanget på det forkerte ben få dage eller uger før den årlige revision. Årshjulet skal suppleres med værktøjer, der gør det let og hurtigt at gemme samt finde dokumentation for alle relevante parter i organisationen. Det uddyber vi i det følgende afsnit.

# It-revision kan skabe værdi

## It-revision er et sundhedstjek

*It-revision er også et sundhedstjek af virksomhedens processer og sikkerhed. I de sidste fem til 10 år er it-sikkerhed gået fra nice-to-have til i dag at være et absolut need-to-have, fordi trusselsbilledet er markant ændret, og fordi manglende it-sikkerhed hurtigt kan betyde meget store problemer for en virksomhed eller helt kan lukke virksomheden.*

## HVORDAN FÅR DU DET TIL AT SKINNE I HVERDAGEN?

Lad et årshjul fastholde de løbende forbedringer, så it-revision ikke er noget, I blot gør nogle få kaotiske uger hvert år, men bliver en kontinuerlig proces, som organisationens har fokus på.

Årshjulet skal suppleres med værktøjer, der gør det nemt for alle relevante parter at arkivere dokumentation og dokumenter, så de er hurtige og lette at finde frem igen. Det kan for eksempel være via en logisk opbygget og søgbar webside på intranettet. Her kan alle relevante medarbejdere med få klik servicere sig selv og fremfinde dokumenter, som allerede er produceret, og som de derfor ikke skal starte forfra på at producere. Denne del kan spare mange organisationer mange ressourcer.

Det er også vigtigt at placere et ejerskab. Det kan være en it-chef, en kvalitetschef, en finans controller eller en intern revisorrolle. Det er ikke så vigtigt hvor, det er placeret. Det vigtige er, at der en ansvarlig til løbende at holde øje med årshjulet, og som har det tilstrækkelige mandat og budget fra topledelsen til at agere på opgaven med at få den løbende it-revision til at virke og leve.

Målet er ikke at genstarte processen fra nul hvert år, men at organisationen har fokus på it-revision året rundt. Det indebærer at opbygge en struktureret proces, at vedligeholde den, og at sikre at processen skaber de ønskede forretningsgevinster i form af mere salg, højere sikkerhed, mere effektiv drift etc.

-//-



**Lars Studstrup og Jens Popp Lybye** har tilsammen mere end 55 års erfaring med ledelse af it-afdelinger i mellemstore og store virksomheder, hvor de har gennemført hundredvis af it-revisioner. Lars Studstrup har 20 års erfaring som infrastruktur-chef i virksomheder som Mærsk-virksomheden DISA, Royal Greenland, Nets Denmark A/S og mere end 10 års erfaring som ekstern konsulent for danske og internationale virksomheder. Jens Popp Lybye har 25 års erfaring med it-strategi, drift og ledelse både som leder i virksomheder som ATP, Lundbeck og IBM og de seneste år som ekstern konsulent og projektleder.



**Maximize Consult** sætter fingeren på udfordringer og udarbejder effektive løsninger til projekt- og driftsorganisationer, og bidrager hermed til at din virksomhed kan nå sine forretningsmål.