



Rådgivning om it

Ydelser inden for it governance og it assurance

It-risikoanalyse

Virksomheder investerer og anvender it mere og mere til at støtte forretningsprocesser med. Dette medfører en øget eksponering og et ændret risikobillede i forhold til de kritiske forretningsprocesser. Udfordringerne med at sikre compliance, tilgængelighed, fortrolighed og integritet af data bliver stadig større.

It-strategi og it-sikkerhedspolitik er vigtige redskaber til at sikre, at disse krav til og rammer for it-anvendelsen i virksomheden overholdes. Fastlæggelse af it-sikkerhedsniveauet bør tage udgangspunkt i en risikoanalyse, der viser virksomhedens sårbarhed på it-området. Dette sikrer en målrettet indsats af it-anvendelsen, hvor virksomheden er mest sårbar. Samtidig sikrer det en bevidsthed om sårbarheden og medvirker til, at der ikke er risikoområder, som er under- eller overbeskyttet.

Resultatet af en it-risikoanalyse giver sikkerhed om virksomhedens it-anvendelse og risikobillede til ledelsen og sparring til it-chefen eller den it-ansvarlige. Denne sikkerhed tager udgangspunkt i virksomhedens konkrete it-anvendelse.

Udfordringer ledelsen har for at have en sikker it-anvendelse

Ledelsen bør være opmærksom på følgende:

- Konsekvenserne, når virksomhedens it helt eller delvist ikke er tilgængelig
- Udenforstående får adgang til at læse, ændre, stjæle eller slette data
- Besvigelser opstår og forbliver uopdaget eller opklares ikke
- Svigt i projekter eller i ændringer til eksisterende systemer
- Ikke-identificerede eller -afklarede konflikter i funktionsadskillelsen
- Sikring af tilgængelighed ved it-nedbrud – hvordan etableres et beredskab, og er der nødplaner, så virksomheden kan fastholde kontinuiteten og re-etablere forretningen?

Svig eller datatyveri – har der været konstateret tilfælde? Eller er det blot en ubekræftet mistanke, som ikke kan dokumenteres?

Manglende dataintegritet – er virksomhedens data korrekte?

Konsoliderede data og ledelsesinformationer er pålidelige

Overholdelse af relevant lovgivning.

Risikoanalyse med Beierholm

Vi anvender en model baseret på god skik inden for it-risikostyring, Cobit IT Risk og COSO til analyse af risici ved it-anvendelsen. På baggrund af vores kendskab til virksomheden samt erfaringer fra lignende virksomheder og branchen kan vi medvirke til at udarbejde en risikoanalyse. Endvidere kan vi komme med forslag til handlingsplaner til håndtering af risici af områder, der ikke er tilstrækkeligt afdækket eller beskyttet. Det er blandt andet denne model, der er anvendt til at fastlægge Beierholms egen it-risikoprofil.

I samarbejde med relevante medarbejdere hos virksomheden kortlægger vi de væsentlige risikofaktorer omkring compliance, fortrolighed, tilgængelighed og integritet. Dette hjælper ledelsen med at få tegnet risikobilledet i virksomhedens it-anvendelse samt med at lægge handlingsplaner til håndtering af de største risici. I samarbejde med virksomheden identificerer vi:

- Kritiske forretningsprocesser
- Trusler – sandsynlighed og omfang
- Risiko for potentielle finansielle og operationelle tab
- Kritisk tid for at få genetableret processer
- Hvorledes risici kan håndteres.

I får et godt overblik over alle væsentlige risici samt en kvantificering af, hvilke risikofaktorer der er mest kritiske. Dermed får I mulighed for at gøre en indsats for at styrke it-sikkerheden. I får desuden vished for, at det ønskede niveau for sikkerhed er kendt, samt at der kan tages stilling til eventuelle restrisici.

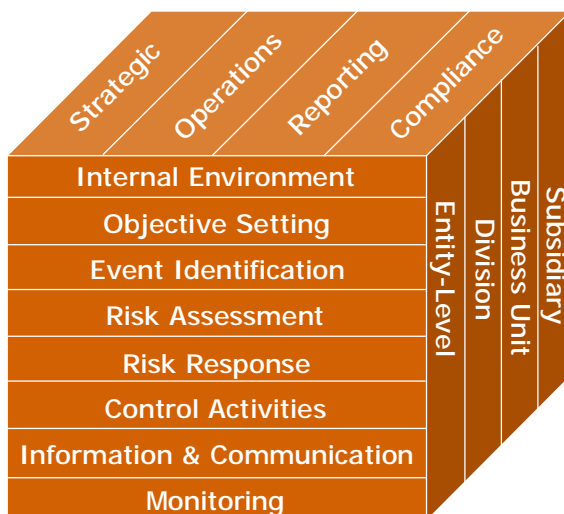
Metoden

Virksomhedens risikobillede tegnes på baggrund af en gennemgang af hændelser, der er tilpasset virksomhedens art og karakter. Fremgangsmåden er følgende:

1. Vurdering af virksomhedens sårbarhed, hvis en hændelse indtræder med udgangspunkt i de allerede etablerede kontroller
2. Vurdering af sandsynligheden for, at hændelsen indtræder
3. Vurdering af konsekvenser for virksomheden, hvis hændelsen indtræder.

Ved at sammenholde disse tre forhold fremkommer virksomhedens restrisiko, som er den risiko, virksomhedens ledelse skal tage stilling til. Er risikoen acceptabel, eller skal der etableres yderligere foranstaltninger for at reducere risikoen? Summen af de to første punkter beskriver risikoen for virksomheden, når skaden er sket.

Med udgangspunkt i risikoanalysen, er det muligt at opbygge en målrettet it-sikkerhedspolitik til fastlæggelse af sikkerheden omkring it-anvendelsen i virksomheden, således at ledelse, it-afdeling og øvrige medarbejdere har klare rammer for sikkerhed og en bevidsthed om virksomhedens risikoprofil.



Hvis du vil vide mere, så kontakt:

Hans Henrik Aa. Berthing

It-revisionschef
Tlf.: 9634 7229
2220 2821 (mobil)
hbb@beierholm.dk