

Hvorfor skal en virksomhed have udarbejdet en **it-risikoanalyse**?

IT-Revision & Risikostyring

Hvorfor udarbejde en it-risikoanalyse?

It-strategien og it-sikkerhedspolitikken er vigtige redskaber til fastsættelse af rammerne for it-anvendelsen i virksomheden. Fastlæggelse af niveauet for sikkerhed bør tage ud-

gangspunkt i en risikoanalyse, der anskueliggør virksomhedens sårbarhed på it-området. Dette sikrer en målrettet indsats på de områder 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.



Hvordan kan Grant Thornton hjælpe?

IT-Revision & Risikostyring har udarbejdet en model til brug for analyse af risici ved it-anvendelsen. Modellen er udarbejdet med udgangspunkt i standarden "National Institute of Standards and Technology - Special Publication 800-30 Risk Management Guide for Information Technology Systems".

Vi kan på baggrund af vores kendskab til klienten og dennes virksomhed samt erfaringer fra tilsvarende virksomheder medvirke til at udarbejde en risikoanalyse med udgangspunkt i nævnte model.

Endvidere kan vi give anbefalinger til modforanstaltninger på områder, der ikke er beskyttet godt nok, således at risikoen kan mindskes. Det er blandt andet denne model, der er anvendt til at fastlægge Grant Thorntons egen it-risikoprofil.

Metoden

Virksomhedens risikobillede findes ved at opstille en række hændelser, der er tilpasset virksomhedens art og karakter. Fremgangsmåden er følgende:

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

Ved at sammenvægte 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? En sammenvægtning af ovenstående to første punkter beskriver risikoen for virksomheden, når skaden er sket.

Resultatet

Til brug for gennemgangen af risikoanalysen, har vi, som tidligere beskrevet, opbygget en model, der samler vurderinger og resultater i et skema. Nedenfor er vist et lille udsnit af risikoanalysen.



nr.	Hændelser	Berører			Beskrivelse af konsekvens	Konsekvens af hændelsen (1-5)	Beskrivelse af de kontrolforanstaltninger mv., der allerede er etableret	Sårbarhed (1-5)	Skaden hvis det sker	Sandsynlighed for hændelsen (1-5)	Rest risiko	Vurdering af restrisiko og skadesrisikoen og eventuelt handlinger til reduktion af risikoen
		F	P	T								
FYSISK SIKKERHED												
F1	Brand i hele huset			X	Data på servere og fysisk klient relaterede materiale ødelægges. Det vil være vanskeligt at fortsætte arbejdet	4	Håndslukke-re rundt omkring. Begrænset antal branddøre	5	Eks-trem	3	Væsent-lig	Der bør foretages en gennemgang af muligheder for brandsikring af en fagmand, og indhentes tilbud på forskellige typer brandsikring som f.eks. Alarmsystem til Falck, Røgmeldere, Inddeling af huset i brandzoner, branddøre osv.
F2	Brand i serverrum			X	Delvis eller totalt ødelagte servere og data. Medarbejderne er ikke i stand til at udveksle elektroniske AP	3	Røgmelder til e-mail, dagtimer til IT-Service, udenfor til privat-mail. Håndslukker uden for døren	4	Væ-sentlig	3	Mindre	
F3	Lynnedslag - større ødelæggelse			X	Strømmen vil forsvinde da HFI relæ aktiveres	2	Fejlstrøm vil tilkoble nødstrøm til servere. HPFI-relæ	2	Minde	2	Lav	
DRIFTSSIKKERHED												
D1	Firewall virker ikke	X	X	X	Enten vil FW ikke tillade trafik ellers vil den behandle og videresende alle forespørgsler. Kan give tab af fortrolighed	4	Ekstern over-vågning men ingen kontrol af denne, herunder kontrol af log. o.l.	4	Kritisk	3	Væsent-lig	Det bør overvejes, om der skal ske en kontrol ved 3. part af, at leverandøren lever op til kontraktens krav. Endvidere bør det overvejes om den nuværende overvågning er tidssvarende.
D2	Manglende backup på grund af fejl			X	Der er ikke taget backup af filer som forventet. Kan ikke genskabe tabte filer	3	Kontrol af backup. Gode båndstationer og andet udstyr. Begrænset adgang	3	Væ-sentlig	3	Mindre	Der bør ske formalisering af backup og ske regelmæssig test heraf.
D3	Konkurs hos central it-leverandør			X	Ikke muligt, at få den ydelse som vi er vant til. Konsulent kendskabet til vores systemer tabes.	1	Mange mulige lev. med det vi anvender, men ingen aftaler. Ingen væsentlige afhængigheder af lev.	3	Lav	2	Lav	Risikoen er acceptabel

(F = Fortrolighed; P = Pålidelighed; T = Tilgængelighed)

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.

Hvordan kommer jeg videre?

I er velkommen til at kontakte IT-Revision & Risikostyring, hvis I vil vide mere.

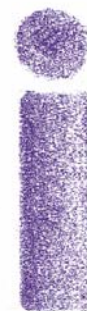
Michael Clement

Director
T +45 35 27 12 36
mic@grantthornton.dk



Rainer Petersen

Manager
T +45 35 27 12 39
frp@grantthornton.dk



grantthornton.dk
Statsautoriseret Revisionsaktieselskab



Stockholmsgade 45 • DK-2100 København Ø
Tlf. 35 27 11 00 • Fax 35 27 11 01
Hjulmagervej 8 K • DK-7100 Vejle
Tlf. 76 43 25 00 • Fax 76 43 25 01