



Vejledning

Risikovurdering

D-mærkets vejledning til risikovurdering af virksomheden og dens registrerede.

Vejledningen tager udgangspunkt i Erhvervsstyrelsens it-risikovurdering, hvortil kvalitative berigelser tilføjes for at kunne anvendes som dokumentation for D-mærkets kriterie 1.3.1.



Introduktion

Erhvervsstyrelsen tilbyder et værktøj, der hjælper både små og mellemstore virksomheder med at bevidstgøre sig om- og risikovurdere forskellige aspekter inden for deres it-sikkerhed. Værktøjet guider nemt og intuitivt virksomheden igennem en række forhold de skal tage stilling til, og der er korte hjælpepetekster til rådighed hele vejen igennem.

Resultatet er et skema i Excel med overblik over identificerede risici. Hertil er det muligt at udbygge det med egne indsatser. Skemaet kan med en mindre præcisering og udbygning anvendes til besvarelse af D-mærkets kriterie 1.3.1 vedr. netop en it-risikovurdering for virksomheden.

Erhvervsstyrelsens værktøj er gratis at anvende.

Formål

Risikovurderinger er et stærkt styringsværktøj for en virksomhed til at sikre at ressourcer allokeres korrekt. På baggrund af risikovurderingen skal virksomheden vurdere behovet for at implementere yderligere sikkerhedsforanstaltninger eller relevante ændringer. Dette er for at sikre at risikoen håndteres, og at den er på et acceptabelt niveau.

Risikovurdering er relevant for alle typer virksomheder. Det giver virksomheden en kompetence, som kan øges og hjælpe virksomheden over tid.

D-mærket anbefaler virksomheder at anvende Erhvervsstyrelsens it-risikovurderingsværktøj, da værktøjet er udviklet af Erhvervsstyrelsen i samarbejde med Virksomhedsforum for Digital Sikkerhed og er gratis at anvende.



Vejledning til udfyldelse

1. Tilgå [Erhvervsstyrelsens værktøj til it-risikovurdering](#)
2. Vælg antal medarbejdere i virksomheden.
3. Besvar de spørgsmål som værktøjet guider dig igennem step for step. Spørgsmålene inddeles i kategorier, som hjælper dig til at vurdere risici forbundet med:
 - Enheder
 - Applikationer og tjenester
 - Egne applikationer
 - Brugere
 - Netværk
 - Data

For hver spørgsmål bedes du vurdere risikoen ud fra sandsynlighed og konsekvens på en skala fra 1-5. Er du i tvivl om vægtningen af skalaerne, kan du under hele besvarelsen, finde en definition af skalaerne øverst til højre over spørgsmålene (se Bilag, 'Skærbillede 1').

4. Download it-risikovurderingen, når alle spørgsmål er besvaret. Dette gøres på sidste trin (se Bilag, 'Skærbillede 2').
5. Åbn den downloadede fil. *OBS! Det kræver Excel eller lignende program at åbne filen.*
6. I regnearket findes bruttolisten af besvarelsenerne udfyldt i Erhvervsstyrelsens værktøj (se eksempel i Bilag, 'Skærbillede 3'). Skemaet skal beriges med en kvalitativ stillingtagen for alle identificerede risici i følgende kolonner:
 - **Kolonne A:** Risikoområde (her navngives de omtalte systemer)
 - **Kolonne C:** Risikoejer (her udfyldes navnet på den medarbejder, der har ejerskab over risikoen)
 - **Kolonne F:** Hvorfor vurderes sandsynligheden til dette? (her udfyldes argumentet for scoringen af den specifikke risikos sandsynlighed)
 - **Kolonne H:** Hvorfor vurderes konsekvensen til dette? Hvad er konsekvensen for den registrerede? (her udfyldes argumentet for scoringen af den specifikke risikos konsekvens baseret på konsekvensen for virksomheden og for den evt. registrerede)
 - **Kolonne J:** Accepteret (ja/nej) (her udfyldes om risikoen er accepteret eller ej)
7. Gem det endelige regneark, når du er færdig med berigelserne fra step 6. Du har nu udarbejdet dokumentation for din virksomheds IT-risikovurdering relevant for D-mærkets kriterie 1.3.1.

**Tip:**

På sigt kan virksomheden med fordel opdatere kolonnerne K-P, der omhandler risikohåndtering. Dette er dog ikke et krav til D-mærkets kriterie 1.3.1. (Se Bilag, 'Skærbillede 4').

Bilag

Skærbillede 1:

Definition af skalaerne for sandsynlighed og konsekvens. Trykker man på krydset udfolder skalaen sig.

Sådan gør du

Du skal vurdere sandsynlighed og konsekvens på to skalaer, som hver har fem svarmuligheder. Skalaerne ser ud som følger.

+ Skala for sandsynlighed

+ Skala for konsekvens

Skærbillede 2:

Når alle spørgsmål i Erhvervsstyrelsens værktøj er besvaret, får du mulighed for at downloade besvarelsene som regneark.



A	B	C	D	E	F	G	H	I	J
Risiko - hvad kan påvirke fortrolighed, tilgængelighed eller integritet?			Risikovurdering						
Risikoområde	Risikoejer	Hvorfor er dette en risiko?	Indtastet sandsynlighed (1-5)	Hvorfor vurderes sandsynligheden til dette?	Indtastet konsekvens (1-5)	Hvorfor vurderes konsekvensen til dette?	Beregnet risiko	Accepteret (ja/nej)	
Enheder	Manglende forsvar mod malware	Enheder som ikke har antivirus eller ikke er opdaterede er særligt sårbare over for malware.	4		4		16		
Enheder	Ukendte enheder i virksomheden	Ukendte enheder (f. eks. IoT-produkter, printere eller smartphones) tilkoblet virksomhedens netværk kan være en usikker indgang til virksomheden eller være skadelige i sig selv.	3		3		9		
Applikationer og tjenester	Manglende overblik over jeres applikationer og tjenester	Et manglende overblik over accepterede og installerede applikationer kan resultere i ondsindet eller uopdateret software på enheder	3		5		15		
Vurdér egne applikationer	Bogføringssystem bliver kompromitteret	Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	2		5		10		
Vurdér egne applikationer	E-mail: E-mail-system bliver kompromitteret	Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	2		3		6		
Vurdér egne applikationer	Filer server: Filer server bliver kompromitteret	Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	3		2		6		
Vurdér egne applikationer	Hjemmeside (CMS): Hjemmeside (CMS) bliver kompromitteret	Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	3		5		15		
Vurdér egne applikationer	Lagerstyring: Lagerstyringssystem bliver kompromitteret	Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	2		5		10		
Vurdér egne applikationer	Vagtplanlægning: Vagtplanlægningssystem bliver kompromitteret	Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	2		1		2		
Brugere	Uopmærksomme brugere	Hackerne tilvinger sig adgang ved at lokke brugerne til at hente og åbne ondsindet malware via deres webbrowsere eller via links i e-mails. Udefrakommende og medarbejders	2		4		8		



IT-risikovurdering af din virksomhed

Du har nu vurderet sandsynlighed og konsekvens af forskellige risikoscenarier for din virksomhed. Dine besvarelser har resulteret i følgende IT-risikovurdering:

[← Tilbage til testen](#)

[Download IT-risikovurdering \(kræver regneark\)](#)

Skærmbillede 3:

Udsnit fra eksempel på bruttoliste af besvarelser udfyldt i Erhvervsstyrelsens værktøj inden kvalitativ berigelse.



Skærbillede 4:

Kolonne K-P omhandler virksomhedens risikohåndtering af den enkelte risiko. Dette kan være en fordel for virksomheden at udfylde på sigt.

K	L	M	N	O	P	Q
Risikohåndtering						
Nye foranstaltninger	Ny sandsynlighed (1-5)	Konsekvens efter nye foranstaltninger	Ny restrisiko	Restrisiko Accepteret	Konklusion	Kilder til håndtering
			0			https://sikkerdigital.dk/virksomhed/hvad-truer-din-virksomhed
			0			https://cfcs.dk/globalassets/cfcs/dokumenter/vejledning
			0			https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed
			0			https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed
			0			https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed
			0			https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed
			0			https://sikkerdigital.dk/virksomhed/fem-gode-raad-der-kan-hjælpe-din-virksomhed
			0			https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed
			0			https://sikkerdigital.dk/virksomhed/fem-gode-raad-der-kan-hjælpe-din-virksomhed