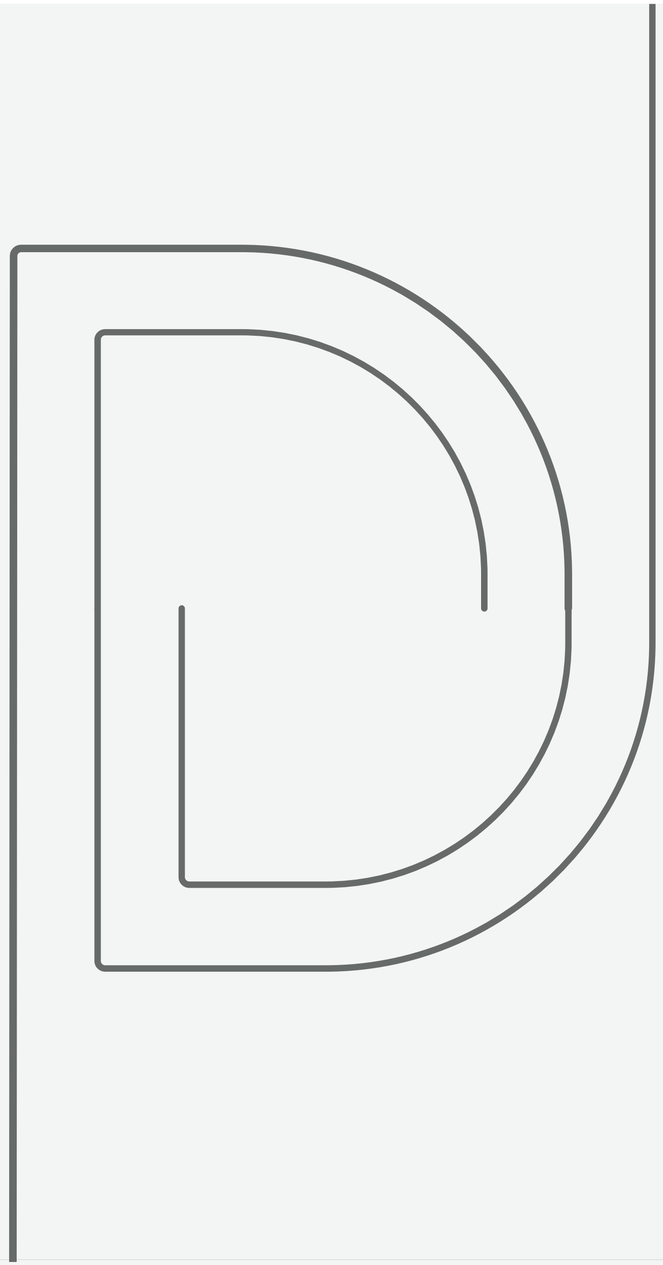
Danmarks nye mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse

Mikael Jensen, D-mærket

Webinar
Cyber- og informationssikkerhed på strategiske niveauer

Arrangører
Bestyrelsesforeningen og Dansk Standard

Tid og sted
9. november 2021 I 11.00 – 11.20 I CBS I Porcelænshaven, Frederiksberg



DANSK ERHVERV

SMVdanmark

Forbrugerrådet Tænk

INDUSTRIENS FOND

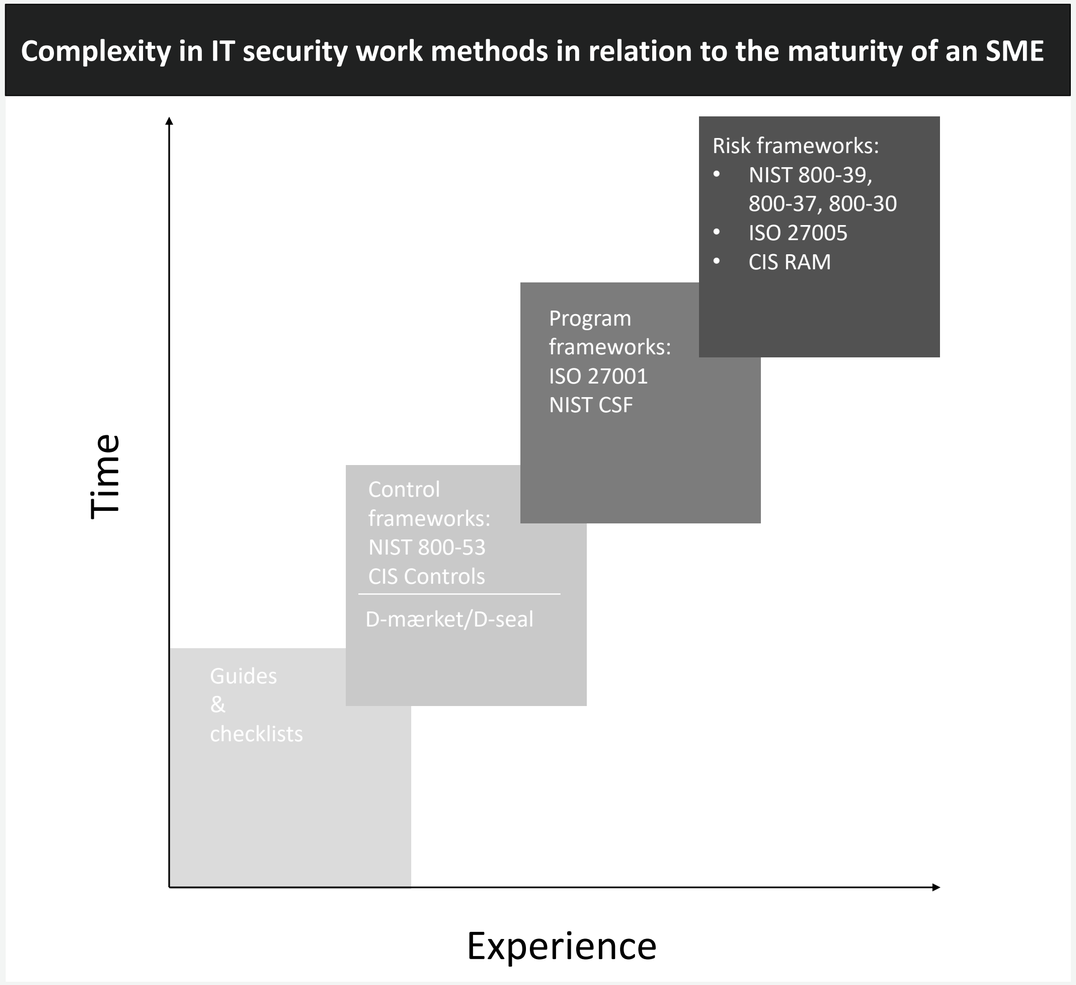
D-mærket …

- … er en efterspørgselsdrevet og frivillig mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse
- … er mærkning af virksomheder og ikke specifikke produkter og tjenester
- … består af 8 overordnede kriterier med fokus på it-sikkerhed, persondatabeskyttelse, kunstig intelligens og dataetik
- … er målrettet såvel en B-2-B og en B-2-C kontekst
- … er ét mærke, men antallet af kriterier vil afhænge af virksomhedens generiske risikoprofil
- … er et markedsføringsredskab til virksomheder

Industriens Fond står bag D-mærket i samarbejde med Dansk Industri, Dansk Erhverv, SMVdanmark og Forbrugerrådet Tænk. D-mærket støttes af Erhvervsstyrelsen og er en uafhængig privat organisation.

Kilde: https://d-maerket.dk/om/

Mærkets rolle set fra et virksomhedsperspektiv



Inspired by: "Anbefaling: En mærkningsordning for it-sikkerhed", Virksomhedsrådet for IT-sikkerhed (December 2018) & CIS Controls V7 poster https://www.cisecurity.org/white-papers/cis-controls-v7-poster/

D-mærkets differentiator/USP og ESSENS

FORBRUGERE

D-mærket giver mig tillid til (deling og anvendelse af) data, og gør det nemt for mig at vælge virksomheder og tjenester, der behandler data sikkert og ansvarligt.

“Skaber digital tryghed for mig!”

VIRKSOMHEDER

D-mærket er en enkel og tillidsfuld guide, der gør det nemt at håndtere data sikkert og ansvarligt og derefter skilte med det.

“Skaber værdi for min forretning!”

SAMFUNDET

D-mærket gør digital sikkerhed og ansvarlig dataanvendelse til et positivt konkurrenceparameter og en dansk styrkeposition.

“Skaber et stærkere digitalt Danmark”

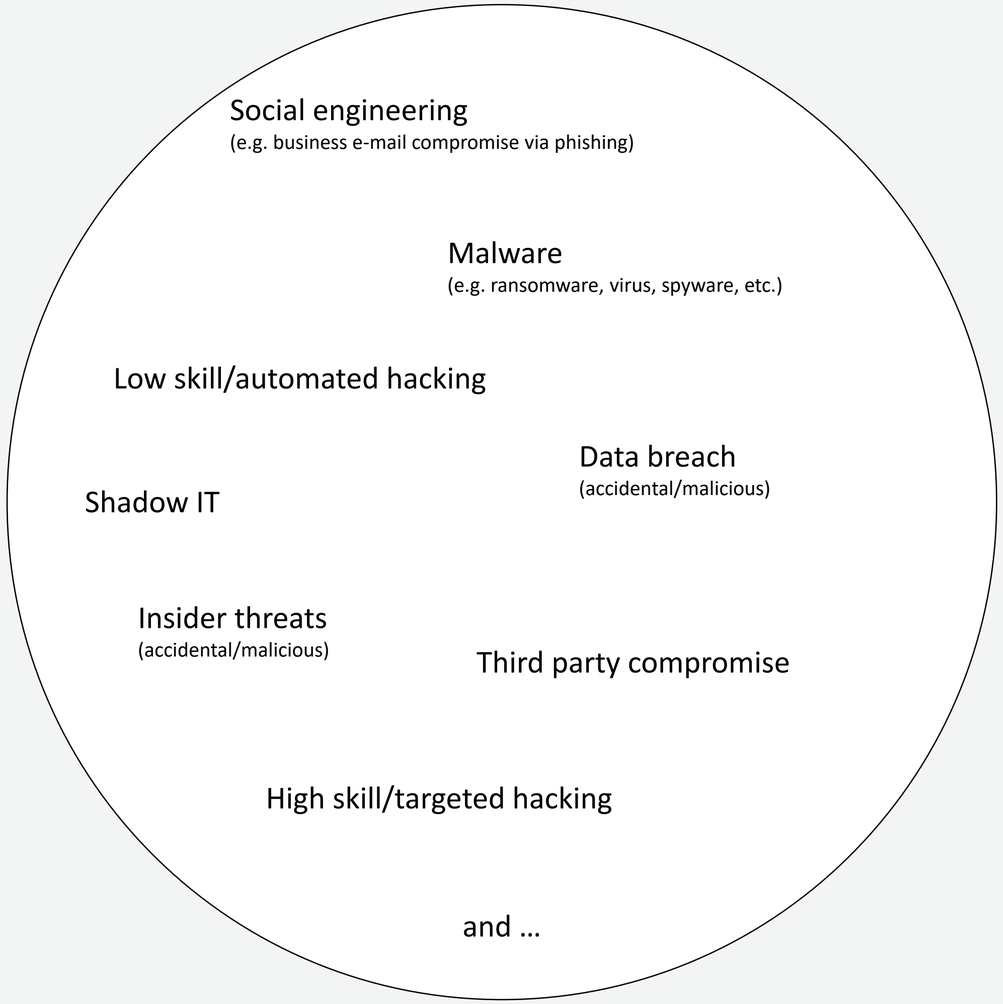
digital tryghed

digital tryghed

digital trust

digital trust

Trusselsbillede: it-sikkerhed og dataetik



Kilder: ENISA Threat Landscape 2021; Trusselsvurdering 2021: Cybertruslen mod Danmark, CFCS; 2018 Institute for the Future and Omidyar Network. (CC BY-NC-SA 4.0). SR-2005 | ethicalOS.org

Hvilken gruppe tilhører din virksomhed?

Antallet af kriterier og krav som virksomheden skal leve op til afhænger af virksomhedsgruppen, men alle virksomheder skal som minimum leve op til kriterie 1, 2, 3 og 5.

Kriterier for indplacering i gruppe	Gruppe I	Gruppe II	Gruppe III	Gruppe IV
Antal ansatte	0-9	10-49	50-249	250+
Nettoomsætning (mio. DKK)	0-7,9	8-155,9	156-313	≥ 313
Leverandør af software eller it-tjenester	Nej	Nej	Ja	Ja
Behandler særlige kategorier af personoplysninger (fx helbredsoplysninger, race, sexualitet)	Nej	Ja	Ja	Ja

Kilde: https://d-maerket.dk/virksomhedsgrupper/

Mærkets kriterier i værdikæden

Kilde: https://d-maerket.dk/kriterier/

Eksempel på udmøntning af kriterier til krav

Kriterie: Niveau 1 (fx 3.0) Overordnede kriterier indenfor it-sikkerhed, privatliv og etik	**Fx 3.0 Teknisk it-sikkerhed**			
Kriterie: Niveau 2 (fx 3.1 – 3.7) Opdeling af overordnede niveau 1 kriterier til håndterbare kriterier på lavere niveau	Fx 3.1 Netværkssikkerhed og kryptering		Fx 3.4 Beskyttelse mod malware	
Kriterie: Niveau 3 (fx 3.1.1 – 3.7.1) Opdeling af niveau 2 kriterier i operationelle kriterier	3.1.1 Beskyttelse af administrative grænseflader, netværk og enheder	3.1.2 Kryptering af ekstern netværksadgang	3.4.1 Implementering af beskyttelsesmekanismer mod malware	3.4.2 Beskyttelse mod uønskede e-mails
Krav til praktisk implementering (fx 3.1.1.1 – 3.7.1.6) Konkrete handlingskrav til praktisk implementering for at opfylde niveau 3-kriterier	3.1.1.1 – 3.1.1.3 Konkrete og handlingsorienterede krav	3.1.2.1 – 3.1.2.3 Konkrete og handlingsorienterede krav	3.4.1.1 – 3.4.1.10 Konkrete og handlingsorienterede krav	3.4.2.1 – 3.4.2.3 Konkrete og handlingsorienterede krav
Tilsyn og kontrol Tilsyns- og kontrolprocesser	Beskrivelse af, hvordan det er bevist, at kravene eller indikatorerne er opfyldt og / eller mængden eller kvaliteten i, hvor langt krav eller indikatorer er opfyldt	Beskrivelse af, hvordan det er bevist, at kravene eller indikatorerne er opfyldt og / eller mængden eller kvaliteten i, hvor langt krav eller indikatorer er opfyldt	Beskrivelse af, hvordan det er bevist, at kravene eller indikatorerne er opfyldt og / eller mængden eller kvaliteten i, hvor langt krav eller indikatorer er opfyldt	Beskrivelse af, hvordan det er bevist, at kravene eller indikatorerne er opfyldt og / eller mængden eller kvaliteten i, hvor langt krav eller indikatorer er opfyldt

Oversigt over D-mærkets kriterier på niveau 1 og 2 samt relation til rammeværker

KRITERIE 1 Styring og forankring i ledelsen	KRITERIE 2 Awareness og sikker adfærd	KRITERIE 3 Teknisk it-sikkerhed	KRITERIE 4 Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse	KRITERIE 5 Transparens & kontrol med data	KRITERIE 6 Privacy & security by design & default	KRITERIE 7 Pålidelige algoritmer & AI	KRITERIE 8 Dataetik
NIVEAU 2 KRITERIER 1.1 Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse 1.2 Overblik over data og systemer 1.3 Risikostyring 1.4 Politik for it-sikkerhed 1.5 It-beredskabsplan 1.6 Politikker for ansvarlig dataanvendelse 1.7 Udviklingsproces	NIVEAU 2 KRITERIER 2.1 Træn bestyrelsen og den øverste ledelse i sikkerhed, databeskyttelse og dataetik 2.2 Awareness om og træning i it-sikkerhed 2.3 Awareness om og træning i ansvarlig dataanvendelse	NIVEAU 2 KRITERIER 3.1 Netværkssikkerhed og kryptering 3.2 Korrekt konfiguration 3.3 Beskyttelse af administrative brugerkonti 3.4 Beskyttelse mod malware 3.5 Kontinuerlig opdatering af software og styresystemer 3.6 Beskyttelse mod tab af vigtige og fortrolige data 3.7 Overvågning af systemaktivitet gennem logning	NIVEAU 2 KRITERIER 4.1 Leverandørlivscyklus og risikovurdering 4.2 Krav til it-sikkerhed hos leverandører 4.3 Krav til ansvarlig databehandling hos leverandører	NIVEAU 2 KRITERIER 5.1 Information i relation til personoplysninger 5.2 Cookies 5.3 Kontrol over egne personoplysninger 5.4 Lettilgængelig klagevejledning	NIVEAU 2 KRITERIER 6.1 Vurdering 6.2 Privacy by design & default 6.3 Security by design & default 6.4 Implementering igennem udviklingsproces	NIVEAU 2 KRITERIER 7.1 Menneskeligt tilsyn og mellemkomst/indgriben og transparens 7.2 Data- og modelkvalitet 7.3 Implementering igennem udviklingsproces	NIVEAU 2 KRITERIER 8.1 Dataetik
EUROPÆISKE KILDER • GDPR	EUROPÆISKE KILDER • GDPR • Europarådet*	EUROPÆISKE KILDER • GDPR • High-Level Expert Group on AI (EU)	EUROPÆISKE KILDER • GDPR	EUROPÆISKE KILDER • GDPR • Datatilsynet (NO) • Datatilsynet (DK) • ENISA**	EUROPÆISKE KILDER • GDPR • Norwegian Data Protection Authority • ENISA**	EUROPÆISKE KILDER • GDPR • Europarådet* • High-Level Expert Group on AI (EU) • AIEI Group (DE) • German Data Ethics Commission (DE) • French Data Protection Authority (CNIL) • DS/PAS 2500 – 1.2020 (DK) • DS/PAS 25000-2.2020 (DK)	EUROPÆISKE KILDER • Den Europæiske Unions charter om grundlæggende rettigheder • Rådet for Digital Sikkerhed (DK) • Dataethics.eu (DK) • Ekspertgruppen om dataetik (DK) • Dataetisk Råd (DK) • UK GOV, Data Ethics Framework (UK) • ICO: Age Appropriate Design Code (UK)
INTERNATIONALE KILDER • ISO/IEC 27001:2013 • ISO/IEC 27701:2019 • NIST-CSF • CIS20	INTERNATIONALE KILDER • ISO/IEC 27001:2013 • ISO/IEC 27701:2019 • NIST-CSF • CIS20	INTERNATIONALE KILDER • ISO/IEC 27001:2013 • ISO/IEC 27701:2019 • NIST-CSF • CIS20 • OECD recommendations on AI	INTERNATIONALE KILDER • ISO/IEC 27001:2013 • ISO/IEC 27701:2019 • NIST-CSF • CIS20	INTERNATIONALE KILDER • ISO/IEC 27001:2013 • ISO/IEC 27701:2019	INTERNATIONALE KILDER • ISO/IEC 27001:2013 • ISO/IEC 27701:2019	INTERNATIONALE KILDER • OECD recommendations on AI • ISO/IEC TR 24028:2020 (Overview of trustworthiness in artificial intelligence)	INTERNATIONALE KILDER • Ethical OS (US)

* Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems
** Privacy and Data Protection by Design–from policy to engineering

Kriterier (niveau 1)	Kriterier (niveau 2)	Kriterier (niveau 3)	Relation til andre rammeværker
K1: Styring og forankring i ledelsen	1.1: Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse	1.1.1: Udpegning af ansvarlig person for it-sikkerhed og ansvarlig dataanvendelse	**GDPR** artikel 24
			ISO/IEC 27001:2013 pkt. 4.2, pkt. 5.3, A.6.1.1
			ISO/IEC 27701:2019 pkt. 6.3.1.1, pkt. 7.2.7, A.7.2.7
			NIST CSF ID.AM-6, ID.GV-2, PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, DE.DP-1, RS.CO-1
	1.2: Overblik over data og systemer	1.2.1: Overblik over personoplysninger	**GDPR** artikel 30, stk. 1
			ISO/IEC 27001:2013 A.8.1.1
			ISO/IEC 27701:2019 pkt. 6.5.1.1, pkt. 7.2.8, A.7.2.8
			NIST CSF ID.AM-1, ID.AM-2
		1.2.2: Overblik over forretningskritiske data	**ISO/IEC 27001:2013** A.8.1.1
			ISO/IEC 27701:2019 pkt. 6.5.1.1
			NIST CSF ID.AM-1, ID.AM-2
		1.2.3: Overblik over it-systemer, tjenester, netværkskomponenter, enheder, software og aktivitetsbaserede algoritmer/AI "use cases"	**GDPR** artikel 30, stk. 1, litra g), artikel 32, stk. 1, litra b)
			ISO/IEC 27001:2013 A.8.1.1
			ISO/IEC 27701:2019 pkt. 6.5.1.1
			NIST CSF ID.AM-1, ID.AM-2
	1.3: Risikostyring	1.3.1: Risikovurdering og -håndtering	**GDPR** artikel 32, stk. 2, artikel 35, stk. 1, artikel 39, stk. 2
			ISO/IEC 27001:2013 pkt. 6.1.1, pkt. 6.1.2, pkt. 6.1.3, pkt. 7.4, pkt. 8.2
			ISO/IEC 27701:2019 pkt. 5.4.1.2
			NIST CSF ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, ID.RM-1, ID.RM-2, ID.RM3
	1.4: Politik for it-sikkerhed	1.4.1: Politik for it-sikkerhed	**GDPR** artikel 32, stk. 1, litra d)
			ISO/IEC 27001:2013 pkt. 5.1, pkt. 5.2, pkt. 5.3, A.5.1.1, A.5.1.2
			ISO/IEC 27701:2019 pkt. 6.2.1.1, pkt. 6.2.1.2
			NIST CSF ID.GV-1
	1.5: It-beredskabsplan	1.5.1: It-beredskabsplan	**GDPR** artikel 32, stk. 1, litra c)
			ISO/IEC 27001:2013 A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7, A.17.1.1, A.17.1.2, A.17.1.3
			ISO/IEC 27701:2019 pkt. 6.13.1.1, pkt. 6.13.1.2, pkt. 6.13.1.3, pkt. 6.13.1.4, pkt. 6.13.1.5, pkt. 6.13.1.6, pkt. 6.13.1.7
			NIST CSF ID.BE-5, ID.RA-4, ID.SC-5, PR.IP-4, PR.IP-7, PR.IP-8, PR.IP-9, PR.IP-10, PR.IP-12, PR.PT-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, DE.DP-4, DE.DP-5, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-4, RS.MI-1, RS.MI-2, RC.RP-1, RC.IM-1, RC.IM-2
	1.6: Politikker for ansvarlig dataanvendelse	1.6.1: Politik for behandling af personoplysninger	**GDPR** artikel 5, stk 2, artikel 24, stk. 1, artikel 24, stk. 2
			ISO/IEC 27001:2013 A.18.1.4
			ISO/IEC 27701:2019 pkt. 6.2.1.1, pkt. 6.2.1.2, pkt. 7.2.2, pkt. 7.3.1, A.7.2.2, A.7.3.1
			NIST CSF ID.GV-3
		1.6.2: Politik for dataetik	**GDPR** artikel 5, stk. 1, litra a)
	1.7: Udviklingsproces	1.7.1: Krav til udviklingsproces	**GDPR** artikel 5, stk. 2
			ISO/IEC 27001:2013 A.14.1.1, A.14.2.1, A.14.2.3, A.14.2.5
			ISO/IEC 27701:2019 pkt. 6.11.1.1, pkt. 6.11.2.1, pkt. 6.11.2.3, pkt. 6.11.2.5,
			NIST CSF PR.IP-1, PR.IP-2, PR.IP-3, PR.IP-12

Kilde: https://d-maerket.dk

Niveau 3 kriterier: virksomhedstype I (minimum)

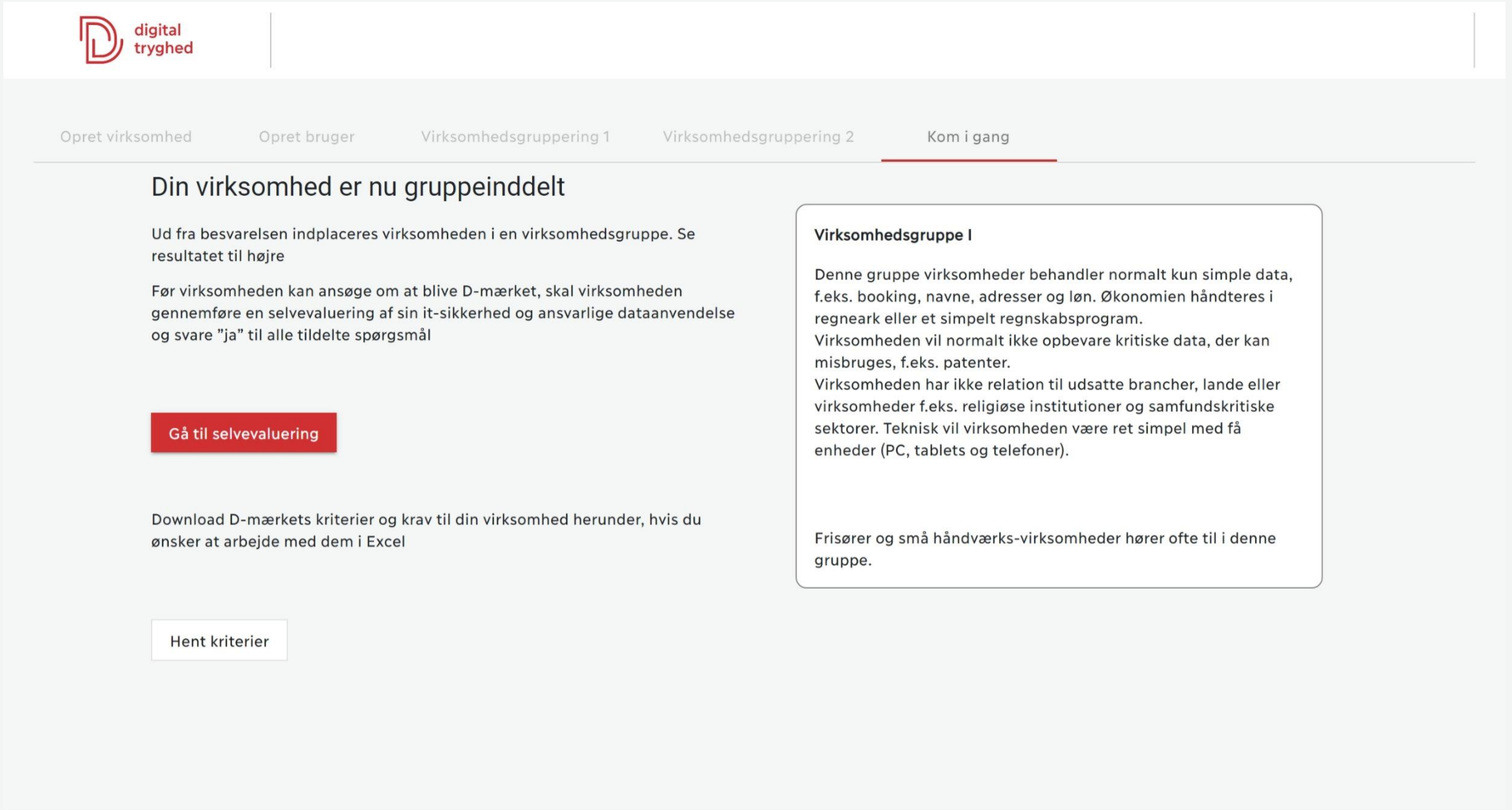
Kriterie: niveau 1		Kriterie: niveau 3	
1	Styring og forankring i ledelsen	1.1.1 1.2.1 1.2.2 1.2.3 1.3.1 1.5.1	Udpegning af ansvarlig person for it-sikkerhed og ansvarlig dataanvendelse Overblik over personoplysninger Overblik over forretningskritiske data Overblik over it-systemer, tjenester, netværkskomponenter, enheder, software og aktivitetsbaserede algoritme/AI ”use cases” Risikovurdering og –håndtering It-beredskabsplan
2	Awareness og sikker adfærd	2.2.1 2.3.1	Træn alle ansattes og brugers viden om it-sikkerhed kontinuerligt Træn alle ansatte og brugeres viden om ansvarlig behandling af personoplysninger kontinuerligt
3	Teknisk it-sikkerhed	3.3.1 3.4.1 3.4.2 3.5.1 3.6.1	Beskyttelse af administrative brugerkonti Implementering af beskyttelsesmekanismer mod malware Beskyttelse mod uønskede e-mails Kontinuerlig opdatering af software og styresystemer Procedure for automatisk og jævnlig backup
4	Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse		Afhænger af scope
5	Transparens og kontrol med data	5.1.1 5.1.2 5.2.1 5.4.1	Oplysningspligt overfor den registrerede Information om samarbejdspartnere der deles data med Cookie-information og -brugervenlighed Lettilgængelig klagevejledning vedrørende ansvarlig dataanvendelse og it-sikkerhed
6	Privacy & security by design & default		Afhænger af scope
7	Pålidelige algoritmer & AI		Afhænger af scope
8	Dataetik		Afhænger af scope

Proces for virksomheder

1. **Anmodning**
2. **Inplacering og kriterier**
3. **Selvevaluering**
4. **Ansøgning og betaling**
5. **Tilsyn og kontrol**
6. **Tildeling af D-mærke**

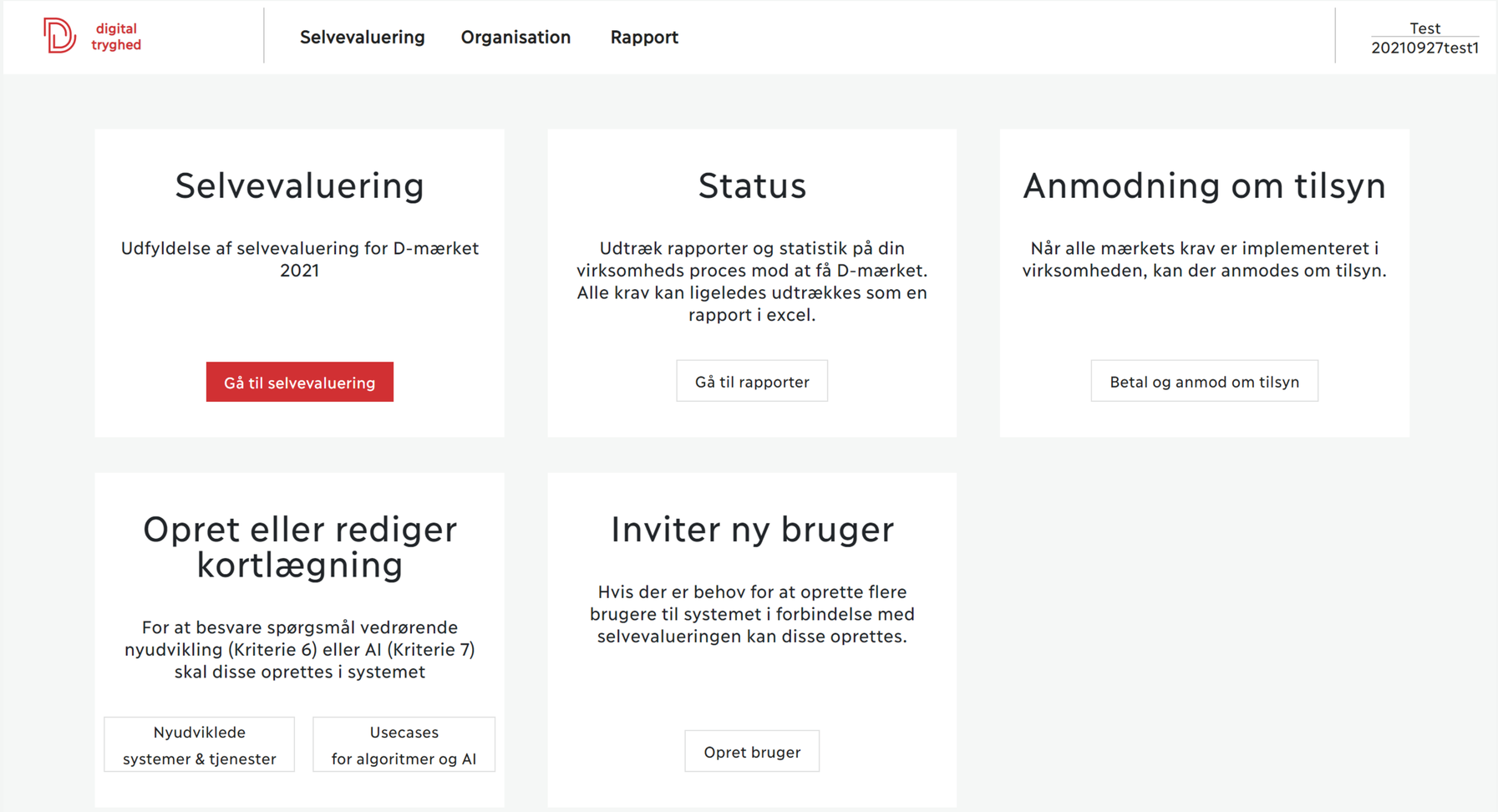
Kilde: https://d-maerket.dk/proces/

D-mærkets selvevalueringsværktøj



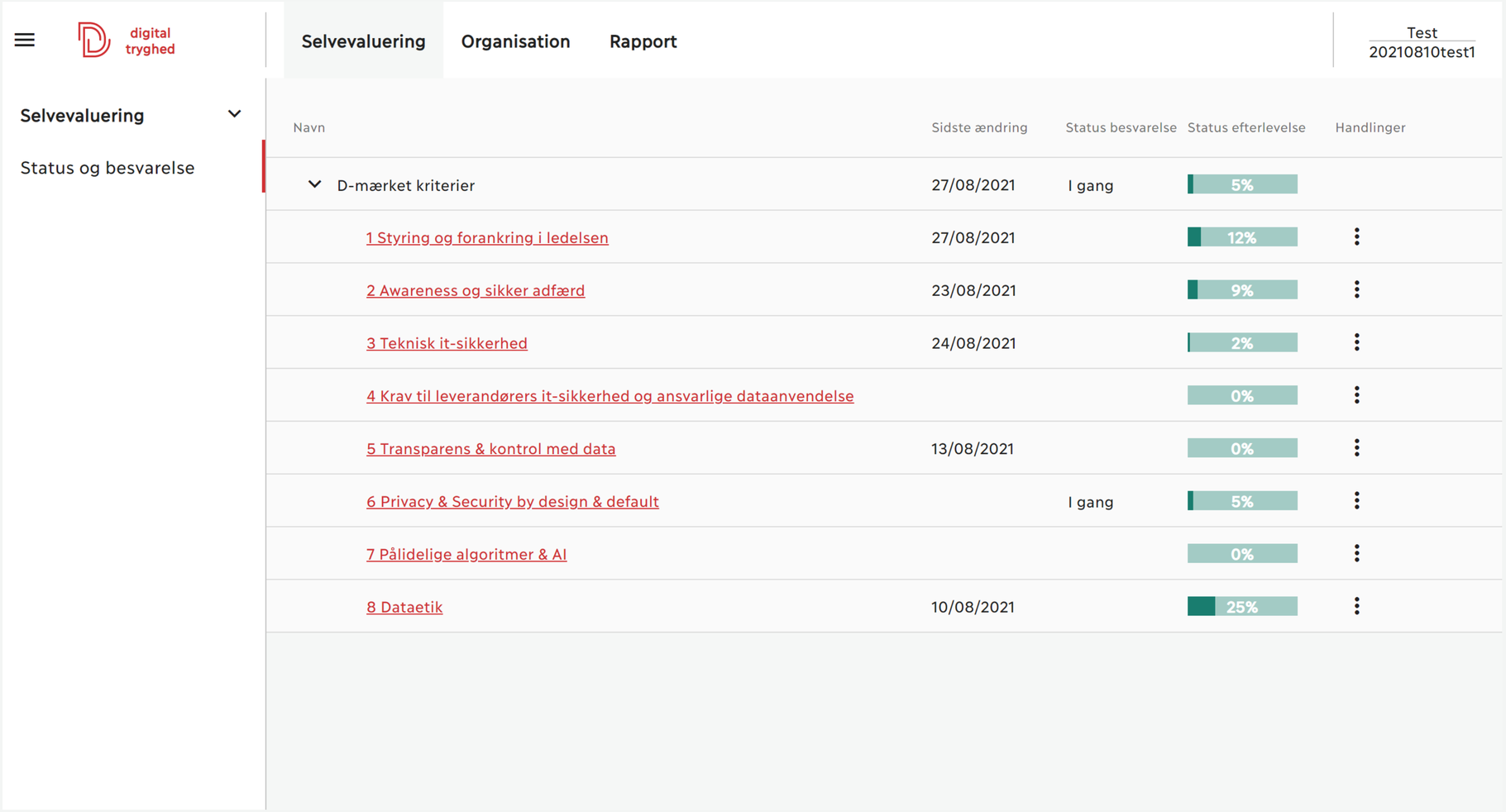
Kilde: https://digital.d-maerket.dk/

D-mærkets selvevalueringsværktøj



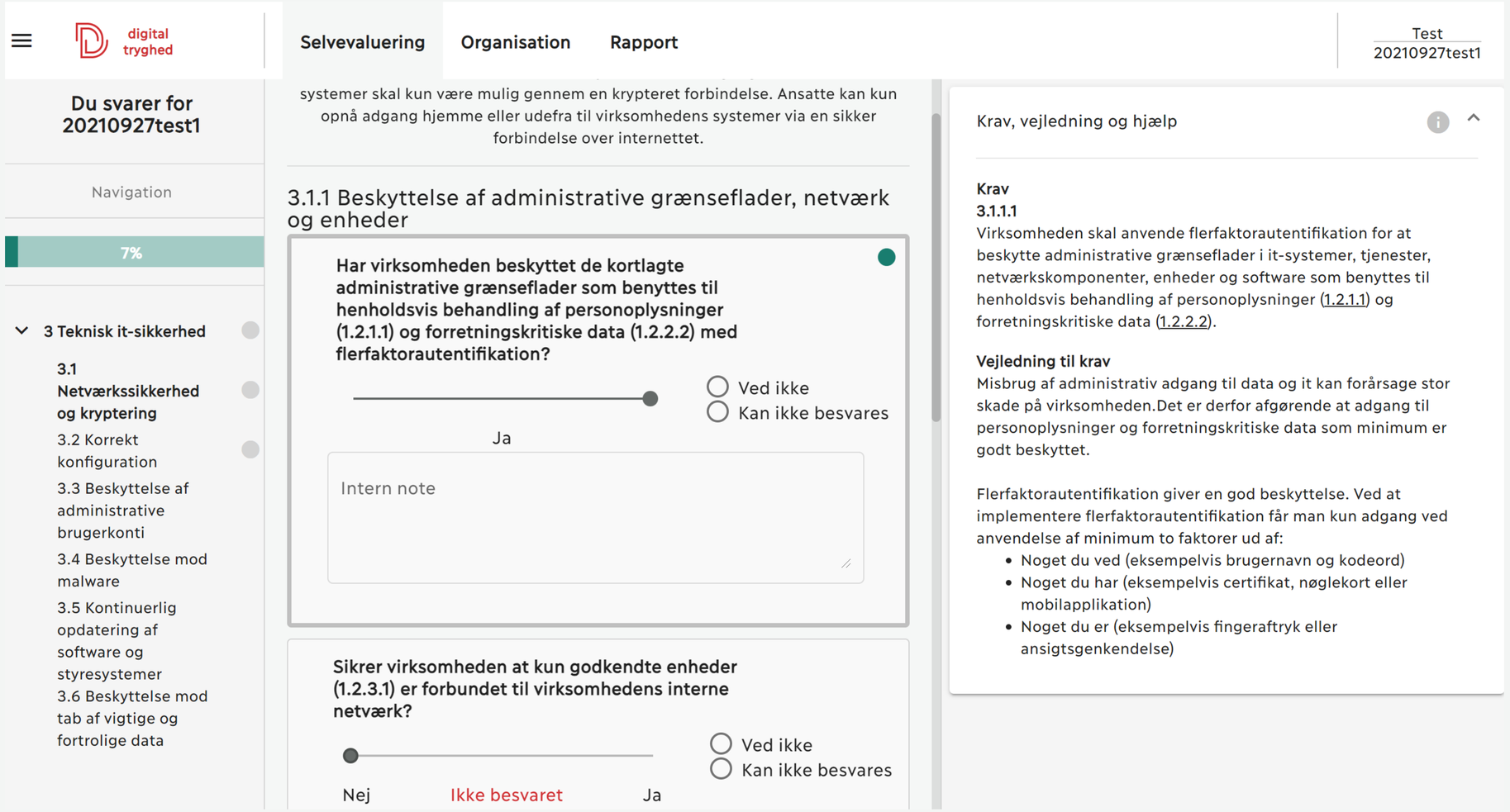
Kilde: https://digital.d-maerket.dk/

D-mærkets selvevalueringsværktøj



Kilde: https://digital.d-maerket.dk/

D-mærkets selvevalueringsværktøj



Kilde: https://digital.d-maerket.dk/

Prismodel

	Gruppe I	Gruppe II	Gruppe III	Gruppe IV	Gruppe IV+
	0-9 ansatte	10-49 ansatte	50-249 ansatte	250-999 ansatte	>1000 ansatte
Pris for tilsyn	**DKK 2.800**	**DKK 8.400**	**DKK 21.000**	**DKK 52.250**	**Afhænger af størrelse**

Undtagelser	**Max pris**	**Rabat**
Hvis under 10 ansatte, men tilhører virksomhedsgruppe III	DKK 8.400	-60%
Under 50 ansatte, men tilhører virksomhedsgruppe III	DKK 12.600	-40%

Kilde: https://d-maerket.dk/priser/

Hvordan skaber D-mærket forretningsværdi?

- Det er hurtigt at komme i gang - og selvevaluering er gratis
- Virksomheden betaler først, når og hvis tilsyns-og kontrolprocessen igangsættes
- Kravene er tilpasset til virksomheden - og er til at forstå
- D-mærket kommer hele vejen rundt om virksomheden
- Virksomheden bestemmer selv farten - og kan få vejledning undervejs
- Godt sted at starte, hvis virksomheden på sigt vil fx ISO/IEC 27001 og ISO/IEC 27701 certificeres
- D-mærket er fremtidssikret – da mærket indeholder krav til PbD/SbD, algoritmer/AI og dataetik
- D-mærket er starten på en digital ansvarlig modenhedsrejse – og virksomheden kan skilte med det

Se D-mærkets lanceringsevent

Onsdag d. 22. sep. 2021

Lanceringsevent hos Digital Hub Denmark, foto af Sebastian Stigsby

Se eller gense D-mærkets lancering d. 22. september 2021. Eftermiddagen bød på oplæg og ekspertpanel, interviews med virksomheder som har testet mærket og ikke mindst officiel lancering.

Kilde: https://d-maerket.dk/events-og-artikler/verdens-forste-maerke-for-digital-ansvarlighed-er-klar-til-brug/

digital tryghed

www.d-mærket.dk

D-mærket/D-seal

@Dmaerket

DANSK ERHVERV

DI

SMVdanmark

Forbrugerrådet Tænk

INDUSTRIENS FOND

H. C. Andersens Boulevard 18, 1553 København V • Telefon: +45 33 77 33 77 • kontakt@d-maerket.dk