Ny guide for risikostyring i forhold til cyber- og informationssikkerhed til SMV'er

Hvem står bag guiden?

cyber hub × DigitalLead.

INDUSTRIENS FOND

ERHVERVSSTYRELSEN

ALEXANDRA INSTITUTTET

DS DANSK STANDARD

Hvorfor er der behov for en guide om risikostyring?

ERHVERVSSTYRELSEN

"…40 pct. af SMV'erne har et for lavt digitalt sikkerhedsniveau i forhold til deres risikoprofil. Desuden anvender ca. hver fjerde SMV fortsat ikke de to mest basale sikkerhedsforanstaltninger; opdatering af styresystemer og backup af data."
(Digital sikkerhed i danske SMV'er 2021)

Hackerangreb har kostet Demant over en halv milliard kroner

(Illustration: Demant)

Hackerangrebet har haft store økonomiske konsekvenser for virksomheden, der efterhånden har fået alle systemer og servere op at køre.

Roskilde Teltudlejning

ABENA

bahne

Hvorfor er der behov for en guide om risikostyring?

If everything is connected, everything can be hacked. Given that resources are scarce, we have to bundle our forces.

And we should not just be satisfied to address the cyber threat, but also strive to **become a leader in cyber security**. It should be here in Europe where cyber defence tools are developed.

-Ursula von Der Leyen
State of the Union, 2021

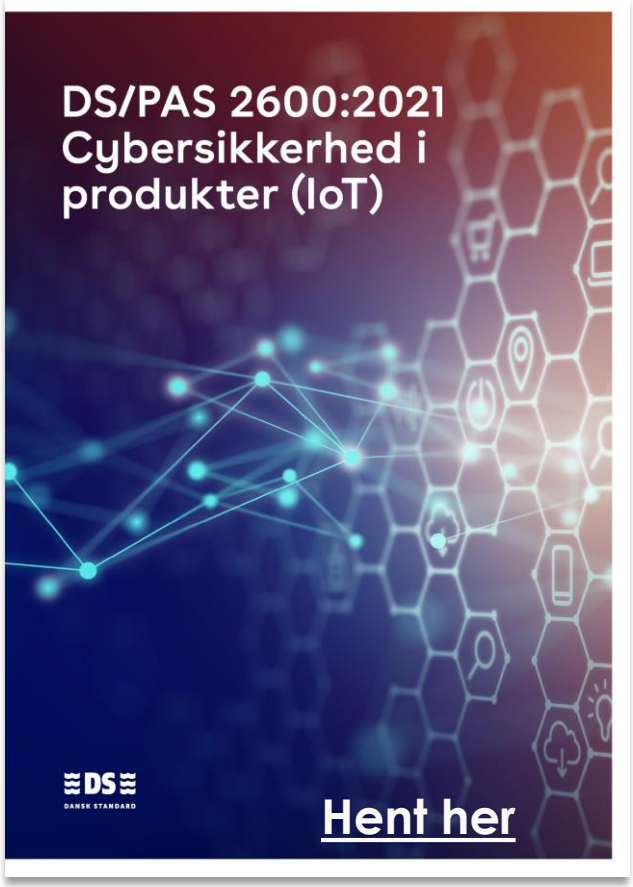
NIS 2
Cyberresilience Act
Cyber Security Act

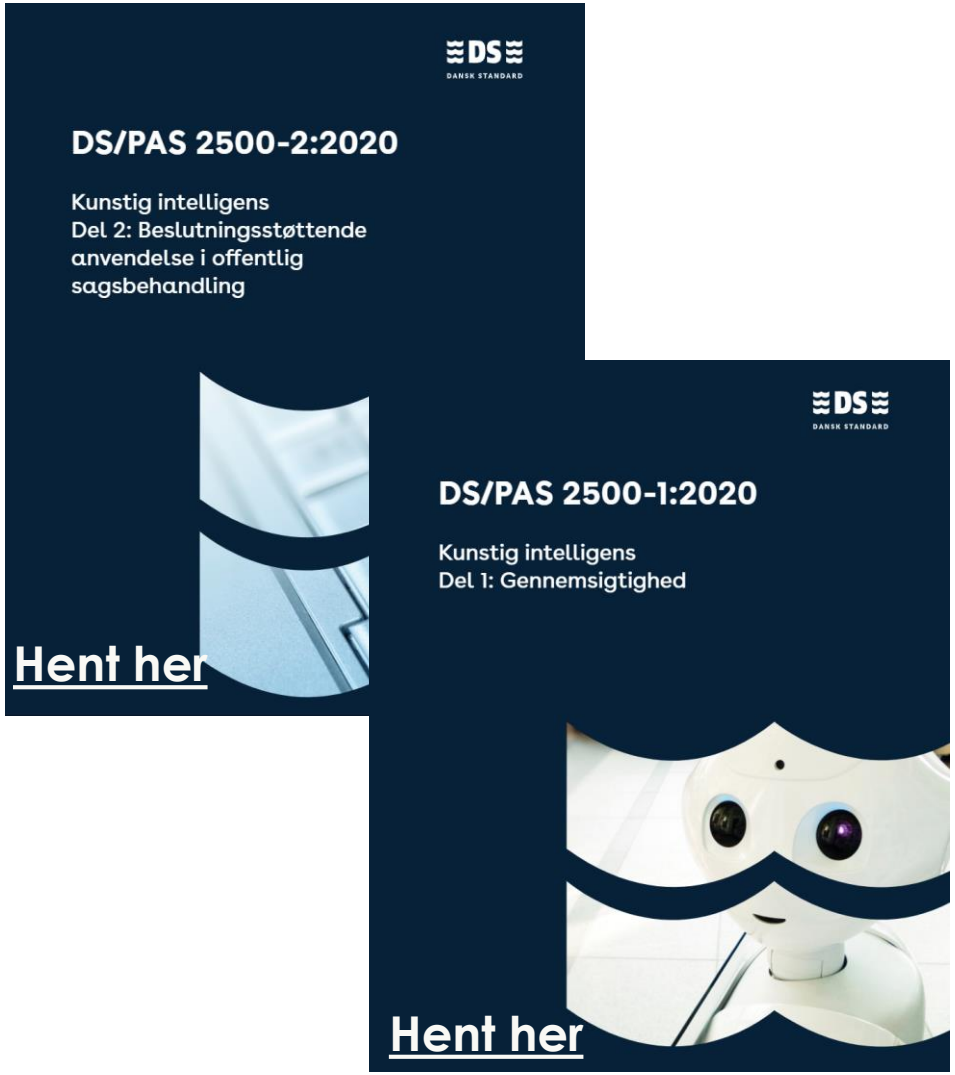
Guiden kort fortalt

- En guide til danske SMV'er, der skal tjene som inspiration til at arbejde med risikostyring i forhold til cyber- og informationssikkerhed
- Guiden bygger på standarden ISO/IEC 27005, men trækker også på andre værktøjer
- Guiden gennemgår risikostyring trin-for-trin i et letforståeligt sprog suppleret med konkrete eksempler og gode råd.
- Guiden udvikles i samspil med fageksperter

Udgives i februar 2023 og er gratis

Dansk Standard har gode erfaringer med at udvikle danske guides





Berit Aadal
Dansk Standard
baa@ds.dk

ANVENDELSESGUIDE FOR RISIKOSTYRING

Michael Stausholm, Senior Security Architect

Sammen kommer vi #forandigitalt

ALEXANDRA INSTITUTTET

Standarder og værktøjer

- ISO/IEC 27005
- OCTAVE Allegro
- NIST SP 800-3x serien
- I mindre grad:
  - STRIDE/DREAD
  - OWASP Risk Rating Methodology

DS/ISO/IEC 27005:2018 / 2023

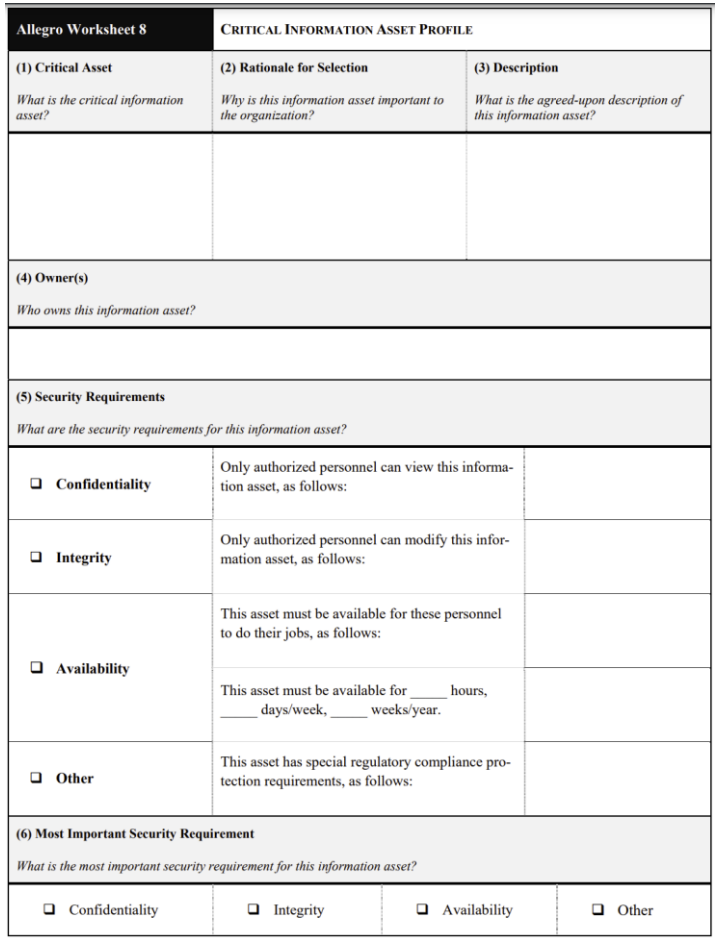
- Vejledende standard i risikoledelse
- Vejleder i de forskellige trin i en risikostyringsproces
- Tiltænkt som støtte til kravstandarden DS/ISO/IEC 27001
- Er under revidering – bedre allignet med 27001 og 27002

Risikostyringsprocessen, jf. ISO/IEC 27005

DANSK STANDARD

OCTAVE Allegro

- Omfattende rammeværk til risiko*vurdering*
- Målrettet større virksomheder
- Indeholder worksheets som gør rammeværket konkret



Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
(4) Owner(s) *Who owns this information asset?*		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
❑ Confidentiality	❑ Integrity	❑ Availability ❑ Other

NIST SP 800-3x serien

- Den Amerikanske udgave ISO 27000-serien
  - SP 800-30 er fokuseret på risiko*analyse*
  - SP 800-37 og 800-39 dækker risiko*styring* (i forskellig grad)
- Meget brugt af myndighederne i USA

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

STRIDE / DREAD

- Fokuseret på trusler og ikke risiko
- STRIDE er kategorier af angreb
- DREAD kan bruges til vurdering af trusler
- Forholdsvis kendte akronymer (af teknikkere)
  - Men ikke særligt formelle

Threats	Spoofing Identity	Tampering with data	Repudiation	Information Disclosure	Denial Of Service	Elevation of Privilege
Threat 1	✓		✓	✓		✓
Threat 2		✓	✓			
Threat 3					✓	
Threat 4	✓		✓	✓		
Threat 5	✓		✓	✓		✓

Threats	D	R	E	A	D	Total	Rating
Threat 1	2	3	3	2	3	13	High
Threat 2	2	3	3	2	2	12	High
Threat 3	1	1	1	3	1	7	Low
Threat 4	2	2	2	2	3	11	Medium
Threat 5	2	3	2	3	3	13	High

OWASP Risk Rating Methodology

- Uformel tilgang til risiko*analyse*
- Simpel måde at beregne sandsynlighed og konsekvens
- Målrettet teknikkere og tager mindre højde for forretningen

Eksempler: Virksomhedstyper

- Hvor digitaliseret er virksomheden?
  - Digitale produkter vs. IT som støttefunktion
- Følsomhed af data
  - GDPR/Sundhedsdata vs. “nice to have”
- Kundesegment/leverandør ansvar
  - Almindelige forbrugere vs. særlige krav (luftfart, forsvar, osv.)

Eksempler: Eksempel virksomheder

- Traditionel virksomhed - Autoværksted
  - IT er primært støtte funktioner (f.eks. ordrehåndtering og bogholderi)
- Meget digitaliseret virksomhed – Vin import
  - IT er kritisk for forretningen (alt kører gennem webshop)
- Større / specialiseret virksomhed - Overvågningssystemer
  - Større krav omkring formalitet og dokumentation

Eksempler: Detaljegrad

Virksomhed B identificerede en risiko omkring manglende kompetencer i forbindelse med IT nedbrud (f.eks. i tilfælde af et ransomware angreb). Selvom virksomheden råder over en kompetent IT-afdeling, er det IT-chefens vurdering at virksomheden ikke har ressourcerne til hurtigt at få gendannet systemerne. Virksomhed B beslutter derfor at tegne en forsikring, der kan hjælpe med ressourcer i tilfælde af et nedbrud og samtidigt dækker noget af det driftstab der forekommer i forbindelse med evt. nedbrud.

TAK
FOR NU

Michael Stausholm · michael.stausholm@alexandra.dk · 20296322

Sammen kommer vi #foran**digitalt**

ALEXANDRA INSTITUTTET