10. marts 2023

Guide til risikostyring

Risikostyring i forhold til cyber- og informationssikkerhed for smv'er

Dagens program

13:00 **Velkommen**

13:05 **Introduktion til guiden for risikostyring**

Michael Bladt Stausholm, Alexandra Instituttet
Berit Aadal, Dansk Standard

13:30 **Værdien af at arbejde risikobaseret i forhold til cyber- og informationssikkerhed**

Anne Dorte Bach, Magenta

13:45 **Spørgsmål og afrunding**

13:55 **Tak for i dag**

Om Dansk Standard

Hvem er Dansk Standard

- Danmarks officielle standardiseringsorganisation
- Erhvervsdrivende fond, grundlagt i 1926
- Ca. 170 medarbejdere
- Erhvervspolitisk partnerskab med Erhvervsministeriet

Vi er medlem af:

En stærk platform af solide brands:

RISIKOSTYRING

MICHAEL STAUSHOLM

PRINCIPAL SECURITY ARCHITECT

Sammen kommer vi #foran**digitalt**

ALEXANDRA INSTITUTTET

Kom foran digitalt

IOT OG SMARTE PRODUKTER

DIGITAL GRØN OMSTILLING

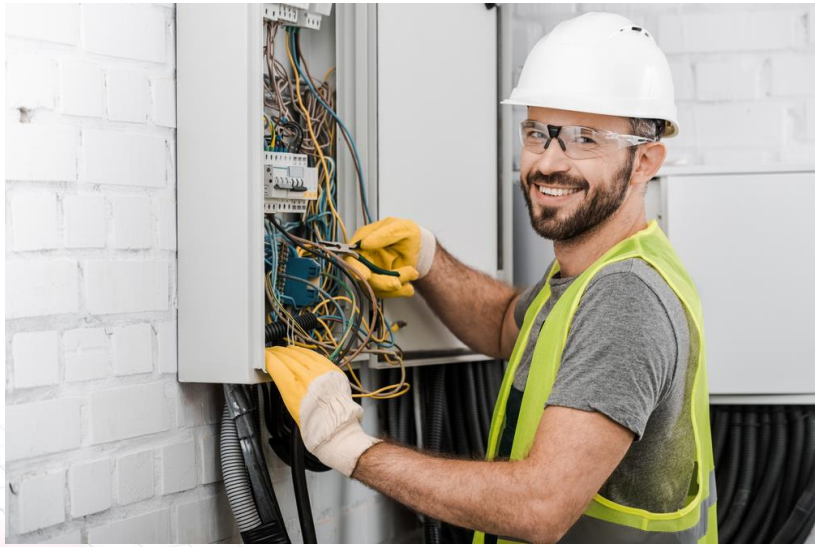
CYBERSIKKERHED

KUNSTIG INTELLIGENS

DIGITAL SUNDHED

COMPUTERGRAFIK, VISION OG SIMULERING

Alle laver risikostyring



Hvorfor risikostyring?

- “Perfekt” cybersikkerhed findes ikke

”

Vi har dygtige ansatte, så selvfølgeligt er vores systemer sikre…

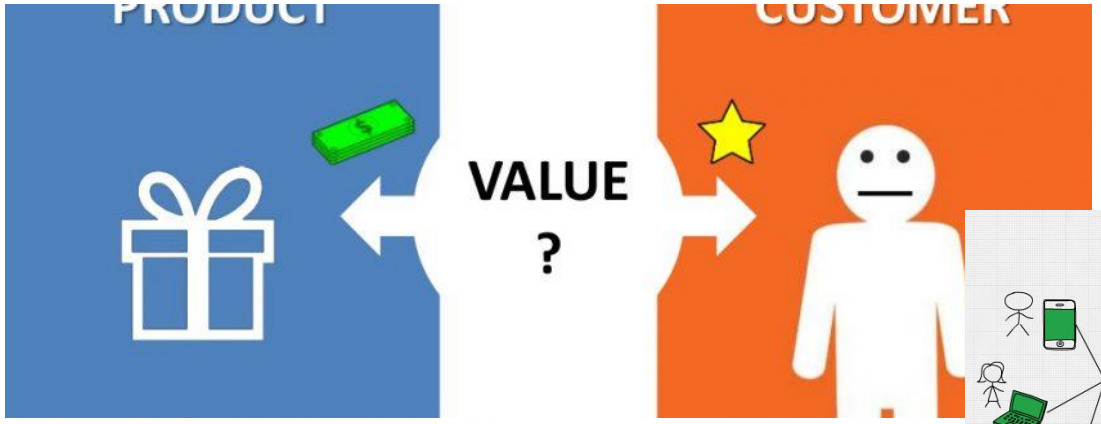
“Vi ved godt der er problemer med X, Y og Z. Vi skal også I gang med W, men har ikke haft tid endnu.”

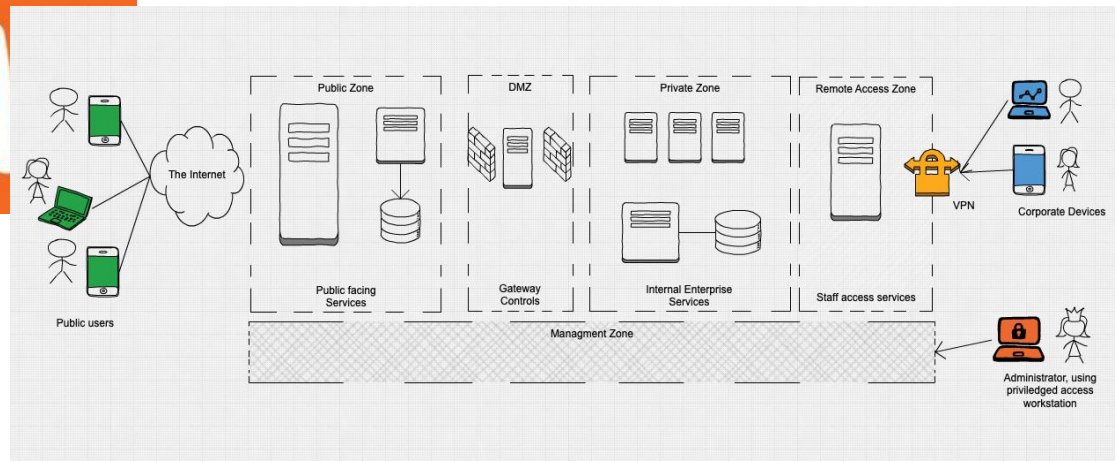
Hvordan ser processen ud?

- Hvad handler sikkerhed om for virksomheden?
  - Er der særlige hensyn?

Hvordan ser processen ud?

- Undersøg virksomheden og systemerne
  - Hvad er vigtigt og skaber værdi? Hvad er mindre vigtigt?
  - Hvordan kan det påvirkes?



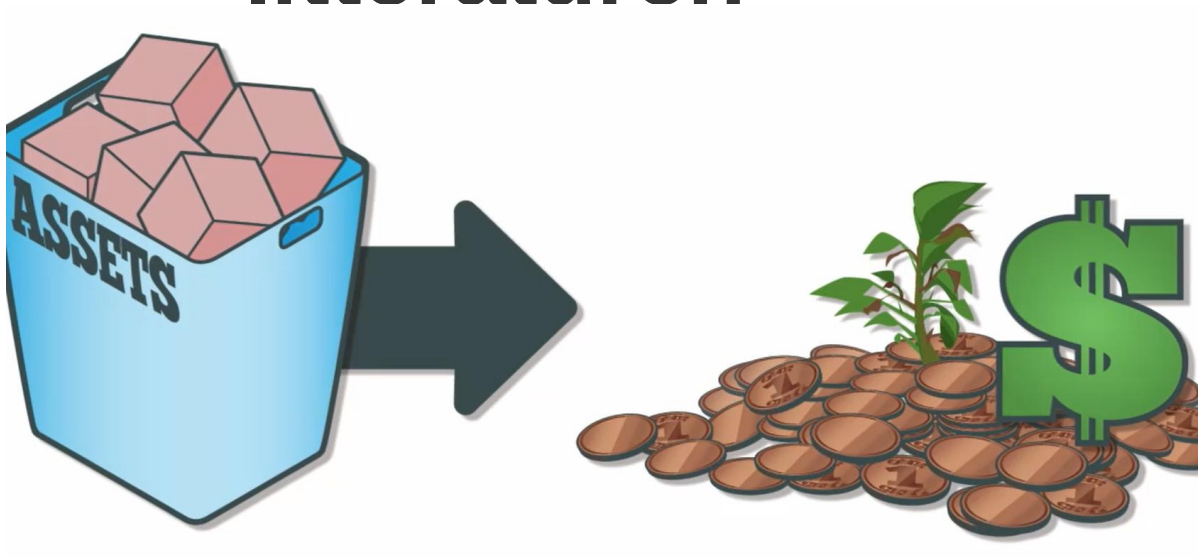


Hvordan ser processen ud?

- Hvad skal forbedres og hvordan?

Udfordringer vi ser i praksis?

Der kan være mange (nye) tekniske begreber i litteraturen



Spoofing	Authentication
Tampering	Integrity
Repudiation	Auditability
Information Disclosure	Confidentiality
DoS	Availability
Elevation of Privilege	Authorization

Udfordringer vi ser i praksis?

Trusselskataloger(!)

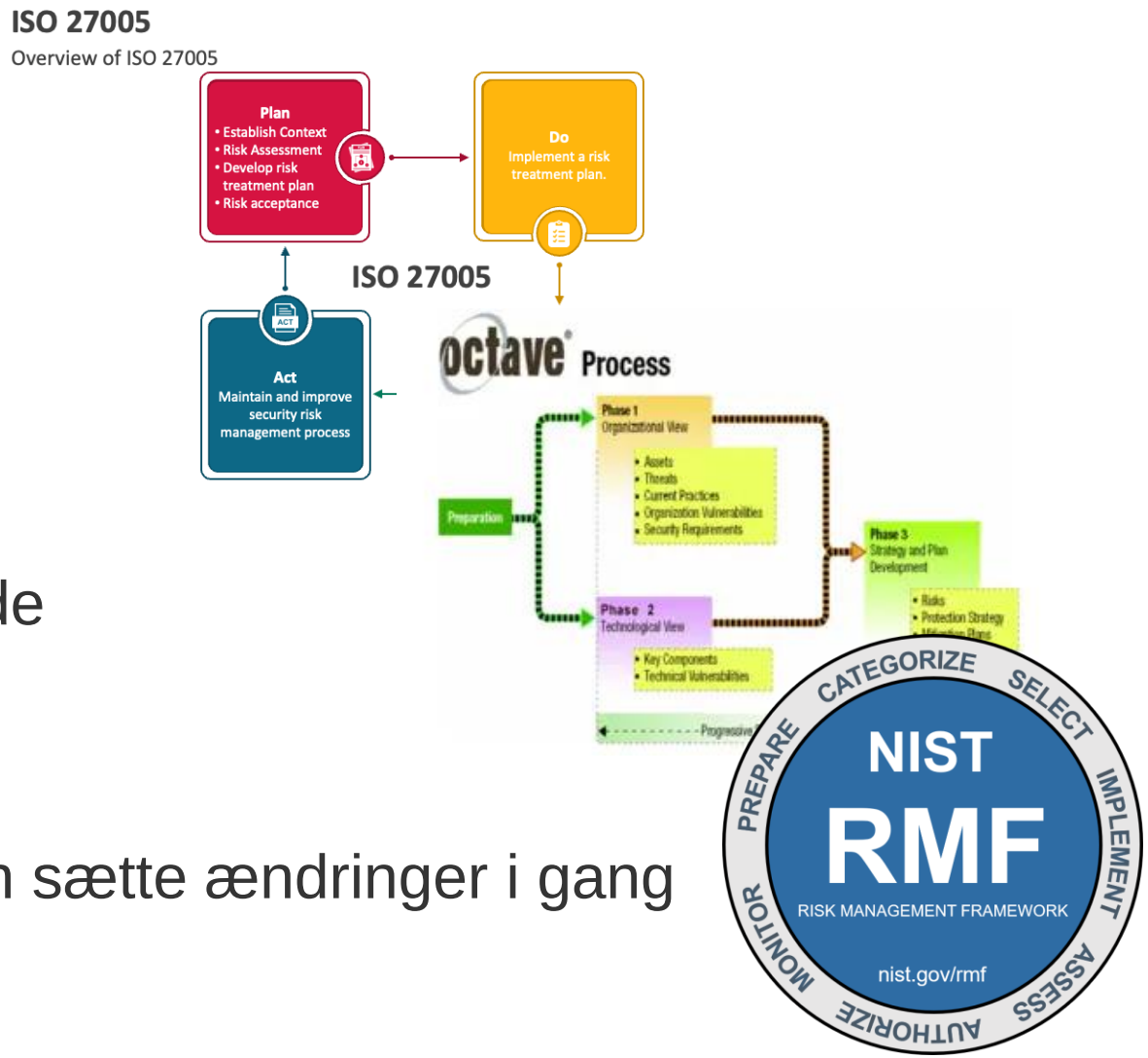
Sub-Category	ID	Threat	Description
			Struggle resulting from incompatible or opposing needs, drives, wishes, or e:
Conflict	LIC1	Sabotage	Deliberate actions aimed to cause disruption or damage to information and,
	LIC2	Terrorism	The use of violence as a means to create terror among masses of people; or religious, or ideological aim.
	LIC3	Vandalism	Deliberate destruction or damage to information and/or IT assets, but not f
	LIC4	Warfare	Damage to assets, facilities, and employees due to war or armed conflict.
Misappropriation			Dishonestly or unfairly taking for one's own use.
	LIM1	Embezzlement	To appropriate something, such as property entrusted to one's care, fraudul through fraud.
	LIM2	Extortion	The act of obtaining money, property, or services from an organization thro of force or intimidation to obtain compliance.
	LIM3	Fraud	Deliberate deception to secure unfair or unlawful gain, or to deprive a victin
	LIM4	Theft	The act of logically stealing and/or removing property with intent to deprive
			Flagrant breaching of time-honored laws and traditions of conduct.
	LIN1	Abuse of Authorizations	Using authorized access to perform illegitimate actions.
	LIN2	Address Space Hijacking	The illegitimate takeover of groups of IP addresses.
	LIN3	Alteration of Software	Unauthorized modifications to code or configuration data, attacking its inte
	LIN4	Anonymous Proxies	Access of websites through chains of HTTP proxies (obfuscation), bypassing t
	LIN5	Autonomous System Hijacking	Overtaking, by the attacker, the ownership of a whole autonomous system a
	LIN6	Brute Force	Unauthorized access via systematically checking all possible keys or passwor
	LIN7	Code Injections	Exploiting a bugs, design flaws, or configuration oversights in an operating s elevated access to resources.
	LIN8	Command Injection	Execution of arbitrary commands on the host operating system via a vulnera Code Injection, in that code injection allows the attacker to add his own cod application. In Command Injection, the attacker extends the default functio system commands, without the necessity of injecting code. Also know as "Re

Name	Type	Description
WEP Shared Key Cracking	AA	802.11 shared key authentication with a cracked shared key or default WEP keys.
WPA-PSK Cracking	AA	Recovering a WPA PSK from captured key handshake frames using dictionary attack tools.
Application Login Theft	AA	Capturing application layer credential information such as email account and password by capturing clear text transmissions.
AP Theft	DoS	Physically removing an AP from a public space.
RF Jamming	DoS	Transmitting noise at the same frequency as the target WLAN.

- Threat Catalog
  - TC.1: Spoofing
  - TC.1a: Identity spoofing when logging in (with a password)
  - TC.1b: Resource Location Spoofing
  - TC.2: Tampering
  - TC.2a: Exploitation of software weaknesses
  - TC.3: Repudiation
  - TC.4: Information Disclosure
  - TC.4a: Interception
  - TC.4b: Data extraction
  - TC.4b1: Firmware extraction
  - TC.4c: Reverse Engineering
  - TC.5: Denial of Service
  - TC.5a: Flooding
  - TC.5b: Jamming
  - TC.5c: Excessive Allocation of Resources
  - TC.6: Elevation of privilege
  - TC.6a: Man-in-the-Middle Attack

Næste trin?

- Gør jer nogle erfaringer
  - Start småt og uformelt…
  - … og begynd derefter at formalisere
- Standarder og frameworks er gode
  - De skal tilpasses virksomheden
- Selv en uformel gennemgang kan sætte ændringer i gang

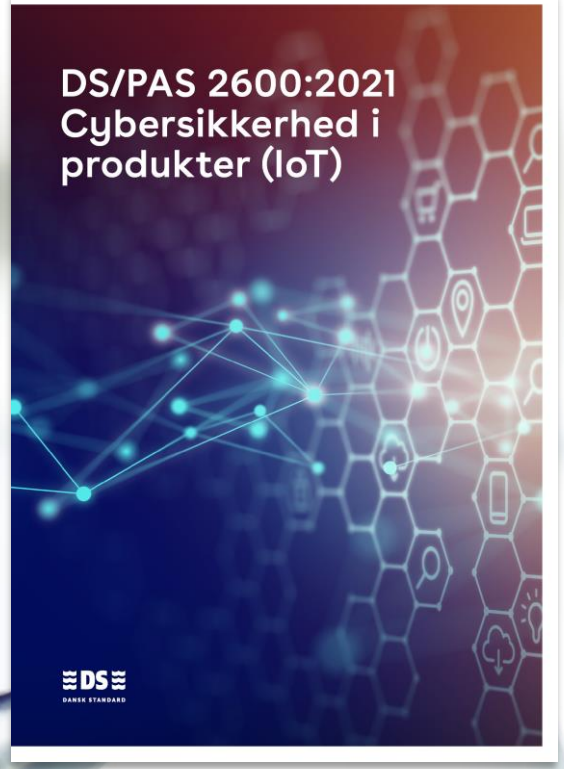


Guide til risikostyring

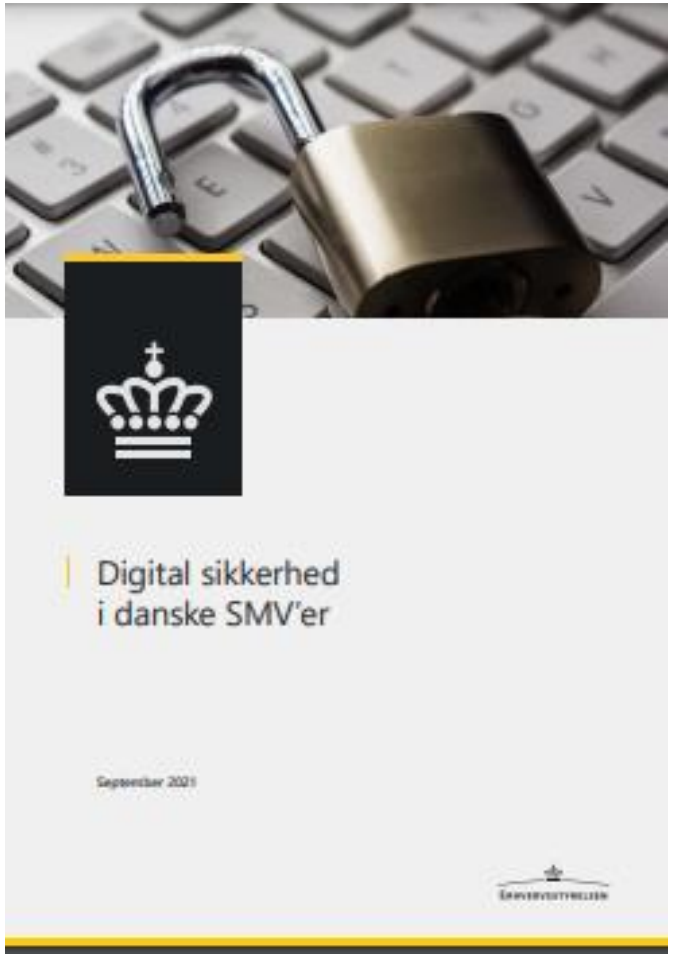
Risikostyring i forhold til cyber- og informationssikkerhed for smv'er

Alexandra Instituttet
Dansk Standard

Dansk Standard har gode erfaringer med at udvikle guides, der skal hjælpe virksomheder med at forstå og arbejde med standarder



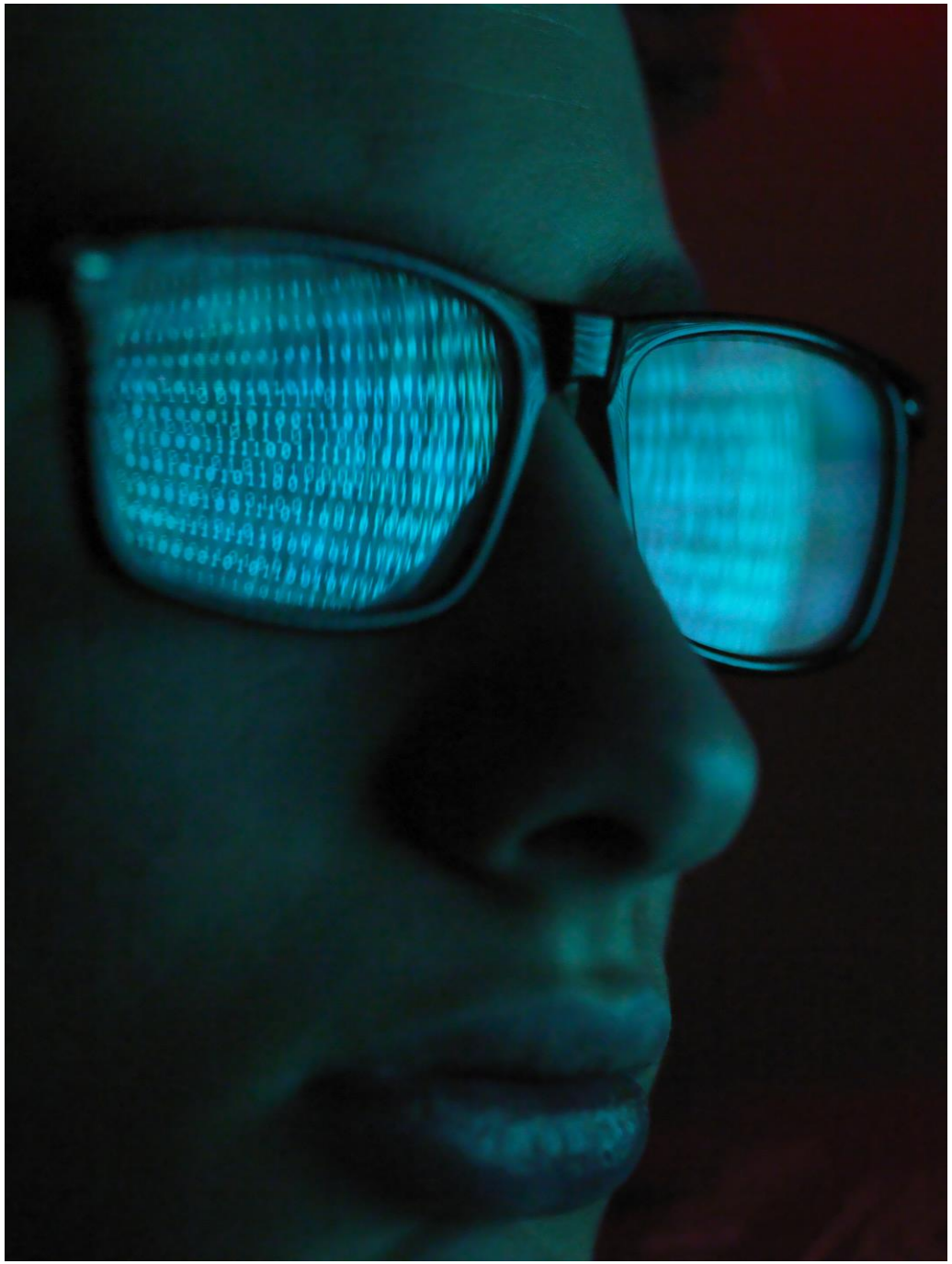
Hvorfor er informationssikkerhed særligt relevant for SMV'er?



40% af de danske smv'er har et for lavt digitalt sikkerhedsniveau i forhold til deres risikoprofil

24% af de danske smv'er opdaterer ikke deres styresystemer eller har backup af data

Kilde: https://erhvervsstyrelsen.dk/digital-sikkerhed-i-danske-smver-2021



Cybertruslen mod Danmark

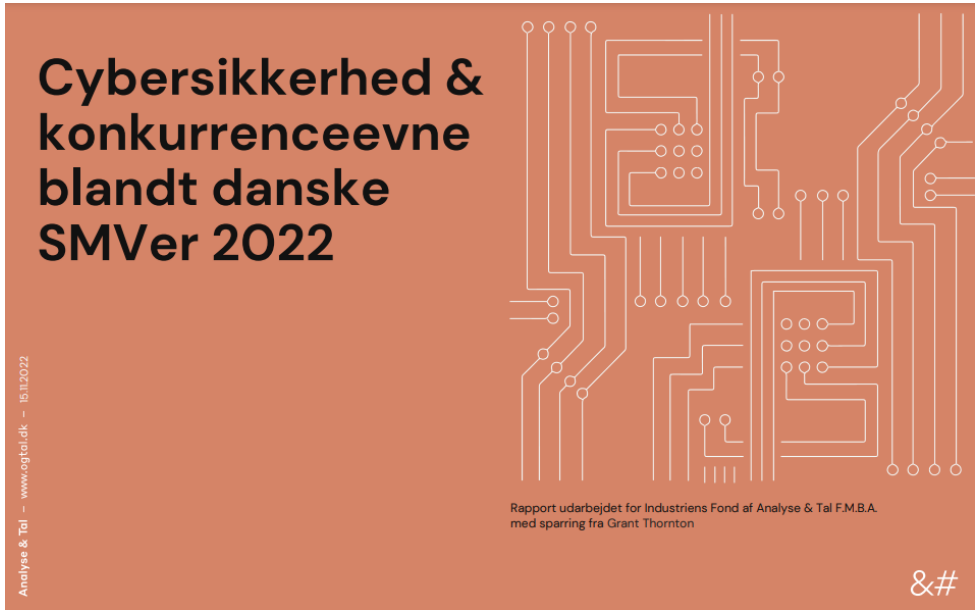
- Truslen fra cyberspionage er **MEGET HØJ**
- Truslen fra cyberkriminalitet er **MEGET HØJ**
- Truslen fra cyberaktivisme er **HØJ**
- Truslen fra destruktive cyberangreb er **LAV**
- Truslen fra cyberterror er **INGEN**

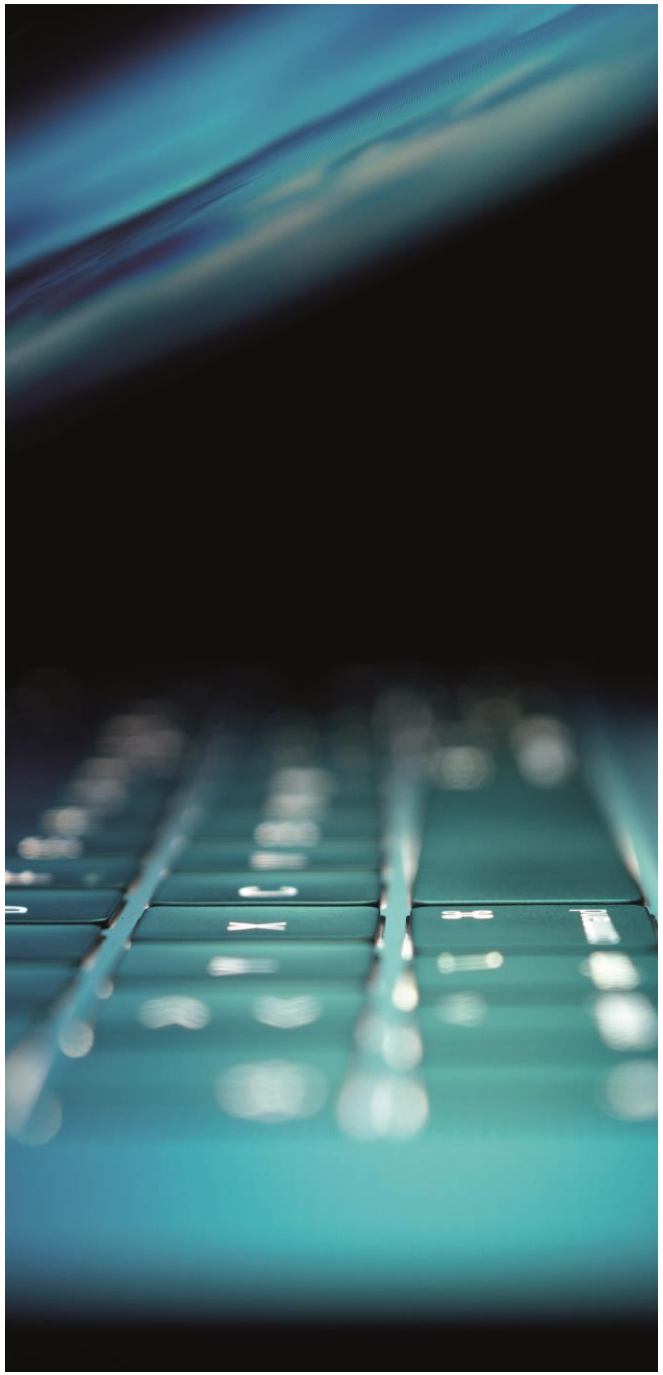
Kilde: CFCS trusselsvurdering februar 2023

Cybersikkerhedstiltag skaber konkurrencefordele for virksomhederne

To af hovedindsigterne fra ny dansk rapport viser at:

- Flere cybersikkerhedstiltag fører til flere konkurrencefordele
- Cybersikkerhed fører til konkurrencefordele i alle brancher





Koblingen til NIS2

Med NIS2 fastsættes der en række minimumskrav til foranstaltninger, der bl.a. indebærer at udarbejde politikker for **risiko**analyse og informationssikkerhed, håndtere hændelser og sikre driftskontinuitet.

"En risikostyringskultur, der indbefatter risikovurderinger og gennemførelse af foranstaltninger til styring af cybersikkerhedsrisici, som står i forhold til de foreliggende risici, bør fremmes og udvikles." (betragtning 77)

Guide for risikostyring i forhold til cyber- og informationssikkerhed

HVAD

Gode råd og redskaber til at arbejde konkret og systematisk med risikostyring i forhold til cyber- og informationssikkerhed.

HVORFOR

Hjælpe danske smv'er i gang med at arbejde med risikostyring og dermed ruste dem mod f.eks. cyberangreb og it-kriminalitet og samtidig bidrage til at styrke danske smv'ers konkurrencefordel.

HVEM

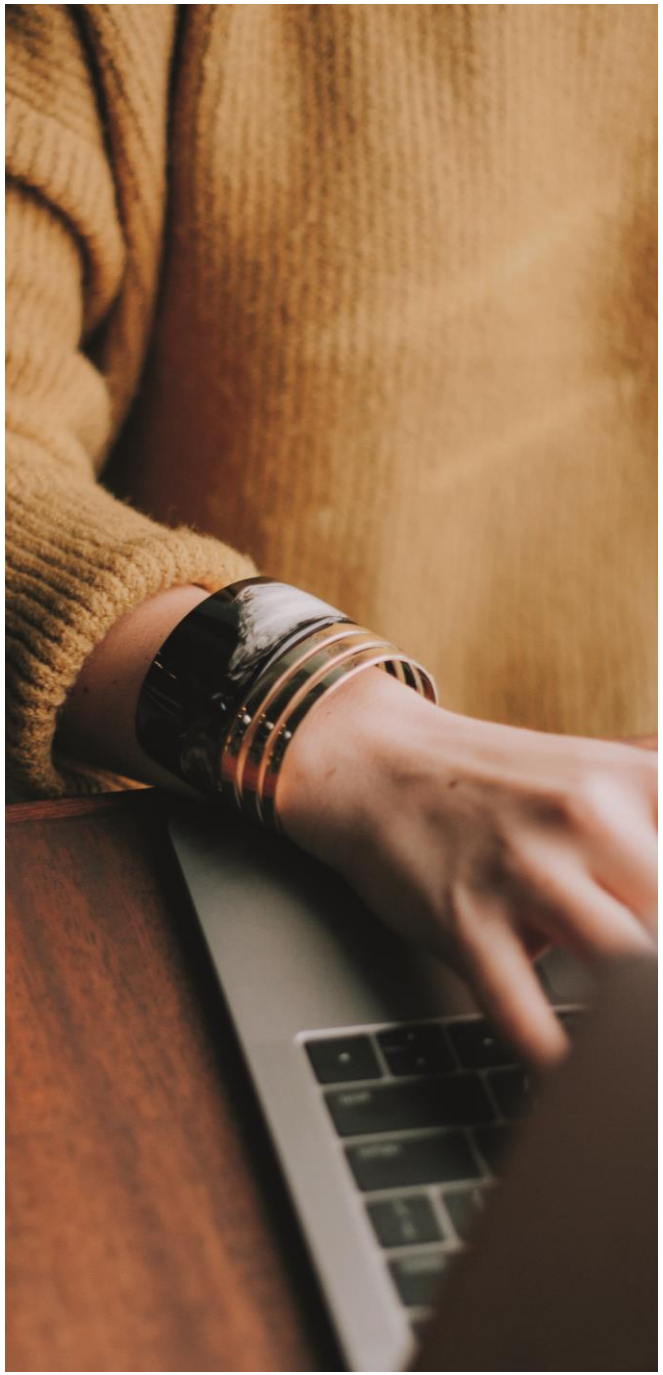
Danske smv'er der gerne vil i gang med risikostyring, men ikke nødvendigvis har den store forhåndsviden.

HVORDAN

Gennemgang af risikostyringsprocessen trin for trin suppleret med virksomhedseksempler.

Guiden er udarbejdet af ALEXANDRA INSTITUTTET og DS DANSK STANDARD

Guiden er støttet af cyber hub og ERHVERVSSTYRELSEN



Parametre der har indflydelse på risikostyringsprocessen

DANSK STANDARD

Digitalisering af virksomheden

Fortrolighed af data anvendt i virksomheden

Virksomhedens placering i leverandørhierarkiet

Antallet af brugere

Guiden benytter sig af tre virksomhedseksempler

VIRKSOMHED A
Autoværkstedet

Mindre autoværksted
Mindre grad af digitalisering. Ingen fortrolige/personfølsomme data. Har private kunder og forskellige leverandører af materialer. Dog ikke kunder med særlige krav. Relativt få brugere.

VIRKSOMHED B
Produktionsvirksomheden

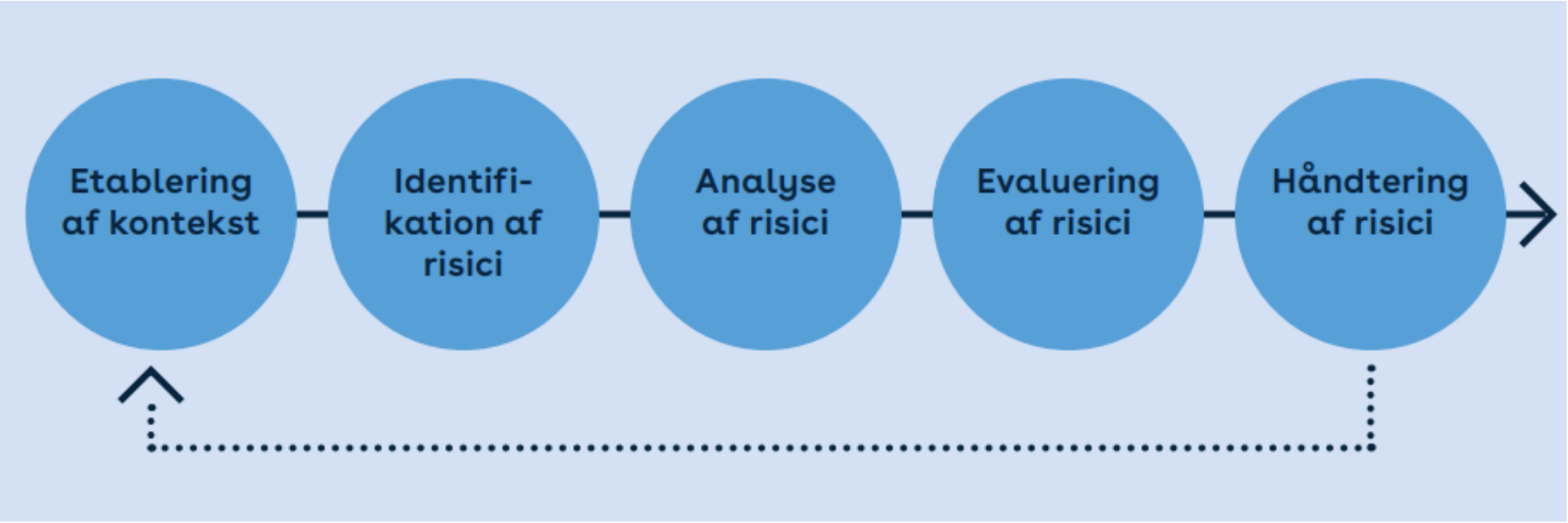
Mellemstor virksomhed
(omkring 85 ansatte), der producerer og installerer videoovervågningssystemer. Høj grad af digitalisering. Stor mængde fortrolige data. Stor snitflade med mange brugere; kunder, samarbejdspartnere, leverandører mm. Leverer til kritisk infrastruktur.

VIRKSOMHED C
Webshoppen

Lille virksomhed
(fire ansatte), der importerer vin. Høj grad af digitalisering (100 % webshop). Mange brugere af webshoppen. Nogen grad af fortrolige data. Benytter sig i høj grad af leverandører i forhold til IT-driften.

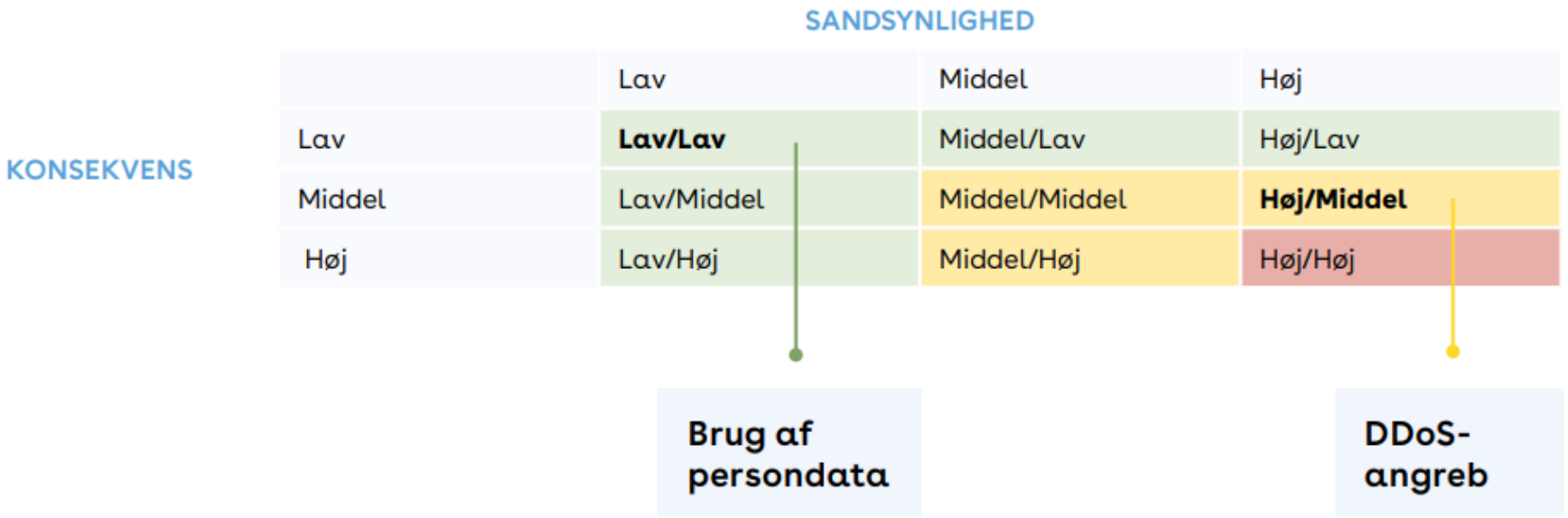
Figur fra guiden

Guiden gennemgår risikostyring trin for trin



Figur fra guiden

Få konkrete input til at arbejde med sandsynlighed og konsekvens



Eksempel fra guiden

Få konkrete input til at arbejde med sandsynlighed og konsekvens

SANDSYNLIGHED

KONSEKVENS

	10-års hændelse	Årligt	Kvartalsvist	Ugentligt	Dagligt
0-50.000 kr.	1	2	3	4	5
50.001-125.000 kr.	2	4	6	8	10
125.001-500.000 kr.	3	6	9	12	15
500.001-2.500.000 kr.	4	8	12	16	20
2.500.001+ kr.	5	**10**	15	**20**	25

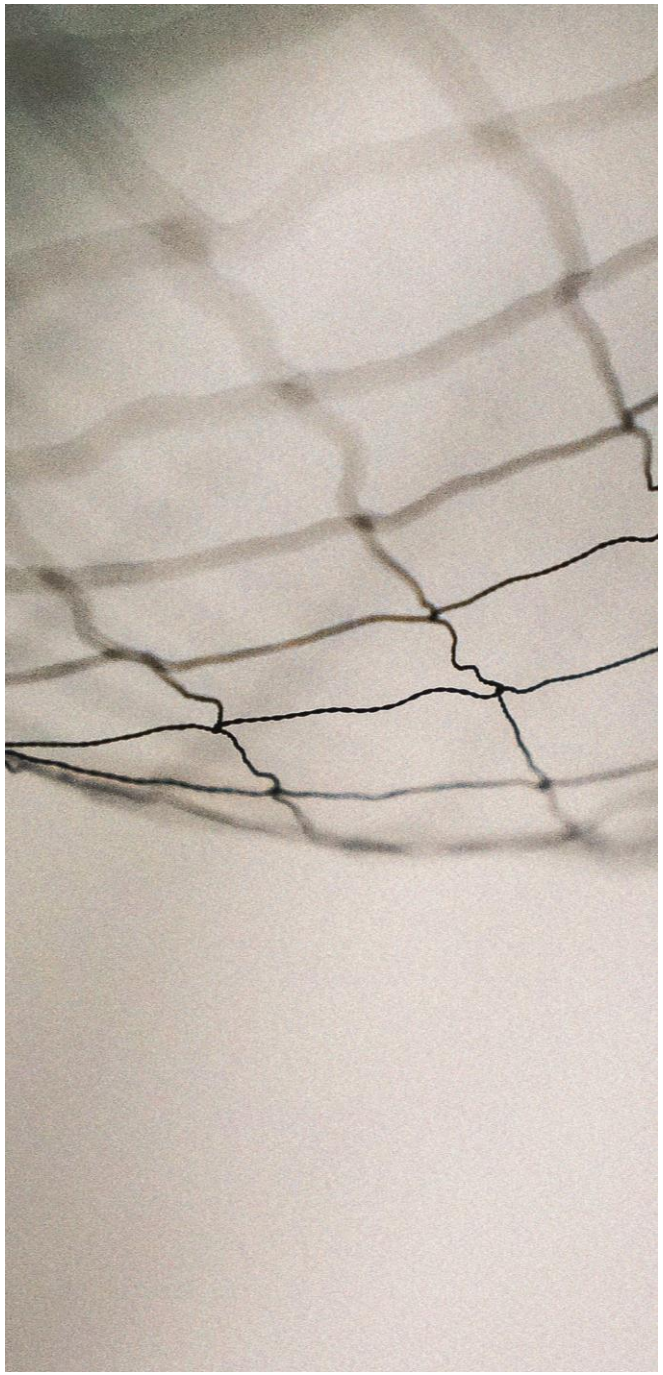
Manglende ekspertise ifm. et cyberangreb

Manglende validering af hvor data stammer fra

empel fra guiden

Guiden trækker på anerkendte standarder og rammeværk for risikostyring

- ISO/IEC 27005 Information security, cybersecurity and privacy protection – Guidance on managing information security risks
- ISO/IEC 29134 Information technology – Security techniques – Guideline for privacy impact assessment
- OCTAVE Allegro
- NIST SP 800-30, SP 800-37 og SP 800-39
- STRIDE/DREAD
- OWASP Risk Rating Methodology
- Erhvervsstyrelsens IT-risikovurderingsværktøj
- Erhvervsstyrelsens Sikkerhedstjek



Giver guiden værdi?

"Mange af de små virksomheder mangler måske nogle it-sikkerhedstiltag, som en specialist ville tænke er helt banale. Men der er bare mange andre ting, der fylder i hverdagen ude hos virksomhedsejerne".

"Vi tager imod sådan nogle initiativer [guiden], der skal hjælpe virksomhederne, med kyshånd - særligt, når de samtidig også er pædagogiske. Der sidder ikke særlig mange it-specialister ude i virksomhederne."

Citat: Lasse Lundquist, konsulent og digitaliseringsansvarlig, SMV Danmark

"For os har det været en øjenåbner at arbejde konkret med risikovurdering, og hvad det betyder for vores forretning. Det giver stor værdi at tage udgangspunkt i vores virkelighed og hvad der rent faktisk kan påvirke os, fremfor at tage udgangspunkt i generiske risici."

Citat: Anne Dorte Bach, projektleder og DPO hos Magenta

Hent guide for risikostyring her:
https://www.ds.dk/risikostyring

Tak

Michael Bladt Stausholm

E: michael.stausholm@alexandra.dk

M: 20 29 63 22

Berit Aadal

E: baa@ds.dk

M: 26 22 46 96

Risikostyring der skaber værdi

Magenta - open source IT

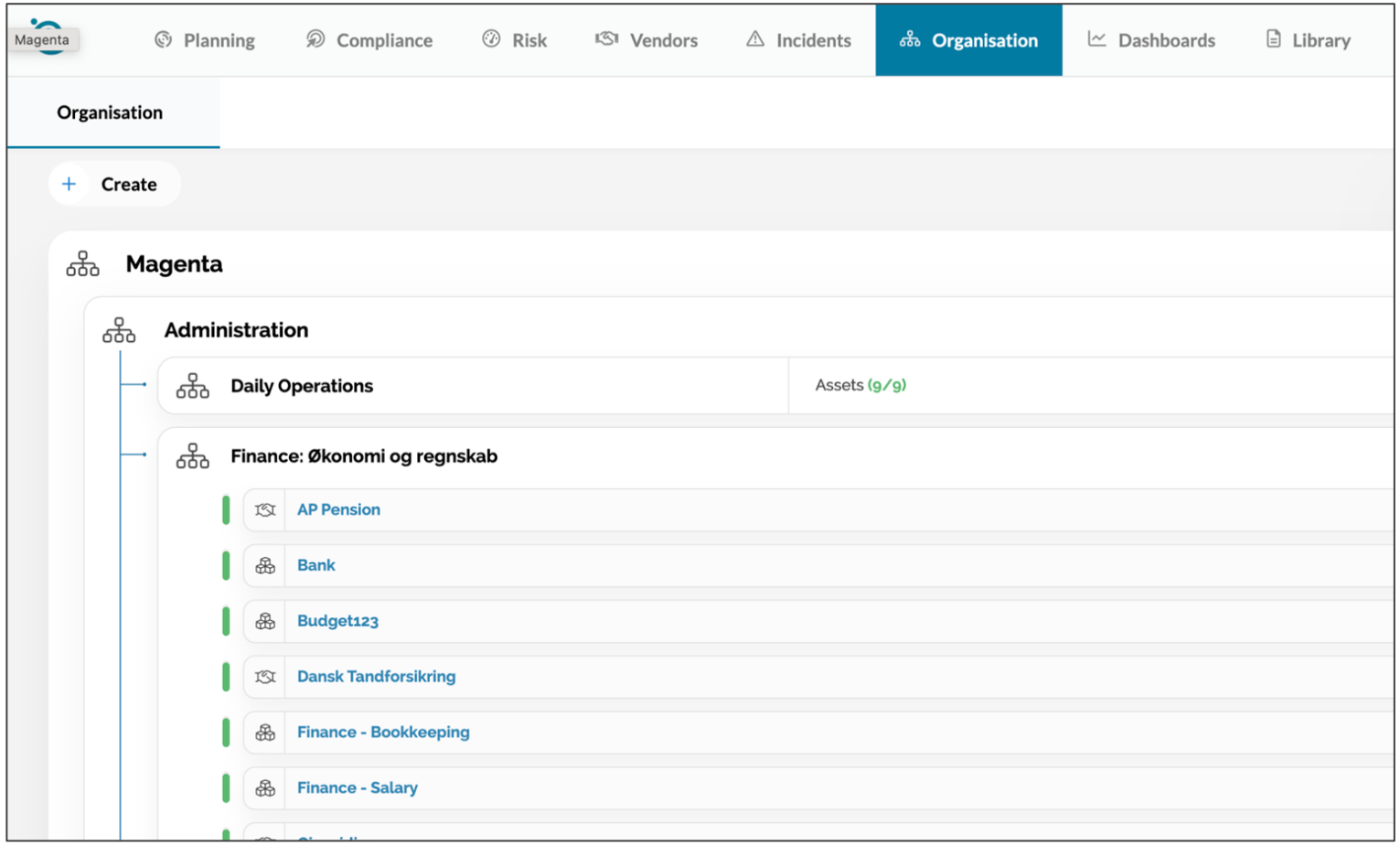
Magenta - open source IT

- ★ Software udvikling - open source kode
- ★ ca 50 ansatte
- ★ Løsninger i fællesskab med kunder
- ★ Høj grad af sikkerhedsawareness
- ★ Gazelle i 2020
- ★ Deltagelse i Security By Design (Alexandra Instituttet/Industriens Fond)

Fra opportunity-styring til risikostyring

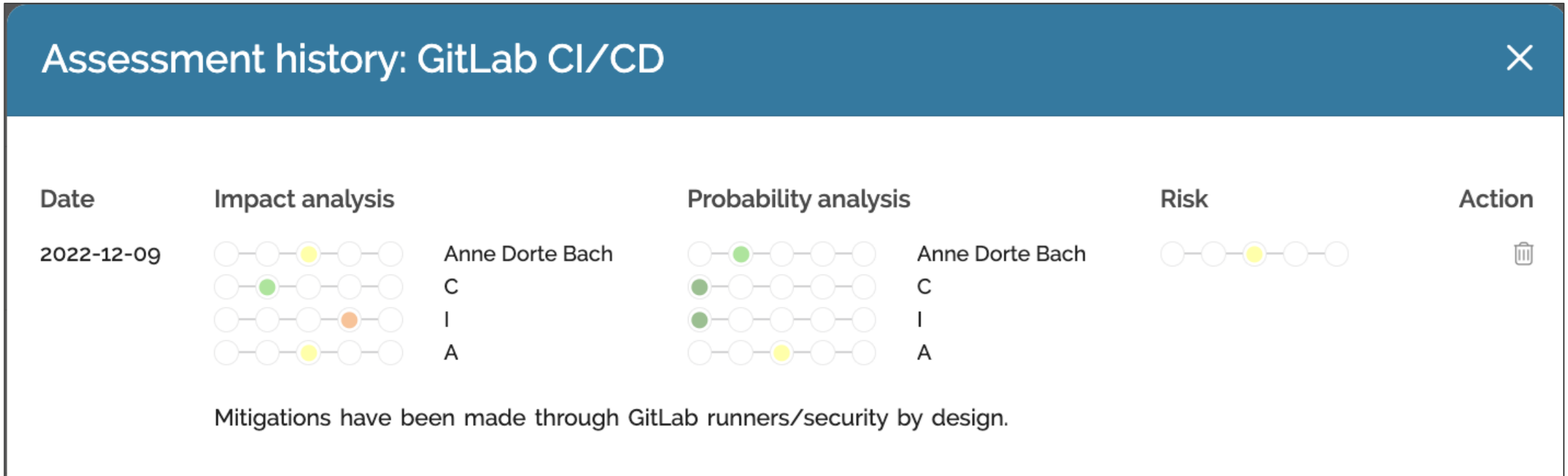
Under/efter Corona	**Ny virkelighed**
Mange projekter/teknologier	Færre produkter/teknologier
Nedgang i opgaver	Stærkere, sikrere infrastruktur
Et dyrt, kuldsejlet projekt	Risikostyret prioritering
Ramt på budgettet	Standardisering - ISO 27001/27701
Nye reguleringer og krav på vej	Robust fundament

Sådan har vi gjort - Overblik over data, processer, systemer og ansvar

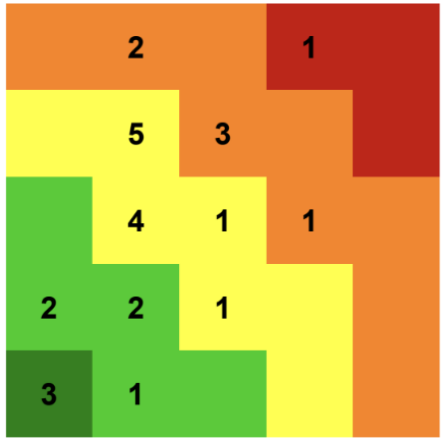


Sådan har vi gjort - trusler og risikovurdering

- Trusselskatalog - tilpas til egen virkelighed
- Risikometode - konsekvens/sandsynlighed (analyser incidents, post mortems, lessons learned)



Resultat - riskooverblik



The chart above, shows the selected assets, plotted into a heatmap.

Asset	Category	(C) Confidentiality	(I) Integrity	(A) Availability	(CIA) Combined Risk
[redacted]	Service (XaaS)	High	Low	Medium	High
[redacted]	Process	Low	Medium	Low	Medium
[redacted]	System	Very Low	Medium	High	Medium
[redacted]	Process	Very Low	Very Low	Very Low	Very Low
[redacted]	Process	Very Low	Very Low	Very Low	Very Low
[redacted]	Service (XaaS)	Very Low	Very Low	Very Low	Very Low
[redacted]	Service (XaaS)	Low	Medium	Medium	Medium
[redacted]	Service (XaaS)	Very Low	Low	Medium	Medium
[redacted]	Service (XaaS)	Low	Medium	Low	Medium
[redacted]	Service Provider	Low	Medium	Medium	Medium
[redacted]	Service (XaaS)	Medium	Medium	Medium	Medium
[redacted]	Process	Very Low	Low	Low	Low
[redacted]	Process	Very Low	Very Low	Very Low	Very Low
[redacted]	Process	Low	Medium	Medium	Medium
[redacted]	Network	Low	Low	Low	Low

Gevinst

- Samlet overblik over forretning og risici
- Igangsætte *prioriterede*, mitigerende tiltag
- Fælles forståelse for *nødvendigt* sikkerhedsniveau

Q&A

Stil dit spørgsmål i chatten

Cyber- og informationssikkerhed

Vi har samlet et overblik over de mest anvendte standarder inden for privatlivsbeskyttelse og cyber- og informationssikkerhed. Klik på figuren herunder for at læse om de enkelte standarder.

www.ds.dk/da/om-standarder/cyber-og-informationssikkerhedsstandarder

DS Cyberdag

Sæt x den 5. oktober

Følg med på ds.dk hvor der kommer flere informationer og program i løbet af året