CYBERSIKRE FØDEVAREVÆRDIKÆDER

GUIDE TIL SCENARIEBESKRIVELSE

Cybersikkerhed og risikoledelse

DECEMBER 2024

INDUSTRIENS FOND

Food & Bio Cluster Denmark

ALEXANDRA INSTITUTTET

SecuriOT

CYBERSIKRE FØDEVAREVÆRDIKÆDER

SIKKERHED STYRKER FORRETNINGEN

FORFATTERE

Jørgen Hartig, SceriOT

Eva Nautrup, Food & Bio Cluster Denmark

Udgivet af

Projektet Cybersikre Fødevareværdikæder

December 2024

Indhold

> Denne guide er udarbejdet i projektet Cybresikre Fødevareværdikæder, og er ment som en hjælp til forberedelserne forud for gennemførelse af Risk assessment i virksomheden

1. Introduktion

1.1 Risikoledelse

Risiko er potentialet for uønskede negative konsekvenser af begivenheder, mens resiliens/modstandskraft kan opfattes som systemets eller organisationens evne til at forhindre, modstå, og komme sig fra disse begivenheder.

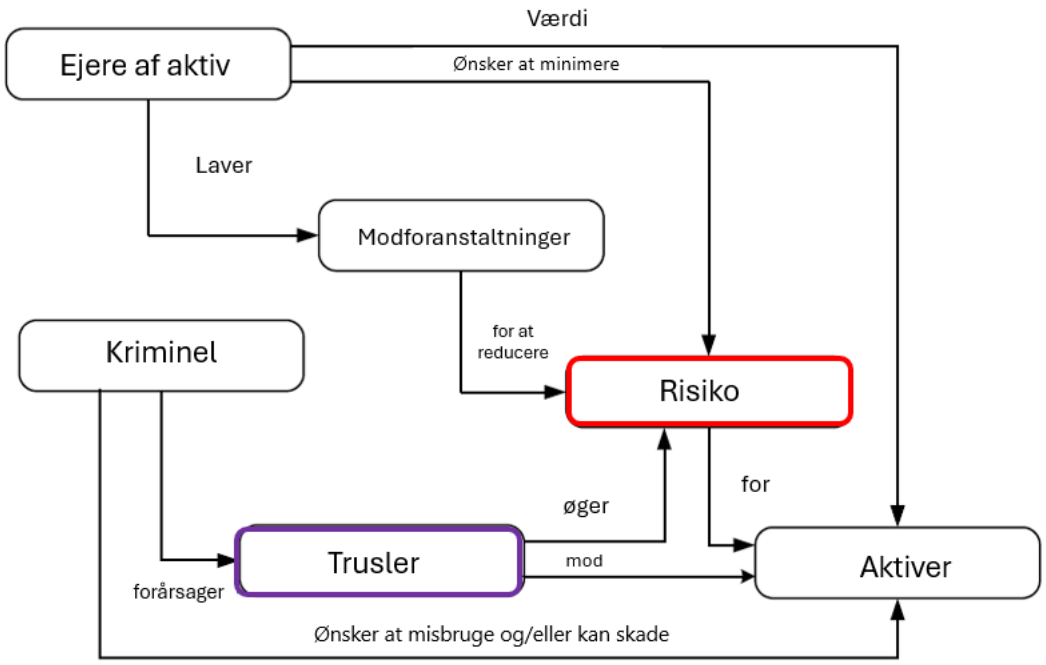
Så risikoledelse handler om:

1. Identifikation og vurdering af potentielle hændelser og disses påvirkninger
2. Forebyggelse af hændelser
3. Afbødning af påvirkning – minimering af de negative konsekvenser af hændelser
4. Retablering efter hændelser

En risikovurdering er en systematisk proces, der bruges til at identificere, analysere og evaluere potentielle risici, der kan påvirke organisationens mål eller aktiviteter. Risikovurderinger er afgørende for at sikre, at ressourcer prioriteres korrekt, og at man er forberedt på mulige trusler, herunder cybersikkerhed.

En af de mest centrale discipliner indenfor sikkerhed, er således at identificere de trusler og risici, som din virksomhed står overfor. Samt at få det sammenholdt med din virksomheds risikoprofil og tolerance.

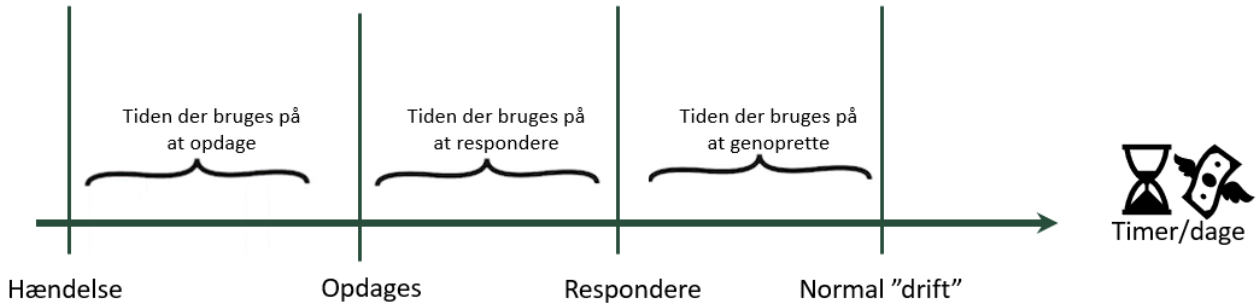
Sammenhænget mellem trusler og risiko kan illustreres med nedenstående figur.



1.2 Cybertruslen

I takt med at cyberangreb ikke længere er noget, der kun rammer sjældent og enkelte virksomheder, men er blevet en reel trussel, som kan ramme alle virksomheder, er cybersikkerhed blevet noget alle bør forholde sig til. Det understreges yderligere af Center for Cybersikkerheds trusselsvurdering, hvor truslen fra cyberkriminalitet vurderes at være meget høj.

Det er derfor at vurdere et "beredskab" i forbindelse med cyberangreb. Når et cyberangreb rammer, kan det typisk opdeles i tre faser, som illustreret nedenfor:



Disse "tidsvinduer" – såsom "Tid til at opdage", " – skal være så snævre som muligt. Jo tidligere en hændelse opdages, jo hurtigere kan der reageres på hændelsen, og jo hurtigere kan virksomheden vende tilbage til normal drift.

Disse faser opfyldes ikke blot ved at have et godt segmenteret netværk, en opdateret anti-malware-løsning eller en god OT-specifik overvågningsløsning. Det kræver også en bred vifte af arbejdsgange og processer, der er forankret i organisationen – og som udføres, hvis det er nødvendigt

2. Trusselsscenarier

Det kan være meget svært at få overblik over om de trusler og risici, som kan være gældende i forhold til cybersikkerheden, og hvilke udfordringer i kan stå overfor i relation til IT- eller OT-infrastrukturene. Spørgsmålene er således mange:

- Hvilke trusselsscenarier står vi overfor?
- Hvad er konsekvens og sandsynlighed hvis scenarierne udspiller sig?
- Hvilke aktiviteter skal sættes i værk for at mitigere disse risici?
- Hvordan skal vi prioritere indsatsen imod disse risici?
- Hvad er "Return On Investment" (ROI) på at mitigere disse risici?

Med denne guide vil vi hjælpe med at identificere potentielle risikoscenarier, som du kan tage udgangspunkt i, i forbindelse med din risk assessment.

Guiden består af to dele – 1. en metode til opbygning af egne scenarier og 2. en liste med en række scenarier, som du kan blive inspireret af.

2.1 Opbygning af scenarier

At opbygge scenarier er en struktureret proces, der hjælper med at udforske fremtidige mulige udviklinger og deres konsekvenser. Metoden bruges ofte i strategisk planlægning, risikostyring og beslutningstagning.

Her er en generel trin-for-trin metode til at opbygge scenarier:

2.1.1 Definer formålet og rammen

Formål: Hvad vil du opnå med scenarierne? Er det at forstå mulige risici, identificere muligheder eller forberede organisationen på fremtidige udfordringer?

Scope: Afgræns emnet og tidshorisonten (f.eks. 5, 10 eller 20 år frem).

Fokus: Identificér det system eller område, som scenarierne skal udforske, f.eks. markedstendenser, teknologisk udvikling eller sikkerhedstrusler.

2.1.2 Identificer drivkræfter

Kortlæg de vigtigste drivkræfter, der kan påvirke udviklingen. Disse kan opdeles i interne og eksterne faktorer:

Eksterne: Teknologiske fremskridt, geopolitisk situation, øget cybertrussel

Interne: Organisationens styrker, svagheder, ressourcer og opmærksomhed

Vælg de drivkræfter, der har størst betydning og giver størst usikkerhed.

2.1.3 Udvælg de kritiske usikkerheder

Identificér de to-tre faktorer med størst usikkerhed og samtidig størst indflydelse på fremtiden.

Eksempel: Hvis du analyserer cybersikkerhed, kan de kritiske usikkerheder være:

- Tempoet i teknologisk udvikling
- Regulatoriske ændringer
- Trusselslandskabets udvikling

2.1.4 Udvikl en matrix

Kombinér de vigtigste usikkerheder i en 2x2 eller 2x3 matrix for at skabe forskellige kombinationer af mulige udfald.

Hver kombination repræsenterer et muligt scenarie.

Eksempel på matrix:

X-akse: "Tempo i teknologisk udvikling" (hurtig/langsom).

Y-akse: "Regulering" (stram/liberal).

Dette giver fire scenarier:

1. Hurtig udvikling + stram regulering.
2. Hurtig udvikling + liberal regulering.
3. Langsom udvikling + stram regulering.
4. Langsom udvikling + liberal regulering.

Et andet eksempel på matrix kunne være:

X-akse: Økonomisk konsekvens (alvorlig/overskuelig)

Y-akse: Hændelsesudspring (internt/eksternt)

1. Intern hændelse + alvorlig konsekvens
2. Intern hændelse + overskuelig konsekvens
3. Ekstern hændelse + alvorlig konsekvens
4. Ekstern hændelse + overskuelig konsekvens

2.1.5 Beskriv scenarierne

Udarbejd detaljerede beskrivelser for hvert scenarie. Start med de trusselsscenarier, som vil få den største konsekvens og højeste kritikalitet for virksomheden.

- Hvad sker der i dette scenarie?
- Hvordan påvirkes organisationen?
- Hvilke muligheder og risici opstår?
- Hvad er det estimerede økonomiske tab ved denne hændelse?
- Hvilken varighed af hændelse er kritisk?

Brug scenarieskabelonen til at beskrive, og få så mange relevante elementer med for at gøre scenarierne realistiske og engagerende.

Elementerne der er relevant at få med i scenariebeskrivelsen:

1. Systembetegnelse for det der bliver ramt
2. Trusselaktør (hvem/hvad)
3. Konsekvens
4. Varighed
5. Økonomi

Et eksempel på en scenariebeskrivelse:

Vores ERF-system i vores datacenter er nede, som følge af et ransomware, og det betyder at systemet er utilgængeligt i 12 timer. Det medfører et tab på DKK 100.000.

Elementerne er med i scenariebeskrivelsen således:

1 [Vores ERF-system i vores datacenter er nede], 2 [som følge af et ransomware], 3 [og det betyder at systemet er utilgængeligt] 4 [i 12 timer]. 5 [Det medfører et tab på DKK 100.000.]

Der er flere måder at beskrive scenarierne på, men det er vigtig, at du får de væsentligste elementer med – brug eventuelt et skema for at sikre det – eksempel vist nedenfor.

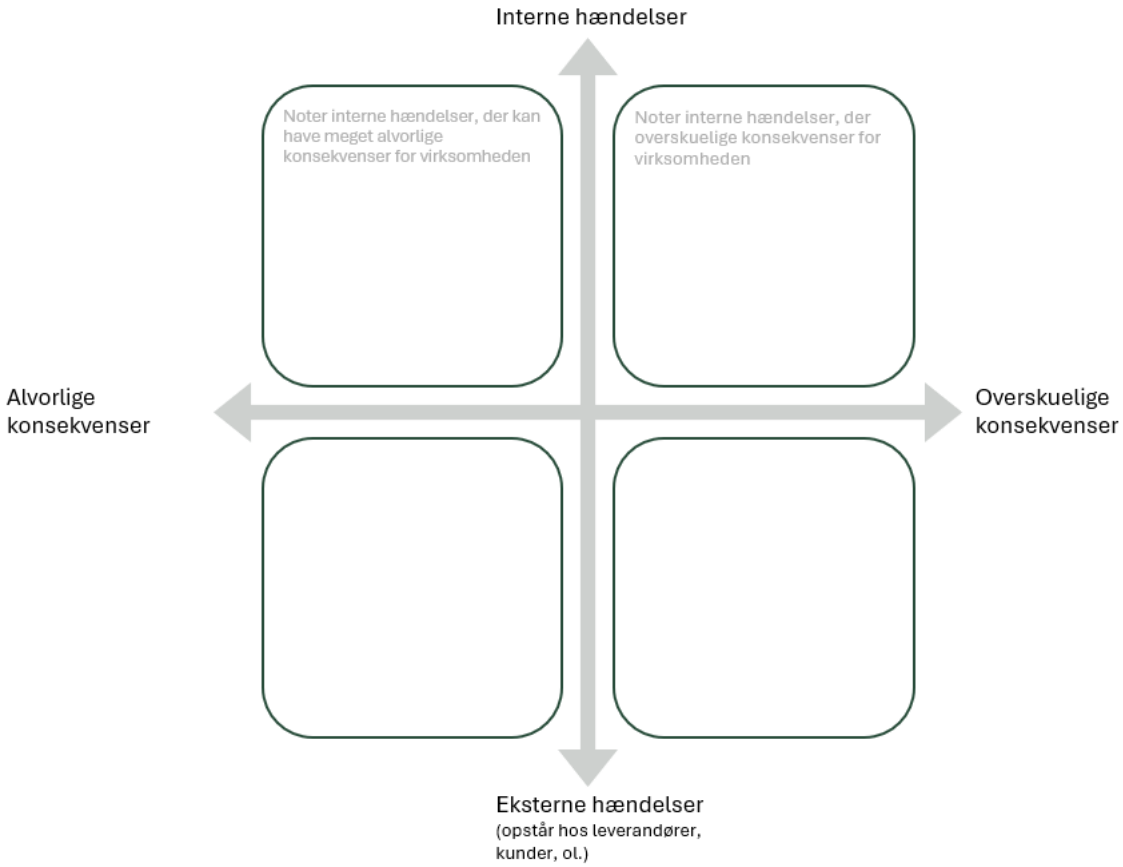
Scenarie 1
Hvad bliver ramt? **Vores ERF-system i vores datacenter er nede**
Hvem/hvad er aktøren? **som følge af et ransomware**
Hvad er konsekvensen? **og det betyder at systemet er utilgængeligt**
Varighed **i 12 timer.**
Økonomi **Det medfører et tab på DKK 100.000**

Skema findes i bilag 1.

2.1.6 Scenarie skabelon

Scenarieskabelonen kan hjælpe med at strukturere udviklingen af de enkelte scenarier.

Husk at start med de vigtigste usikkerheder.



Skabelon findes i bilag 2.

2.2 Inspirationsliste over mulige scenarier

Få inspiration til egne mulige trusselscenarier af nedenstående liste:

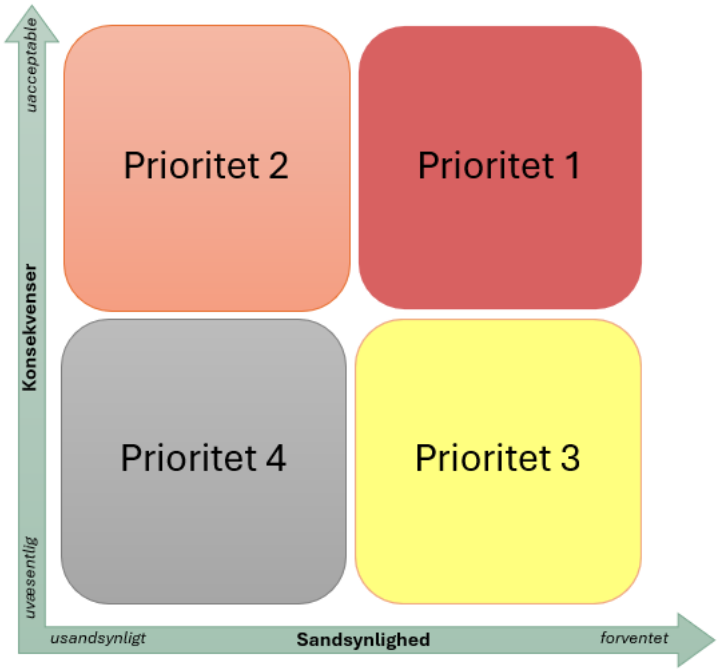
- En medarbejder i økonomiafdelingen klikker på et link som betyder at flere PC'ere inficeres med krypteringssoftware, og det administrative netværk er nede i 14 timer.
  SAP applikation hos Hosting provider er utilgængelige på grund af ransomware angreb, og applikationer er ikke tilgængelig i 24 timer.
- Produktionssystem er nede på grund af fejl ved en software opdatering og produktionen står stille i 7,5 time
- Køle anlægget i produktionen stopper pgra. fejl i software styringen og genetableringen tager mere end 6 timer.
- Der opnåes remote access adgang til et system, og systemet inficeres med malware som er utilgængeligt i 8 timer.

- Malware befinder sig på en server i OT-infrastrukturen, og udfører konfigurationsændringer, da data er upålidelige.
- En autoriseret lokal bruger har malware på en pc tilknyttet på netværket, og et system inficeres af malware.
- En uvelkommen person trænger ind på en fabrik, eller et andet produktionssted, og implementere en wireless enhed, som skal forstyrres netværks kommunikationen.

2.3 Prioritering af trusselsscenarierne

En måde at prioritere de beskrevne trusselsscenarier på er ved at vurdere de forretningsmæssige konsekvenser i forhold til sandsynligheden for at scenariet bliver en realitet.

Man får således en prioritering.



Skabelon findes i bilag 3.

3. Bilag

1. Scenarie beskrivelse
2. Scenarie skabelon
3. Scenarie prioritering

Bilag 1 – Scenariebeskrivelser

Scenarie 1
Hvad bliver ramt?
Hvem/hvad er aktøren?
Hvad er konsekvensen?
Varighed
Økonomi
Scenarie 2
Hvad bliver ramt?
Hvem/hvad er aktøren?
Hvad er konsekvensen?
Varighed
Økonomi

Scenarie 3

Hvad bliver ramt?

Hvem/hvad er aktøren?

Hvad er konsekvensen?

Varighed

Økonomi

Scenarie 4

Hvad bliver ramt?

Hvem/hvad er aktøren?

Hvad er konsekvensen?

Varighed

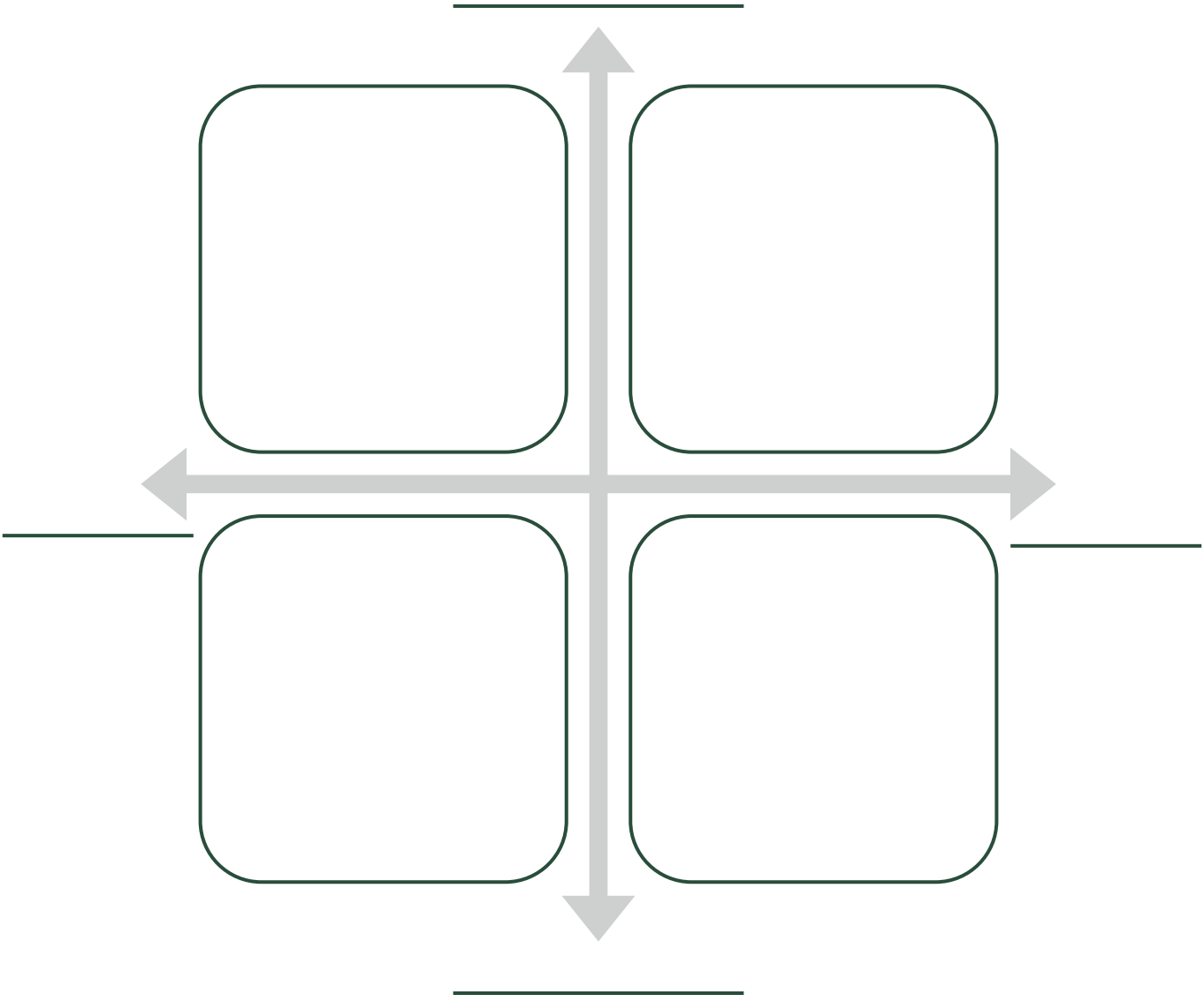
Økonomi

CYBERSIKRE FØDEVAREVÆRDIKÆDER

SIKKERHED STYRKER FORRETNINGEN

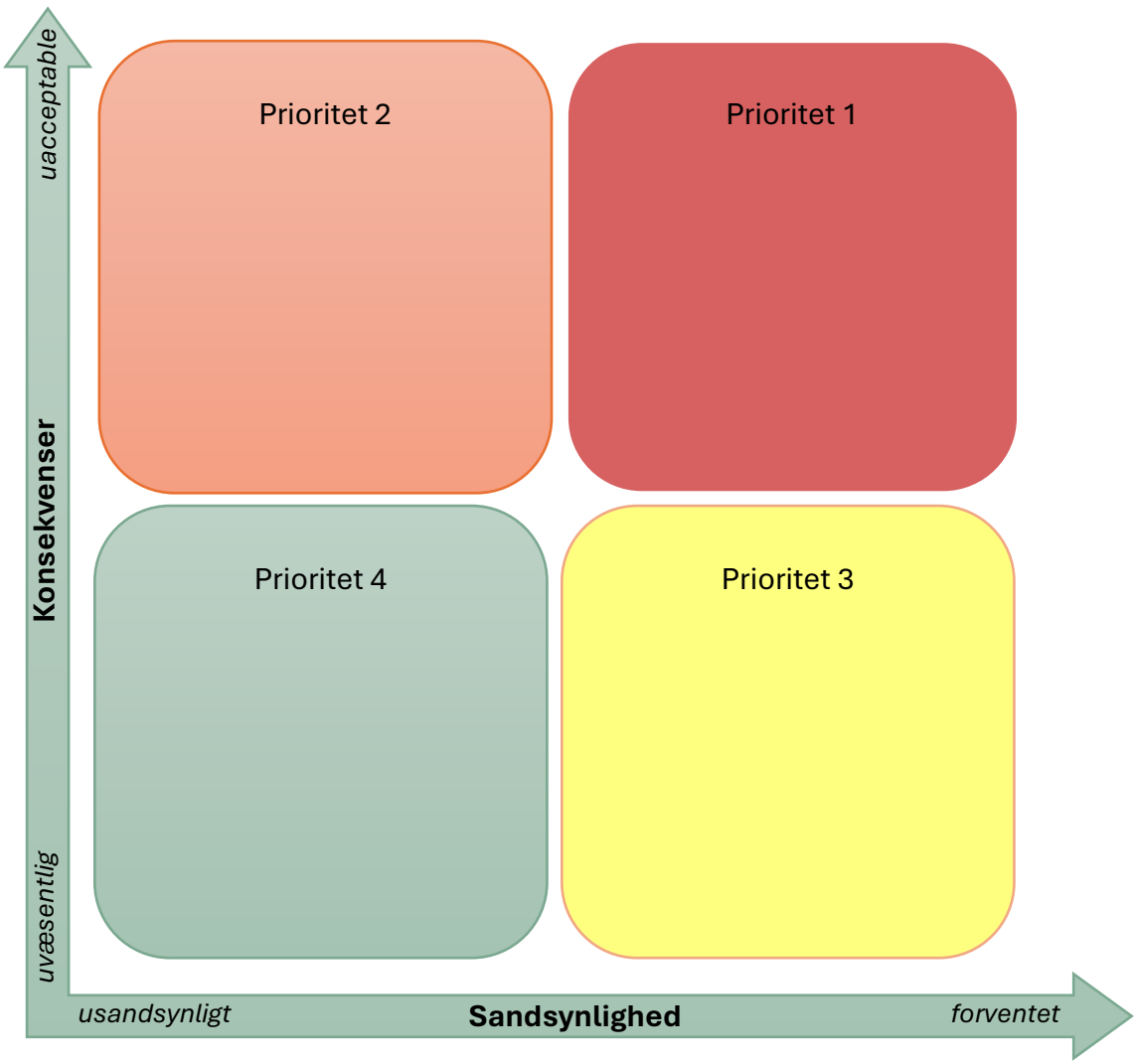
Bilag 2 – Scenarie skabelon

Faktorer med størst usikkerhed og samtidig størst indflydelse på cybersikkerheden:



Bilag 3 – Scenarie prioritering

Prioriter de beskrevne trusselsscenarier ved at vurdere de forretningsmæssige konsekvenser i forhold til sandsynligheden for at scenariet bliver en realitet:



Cybersikre Fødevareværdikæder er et projekt, der arbejder med at styrke cybersikkerheden i fødevareværdikæderne – dels for at virksomhederne skal stå stærkt i kampen mod stadig mere avancerede hackerangreb – dels for derigennem at styrke deres konkurrenceevne.

Projektet er finansieret af Industriens Fond og gennemføres i et samarbejde mellem Food & Bio Cluster Denmark, Alexandra Instituttet, SecuriOT, Dansk Cater, Salling Group, DI Fødevarer og Landbrug & Fødevarer.

INDUSTRIENS FOND Food & Bio Cluster Denmark ALEXANDRA INSTITUTTET SecuriOT

CYBERSIKRE FØDEVAREVÆRDIKÆDER

SIKKERHED STYRKER FORRETNINGEN