LUNDS UNIVERSITET
Ekonomihögskolan
*Institutionen för informatik*

# Säkerhet i förändring

## Implementering av cybersäkerhetslagen inom den svenska livsmedelsindustrin

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Victoria O'Bryan
Tomas Jansson
Emelie von Schantz

Handledare: Nicklas Holmberg

Rättande lärare: Osama Mansour
Umberto Fiaccadori

# Säkerhet i förändring: Implementering av cybersäkerhetslagen inom den svenska livsmedelsindustrin

ENGELSK TITEL: Security in Transition: Implementation of the Swedish Cybersecurity Act within the Food Industry

FÖRFATTARE: Victoria O'Bryan, Tomas Jansson, Emelie von Schantz

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, Docent

FRAMLAGD: juni, 2026

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 70

NYCKELORD: cybersäkerhetslagen, NIS2-direktivet, compliance capability, informationssäkerhet, cybersäkerhet, livsmedelsindustrin, TOE-ramverket, digital mognad, EU-regleringar

SAMMANFATTNING (MAX. 200 ORD):
Denna studie undersöker hur stora verksamhetsutövare inom livsmedelssektorn arbetar med implementeringen av den svenska cybersäkerhetslagen samt vilka förutsättningar, utmaningar och tolkningar som påverkar implementeringen. Lagen bygger på EU:s NIS2-direktiv och syftar till att stärka cybersäkerheten och motståndskraften inom samhällsviktiga verksamheter i Europa. Genom NIS2-direktivet har livsmedelssektorn för första gången inkluderats som en samhällsviktig sektor och omfattas därmed av nya krav kopplade till cybersäkerhet och riskhantering. Implementeringen sker samtidigt i en sektor präglad av varierande organisatoriska och tekniska förutsättningar, trots att cyberrelaterade hot kan få konsekvenser för både livsmedelsförsörjning och samhällsförsörjning. Studien bygger på en kvalitativ forskningsansats baserad på semistrukturerade intervjuer med informanter i CISO-liknande roller från sex stora verksamhetsutövare inom livsmedelssektorn. TOE-ramverket används

som ett strukturellt ramverk för att sera empiri och diskussion, medan compliance capability används för att analysera organisationernas förutsättningar att hantera och efterleva regulatoriska krav kopplade till cybersäkerhet. Resultatet visar att implementeringen präglas av varierande organisatoriska förutsättningar, cybersäkerhetsmognad och tolkningar av regulatoriska krav. Studien indikerar även att NIS2-direktivets flexibla och riskbaserade utformning kan skapa osäkerhet kring regulatorisk tolkning och nationell implementering.

# Innehåll

## Figurer



## Tabeller

# Begreppslista

**Direktiv (EU):** En rättsakt inom Europeiska Unionen (EU) som sätter upp bindande mål för medlemsstaterna, men där det överlämnas till de nationella myndigheterna att bestämma form och tillvägagångssätt för genomförandet. (Europeiska unionen, 2026)

**Förordning (EU):** En rättsakt inom Europeiska Unionen (EU) som är bindande i sin helhet och direkt tillämplig i alla medlemsstater utan att behöva införas i nationell lagstiftning. (Europeiska unionen, 2026)

**Föreskrift**: Bindande och detaljerade regler som meddelas av en myndighet som är bemyndigad av regeringen att precisera hur lagar och förordningar inom definierade områden ska tillämpas i praktiken. (MCF, 2025)

**Verksamhetsutövare**: Den juridiska eller fysiska person som har det yttersta rättsliga ansvaret för att regleringar följs hos en registrerad och enligt nationell lagstiftning erkänd verksamhet (Direktiv (EU) 2022/2555).

**Medelstor verksamhetsutövare**: Definieras enligt Direktiv (EU) 2022/2555 i enlighet med kriterierna i kommissionens rekommendation 2003/361/EG. Detta innebär en verksamhet som sysselsätter mellan 50 och 249 personer, och som har en årsomsättning eller balansomslutning som överstiger 10 miljoner euro men inte överstiger 50 miljoner euro i omsättning eller 43 miljoner euro i balansomslutning. (Direktiv (EU) 2022/2555)

**Stor verksamhetsutövare**: Definieras enligt Direktiv (EU) 2022/2555 som en enhet vars storlek överskrider taket för medelstora företag. Detta avser verksamheter som sysselsätter 250 personer eller fler, eller som har en årsomsättning som överstiger 50 miljoner euro och en balansomslutning som överstiger 43 miljoner euro. (Direktiv (EU) 2022/2555)

**Grossisthandel:** ”Lagring och/eller tillhandahållande av livsmedel till andra företag (B2B), inklusive livsmedelsföretag som är nödvändiga för att tillhandahålla livsmedel till andra företag. Tillhandahållande av livsmedel direkt till slutkonsument omfattas inte.” (Livsmedelsverket, 2026, s.7)

**Industriell produktion och bearbetning:** ”Storskalig produktion och/eller bearbetning av livsmedel som har ett betydande beroende av nätverks- och informationssystem för leveransen av tjänsten.” (Livsmedelsverket, 2026, s.7)

**Incidentrapportering**: Den lagstadgade skyldigheten för verksamhetsutövare att utan onödigt dröjsmål anmäla säkerhetsincidenter som har en betydande inverkan på tillhandahållandet av deras tjänster. (Direktiv (EU) 2022/2555)

**Information Technology (IT):** Teknologiska system, inklusive hårdvara, mjukvara och nätverksinfrastruktur, som används för att samla in, lagra, bearbeta, överföra och presentera digital data och information, primärt affärsadministrativa processer och informationsflöden. (NIST, 2023)

**Operational Technology (OT):** Teknologiska system, inklusive hårdvara, mjukvara och nätverksinfrastruktur, som används för att direkt övervaka, styra och automatisera fysiska processer och infrastruktur, primärt inom industriella produktionsmiljöer. (NIST, 2023)

# 1 Introduktion

## 1.1 Bakgrund

### *1.1.1 NIS2 och cybersäkerhetslagen*

I och med att cybersäkerhetslagen trädde i kraft i januari 2026 i Sverige, som en implementering av NIS2-direktivet (Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen), ställs nya krav på organisationer som bedriver storskalig industriell produktion och bearbetning av livsmedel. NIS2-direktivet syftar till att uppnå en hög gemensam nivå av cybersäkerhet inom EU genom att stärka skyddet av nätverks- och informationssystem samt säkerställa kontinuiteten i samhällsviktiga tjänster (Direktiv 2022/2555). Direktivet utgår från att cyberattacker i allt högre grad är gränsöverskridande och kan få omfattande konsekvenser för kritisk infrastruktur och samhällsviktiga tjänster, däribland livsmedelssektorn. Den svenska cybersäkerhetslagen innebär bland annat krav på riskhantering, incidentrapportering samt säkerhet i nätverks- och informationssystem.

Forskning om implementeringen av NIS2 visar samtidigt att efterlevnaden av direktivet innebär samverkan mellan flera olika aktörer och tillsynsnivåer. Seeba et al. (2025) beskriver hur verksamhetsutövare, tillsynsmyndigheter, medlemsstater och andra intressenter behöver samordna arbete kring säkerhetsutvärdering, rapportering och uppföljning för att vara NIS2-compliant. Inom livsmedelssektorn innebär detta att Livsmedelsverket ansvarar för tillsynen av att cybersäkerhetslagen efterlevs (Länsstyrelsen Stockholm, u.å).

Myndigheten för civilt försvar (MCF) har föreskriftsrätt inom området och ansvarar för att ta fram föreskrifter vilka konkretiserar hur kraven ska uppfyllas i en svensk kontext. Utformningen av dessa föreskrifter har samtidigt blivit föremål för debatt, särskilt avseende graden av detaljstyrning och hur kraven påverkar organisationers praktiska arbete med informationssäkerhet.

### *1.1.2 Livsmedelsföretag som viktiga verksamhetsutövare*

NIS2-direktivet innebär att livsmedelssektorn för första gången inkluderas explicit som en samhällsviktig sektor inom EU:s regelverk för cybersäkerhet. I NIS2-direktivet faller

livsmedelssektorn, som i direktivet benämns som sektorn för ”Produktion, bearbetning och distribution av livsmedel”, under bilaga II: ”Andra kritiska sektorer”. I likhet med NIS2-direktivet skiljer cybersäkerhetslagen mellan väsentliga och viktiga verksamhetsutövare (Direktiv (EU) 2022/2555; SFS 2025:1506).

Klassificeringen baseras bland annat på verksamhetens sektor, storlek och samhällskritiska betydelse och påverkar både tillsyn och möjliga sanktionsavgifter vid bristande efterlevnad. Verksamhetsutövare inom livsmedelssektorn omfattas huvudsakligen som viktiga verksamhetsutövare enligt cybersäkerhetslagen.

Vid bristande efterlevnad kan sanktionsavgifter utdömas. För viktiga verksamhetsutövare kan avgiften uppgå till det högsta av 7 000 000 euro eller 1,4 % av den globala årsomsättningen, medan motsvarande nivå för väsentliga verksamhetsutövare är 10 000 000 euro eller 2,0 % av den globala årsomsättningen (SFS 2025:1506).

### *1.1.3 Oro inom livsmedelssektorn*

Företrädare för livsmedelssektorn har i Svenska Dagbladet (2025-12-08) uttryckt oro över den remiss som avser föreskrifter kopplade till cybersäkerhetslagen. Remissen har tagits fram av Myndigheten för civilt försvar (MCF), tidigare Myndigheten för samhällsskydd och beredskap (MSB), som ansvarar för att utforma dessa föreskrifter. Enligt företrädarna upplevs de föreslagna reglerna som oproportionerligt detaljstyrda och kostsamma. Liknande synpunkter har framförts i Dagens Industri (2026-01-07), där det framhålls att en hög grad av detaljstyrning riskerar att styra organisationers arbete mot dokumentation och formalia snarare än mot åtgärder som faktiskt stärker informationssäkerheten.

Även Svenskt Näringsliv (2025) har riktat kritik mot föreskrifterna och menar att delar av förslaget går längre än vad NIS2-direktivet och cybersäkerhetslagen kräver, vilket riskerar att skapa oproportionerliga administrativa kostnader och försvåra möjligheter till regelefterlevnad för verksamhetsutövare.

Remissen, som dåvarande MSB skickade ut i december 2025, innehåller omfattande och detaljerade krav på verksamhetsutövare. Dessa omfattar bland annat krav på ett systematiskt och riskbaserat cybersäkerhetsarbete, dokumenterade interna regler och arbetssätt, återkommande riskanalyser och uppföljning samt en tydlig ansvarsfördelning mellan roller inom organisationen (MSB, 2025).

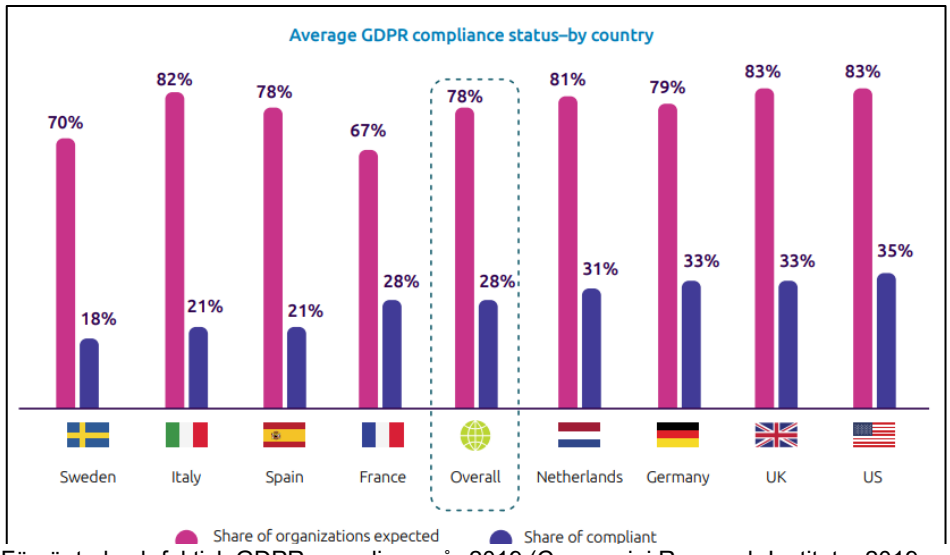
Den kritik som framförs i debatten kan även sättas i relation till tidigare studier om implementeringen av EU:s regleringar inom informationssäkerhetsområdet.

### *1.1.4 GDPR*

Zaguir et al. (2024) beskriver att organisationer möter både teknologiska och organisatoriska utmaningar vid implementeringen av regulatoriska krav. Studien fokuserar på implementeringen av General Data Protection Regulation (GDPR), EU:s dataskyddsförordning som trädde i kraft 2018, och visar att dessa utmaningar delvis kan förklaras av att regelverk i flera fall saknar konkreta riktlinjer för hur kraven ska omsättas i praktiken.

Tidigare rapporter visar att många organisationer underskattade omfattningen av det arbete som krävdes för att uppnå compliance med GDPR. I en studie genomförd bland 1000 europeiska och amerikanska organisationer uppgav 78% av organisationerna att de förväntade sig att vara compliant med GDPR vid regleringens ikraftträdande, medan endast 28% uppgav att de faktiskt var compliant ett år senare (Capgemini Research Institute, 2019).

Figur 1.1 illustrerar skillnaden mellan organisationers förväntningar på att uppnå GDP-compliance vid regleringens ikraftträdande och den faktiska graden av compliance ett år senare.




**Figur 1.1:** Förväntad och faktisk GDPR-compliance år 2019 (Capgemini Research Institute, 2019, s. 5)

Detta tyder på att implementeringen av GDPR var mer omfattande och komplex än många organisationer initialt förväntade sig.

### *1.1.5 NIS-direktivet*

Network and Information Systems Directive (NIS-direktivet), Europaparlamentets och rådets direktiv (EU) 2016/1148, som antogs 2016 och utgjorde föregångaren till NIS2-direktivet, är ett annat exempel på EU-reglering inom informationssäkerhetsområdet. Tidigare forskning visar att implementeringen av direktivet skiljde sig åt mellan medlemsstaterna, vilket skapade ojämna förutsättningar (Vandezande, 2024).

Denna problematik med ojämna förutsättningar bekräftas även av det empiriska underlag som föregick utformningen av NIS2-direktivet. Under 2020 genomförde Europeiska kommissionen ett offentligt samråd i syfte att utvärdera det ursprungliga direktivet och utforma framtida lagstiftning. I samrådsrapporten sammanställdes svar från totalt 206 aktörer, och deltagarna utgjordes av branschorganisationer, verksamhetsutövare och leverantörer av digitala tjänster, experter inom cybersäkerhet, nationella myndigheter samt medborgare.

Över 40% av respondenterna höll med om att direktivets implementering ledde till signifikanta skillnader i hur direktivet implementerades mellan medlemsländer, bland annat skilda tröskelvärden och säkerhetskrav, och att detta hade en stark negativ inverkan på

konkurrensvillkoren. I en rapport av ENISA (2020) framgår dessutom att en av de största utmaningarna vid implementeringen av NIS-direktivet var bristande tydlighet från nationella myndigheter, vilket 32% av organisationerna inom de berörda sektorerna upplevde. I samma rapport framgår det även att 29,7% av organisationerna tvingades anställa personal specifikt för att klara implementeringen.

EU-kommissionens rapport synliggjorde i övrigt ett tydligt behov av att utöka direktivets räckvidd till nya sektorer. Drygt hälften av de svarande aktörerna (50,5%) ansåg specifikt att livsmedelssektorn borde inkluderas i framtida cybersäkerhetslagstiftning.

### *1.1.6 Särskilda utmaningar för livsmedelssektorn*

Ovan belyser att organisationer i stor utsträckning själva behöver tolka och operationalisera kraven som implementerats på nationell nivå, vilket visar att formuleringen av regulatoriska krav på informationssäkerhet utgör en avgörande faktor för hur de implementeras i praktiken. Konsekvenserna av detta blir tydliga i organisationers arbete med efterlevnad, vilket ofta kräver omfattande förändringar i befintliga informationssystem, processer och styrning, samtidigt som organisationer behöver hantera ökad komplexitet och krav på resurser.

Dessa utmaningar kopplade till implementering och efterlevnad av regulatoriska krav blir särskilt framträdande i livsmedelssektorn, där moderna produktions- och distributionssystem i hög grad utgör cyber-fysiska system, det vill säga att digitala och fysiska processer är tätt integrerade (Smetana et al. 2021). Dessutom beskriver Yerinde et al. (2025), i en sektorsrapport om cybersäkerhet i livsmedelssektorn framtagen inom ramen för det EU-finansierade forskningsprojektet Extreme Food Risk Analytics (EFRA), att livsmedelssektorn står inför en bred och komplex hotbild, där cyberattacker kan rikta sig mot såväl produktionssystem som informationsflöden. Detta förstärker därmed behovet av robusta och välanpassade säkerhetsåtgärder.

Livsmedelssektorn präglas samtidigt av variation mellan aktörer, där organisationer i olika delar av värdekedjan har kommit olika långt i sin digitala utveckling och har varierande organisatoriska förutsättningar. Vilket stärks av branschrapporter, såsom Blue Institute (2020), som visar att variationer i resurser, kompetens och teknikanvändning är betydande inom sektorn. Detta påverkar i sin tur sektorns möjligheter att implementera nya krav.

### *1.1.7 NIS-direktivets påverkan på hälso- och sjukvården*

För att bättre förstå vilka konsekvenser implementeringen av NIS2-direktivet kan medföra för en sektor med varierande grad av digital utveckling har vi gjort en jämförelse med hur införandet av NIS-direktivet påverkade hälso- och sjukvårdssektorn.

I en rapport från Boston Consulting Group (2020) framgår det att hälso- och sjukvården, vid tidpunkten för rapporten, var en av de minst digitalt mogna branscherna globalt med ett mognadsindex på 44 av 100, en nivå som var 20% lägre än de ledande branscherna. Vidare framgår det av Europiska kommissionens samrådsrapport (2020) att hälso- och sjukvården bedömdes ha den lägsta beredskapen mot cyberhot. Vid samma tidpunkt allokerade

livsmedelssektorn endast 2,8% av sin totala IT-budget till informationssäkerhet och placerade sig under det europeiska snittet (ENISA, 2020).

Data från ENISA:s rapport visar att lagkraven till följd av NIS-direktivet innebar en markant större ”compliance burden” för hälso- och sjukvårdssektorn än för de övriga berörda sektorerna, där 42,4% av aktörerna inom sektorn tvingades anställa personal specifikt för att klara implementeringen av NIS-direktivet i kontrast till det generella snittet på 29,7%.

## 1.2 Problem

De nya kraven som cybersäkerhetslagen medför innebär att organisationer inom livsmedelssektorn behöver anpassa sina befintliga informationssystem och säkerhetsåtgärder. I en sektor, där produktionen är starkt beroende av integrerade och ofta långlivade informationssystem kan sådana förändringar få direkta konsekvenser för drift och verksamhetens kontinuitet (Smetana et al. 2021).

Samtidigt har kritik redan riktats mot att MCF:s föreslagna föreskrifter är detaljstyrda (Dagens Industri, 2026; Svenska Dagbladet, 2025; Svenskt Näringsliv, 2025) och i vissa fall riskerar att styra arbetet mot formell efterlevnad snarare än mot faktisk säkerhetsförbättring (Veigurs et al. 2024). Detta ger upphov till en spänning mellan regulatoriska krav och organisationers praktiska förutsättningar att implementera dem.

För organisationer med befintliga informationssystem och informationssäkerhetsstrukturer kan implementeringen innebära att anpassningen inte enbart handlar om att införa nya lösningar, utan även om att integrera nya krav i befintliga tekniska och organisatoriska strukturer (Baker, 2012). Detta kan medföra begränsningar, organisatoriska utmaningar och ökade resurskrav (Busetti & Scanni, 2025).

Mot denna bakgrund är den empiriska kunskapen om hur dessa utmaningar konkret tar sig uttryck i praktiken begränsad, särskilt inom livsmedelssektorn där informationssystem är integrerade i verksamhetsprocesser (Smetana et al. 2021), variationen i den digitala utvecklingen är betydande (Blue Institute, 2020) och sektorn först genom NIS2-direktivet explicit inkluderats som samhällsviktig (Direktiv (EU) 2022/2555).

## 1.3 Forskningsfråga

*Vad präglar implementeringen av den svenska cybersäkerhetslagen hos stora verksamhetsutövare inom livsmedelssektorn?*

## 1.4 Syfte

Syftet med studien är att skapa förståelse för hur stora verksamhetsutövare inom den svenska livsmedelssektorn arbetar med implementeringen av cybersäkerhetslagen samt hur organisatoriska förutsättningar, regulatoriska tolkningar och tidigare erfarenheter av regulatorisk efterlevnad påverkar implementeringsarbetet.

## 1.5 Avgränsningar

Studien avgränsas till stora verksamhetsutövare inom livsmedelssektorn som omfattas av cybersäkerhetslagen. Medelstora verksamhetsutövare inkluderas därmed inte i studien. Avgränsningen till stora verksamheter motiveras av att dessa bedöms ha mer etablerade informationssäkerhetsstrukturer samt i högre grad ha påbörjat implementeringsarbetet kopplat till lagens krav. Studien behandlar huvudsakligen svenska verksamhetsutövare, även om en informant är verksam utanför Sverige och inkluderats för att bidra som ett kompletterande perspektiv kopplat till implementeringen av NIS2-direktivet.

Studien omfattar verksamheter inom grossisthandel samt industriell produktion och bearbetning av livsmedel, vilka enligt Livsmedelsverkets vägledning (Livsmedelsverket, 2026) omfattas av cybersäkerhetslagen inom livsmedelssektorn. Verksamheter inom primärproduktion och konsumentledet inkluderas därmed inte.

Studien undersöker informanternas upplevelser, tolkningar och arbete med implementeringen av cybersäkerhetslagen snarare än att fastställa faktisk efterlevnad eller utvärdera lagstiftningens juridiska innehåll.

# 2 Teoretiskt referensram

I detta kapitel presenteras studiens teoretiska referensram. Kapitlet består av ett strukturellt ramverk samt ett analytiskt ramverk, som tillsammans används för att strukturera och analysera organisationers implementering av cybersäkerhetsrelaterade krav.

Det strukturella ramverket i denna studie består av Technology-Organization-Environment (TOE)-ramverket. TOE-ramverket är framtaget för att strukturera och kategorisera faktorer som påverkar organisationers implementering av nya tekniska och regulatoriska krav. I denna studie används ramverket för att strukturera och kategorisera olika faktorer som påverkar livsmedelssektorns implementation av cybersäkerhetslagen.

Det analytiska ramverket i denna studie består av compliance capability i relation till regulatorisk implementering och används för att analysera organisationers förutsättningar att implementera och upprätthålla cybersäkerhetsrelaterade regulatoriska krav.

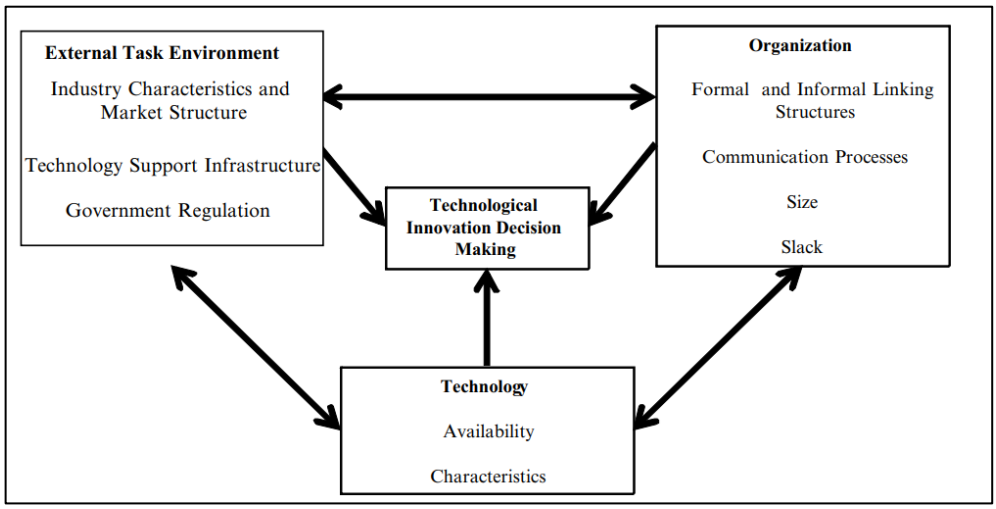
## 2.1 Strukturellt ramverk: Technology-Organization-Environment

Technology-Organization-Environment (TOE) introducerades av Tornatzky och Fleischer (1990) och är ett ramverk som används för att analysera organisatoriska implementeringsprocesser utifrån tre kontexter: teknologi, organisation och extern miljö. TOE-ramverket har senare vidareutvecklats av bland annat Baker (2012).

Enligt Baker (2012) möjliggör denna kategorisering en analys av hur olika kontexter påverkar organisationers arbete med att anpassa sig till förändrade teknologiska och regulatoriska krav. Kontexterna bör dock inte ses som isolerade från varandra, utan samverkar i organisationers implementeringsarbete.

Ramverket är relevant eftersom studien omfattar faktorer kopplade till organisationers tekniska system, interna resurser och kompetenser samt externa aktörer, regulatoriska krav och branschförhållanden. Eftersom TOE-ramverket har en relativt hög abstraktionsnivå används det i denna studie främst som en övergripande struktur för att organisera olika typer av faktorer som påverkar implementeringsarbetet.

Figur 2.1 illustrerar hur de tre kontexterna relaterar till varandra inom TOE-ramverket.




**Figur 2.1** TOE-ramverket (Baker, 2012, s. 236)

### *2.1.1 Teknologisk kontext*

Den teknologiska kontexten omfattar de teknologier som är relevanta för organisationen, både de som redan används och de som finns tillgängliga men ännu inte har implementerats. Särskilt betydelsefulla är organisationens befintliga teknologier eftersom dessa sätter ramar för hur förändringar kan genomföras (Tornatzky & Fleischer, 1990).

Enligt Baker (2012) kan befintliga system, inklusive så kallade legacy-system, både möjliggöra och begränsa införandet av nya lösningar, exempelvis genom tekniska beroenden, integrationskrav och tidigare investeringar. Legacy-system avser äldre tekniska system som fortfarande används inom verksamheten trots att de ofta bygger på äldre teknologiska lösningar. Eftersom dessa system ofta är långlivade och djupt integrerade i verksamheten, kan förändringar kräva omfattande anpassningar, vilket kan göra implementeringen av nya krav och tekniska anpassningar både komplex och resurskrävande.

Sådana system kan samtidigt vara väl anpassade till verksamhetens specifika behov, men mindre flexibla vid införandet av nya krav, vilket skapar en avvägning mellan funktionell anpassning och förändringsbarhet (Baker, 2012). Mot denna bakgrund kan organisationer i högre utsträckning välja standardiserade systemlösningar från externa leverantörer, vilket kan

underlätta uppfyllandet av nya krav genom etablerade funktioner och standarder, men samtidigt innebära ett ökat beroende av externa aktörer.

Baker (2012) betonar att teknologiska förutsättningar samtidigt är beroende av organisatoriska faktorer, såsom tillgång till kompetens och interna resurser, vilket påverkar organisationens möjlighet att underhålla, anpassa och vidareutveckla sina system.

### *2.1.2 Organisatorisk kontext*

Den organisatoriska kontexten avser organisationens interna egenskaper och resurser, såsom organisationsstruktur, kommunikationsmetoder, tillgång till resurser samt ledningens roll (Tornatzky & Fleischer, 1990). Dessa faktorer påverkar organisationens förmåga att genomföra förändringar och implementera nya teknologiska och regulatoriska krav.

Enligt Baker (2012) kan tillgång till kompetens, tydlig ansvarsfördelning och stöd från ledningen underlätta förändringsarbete, medan brist på resurser eller otydliga strukturer kan utgöra hinder. Även organisationens interna arbetsprocesser och rutiner påverkar hur förändringar omsätts i praktiken.

Graden av formalisering i organisationers arbetsprocesser kan vidare variera, vilket påverkar i vilken utsträckning nya krav implementeras systematiskt och integreras i verksamheten.

### *2.1.3 Extern kontext*

Den externa kontexten innefattar externa faktorer som påverkar organisationen, såsom branschstruktur, konkurrensförhållanden, tillgång till teknologiska resurser samt regulatoriska krav (Tornatzky & Fleischer, 1990).

Den innefattar även relationer mellan olika aktörer, såsom myndigheter, leverantörer och andra organisationer inom samma bransch, vilka kan påverka hur krav kommuniceras, tolkas och omsätts i praktiken.

Regleringar kan exempelvis fungera som drivkrafter genom att ställa krav på förändring, men även utgöra hinder beroende på hur de är utformade och implementeras (Baker, 2012).

Vidare menar Baker (2012) att externa krav kan vara föremål för tolkning, vilket innebär att organisationer själva behöver konkretisera hur dessa ska omsättas i praktiken. Detta kan bidra till variation i implementering mellan organisationer, då externa krav påverkar såväl organisatoriska som tekniska förutsättningar, särskilt i situationer där riktlinjer är otydliga eller lämnar utrymme för tolkning.

Den externa kontexten påverkar därmed hur organisationer tolkar, prioriterar och implementerar regulatoriska krav i relation till sina egna teknologiska och organisatoriska förutsättningar.

## 2.2 Analytiskt ramverk: Compliance capability

### *2.2.1 Compliance som regulatorisk och organisatorisk efterlevnad*

Compliance avser i vilken utsträckning organisationer efterlever externa krav, såsom lagar, regler och standarder, samt hur dessa krav operationaliseras genom interna regler och arbetssätt (Papazafeiropoulou ,& Spanaki, 2016). Regulatorisk efterlevnad avser därmed organisationers efterlevnad av externa krav och regelverk, medan organisatorisk efterlevnad omfattar de interna processer, strukturer och kontrollmekanismer som krävs för att omsätta dessa krav i praktiken.

Herath och Rao (2009) betonar att medarbetares efterlevnad av informationssäkerhetspolicys utgör en central del av organisationers informationssäkerhetsarbete och att sådan efterlevnad påverkas av organisatoriska mekanismer såsom styrning, kontroll, social påverkan och individers upplevda betydelse av det egna säkerhetsarbetet. Författarna framhåller vidare att compliance påverkas av både formella och informella organisatoriska mekanismer. Formella mekanismer omfattar exempelvis säkerhetspolicys, kontrollsystem och övervakning, medan informella mekanismer inkluderar organisatoriska normer, social påverkan och individers uppfattning om betydelsen av det egna säkerhetsarbetet.

Detta innebär att organisatorisk efterlevnad inte enbart handlar om implementering av tekniska eller administrativa kontrollåtgärder, utan även om organisationers förmåga att etablera organisatoriska processer och en säkerhetskultur som stödjer långsiktig efterlevnad. Organisationers förmåga att utveckla, samordna och upprätthålla sådana processer, strukturer och mekanismer över tid kan förstås som deras compliance capability.

### *2.2.2 Organisatoriska processer och compliance capability*

Compliance capability handlar därmed om organisationers förmåga att integrera regulatoriska krav i den löpande verksamheten genom styrning, riskhantering och organisatoriska processer. Detta kan relateras till ett bredare governance, risk and compliance-perspektiv (GRC), där organisationer arbetar integrerat med styrning, riskhantering och regulatorisk efterlevnad. Racz et al. (2010) beskriver GRC som ett integrerat perspektiv där organisationers processer, teknologier och organisatoriska strukturer samordnas för att hantera styrning, risk och regulatoriska krav på ett sammanhängande sätt. Racz et al. (2010) beskriver samtidigt regulatorisk efterlevnad som en central drivkraft bakom organisationers arbete med governance och riskhantering i takt med ökade regulatoriska krav och mer komplexa riskmiljöer.

Papazafeiropoulou och Spanaki (2016) betonar att detta perspektiv syftar till att skapa en helhetsbild av hur organisationens styrning och kontroll fungerar, där processer, roller och ansvar struktureras för att möjliggöra kontinuerlig övervakning och uppföljning. Compliance capability omfattar därmed organisationers samlade förmåga att utveckla, samordna och upprätthålla de resurser, processer och styrningsmekanismer som krävs för långsiktig regulatorisk och organisatorisk efterlevnad (Labadie & Legner, 2023). Detta kan även relateras till begreppet digital mognad, vilket avser organisationers förmåga att effektivt implementera och använda digitala teknologier i verksamheten (Senna et al. 2023). I relation till cybersäkerhetsrelaterade regulatoriska krav innefattar detta även cybersäkerhetsmognad, vilket omfattar organisationers förmåga att utveckla och upprätthålla organisatoriska

processer, kompetenser och säkerhetsrutiner för att hantera cybersäkerhetsrisker och långsiktig regulatorisk efterlevnad. Organisationers resurser, kompetenser och organisatoriska strukturer kan påverka deras förutsättningar att hantera digital förändring och implementering av nya cybersäkerhetsrelaterade krav (Njah et al. 2026).

Busetti och Scanni (2025) visar att implementeringen av cybersäkerhetsrelaterade regulatoriska krav påverkas av variationer i organisatorisk kapacitet mellan både organisationer och sektorer. Faktorer såsom personalbrist, begränsad teknisk kompetens, organisatorisk tröghet och resursbegränsningar kan försvåra incidenthantering, incidentrapportering och långsiktig compliance. Förutsättningarna för regulatorisk implementering påverkas därmed inte enbart av den enskilda organisationens resurser och strukturer, utan även av sektorspecifika förhållanden och varierande nivåer av cybersäkerhetsmognad inom samhällsviktiga verksamheter (Busetti & Scanni, 2025).

Teichmann (2025) framhåller vidare att implementeringen av regulatoriska cybersäkerhetskrav inte enbart är en teknisk eller juridisk fråga, utan även förutsätter organisatorisk styrning, ledningsansvar och samordning mellan olika interna och externa aktörer. Organisationer behöver därmed arbeta systematiskt med både riskhantering och organisatoriska processer för att uppnå regulatorisk efterlevnad.

Busetti och Scanni (2025) beskriver att cybersäkerhetsrelaterade regulatoriska krav i stor utsträckning bygger på incidentrapportering, informationsdelning och samordnad incidenthantering mellan organisationer och ansvariga myndigheter. Incidentrapportering fyller inte enbart en kontroll- och rapporteringsfunktion, utan kan även bidra till organisatoriskt och regulatoriskt lärande. Genom incidenthantering, informationsdelning och efterföljande analys kan organisationer utveckla förbättrade säkerhetsrutiner, stärkt riskhantering och ökad organisatorisk resiliens över tid (Busetti & Scanni, 2025). Sådana processer kan därmed även bidra till utveckling av organisationers cybersäkerhetsmognad och stärkt compliance capability genom förbättrade organisatoriska processer, riskhantering och incidenthantering.

### *2.2.3 Regulatorisk implementering och externa utmaningar*

Samtidigt kan implementeringen av regulatoriska krav medföra ytterligare organisatoriska och regulatoriska utmaningar kopplade till hur sådana krav formuleras, tolkas och omsätts i praktiken.

Veigurs et al. (2024) analyserar implementeringen av NIS2-direktivet och lyfter flera centrala risker och barriärer kopplade till hur regulatoriska krav omsätts i praktiken. En av dessa risker är så kallad compliance burden, vilket innebär att organisationer behöver avsätta omfattande resurser för att uppfylla administrativa krav såsom dokumentation, rapportering och uppföljning. Detta kan leda till att fokus förskjuts från faktisk säkerhetsförbättring till formalia, där administrativa processer prioriteras framför konkreta säkerhetsåtgärder (Veigurs et al. 2024).

Schmitz-Berndt och Schiffner (2021) beskriver samtidigt att cybersäkerhetsrelaterade regelverk kan innehålla överlappande eller delvis motstridiga rapporteringskrav, vilket kan skapa ytterligare organisatorisk och regulatorisk komplexitet vid regulatorisk implementering och organisatorisk efterlevnad. Skillnader i regulatoriska syften, rapporteringskrav och

tidsramar kan försvåra samordning mellan organisatoriska och regulatoriska processer, särskilt vid incidenthantering och informationsdelning.

Vidare visar Veigurs et al. (2024) att implementeringen av NIS2 påverkas av medlemsstaternas olika tolkningar och förutsättningar, vilket i sin tur kan leda till variation i hur regelverket omsätts nationellt. Teichmann (2025) betonar att skillnader i nationell tillsyn, samordning och implementering kan försvåra arbetet med att skapa en mer enhetlig cybersäkerhetsnivå mellan medlemsstater och sektorer.

Detta kopplas till fenomenet gold-plating, vilket enligt Squintani (2019), avser situationer där nationell implementering går längre än vad som är nödvändigt för att uppfylla EU-direktiv, exempelvis genom utvidgat tillämpningsområde, striktare krav eller mer omfattande kontroll- och sanktionsmekanismer.

Veigurs et al. (2024) betonar att detta är särskilt relevant för NIS2, eftersom direktivet medvetet innehåller en viss grad av flexibilitet, vilket ger utrymme för olika nationella tolkningar och därmed risk för ökad compliance burden. Detta kan skapa osäkerhet kring vad som utgör faktisk compliance samt leda till variation i hur regelverket implementeras mellan organisationer och medlemsstater. Exempelvis kan definitioner av kritisk infrastruktur och vilka aktörer som omfattas skilja sig åt, vilket ytterligare förstärker denna variation (Veigurs et al. 2024).

Busetti och Scanni (2025) beskriver även att otydlighet kring definitioner av rapporteringspliktiga incidenter och bedömningar av incidenters allvarlighetsgrad kan skapa variation i hur regulatoriska krav tolkas och omsätts i praktiken. Detta kan bidra till skillnader i incidentrapportering och organisatorisk efterlevnad mellan olika organisationer och sektorer.

Veigurs et al. (2024) betonar även att skillnader i nationella styrningsstrukturer, samordningsmekanismer och system för incidenthantering kan försvåra informationsdelning och hantering av cybersäkerhetsincidenter som påverkar flera organisationer eller medlemsstater samtidigt. Författarna beskriver också att NIS2 saknar tydliga mekanismer för samverkan och informationsdelning mellan verksamhetsutövare, vilket innebär att sådant samarbete i stor utsträckning blir beroende av verksamhetsutövarnas egna initiativ.

### *2.2.4 Samverkande faktorer vid regulatorisk implementering*

Regulatorisk implementering av cybersäkerhetsrelaterade krav påverkas av ett samspel mellan organisatoriska, tekniska och externa regulatoriska faktorer. Compliance omfattar både regulatorisk efterlevnad av externa krav och organisatorisk efterlevnad genom interna processer, strukturer och kontrollmekanismer (Papazafeiropoulou & Spanaki, 2016).

Organisationers förutsättningar att uppnå långsiktig regulatorisk efterlevnad påverkas därmed av resurser, kompetenser, organisatoriska processer och cybersäkerhetsmognad, men även av hur regulatoriska krav formuleras, tolkas och implementeras i praktiken (Racz et al. 2010; Senna et al. 2023; Veigurs et al. 2024). Variationer i nationell implementering, regulatorisk flexibilitet och tillsyn kan samtidigt skapa skillnader i hur sådana krav omsätts mellan organisationer och sektorer (Teichmann, 2025; Squintani, 2019; Veigurs et al. 2024).

Implementeringen kan även påverkas av överlappande regulatoriska krav, variation i incidentrapportering och otydlighet kring hur cybersäkerhetsincidenter ska bedömas och rapporteras (Schmitz-Berndt & Schiffner, 2021; Busetti & Scanni, 2025). Variationer i nationell implementering, regulatorisk flexibilitet och tillsyn kan samtidigt skapa skillnader i hur sådana krav omsätts mellan organisationer och sektorer (Teichmann, 2025; Squintani, 2019; Veigurs et al. 2024).

Compliance capability kan därmed förstås som organisationers förmåga att utveckla, samordna och upprätthålla de organisatoriska processer, resurser och styrningsmekanismer som krävs för långsiktig regulatorisk och organisatorisk efterlevnad av cybersäkerhetsrelaterade regulatoriska krav (Racz et al. 2010; Labadie & Legner, 2023).

# 3 Litteraturgenomgång

Detta kapitel behandlar centrala EU-regleringar inom informationssäkerhet och cybersäkerhet med fokus på GDPR-förordningen, NIS-direktivet och NIS2-direktivet. Under de senaste åren har dessa regleringar fått en allt större betydelse för hur organisationer inom EU arbetar med skydd av information, digitala system och hantering av säkerhetsrelaterade risker. Kapitlet syftar till att ge en översikt över centrala begrepp, regleringarnas bakgrund samt belysa hur regleringar relaterar till organisationers arbete med informationssäkerhet och cybersäkerhet.

Vidare behandlas tidigare forskning om regulatorisk implementering och hur ökade cybersäkerhetskrav påverkar verksamheter inom EU. Särskild uppmärksamhet riktas mot livsmedelssektorn, som genom NIS2-direktivet inkluderats som en samhällsviktig sektor och därmed omfattas av nya krav kopplade till cybersäkerhet, riskhantering och organisatorisk motståndskraft. I slutet av kapitlet behandlas även hur arbetet med cybersäkerhet ser ut ur ett mer tekniskt perspektiv idag och utmaningar med dessa.

## 3.1 Informationssäkerhet och cybersäkerhet

Säkerhetsarbete inom organisationer omfattar flera dimensioner där fysisk säkerhet, informationssäkerhet och cybersäkerhet tillsammans syftar till att skydda verksamheter, tillgångar, information och samhällsviktiga funktioner mot olika typer av hot och störningar (Sinha et al. 2018). Fysisk säkerhet avser skydd av exempelvis byggnader, utrustning, produktionsmiljöer och fysisk infrastruktur mot obehörig åtkomst, sabotage och andra fysiska hot. Informationssäkerhet och cybersäkerhet används ofta synonymt, även om forskning beskriver vissa begreppsliga skillnader mellan dem (von Solms & van Niekerk, 2013).

För att förstå relationen mellan begreppen behöver informationssäkerhet först definieras. Informationssäkerhet avser skydd av information utifrån principerna om konfidentialitet (Confidentiality), riktighet (Integrity) och tillgänglighet (Availability), ofta benämnt CIA-triaden. ISO/IEC 27000, som utgör en internationellt etablerad standard inom informationssäkerhet, framhåller även att autenticitet, ansvarsskyldighet och tillförlitlighet kan omfattas av begreppet informationssäkerhet. Von Solms och van Niekerk (2013) betonar

samtidigt att information kan förekomma i flera olika former, exempelvis digitalt, fysiskt och muntligt, vilket innebär att informationssäkerhet omfattar skydd av information oavsett lagrings-, behandlings- eller kommunikationsform. Informationssäkerhet blir därmed central för organisationer eftersom information betraktas som en viktig verksamhetstillgång som behöver skyddas på samma sätt som andra kritiska resurser inom verksamheten. Samtidigt framhåller både ISO/IEC 27000 och von Solms och van Niekerk (2013) att informationssäkerhet inte enbart kan uppnås genom tekniska lösningar, utan även kräver organisatorisk styrning, processer och administrativa säkerhetsåtgärder.

Cybersäkerhet relateras däremot i större utsträckning till skydd av digitala system, nätverk och tillgångar som påverkas via cyberspace. Von Solms och van Niekerk (2013) menar att cybersäkerhet går bortom traditionell informationssäkerhet eftersom begreppet inte enbart omfattar skydd av information och informationssystem, utan även skydd av individer, organisationer, fysisk infrastruktur och samhälleliga funktioner som kan påverkas av cyberrelaterade hot. Cybersäkerhet beskrivs därmed som en vidareutveckling av informationssäkerhet, där skyddet omfattar både digitala och samhälleliga tillgångar som påverkas genom cyberrymden. Denna syn ligger även i linje med NIS2-direktivets definition av cybersäkerhet, som hänvisar till artikel 2.1 i EU:s Cybersecurity ACT (Förordning (EU) 2019/881) och definierar cybersäkerhet som ”all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot” (Direktiv (EU) 2022/2555; Förordning (EU) 2019/881).

Säkerhetsarbete kan därmed förstås som ett område där fysiska, organisatoriska och digitala säkerhetsaspekter blivit allt mer integrerade, särskilt inom verksamheter som är beroende av nätverks- och informationssystem och där störningar kan påverka samhällsviktiga funktioner (Sinha et al. 2018).

## 3.2 Tidigare forskning om cybersäkerhet och regulatorisk implementering

Under de senaste åren har cybersäkerhet och informationssäkerhet fått en allt större regulatorisk betydelse inom EU, bland annat till följd av ökade cyberhot, ökad digitalisering och växande beroenden mellan organisationer, leverantörer och samhällsviktiga verksamheter. Forskning visar även att digitaliseringens fortsatta utveckling innebär att frågor kopplade till dataskydd, informationssäkerhet och hantering av digital information får en allt större betydelse för både organisationer och samhället (Rösch et al. 2019). I takt med att verksamheter blivit mer beroende av digitala nätverks- och informationssystem har även fysiska, organisatoriska och digitala säkerhetsaspekter blivit mer integrerade. Störningar eller cyberincidenter kan därmed påverka såväl produktion som logistik, leveranskedjor och informationshantering. EU har därmed infört ett flertal omfattande regleringar inom dataskydd, informationssäkerhet och cybersäkerhet i syfte att stärka säkerhet, riskhantering och motståndskraft inom medlemsstaterna.

### *3.2.1 GDPR*

Ett centralt exempel är General Data Protection Regulation (GDPR). I enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 trädde regelverket i kraft 2018 med syftet att skapa gemensamma regler för dataskydd inom EU och stärka skyddet av

personuppgifter. Labadie och Legner (2023) beskriver GDPR som en central del av EU:s strategi för att stärka individers kontroll över sina personuppgifter och skapa ökat förtroende för digital informationshantering. GDPR utgör en horisontell reglering, vilket innebär att regelverket tillämpas brett över flera sektorer och verksamhetstyper inom både offentlig och privat sektor vid behandling av personuppgifter (Förordning (EU) 2016/679).

Regleringen innebar ett omfattande skifte för många organisationer, då förordningen ställde ökade krav på bland annat informationshantering, dokumentation, ansvarsfördelning och hantering av personuppgifter (Labadie & Legner, 2023). Detta omfattade bland annat principer för behandling av personuppgifter, såsom transparens, ändamålsbegränsning och lagringsbegränsning, samt krav på tekniska och organisatoriska säkerhetsåtgärder för att säkerställa ”förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna” (Förordning (EU) 2016/679, artikel 32). GDPR introducerade även krav på rapportering av personuppgiftsincidenter till tillsynsmyndigheter och i vissa fall även till berörda individer, vilket ställde ökade krav på organisationers incidenthantering, riskbedömning och interna rapporteringsprocesser (Förordning (EU) 2016/679; Schmitz-Berndt & Schiffner, 2021).

Förordningen innehåller omfattande sanktioner vid bristande efterlevnad, där avgifter i vissa fall kan uppgå till 20 miljoner euro eller fyra procent av en organisations globala årsomsättning (Förordning (EU) 2016/679). De höga sanktionsavgifterna bidrar därmed till ett ökat regulatoriskt tryck på organisationer att implementera dataskydds- och säkerhetsåtgärder.

Labadie och Legner (2023) beskriver att implementeringen av GDPR ofta krävde anpassningar av organisationers befintliga informationssystem och processer. Regleringen specificerade samtidigt inga exakta implementeringslösningar, vilket innebar att organisationerna själva behövde tolka och anpassa dem till sina egna verksamheter (Labadie & Legner, 2023; Rösch et al. 2019). Detta skapade ett behov av både tekniska och organisatoriska anpassningar för att omsätta regleringens krav i praktiken. Labadie och Legner (2023) beskriver vidare att implementeringen av regulatoriska krav inte enbart handlar om juridisk efterlevnad, utan även om organisationers förmåga att skapa organisatoriska och tekniska förutsättningar för att omsätta kraven i praktiken.

### *3.2.2 NIS-direktivet*

Ett annat exempel på EU-reglering inom informationssäkerhetsområdet är Network and Information Systems Directive (NIS-direktivet), Europaparlamentets och rådets direktiv (EU) 2016/1148, som antogs 2016 och utgör föregångaren till NIS2-direktivet. Direktivet syftade till att uppnå en gemensam hög nivå av säkerhet i nätverks- och informationssystem inom EU, bland annat genom krav på säkerhetsåtgärder och incidentrapportering för verksamhetsutövare inom samhällsviktiga sektorer (Direktiv (EU) 2016/1148).

NIS-direktivet innefattade följande sju samhällsviktiga sektorer:

1. Energi
2. Transport
3. Bankverksamhet
4. Finansmarknadsinfrastruktur
5. Hälso- och sjukvård
6. Dricksvatten

7. Digital infrastruktur

(Direktiv (EU) 2016/1148, bilaga II)

Livsmedelssektorn omfattades därmed inte som en samhällsviktig sektor inom ramen för NIS-direktivet.

Vandezande (2024) beskriver NIS-direktivet som ett betydande steg i utvecklingen av EU:s cybersäkerhetspolitik, då direktivet etablerade gemensamma cybersäkerhetskrav och samarbetsmekanismer mellan medlemsstaterna. Samtidigt visar tidigare forskning att implementeringen av direktivet skiljde sig åt mellan medlemsstaterna, vilket delvis berodde på att medlemsstaterna gavs relativt stort utrymme att utforma nationella strategier och implementera direktivets krav utifrån nationella förutsättningar (Markopoulou et al. 2019).

Detta bidrog enligt Vandezande (2024) till variation i hur cybersäkerhetskraven omsattes nationellt, vilket skapade ojämna förutsättningar mellan medlemsstaterna och bristande beredskap inför nya och föränderliga cybersäkerhetshot. Detta lyftes som en viktig bakomliggande faktor till att NIS-direktivet upphävdes den 18 oktober 2024 och ersattes av NIS2-direktivet, vilket syftade till att skapa en mer omfattande och harmoniserad cybersäkerhetsreglering inom EU.

### *3.2.3 NIS2 och livsmedelssektorn*

NIS2-direktivet (Direktiv (EU) 2022/2555) speglar en bredare syn på vilka sektorer och verksamheter som anses samhällsviktiga ur ett cybersäkerhetsperspektiv inom EU. Detta innebar bland annat att antalet omfattade sektorer utökades från sju till arton, däribland livsmedelssektorn, samt att de omfattade verksamheterna vidare delades in i kategorierna väsentliga och viktiga verksamheter (essential och important entities).

Kategoriseringen innebär skillnader i tillsyn, regulatoriskt ansvar och potentiella sanktionsavgifter, där väsentliga verksamheter omfattas av mer omfattande tillsynsåtgärder och striktare regulatoriska krav än viktiga verksamheter.

Enligt direktivets bilaga II inkluderas verksamheter inom produktion, bearbetning och distribution av livsmedel inom livsmedelssektorn och klassificeras huvudsakligen som viktiga verksamheter. Direktivet ger dock medlemsstaterna möjlighet att omklassificera vissa aktörer från viktiga till väsentliga verksamheter (Direktiv (EU) 2022/2555 Bilaga II).

Den utvidgade inkluderingen av livsmedelssektorn i NIS2-direktivet kan relateras till sektorns ökade digitalisering och beroende av integrerade informations- och produktionssystem.

Annosi et al. (2020) betonar att livsmedelssektorn präglas av omfattande digitalisering och integration mellan digitala och fysiska processer, där produktion, bearbetning, logistik och distribution i allt högre grad är beroende av digitala system och informationsflöden. Forskning visar att sådana integrerade miljöer kan skapa ökade attackytor och ökad sårbarhet för cyberincidenter (Kannelønning & Katsikas, 2024). Detta innebär att störningar i ett system kan få konsekvenser för flera delar av verksamheten samtidigt, vilket ökar komplexiteten i arbetet med cybersäkerhet och compliance.

NIS2-direktivet innebär även ett ökat fokus på leverantörskedjor och tredjepartsrisker (Direktiv (EU) 2022/2555), vilket är särskilt relevant inom livsmedelssektorn där beroenden mellan produktion, logistik och externa tjänsteleverantörer kan vara omfattande. Störningar i sådana beroenden kan få konsekvenser för både livsmedelssäkerhet och samhällsförsörjning.

Annosi et al. (2020) beskriver livsmedelssektorn som heterogen, där verksamheter kan ha varierande organisatoriska och tekniska förutsättningar för digitalisering. Detta kan bero på skillnader i kompetens, resurser och teknologisk beredskap, vilket i sin tur kan relateras till hur organisationers digitala mognad och cybersäkerhetsmognad påverkar deras förutsättningar att hantera regulatoriska krav såsom NIS2-direktivet.

### *3.2.4 Tekniska förutsättningar och säkerhetsanpassningar*

#### *3.2.4.1 Legacy-system och teknologiska anpassningar*

Som beskrivet i teorikapitlet kan befintliga teknologiska system både möjliggöra och begränsa införandet av nya lösningar (Baker, 2012). En ytterligare dimension ges av att livsmedelssektorn, med ett beroende av cyber-fysiska system, ofta har en tät integration mellan IT och OT. Medan konventionell IT-säkerhet vilar på CIA-triaden (konfidentialitet, integritet, tillgänglighet), är prioritetsordningen i OT-miljöer ofta den omvända (Mosteiro-Sanchez et al. 2020), vilket återspeglas i Figur 3.1.

| Priority level | OT | IT |
|---|---|---|
| 1 | Availability | Confidentiality |
| 2 | Integrity | Integrity |
| 3 | Confidentiality | Availability |

**Figur 3.**1 Prioritisation of security requirements for IT and OT networks (Mosteiro-Sanchez et al. 2020, s.368)

För livsmedelsföretag är OT-systemen ofta avgörande för produktionen och även korta avbrott kan riskera säkerhet, miljö och ekonomi (Makrakis et al., 2021). Studier belyser att implementering av standardmässiga IT-kontroller som exempelvis systemuppgraderingar eller patchningar inte är applicerbara inom OT-miljöer, eftersom byten eller experimenterande med konfigurationer kan leda till driftstopp eller latens i tidskritiska processer, vilket kan leda till stora ekonomiska konsekvenser (Mosteiro-Sanchez et al., 2020; Makrakis et al., 2021).

Historiskt sett har OT-system isolerats nätverksmässigt, och på grund av detta har det saknats incitament att bygga in säkerhetsfunktioner från start (Makrakis et al. 2021). Detta märker man konsekvenserna av idag. Inbyggda begränsningar innebär att det är svårt att implementera moderna kontroller i systemen, särskilt när de körs på föråldrade operativsystem eller integreras med egenutvecklad hårdvara (Mosteiro-Sanchez et al. 2020; Makrakis et al. 2021; Shewale, 2025).

System som är svåra att underhålla men fortfarande fyller en funktion i verksamheten kan refereras till som legacy-system, och förändringar i krav kräver ofta omfattande anpassningar av dem (Baker, 2012). Forskare framhåller att arbetet med det tekniska säkerhetsarbetet i legacy OT-system ofta tar sig uttryck i arkitektoniska skydd runtomkring, såsom brandväggar, nätverksövervakning, segmentering och fysiskt skydd (Wai & Lee, 2023), vilket är bitar som överlappar med hur organisationer arbetar med informationssäkerhet generellt idag.

ISO 27001 är den etablerade standarden för informationsäkerhet (Culot et al. 2021), och NIST Cyber Security Framework (CSF) är ett av de globalt mest erkända ramverken (Salas-Riega et al. 2025). I en syntes av dessa lyfts det fram att nätverks- och mjukvarusäkerhet är en ömsesidigt central kontrollkategori, tillsammans med accesskontroll, övervakning och nätverksskydd, såsom segmentering och brandväggar (Tanjung et al. 2024). Ett modernt sätt att förstärka försvaret av ett system beskrivs som "defense in depth", där flera av skikten, bland annat kompletterat med loggning, kombineras för att hantera riskerna när system inte kan göras säkra i sig själva (Chandra et al. 2015). Även Zero Trust-principer som minsta behörighet (Principle of Least Privilege) och kontinuerlig autentisering lyfts fram som sätt att begränsa lateral rörelse (Narayanan et al. 2026).

Studier om IT och OT-miljöer beskriver även en trend i teknologisk förflyttning från proprietära legacy-lösningar till standardiserade plattformar och molnbaserade tjänster, ofta levererade av specialiserade leverantörer (Hajra & Goel, 2025; Bhamare et al. 2020). I sådana miljöer kan säkerhetskontroller implementeras mer enhetligt och skalbart, exempelvis genom konsekvent kryptering, rollbaserad åtkomstkontroll, central loggning och standardiserad patchhantering (Nankya et al. 2023; Sharma, 2025).

Fördelen gällande standardiserade molnbaserade lösningar beskrivs vara att dessa kan upprätthålla en hög säkerhetsnivå genom certifieringsramverk som exempelvis ISO 27001, automatiserade uppdateringar och centraliserad övervakning, vilket minskar beroendet av lokalt förvaltade legacy-plattformar (Khokrale, 2025).

Utöver att höja den rent tekniska säkerhetsnivån fungerar etablerade branschstandarder som ett verktyg för att hantera en alltmer komplex global lagstiftning gällande dataskydd och informationssäkerhet. Rakshan (2025) framhåller att ISO 27001 erbjuder en tillgänglig och globalt erkänd struktur för företag att systematiskt möta och efterleva dessa strikta regulatoriska krav. Detta stöds även av Folorunso et al. (2024), som betonar att införandet av ISO-standarder inte bara förbättrar riskhantering och incidentberedskap utan även stärker organisationers anpassning till regulatoriska ramverk såsom GDPR. Inom OT-området argumenteras det på ett liknande sätt för att en anpassning till specifika branschramverk, däribland IEC 62443, ger betydligt bättre förutsättningar och strukturellt stöd för att möta moderna regulatoriska krav (de Freitas et al. 2025).

Samtidigt framhålls leverantörsinlåsning och integrationsberoenden som en konsekvens av standardiserade applikationer. Beroendet av en leverantörs säkerhetsmodell, livscykel och licensregim kan begränsa flexibiliteten och göra framtida migreringar kostsamma (Hustad et al. 2021, Opara-Martins et al, 2016).

## 3.3 Sammanfattning av litteraturgenomgång

Litteraturgenomgången visar att cybersäkerhet och informationssäkerhet fått en allt större regulatorisk betydelse inom EU till följd av ökad digitalisering, växande beroenden mellan organisationer samt ett ökat behov av att skydda samhällsviktiga funktioner (Rösch et al. 2019; Sinha et al. 2018). Tidigare forskning beskriver informationssäkerhet som skydd av information utifrån principerna om konfidentialitet, riktighet och tillgänglighet, medan cybersäkerhet även omfattar skydd av digitala system, nätverk och samhälleliga funktioner som påverkas av cyberrelaterade hot (von Solms & van Niekerk, 2013).

Vidare beskriver litteraturen att implementeringen av GDPR och NIS-direktivet inneburit omfattande organisatoriska och tekniska förändringar för många verksamheter inom EU (Labadie & Legner, 2023; Vandezande, 2024). Tidigare forskning visar även att implementeringen av regulatoriska krav ofta präglas av organisatoriska anpassningar, nationella variationer och osäkerhet kring hur regelverk ska tolkas och omsättas i praktiken (Markopoulou et al. 2019; Rösch et al. 2019).

Litteraturen indikerar även att NIS2-direktivet innebär en utvidgning av EU:s cybersäkerhetsreglering där livsmedelssektorn för första gången tydligt inkluderas som samhällsviktig sektor (Direktiv (EU) 2022/2555). Livsmedelssektorn präglas samtidigt av omfattande digitalisering, cyber-fysiska beroenden och komplexa leverantörskedjor, vilket kan öka sårbarheten för cyberincidenter och skapa särskilda utmaningar kopplade till cybersäkerhet och regulatorisk efterlevnad (Annosi et al. 2020; Kannelønning & Katsikas, 2024).

Den tekniska integrationen mellan IT och OT, där driftsäkerhet och tillgänglighet prioriteras framför konventionell datakonfidentialitet (Mosteiro-Sanchez et al. 2020), komplicerar arbetet. Att möta nya regulatoriska krav försvåras ofta av äldre, så kallade legacy-system med inbyggda tekniska begränsningar som omöjliggör standardmässig patchhantering och uppgradering (Makrakis et al. 2021). Litteraturen pekar därför på en teknologisk förflyttning mot molnbaserade SaaS-lösningar och införandet av ramverk som ISO 27001 och IEC 62443 för att uppnå både en skalbar "defense-in-depth"-arkitektur och strukturerad regelefterlevnad (Rakshan, 2025; de Freitas et al. 2025). Samtidigt medför denna standardisering nya risker i form av leverantörsinlåsning och minskad flexibilitet (Hustad et al. 2021). Organisationers varierande resurser, kompetenser och digitala mognad kan dessutom påverka deras förutsättningar att implementera och upprätthålla cybersäkerhetsrelaterade regulatoriska krav.

# 4 Metod

I detta kapitel presenteras hur relevant litteratur har identifierats och valts ut, följt av studiens forskningsansats, datainsamling och analysmetod. Avslutningsvis redogörs för de etiska överväganden som gjorts.

## 4.1 Litteratururval

Litteratur till studiens teori- och litteraturkapitel identifierades genom sökningar via Finn, Lunds universitets biblioteksportal, samt genom kompletterande sökningar i Google Scholar och ResearchGate. För mer riktade sökningar inom cybersäkerhet och informationssystem användes databaser och publikationsplattformar såsom ACM Digital Library och IEEE Xplore. Vetenskapliga artiklar identifierades även genom sökningar i enskilda vetenskapliga tidskrifter, däribland Management Decision.

Urvalet av litteratur avgränsades huvudsakligen till peer review-granskade publikationer samt vetenskapligt etablerade böcker och konferenspublikationer.

I Tabell 4.1 presenteras övergripande exempel på sökord som användes vid litteratursökningarna. Sökorden användes både separat och i olika kombinationer för att identifiera relevant litteratur inom studiens forskningsområden.

**Tabell 4.1** Övergripande sökord för litteraturinsamling

| Ämne | Exempel på sökord |
|---|---|
| TOE-ramverket | "TOE", "TOE framework", "Technology–Organization–Environment framework" |
| Digital mognad | "digital maturity", "digital transformation" "DMM", digital maturiy model", "cybersecurity maturity" |
| Informationssäkerhet och cybersäkerhet | "information security and cybersecurity", "cybersecurity definition" |
| Compliance | "Compliance", GRC", "regulatory compliance", "organizational compliance", "compliance capability" |
| GDPR | "GDPR", "GDPR compliance", "EU data protection law" |
| NIS, NIS2 | "NIS", "EU regulation", "EU cybersecurity", "NIS2" |
| Livsmedelssektorn och cyberssäkerhet | "food industry cybersecurity", "cyber physical systems" |
| Tekniska förutsättningar och säkerhetsanpassningar | "legacy systems", "operational technology security", "legacy infrastructure adaptation", "CIA triad", "cyber physical systems security" |

Relevanta publikationer identifierades i vissa fall även genom genomgång av referenslistor och återkommande hänvisningar i tidigare identifierad litteratur. Inom litteratur relaterad till TOE-ramverket framstod exempelvis Tornatzky och Fleischer (1990) samt Baker (2012) som återkommande refererade verk, vilket bidrog till att dessa valdes som teoretiska utgångspunkter i studien.

För att bedöma publikationernas vetenskapliga kvalitet användes även Kanalregistret. De vetenskapliga publikationer som inkluderades i studien publicerades i etablerade vetenskapliga tidskrifter och konferenser motsvarande minst nivå 1 i Kanalregistret.

Utöver vetenskapliga publikationer inkluderades även relevanta lagtexter, EU-direktiv och förordningar som centrala källor för studiens regulatoriska kontext.

I Tabell 4.2 och Tabell 4.3 presenteras en översikt över centrala forskningsområden och tillhörande källor inom studiens teoretiska referensram och litteraturgenomgång.

**Tabell 4.2** Källor inom den teoretiska referensramen

| Teoretisk referensram | |
|---|---|
| **Område** | **Källor** |
| TOE-ramverket | Tornatzky & Fleischer (1990); Baker (2012) |
| Compliance som regulatorisk och organisatorisk efterlevnad | |

| | |
|---|---|
| | Papazafeiropoulou & Spanaki (2016); Racz et al. (2010)g |
| Organisatoriska processer och compliance capability | Racz et al. (2010); Labadie & Legner (2023); Senna et al. (2023); Njah et al. (2026) |
| Regulatorisk implementering och externa utmaningar | Veigurs et al. (2024); Schmitz-Berndt & Schiffner (2021); Squintani (2019); Teichmann (2025); Busetti & Scanni (2025) |

**Tabell 4.3** Källor för litteraturgenomgång

| **Litteraturgenomgång** | |
|---|---|
| **Område** | **Källor** |
| Informationssäkerhet och cybersäkerhet | von Solms & van Niekerk (2013); Direktiv (EU) 2022/2555; Förordning (EU) 2019/881; Sinha et al. 2015 |
| GDPR | Förordning (EU) 2016/679; Labadie & Legner (2023); Rösch et al. (2019); Schmitz-Berndt & Schiffner (2021) |
| NIS-direktivet | Direktiv (EU) 2016/1148; Vandezande (2024); Markopoulou et al. (2019) |
| NIS2 och livsmedelssektorn | Direktiv (EU) 2022/2555; Annosi et al. (2020); Smetana et al. (2021); Kannelønning & Katsikas (2024); Veigurs et al. (2024) |
| Tekniska förutsättningar och säkerhetsanpassningar | Baker (2012); Bhamare et al. (2020); Chandra et al. (2015); Culot et al. (2021); de Freitas et al. (2025); Folorunso et al. (2024); Hajra & Goel (2025); Hustad et al. (2021); Khokrale (2025); Makrakis et al. (2021); Mosteiro-Sanchez et al. (2020); Nankya et al. (2023); Narayanan et al. (2026); Opara-Martins et al. (2016); Rakshan (2025); Salas-Riega et al. (2025); Sharma (2025); Shewale (2025); Tanjung et al. (2024); Wai & Lee (2023) |

## 4.2 Forskningsmetod

Studien tillämpar en kvalitativ forskningsansats inom ett interpretivistiskt paradigm, vilket Oates et al. (2022) menar innebär att forskningen syftar till att förstå den sociala kontexten snarare än att testa hypoteser. Inom detta paradigm betraktas verkligheten som socialt konstruerad, där individer och grupper tillskriver fenomen olika innebörder beroende på sin egen kontext.

Mot bakgrund av detta är en kvalitativ ansats lämplig för studiens syfte. Oates et al. (2022) beskriver hur en kvalitativ ansats lämpar sig när forskningsfrågans fokus ligger på mening, upplevelse och förståelse snarare än kvantifierbara utfall. För att fånga hur organisationer uppfattar och resonerar kring ett fenomen krävs enligt Oates et al. (2022) tillgång till respondenternas egna beskrivningar. Creswell (2014) lyfter vidare att kvalitativ forskning lämpar sig när forskningsprocessen är av framväxande karaktär, det vill säga när det initiala upplägget inte kan förutbestämmas i detalj eftersom fenomenet är relativt outforskat. Cybersäkerhetslagen trädde i kraft i januari 2026, vilket innebär att organisationers anpassning till lagen är ett nytt fenomen med begränsad dokumentering och således lämpar sig för explorativ kvalitativ undersökning.

En kvantitativ ansats har bedömts som olämplig för studiens syfte. Creswell (2014) beskriver kvantitativ forskning som ett tillvägagångssätt för att testa objektiva teorier genom att undersöka mätbara relationer mellan variabler. Detta förutsätter att det som studien avser studera kan operationaliseras och kvantifieras. Organisationers upplevelser av och förhållningssätt till cybersäkerhetslagen kan inte fångas på ett sådant sätt, således är en kvalitativ ansats det mer lämpliga valet för att uppnå denna studies syfte.

## 4.3 Datainsamling

Studiens primärdata samlades in genom individuella semistrukturerade intervjuer. Intervjuer är en fördelaktig datainsamlingsmetod när studien söker detaljerad information, när erfarenheter och uppfattningar undersöks som inte kan fångas genom fördefinierade svarsalternativ samt när komplexa frågor ställs som kräver följdfrågor och fördjupning (Oates et al. 2022). Den semistrukturerade intervjuformen valdes då den ger respondenten möjlighet att utveckla sina svar och lyfta aspekter som inte har förutsetts, samtidigt som intervjun styrs av på förhand bestämda teman (Oates et al. 2022). I enlighet med Creswell (2014) kännetecknas kvalitativa intervjuer av öppna och flexibla frågor, vilket möjliggör för deltagarna att uttrycka sina egna perspektiv och erfarenheter.

### *4.3.1 Val av organisationer*

Organisationerna har valts genom purposive sampling, vilket Oates et al. (2022) beskriver som att forskaren medvetet väljer fall som sannolikt kan bidra med värdefulla data för studiens syfte. Urvalet har baserats på Livsmedelsverkets (2026) vägledning i enlighet med studiens avgränsningar (se avsnitt 1.5). Inom denna ram har studien riktat in sig på stora verksamhetsutövare, då dessa bedöms ha etablerade strukturer för informationssäkerhetsarbete samt ha påbörjat implementeringsarbetet till följd av cybersäkerhetslagen. Således bedöms deras erfarenheter och uppfattningar vara relevanta för studiens syfte.

### *4.3.2 Val av informanter*

Personer med relevanta roller inom de utvalda organisationerna identifierades genom organisationernas hemsidor samt LinkedIn, varefter kontakt etablerades via e-post. I de fall e-postadress saknades togs kontakt direkt via LinkedIn. I vissa fall hänvisades studien vidare till en annan person inom organisationen som bedömdes mer lämpad att besvara studiens frågor,

vilket Oates et al. (2022) beskriver som snowball sampling. Samtliga informanter innehar det operativa ansvaret för organisationens arbete med cybersäkerhetslagen och bedöms därmed besitta den insyn som krävs för att uttala sig om hur organisationen förhåller sig till lagens krav. De specifika yrkesrollerna anges inte då dessa i kombination med övriga uppgifter om organisationen skulle kunna bidra till identifiering av enskilda individer. En av intervjuerna genomfördes med två informanter gemensamt, vilka benämns IP1a och IP1b i studien.

En av de kontaktade organisationerna hänvisade vid kontakt vidare till den medarbetare på koncernnivå som bedömdes bäst lämpad att besvara studiens frågor. Denna informant är verksam utanför Sverige och benämns IP4 i studien. Intervjumaterialet från denna intervju behandlas därför som ett kompletterande perspektiv snarare än en del av det svenska empiriska underlaget, med beaktande av att den regulatoriska kontexten skiljer sig från den svenska.

En fullständig deltagarförteckning återfinns i Tabell 4.4.

**Tabell 4.4** Deltagarförteckning

| Intervju | Informant | Företag | Kategori | Intervjuguide | Intervjuform | Tid |
|---|---|---|---|---|---|---|
| Intervju 1 | IP1a<br>IP1b | F1 | Distribution, Produktion och Bearbetning | Intervjuguide 1 | Fysisk & kompletterad skriftligen av IP1a | 1h 37 min |
| Intervju 2 | IP2 | F2 | Distribution, Produktion och Bearbetning | Intervjuguide 1 | Zoom | 1h 12 min |
| Intervju 3 | IP3 | F3 | Distribution, Produktion och Bearbetning | Intervjuguide 1 | Teams | 53 min |
| Intervju 4 | IP4 | F4 | Distribution, Produktion och Bearbetning | Intervjuguide 2 | Zoom | 49 min |
| Intervju 5 | IP5 | F5 | Distribution, Produktion och Bearbetning | Intervjuguide 1 | Zoom | 45 min |
| Intervju 6 | IP6 | F6 | Distribution, Produktion och Bearbetning | Intervjuguide 1 | Fysisk | 51 min |

### *4.3.3 Intervjuguide*

En intervjuguide har utformats med utgångspunkt i TOE-ramverkets tre kontexter, teknologisk, organisatorisk och extern, vilket presenteras i kapitel 2. Den teknologiska kontexten kopplar till frågor om teknisk anpassningsbarhet, där Baker (2012) betonar att befintliga system både kan möjliggöra och begränsa implementeringen av nya krav. Den organisatoriska kontexten kopplar till frågor om intern samordning och ledningens roll, där Teichmann (2025) framhåller att regulatorisk implementering förutsätter organisatorisk styrning och tydlig ansvarsfördelning. Den externa kontexten kopplar till frågor om tolkning av MCF:s föreskrifter och incidentrapportering, då Baker (2012) uppger att externa krav kan vara föremål för tolkning och att organisationer själva behöver konkretisera hur dessa ska omsättas i praktiken. Detta speglar även de utmaningar kopplade till compliance burden och otydliga rapporteringskrav som Veigurs et al. (2024) identifierade vid implementeringen av NIS2-direktivet.

Frågorna är öppna för att möjliggöra utvecklade svar och ordningen följer en utveckling från allmänna bakgrundsfrågor till mer specifika teman. Känsligare frågor placeras medvetet senare i intervjun, då Oates et al. (2022) framhäver vikten av att etablera förtroende hos respondenten för att möjliggöra öppna och ärliga svar. Frågorna har även utformats med hänsyn till de utmaningar som identifieras vid implementeringen av NIS-direktivet, där bristande tydlighet från nationella myndigheter och ökade resurskrav visade sig vara återkommande problem (ENISA, 2020).

Intervjuguiden utformades med utgångspunkt i TOE-ramverkets tre kontexter i ett tidigt skede av forskningsprocessen. Compliance capability fastställdes som studiens analytiska ramverk först i ett senare skede, vilket är förenligt med den framträdande karaktär som kännetecknar kvalitativ forskning, där studiens analytiska ansats kan förändras dynamiskt under studiens gång (Creswell, 2014). Frågorna bedöms dock fånga de aspekter som identifieras i compliance-ramverket, såsom compliance burden, incidentrapportering och organisatorisk efterlevnad. Materialet bedöms därför vara lämpat för analys utifrån båda perspektiven.

En av intervjuerna genomfördes med en informant verksam utanför Sverige. En anpassad intervjuguide utformades inför denna intervju, där frågorna formulerades med utgångspunkt i NIS2-direktivet snarare än den svenska cybersäkerhetslagen, med hänsyn till att den regulatoriska kontexten skiljer sig från den svenska. Frågor som specifikt berör MCF och cybersäkerhetslagen exkluderades.

## 4.4 Analysmetod

Intervjuerna transkriberades med hjälp av transkriberingsverktyg, där Sunet Scribe användes för de svenska intervjuerna och Whisper för den intervju som inte genomfördes på svenska, då det senare verktyget visade sig vara mer lämpat för det aktuella språket. För en av intervjuerna genomförda på svenska saknas ljudinspelning, då informantens organisations integritetsregler endast tillät informanten själv att spela in i samtalet via Microsoft Teams, vilket var den plattform som intervjun genomfördes på. Transkriberingen sköttes därför via Teams inbyggda transkriberingsverktyg och skickades till studiens författare i efterhand.

Övriga transkriberingar genomlästes i sin helhet och kontrollerades mot ljudinspelningarna, varvid enstaka felaktigt återgivna ord och felaktigt tillskrivna talare korrigerades. Ingen språklig anpassning har gjorts av transkriberingarna. Vid användning av citat i analysen har irrelevanta passager och fyllnadsord utelämnats och markerats med tre punkter i följd (…), vilket är en redigering som Oates et al. (2022) påpekar är acceptabel under förutsättningen att innebörden inte förändras.

Det insamlade materialet analyseras genom en hybrid tematisk analys som kombinerar deduktiva och induktiva inslag. Creswell (2014) beskriver att forskare kan välja att antingen utveckla koder enbart utifrån det insamlade materialet, använda förutbestämda koder baserade på teori eller tillämpa en kombination av de båda. Oates et al. (2022) betonar vikten av att inte vara alltför bunden till ett givet teoretiskt ramverk då detta kan orsaka att andra teman i materialet förbises. Analysen har därför hållits öppen för teman som vuxit fram induktivt ur materialet.

TOE-ramverkets tre kontexter, teknologisk, organisatorisk och extern, utgör den strukturella grunden för analysen. Compliance-ramverket utgör den teoretiska ansatsen och används för att tolka och förstå de mönster som identifieras inom respektive kontext. Analysprocessen inleddes med att en överblick skapades genom att hela materialet lästes igenom i sin helhet. Därefter identifierades relevanta segment vilka sedan kodades och grupperades i kategorier och teman i enlighet med de steg Creswell (2014) beskriver. Analysprocessen dokumenterades löpande i ett strukturerat kodningsprotokoll i Excel med kolumnerna TOE-kontext, tema, kategori, informant och citat. Oates et al. (2022) rekommenderar användning av visuella hjälpmedel såsom tabeller för att synliggöra analysens steg och möjliggöra upprepning av studien, vilket kodningsprotokollet utgör. En förenklad översikt över analysens tematisering, exklusive informant och citat, presenteras i Tabell 4.5.

**Tabell 4.5** Kodningsschema

| TOE-kontext | Tema | Kategori |
|---|---|---|
| **Teknologisk** | Tekniska förutsättningar och säkerhetsanpassning | Legacy System |
| | | Teknologisk förändring till följd av cybersäkerhetslagen |
| **Organisatorisk** | Compliance: organisatorisk börda och kapacitet | Compliance- och administrativ börda |
| | | Syn på den egna organisationens nuvarande compliance i relation till NIS2 |
| | Regulatoriska krav som intern förändringskraft | Interna vs externa initiativ |
| | | Cybersäkerhetslagen som regulatorisk katalysator |
| | | Regulatoriska kravs påverkan på informationssäkerhetsrollen |
| | | Hur organisationen arbetar med informationssäkerhet |

| | | |
|---|---|---|
| | Säkerhetsarbete: förhållningssätt och arbetssätt | Förhållningssätt: Arbete med informationssäkerhet |
| | | Organisationsledningens roll |
| | | Samordning informationssäkerhet |
| **Extern** | Navigering i det regulatoriska landskapet | Otydliga krav gällande incidentrapportering |
| | | Gold-Plating |
| | | Dialog med tillsynsmyndigheter |
| | | Branschsamverkan och erfarenhetsutbyte |
| | Ojämna förutsättningar och delat samhällsansvar | Konkurrenspåverkan |
| | | Roll i totalförsvaret |

Vid tidpunkten för intervjuernas genomförande hade de slutgiltiga föreskrifterna från MCF ännu inte fastställts, varför informanterna i flera fall refererar till NIS2-direktivet snarare än till cybersäkerhetslagen specifikt. Cybersäkerhetslagen utgör den svenska implementeringen av NIS2-direktivet och informanterna har i stor utsträckning använt begreppen synonymt. Kodningen har därför skett utifrån det fenomen som beskrivs snarare än vilket begrepp informanten använder, med undantag för de fall där informanter uttryckligen diskuterar skillnader mellan direktiv och lag, exempelvis avseende nationella tillägg som går utöver direktivets minimikrav.

Materialet från den intervju som genomfördes med informanten som är verksam utanför Sverige har kodats och kategoriserats på samma sätt som övriga intervjuer, eftersom de fenomen som beskrivs bedöms vara jämförbara med de svenska informanternas erfarenheter. Intervjumaterialet behandlas dock som ett kompletterande perspektiv och ingår inte i det svenska empiriska underlaget.

## 4.5 Tillförlitlighet och giltighet

### *4.5.1 Intern giltighet*

Creswell (2014) beskriver att kvalitativ validitet innebär att forskaren kontrollerar fyndens riktighet genom att tillämpa vissa procedurer. Intervjufrågorna utformades med utgångspunkt i TOE-ramverkets tre kontexter och tidigare forskning om implementering av cybersäkerhetsrelaterade EU-regleringar, vilket säkerställer att frågorna är direkt kopplade till studiens forskningsfråga. Urvalet av informanter har säkerställt att samtliga respondenter besitter direkt insyn i eller ansvar för det fenomen som studien undersöker, vilket stärker den interna giltigheten. Handledningssamtal vid Lunds universitet har genomförts under forskningsprocessen, vilket utgör en form av det Creswell (2014) beskriver som peer debriefing. Informanternas utsagor presenteras konsekvent som subjektiva upplevelser snarare än faktapåståenden, och citat återges i sitt ursprungliga sammanhang för att säkerställa att

innebörden inte förändrats genom utelämningar eller redigering, i enlighet med Oates et al. (2022) krav på att forskaren inte manipulerar materialet för att stödja ett visst argument.

### *4.5.2 Extern giltighet*

Extern giltighet avser i vilken utsträckning studiens resultat kan generaliseras till andra sammanhang. Creswell (2014) betonar att kvalitativa studier sällan möjliggör full generaliserbarhet, men att en tillräckligt detaljerad beskrivning av kontexten gör det möjligt för läsaren att bedöma om fynden är relevanta i ett liknande sammanhang. Studiens urval är begränsat till sex stora verksamhetsutövare inom den del av den svenska livsmedelssektorn som omfattas av cybersäkerhetslagen, vilket innebär att generaliserbarheten till andra delar av sektorn bör beaktas med försiktighet. Det intervjumaterial som inte genomfördes på svenska behandlas som ett kompletterande perspektiv och ingår inte i det svenska empiriska underlaget, varför det inte påverkar studiens externa giltighet avseende den svenska kontexten.

### *4.5.3 Tillförlitlighet*

Creswell (2014) anger att kvalitativ reliabilitet innebär att forskarens tillvägagångssätt är konsekvent. Samma intervjuguide användes för samtliga svenska informanter. För den intervju som inte genomfördes på svenska anpassades intervjuguiden med hänsyn till att den regulatoriska kontexten skiljer sig från den svenska. Intervjulängderna varierade mellan 45 minuter och 1 timme 37 minuter, vilket kan ha påverkat djupet i det insamlade materialet för olika informanter. Transkriberingarna har genomlästs och kontrollerats för att minimera risken för felaktig återgivning av materialet, i enlighet med Gibbs (2007, citerad i Creswell, 2014) rekommendation.

## 4.6 Etik

Inför intervjuernas genomförande inhämtades samtycke från samtliga informanter. Informanterna informerades om studiens syfte, hur materialet kommer att användas samt att deltagandet är frivilligt och kan avbrytas när som helst, i enlighet med de principer för informerat samtycke och deltagarrättigheter som Oates et al. (2022) beskriver. Samtycke till inspelningen inhämtades muntligen innan intervjun påbörjades.

En av intervjuerna genomfördes inte på svenska, således analyserades transkriberingen på originalspråket och enskilda citat översattes till svenska inför presentation i uppsatsen. Vid användning av citat från denna intervju har hänsyn tagits till att översättningen kan ha medfört mindre nyansskillnader jämfört med originalspråket.

Respondenternas konfidentialitet säkerställs genom pseudonymisering, vilket innebär att informanter och organisationer ersätts med neutrala beteckningar som omöjliggör direkt identifiering men möjliggör koppling mellan utsagor från samma källa (Oates et al. 2022). Samtliga informanter benämns IP1-IP6 och tillhörande företag benämns F1-F6.

Då den första intervjun genomfördes med två informanter gemensamt benämns dessa IP1a och IP1b. Oates et al. (2022) poängterar även att kombinationen av organisationstillhörighet,

roll och specifika uttalanden kan göra informanter identifierbara trots pseudonymisering. Således har citat utelämnats eller anpassats i de fall då de innehåller uppgifter som kan bidra till identifiering av individer eller organisationer, exempelvis uppgifter om vilken delbransch som organisationen befinner sig i eller typer av specifika produkter och livsmedel. Inspelningar och transkriptioner lagras på ett säkert sätt och används uteslutande för denna studies ändamål, i enlighet med Oates et al. (2022) krav på att informanternas rätt till konfidentialitet respekteras.

# 5 Empiri

I detta kapitel presenteras studiens empiriska resultat baserat på de genomförda intervjuerna. Empirin har analyserats genom en tematisk analys och strukturerats utifrån återkommande mönster i materialet. Resultaten presenteras i relation till TOE-ramverkets tre kontexter: den teknologiska, den organisatoriska och den externa, där identifierade teman organiseras utifrån respektive kontext.

Fokus ligger på att synliggöra hur respondenterna beskriver arbetet med informationssäkerhet i relation till cybersäkerhetslagen, med särskild betoning på centrala utmaningar, förändringar och konsekvenser i praktiken.

## 5.1 Teknologisk kontext

### *5.1.1 Tekniska förutsättningar och säkerhetsanpassningar*

Informanterna beskriver en utveckling mot att i högre grad använda externa, standardiserade system. Samtidigt kvarstår vissa legacy-system, vilka beskrivs som svåra och kostsamma att ersätta. Dessa system är ofta verksamhetskritiska och djupt integrerade i befintliga processer, vilket försvårar utbyte.

I stället framkommer det att säkerhetsarbetet i vissa fall anpassas genom kompletterande lösningar. När det inte är möjligt att implementera säkerhetsåtgärder direkt i systemen, sker skyddet genom omgivande strukturer, exempelvis genom segmentering och kontroll av nätverkstrafik. Detta framkommer bland annat hos IP1a, där informanten beskriver att det ibland inte är möjligt att skydda systemen i sig själva: "Och om det inte går i systemet i sig, så det som är runtomkring. Så att man ger den en krockkudde." (IP1a, 01:22:15). På liknande sätt beskriver IP2 att skyddet av legacy-system i produktionsmiljöer sker genom att begränsa fysisk och nätverksmässig åtkomst samt att i så hög utsträckning som möjligt låsa ner systemen. Likaså jobbar IP3 och IP5 med segmentering på nätverksnivå, men med patchningar på systemnivå (IP5). Även IP6 menar att de teknologiska anpassningarna inte nödvändigtvis sker i systemen som sådana, utan att man adderar lager som logging på server- och applikationsnivå ovanpå systemen.

IP5 förklarar uppfattningen om att säkerheten är svår att hantera med att utvecklare tidigare har prioriterat funktion framför säkerhet, och en annan anledning framförs vara att implementationen kan blockeras på grund av att systemen körs på gamla operativsystem (IP6). Vidare beskriver IP5 det säkerhetsmässiga underhållet av äldre system som känsligt. Även om man styr säkerheten med behörighetskontroller så arbetar man inte med flera lager:

> … det är klart att det är ju känsligare, de är svårare underhålla liksom säkerhetsmässigt. Så är det ju. Och det finns inte så mycket inbyggda för att en utvecklare tänker inte så mycket på säkerhet alla gånger utan det är mer liksom bara funktion. Sen kanske man styr det med behörighets[kontroller], men det är ju inte många lager och så där. (IP5, 00:35:35)

IP4, som är verksam utanför den svenska kontexten, är den enda informanten som inte upplever dessa svårigheter med legacy-system. I stället för att utveckla egna system köpte de tidigt in de dyraste systemen som fanns för deras ändamål, bland annat SAP som även andra informanter använder. Några av informanterna beskriver upphandling av branschstandardiserade system, utvecklade av externa leverantörer, som ett säkrare alternativ än att utveckla egna system. Detta kopplas bland annat till att standardiserade system upplevs ha bättre inbyggda säkerhetsfunktioner, vilket IP5 beskriver:

> ... på något vis har du bättre inbyggd säkerhetsfunktion och lättare säkerhetsuppdatering om det är så att säga mer standardiserade system. Så är det ju faktiskt. En sak till att man går till standardiserade system, att de är lättare att underhålla ur den aspekten (IP5, 00:34:44).

## 5.2 Organisatorisk kontext

### *5.2.1 Compliance: organisatorisk börda och kapacitet*

Den ökade administrativa belastningen framträder som en konsekvens av ökande regulatoriska krav, såsom cybersäkerhetslagen. Säkerhetsarbetet beskrivs ha förskjutits från ett operativt arbetssätt till ett mer dokumentationsdrivet arbete. Fokus har därmed gått från att praktiskt hantera säkerhet till att kunna visa, motivera och bevisa genomförda åtgärder för externa aktörer.

Detta illustreras i Intervju 1, där IP1a beskriver hur arbetet "har blivit lite mycket mer administrativt" och att det idag handlar om att "bevisa att vi har gjort en riskbedömning". Utvecklingen upplevs dock inte nödvändigtvis bidra till förbättrad säkerhet, utan snarare som en omfördelning av resurser från problemlösning till administration. IP1a uttrycker exempelvis en oro för att "de här föreskrifterna kommer att peka ut saker som gör att vi bara får en massa administration" (IP1a, 00:22:27) samtidigt som IP1b menar att krav på incidentrapportering riskerar att innebära att resurser läggs på rapportering snarare än att "lösa problemet" (IP1b, 00:50:45).

IP3 menar att de dagligen drabbas av compliance burden, särskilt eftersom kraven på vad som är relevant och ska rapporteras är otydliga, vilket orsakar "overhead på overheaden" (IP3, 00:31:03), alltså allmänna omkostnader till följd av bland annat administration. Kostnaden beskrivs som extrem och att det märks i organisationen. Hen tror att detta är en effekt som

direktivet inte var tänkt att orsaka från början. Även IP2 och IP6 upplever att de inte får något tillbaka för de resurser de lägger ned, särskilt på rapportering (IP2). IP6 beskriver det som att man lägger pengar på något som ”eventuellt kommer hända i världshistorien” (IP6, 00:11:31) och att det hade varit bättre inkomstmässigt att lägga resurser på att sälja produkter i stället. På samma sätt menar IP2 att investeringarna som krävs i tid och pengar tar emot särskilt på grund av att försäljningen sätts i andra hand. Samtidigt menar hen att compliance å andra sidan gör att de överhuvudtaget tillåts fortsätta bedriva näring.

IP5 belyser vidare att livsmedelsbranschen redan har små marginaler. Det finns inte utrymme för den ytterligare omfattande administrationen som lagkraven medför delvis på rapportering, men även på utformning av policyer och mer generellt på arbetet med att överhuvudtaget förstå vad som förväntas av en. En överväldigande majoritet av intervjupersonerna menar att de behöver anställa ny personal till följd av den ökade administrationen. IP6 beskriver att även om man kan outsourca (utkontraktera) compliance-arbetet till utomstående leverantörer krävs det mycket internt arbete för att reda ut vad man överhuvudtaget behöver hjälp med att uppnå: ”vi kan ju inte bara säga till dem fixa vår policy” (IP6, 00:29:27).

Baserat på dialog med Livsmedelsverket menar IP5 att den administrativa biten inte verkar gå att komma runt och att det faktumet är tungt, men att ”det är ju som det är” (IP5, 00:39:35). IP2 tror däremot att man ur ett större perspektiv kommer att uppnå en balans i bördan kopplad till compliance längre fram, baserat på att Livsmedelsverket upplevs som enkla att samarbeta med.

IP6 menar dock att man inte får glömma bort syftet med rapportering, eftersom poängen är att man på samhällsnivå ska ha koll på vilka incidenter som sker och kunna varna andra. Å andra sidan ser hen även nackdelarna med den administration som tillkommer och menar att detta är känt även från centralt håll och att det pågår ett aktivt arbete i EU med att förenkla den. Hen menar att EU har för avsikt att lätta upp på rättsakter så mycket som möjligt eftersom det annars finns en risk att företag flyttar sin verksamhet utanför EU eller säljer av delar av den, vilket anses vara negativt ur säkerhetssynpunkt.

I fråga om den egna organisationens compliance i relation till NIS2 framträder olika uppfattningar om hur långt arbetet har kommit. Vissa anser att de redan har en stabil grund och uppfyller kraven, medan andra fortfarande är i ett tidigt skede där processernas mognad och förmåga ifrågasätts.

De organisationer som anser sig ha kommit längst beskriver implementeringen som nästan helt klar. IP2 känner sig trygg med att de följer reglerna och betonar att de formella kraven, som registrering hos tillsynsmyndigheten, är uppfyllda:

> Vi är NIS2 compliant. Vi har rapporterat in till MCF, även fast jag inte har fått svar ifrån dem, men de bitarna finns på plats (IP2, 00:11:09)
>
> Eftersom vi faller under NIS 2 så har vi gjort det arbetet. Vi har gått igenom, vilka affärskritiska system har vi? Har vi verksamhetsägare till dem? Det finns kontinuitetsplaner. Vi har upprättat alla de bitarna. Vi har anmält oss till MCF, så att vi finns med. (IP2, 00:11:06)

En liknande utgångspunkt återfinns hos IP3, som menar att man har en stabil utgångspunkt eftersom organisationen började arbeta med cybersäkerhetsfrågor tidigt. En stor fördel var att

det gamla NIS-direktivet redan fanns på plats, vilket gav en ”bra grundplåt” (IP3, 00:20:47). IP3 beskriver hur de har arbetat strategiskt med att hitta sina brister för att skapa en tydlig lägstanivå:

> … alla de delarna… som vi verkligen kan stänga ner, de andra får ju, det är ju en accepterbar risk förmodligen som man kommer ha i slutändan. Men det gäller ju att skapa den här baselinen så att man har en bra linje och hålla sig till för då kommer det vara enklare för oss framåt sen också. (IP3, 00:20:47)

För vissa organisationer innebär NIS2-kraven att de måste fokusera mer på hela värdekedjan. IP5 säger att de har bra kontroll idag, men att de nu måste utöka sitt arbete. Det räcker inte längre att bara ha översikt över leverantörerna, utan de måste också börja granska leverantörernas cybersäkerhetsförmåga och arbetssätt mer noggrant.

Till skillnad från de organisationer anser sig ha kommit långt beskriver IP6 en mycket lägre mognadsgrad. Verksamheten är fortfarande i ”ett tidigt stadium” (IP6, 00:15:43). IP6 är självkritisk till de nuvarande strukturerna och ifrågasätter om incidentprocessen är tillräckligt mogen, hur den används och hur väl den stämmer överens med koncernens processer. Bristen på mognad märks särskilt när det gäller lagens strikta tidskrav för incidentrapportering, där IP6 konstaterar att organisationens operativa förmåga inte är tillräcklig:

> ...vi är inte riktigt redo om det skulle hända imorgon det här inom 72 timmar ska du ha en första rapport. (IP6, 00:48:23)

### *5.2.2 Regulatoriska krav som intern förändringskraft*

En återkommande uppfattning bland informanterna är att regulatoriska krav är betydligt enklare att få genomslag för internt än säkerhetsinitiativ utan motsvarande regulatoriskt stöd. Internt kan man ”peka med hela handen” (IP1a, 01:32:02) mot lagkraven utan att någon diskussion krävs. Det står i linje med IP2, IP3, IP5 och IP6:s upplevelser av att kunna luta sig mot lagkraven vid genomdrivande av nya beslut. Straffavgifter och näringsförbud ges som exempel på konsekvenser som skapar drivkraft (IP6). Även om dessa kanske främst motiverar organisationsledningen, menar hen att om förståelsen existerar på denna nivå kommer den att sprida sig nedåt i organisationen.

Motståndet som intervjupersonerna upplever vid interna initiativ beskrivs uppstå på grund av att nya införanden är både monetärt och resursmässigt kostsamma (IP3) och ofta upplevs som jobbiga (IP1a; IP2; IP6). Kostnaden ses inte alltid som befogad eftersom initiativen inte bidrar till att de ”säljer mer och tjänar pengar” (IP5, 00:11:41). Motståndet tar sig uttryck i ifrågasättanden (IP3) och det krävs interna förhandlingar, diskussioner och dialoger för att övertyga organisationen att tillämpa förslagen (IP1). Att driva igenom interna initiativ ses av IP3 som en ”jätteutmaning” (IP3, 00:15:13) och en effekt av den friktion som uppstår är att initiativen skjuts på framtiden (IP1a).

IP4 skiljer sig något från de svenska informanterna då hen menar att inställningen till initiativ påverkas av förståelsen för de verksamhetsmässiga följderna av att inte genomföra dem. Även om regleringar anses vara mer motiverande ju lägre förståelse som innehas för informationssäkerhet, krävs nödvändigtvis inget aktivt förhållande till tekniken i sig eller någon förståelse av den för att förstå varför säkerhetsinitiativ är viktiga. Som exempel görs det att man på fabriksnivå, där arbetet är långt ifrån att handla om informationssäkerhet eller

EU-regleringar, mycket väl förstår vad ett driftstopp innebär kostnadsmässigt, och att denna förståelse kan räcka som motivering för implementering:

> Ta till exempel fabriksnivån – de är väldigt långt ifrån EU-reglering, men de vet utmärkt väl vad en timmes driftstopp kostar och vad det innebär. De är därför bara intresserade av att se till att sådana driftstopp kan undvikas på alla möjliga sätt, och de är jätteenkla att jobba med. (IP4, 00:30:15)

Utöver att underlätta genomdrivandet av säkerhetsinitiativ beskrivs cybersäkerhetslagen även ha bidragit till ett mer omfattande säkerhetsarbete i organisationerna. Detta tar sig bland annat uttryck genom implementeringen av kontinuitetsplaner och andra säkerhetsrelaterade åtgärder (IP2). Kontinuitetsplanerna är något som även IP5 nämner som särskilt givande. IP5:s organisation har numera en fullständig plan för hur exakt de kommer hantera exempelvis en dataläcka, och att denna inte hade skapats annars. Hen upplever att lagen har utvecklat säkerhetstänket, att detta har övergått från ”nu gör vi det, och sen är det bra” (IP5, 00:16:13) till att man har bättre koll på säkerhetsarbetet som helhet, vilket har inneburit en säkerhetsförbättring för deras organisation. Utöver införandet av kontinuitetsplaner, som ses som en ”jättebra” (IP2, 00:09:10) effekt, uppskattar IP2 även kraven på regelbundna behörighetskontroller.

IP5 och IP6 menar att cybersäkerhetslagen har medvetandegjort vikten av cybersäkerhetsåtgärder, vilket har bidragit till ett större engagemang och till att gemene man har fått en större förståelse för införande av sådana. Detta har underlättat arbetet med dessa frågor.

IP4 uttrycker att cybersäkerhetslagen ”utan tvekan” (00:12:05) har fungerat som en katalysator för organisationer som saknat ett tydligt säkerhetsarbete. IP2 utvecklar detta och menar att om en organisation saknar starka profiler eller kunskap om säkerhetsåtgärder i sig är cybersäkerhetslagen särskilt värdefull. En konstruktiv effekt av lagen är att man blir tvingad att se över sina system, vilket ses som ”bara positivt” (IP2, 01:08:50). I kontrast till denna uppfattning upplever däremot IP1 att lagen även medför negativa effekter. Även om det är enklare att implementera säkerhetsåtgärder till följd av lagen, påpekar hen att föreskrifterna å andra sidan inte nödvändigtvis är facit och att detta påverkar deras säkerhetsarbete negativt. Genom cybersäkerhetslagens implementering begränsas man till tekniska åtgärder som bestäms av regulatoriska krav och nyttan som kan dras av organisationers individuella förmågor negligeras. I stället för att implementera egna lösningar som främjar organisationens säkerhet tvingas de välja tekniker som de inte behärskar. Detta ses som en “jätterisk” (IP1a, 00:50:32) och kan i sin tur påverka systemens säkerhet:

> Om vi hade fått lov att själv tänka ut hur vi ville lösa de här sakerna och att det hade varit mer generellt skrivet. Så hade vi kunnat lägga pengar på rätt saker, vi hade kunnat blivit bättre. Men som det är skrivet nu och de remisserna som har varit ute är precis tvärtom. Det kommer att göra att vi måste välja tekniker som vi inte kan, vi inte har behov av och vi absolut inte vill använda. Istället för att ta någonting annat som vi är duktiga på, som vi ser löser våra problem och som gör det säkrare. Men de får vi inte använda för de stämmer inte med lagen. (IP1a, 00:51:21**)**

IP3 uttrycker liknande tankar och menar att oavsett om ”man har en cybersäkerhetslag eller rapporteringsskyldighet” (IP3, 00:11:03) eller inte så kommer man skydda sitt företag och sin

data, och att det finns krav i cybersäkerhetslagen som fokuserar på andra åtgärder än de som är viktiga för organisationen.

Regulatoriska krav beskrivs inte enbart påverka organisationernas säkerhetsarbete, utan även hur informationssäkerhetsroller utformas och utvecklas över tid. Informanternas erfarenheter från tidigare regelverk, såsom införandet av dataskyddsförordningen (GDPR), visar att regulatoriska krav har tenderat att förändra hur organisationerna har strukturerat sina roller och ansvarsområden. IP5 förklarar att medan det tekniska säkerhetsarbetet redan är väl etablerat, är det kraven på organisatorisk systematik som numera transformerar rollens innehåll:

> Det som har skilt sig mycket … är ju teknisk säkerhet och så organisatorisk säkerhet. …Teknisk säkerhet där har vi jobbat väldigt mycket. … Sen är det ju det här med det organisatoriska, det är där det har börjat skilja väldigt mycket mer för mig. …Du måste ha en systematik i arbetet, att det är dokumenterat, hur vi gör och hur vi arbetar. Där har vi lagt mycket mer tid. (IP5, 00:06:44)

> ...vi har ju fått bli mycket mer, mer spindeln i nätet, så vi är ju inte bara liksom skyddar oss liksom med brandväggar, väggar och DOS-attacker och sånt där. Utan nu är det mycket mer organisatoriska frågor. (IP5, 00:09:29)

För aktörer som redan har arbetat strukturerat och systematiskt med informationssäkerhet under en längre tid innebär de nya regulatoriska kraven sällan någon större omställning. IP1a beskriver att det för mogna verksamheter snarare handlar om en ren formaliserings- och förfiningsfråga, medan det för mindre erfarna organisationer kan innebära ett betydligt större och mer krävande organisatoriskt steg.

I takt med att lagstiftningen utvecklas inser man att den traditionella IT-säkerhetsrollen håller på att fasas ut. Den regulatoriska pressen skapar ett behov av en ny typ av roll som inte bara hanterar teknik utan som långsiktigt kan röra sig mellan operativ styrning, juridik och verksamhetsstrategiska frågor. IP4 tror att informationssäkerhet kommer vara mer kopplad till supply-chain (leverantörskedjan) i framtiden, vilket kommer ställa krav på en tydlig organisationsstruktur.

### *5.2.3 Säkerhetsarbete: förhållningssätt och arbetssätt*

För många av intervjupersonerna påverkas samordningen av kombinationen av ett centraliserat initiativtagande och ett decentraliserat ansvar för genomförandet. Även om ledningen bär det yttersta ansvaret, visar empirin att det operativa ansvaret för att driva och samordna säkerhetsarbetet ofta faller på IT-avdelningen, trots att frågorna berör hela organisationen.

Ett återkommande tema är svårigheten att definiera och fördela ägarskapet för informationssäkerhet utanför den rena IT-infrastrukturen. IP3 belyser denna problematik genom att beskriva hur gränsdragningar mellan IT-säkerhet, fysisk säkerhet och regulatorisk efterlevnad ofta blir otydliga och bollas tillbaka till IT:

> En stor utmaning är att hitta, det likadant som med GDPR frågor och sånt där, vem ska äga frågan? Jag frågar HR, så vägrar HR GDPR. Nej, de vill inte ha det

> så hamnar det på IT för ni kan det här. Det blir många såna här bollningar fram och tillbaka för den uppgift som vi inte är staffade för ännu. (IP3, 00:28:41)

Denna bild delas av IP5, som betonar att IT-avdelningen tvingas initiera och driva processer eftersom det saknas en naturlig mottagare i verksamheten, trots en medvetenhet om och ett argumenterande för att IT inte äger själva informationen:

> Vi försöker alltid skjuta liksom ansvaret där det hör hemma. Men det här är en sån där fråga som ofta blir att vem håller ihop det liksom och vem driver det? (IP5, 00:09:58)

För att hantera detta har IP5:s organisation dedikerat en resurs i sitt team som enbart fokuserar på informationssäkerhet. Vidare lyfter hen fram att de har utvecklat ett nära samarbete med HR, som fungerar som en mellanhand i diskussionerna med verksamheten.

Organisatoriska strukturer påverkar också hur samordningen ser ut i praktiken. IP4 beskriver en centralt distribuerad struktur där koncernen sätter kraven medan de enskilda affärsenheterna i olika länder bär ansvaret för genomförandet:

> Tanken är att det som görs på central nivå görs för NIS 2. Därefter är det varje affärsenhet i respektive land som ansvarar för att kartlägga om, och i så fall vilka, avvikelser som finns i deras eget land jämfört med NIS 2. De kommer sedan att ansvara för att åtgärda detta med stöd från centralt håll... (IP4, 00:01:53)

IP4 lyfter även fram att placeringen av säkerhetsfunktionen i den egna organisationen kan vara problematisk ur ett samordningsperspektiv. Att rapportera via IT-chefen till CFO:n beskrivs som ett traditionellt men mindre modernt upplägg. Vidare pekar IP4 på att kritiska områden som incidenthantering, kontinuitetsstyrning och krishantering egentligen borde ägas av supply-chain-organisationen, då det är de som i slutändan måste se till att verksamheten kan leverera, men att ansvaret ändå hamnar på IP4 på grund av specifik kompetens.

IP4 menar samtidigt att upp till 80 procent av deras praktiska arbete ligger hos en extern leverantör på grund av att deras system inte är egenutvecklade. För hen handlar det mest om att ställa höga krav på kollegorna att ha kontroll över organisationens digitala tillgångar.

Samordningsbehovet mellan IT och OT tas upp som en central aspekt kopplad till lagkrav (IP6). IP6 förklarar att NIS2 ställer krav på en segregering mellan IT och OT, vilket kräver ett samarbete med dem som är ansvariga för OT på produktionssidan. Enligt IP6 saknar OT-sidan egna resurser som arbetar aktivt med NIS 2, vilket gör att IT-avdelningen måste hjälpa till och samordna arbetet, även om de inte äger själva implementeringen. För att stötta detta arbete i en internationell kontext beskriver IP6 hur modersbolaget i Europa har format en expertgrupp som erbjuder ett ramverk, regelbundna möten och support till de enskilda länderna.

IP3 lyfter fram att det finns interna utmaningar och oklarheter kring vem som faktiskt bär rapporteringsansvaret kontra vem som bara sammanställer datan, något som IP5:s organisation undviker genom en centraliserad modell:

> … det ligger inte ute i verksamheten att någon ska rapportera in till den här inrapporteringsmyndigheten, utan det gör vi [centralt på IT] (IP5, 00:43:06)

Utöver den operativa samordningen framträder även organisationsledningens roll som central för informationssäkerhetsarbetet. Intervjupersonerna är överlag positiva till att det nu är organisationsledningen som har det yttersta ansvaret för informationssäkerheten enligt den nya lagen. Det här ansvaret ger säkerhetsarbetet mer tyngd och resurser, vilket gör det lättare att driva igenom viktiga initiativ.

Enligt IP4 är det viktigaste med NIS2 just att ledningen har ansvaret för informationssäkerheten. Informanten påpekar att det ofta har varit så att organisationer anställer en säkerhetsansvarig och sedan tror att ledningen inte längre behöver tänka på säkerhet. Om den säkerhetsansvarige inte får budget, mandat eller direkt kontakt med styrelsen kan arbetet stanna av helt. Därför ger lagens krav på rapportering till ledningen en tydlig och viktig roll för säkerhetsarbete.

Även IP6 tycker att det mest intressanta med NIS2 är att ansvaret flyttas till högsta ledningen, eftersom informationssäkerhet tidigare ofta har setts som en fråga enbart för IT-avdelningen och ansvaret hamnat långt ner i organisationen, ibland under finans- eller ekonomiavdelningen.

> ...det ligger ju liksom på IT-avdelningen, informationssäkerhet, vilket är korrekt. Men det som man alltid har fått kämpa med länge är just det här att det här är ju en angelägenhet för hela verksamheten. Det är ju inte liksom en IT-fråga som man bara dumpar hos IT-avdelningen och sen har man löst det. … Det jag tycker är intressant med NIS 2 är ju att man verkligen vill lyfta det och lägga ansvaret på ledningen och säga att det här är ert ansvar och ni kan inte komma undan. … Man kan till och med få näringsförbud om man inte följer lagen. (IP6, 00:01:18)

IP5 menar att de har haft en person i ledningsgruppen som har drivit säkerhetsfrågorna ”väldigt hårt” (IP5, 00:27:41) och att detta har inneburit ett genomslag. Numera är ledningen lyhörd när de tar beslut om investeringar.

Som nämns i 5.2.2 menar IP6 att de tydliga konsekvenserna av att inte vara compliant, som risken för näringsförbud, skapar en drivkraft i organisationen och att insikten om allvaret naturligt sprider sig till resten av organisationen när ledningen är investerad. För att tydliggöra ansvaret har IP6 hållit en session med alla direktörer i ledningsgruppen för att trycka på att ingen kan ignorera eller skjuta ifrån sig frågan. Samtidigt ser IP6 att det praktiska arbetet fortfarande ofta hamnar på IT-avdelningen och att övriga i ledningen förväntar sig att de tar hand om det om de inte tvingas till att agera.

I informanternas beskrivningar framträder även olika arbetssätt för hur informationssäkehetsarbetet organiseras och bedrivs i praktiken. Organisationernas cybersäkerhetsarbete bygger på tekniska skyddsåtgärder, etablerade ramverk och policyer samt utbildningsinsatser. Samtidigt framkommer olika strategier för hur cybersäkerhet integreras i verksamhetens processer.

IP2 beskriver ett traditionellt säkerhetsarbete med fokus på att skydda infrastrukturen genom löpande underhåll och restriktiva behörigheter:

> Vi har ju ett traditionellt cybersäkerhetsarbete som handlar om att skydda oss, se till att våra system är uppdaterade, alla sådana saker. Du patchar dina servrar och du låser ner saker. Du jobbar med behörigheter ska inte vara breda utan smala och tillfälliga. (IP2, 00:05:22)

IP2 genomför även behörighetskontroller på ett strikt och återkommande sätt, vilket cybersäkerhetslagen var en katalysator för (se 5.2.2) Dessutom har man numera en etablerad informationssäkerhetspolicy, en AI-policy och standardiserade utbildningar. Hen menar samtidigt att de har varit mer fokuserade på de tekniska delarna och att de har behövt utveckla sitt operativa och strategiska säkerhetstänk.

IP1a, IP2 och IP5 nämner kontinuitetsplaner kopplade till cybersäkerhetsarbetet. IP2 och IP5 menar att deras organisationer har sådana på plats, medan IP1a menar att en sådan existerar men inte är dokumenterad ännu "i huvudet på folk. Finns ju inte dokumenterat tyvärr. Utan det är ju det vi vill göra nu." (IP1a, 01:03:38).

Informanternas beskrivningar visar att organisationerna använder internationella ramverk och standarder för att strukturera cybersäkerhetsarbetet, även om ambitionsnivån för certifieringar varierar. IP2 följer NIST Cyber Security Framework (CSF), men anger att det inte är fullt implementerat. IP4 har utvecklat en egen cyberkatalog baserad på CSF, vilket möjliggör kartläggning av styrning, identifiering och ansvarsfördelning. IP1a, IP3 och IP5 menar att deras organisationer också använder etablerade informationssäkerhetsstandarder; där F1 och F3 följer ISO 270001 och F5 arbetar mot NIST. F3 är inte certifierade, men IP3 påpekar att leverantörskrav kopplade till ISO 27001 gör att de arbetar mer mot standarden och överväger framtida certifiering**.** I motsats till detta ser IP1a inte nyttan med att "lägga den tiden" (IP1a, 01:00:22) på certifiering, utan menar att de ser en anpassad riskhantering som mer i linje med sina behov. Bland annat har man hållit i workshops med IT-avdelningen för att bena ut vilka cybersäkerhetsrisker som finns och IP1a menar samtidigt att dessa frågor kan kopplas till fysisk säkerhet.

Samarbete med externa parter och outsourcing är centrala delar av arbetssättet och påverkar riskhanteringen. IP2 genomförde penetrationstester när affärssystemet flyttades till leverantörens molnlösning. IP4, som outsourcar IT-infrastruktur och servrar, betonar att ansvaret kvarstår hos den egna organisationen. De ansvarar för att leverantören följer best practice för konfigurering och utför själva konfigurationer i egna affärsapplikationer.

Den mänskliga aspekten och cybersäkerhetskulturen adresseras genom utbildning och medvetandegörande. IP1, IP3 och IP6 beskriver hur de regelbundet genomför riktade utbildningar och simulerade phishingkampanjer med falska mejl. IP6 belyser att dessa kampanjer ger användarna en möjlighet att rapportera misstänkta mejl och få en direkt bekräftelse på att de har agerat rätt, vilket tränar organisationen på att vara resistent mot social manipulation. IP4 som är verksam utanför Sverige menar att även de tillämpar ett liknande upplägg med årliga kurser och phishing-kampanjer, och poängterar att nyanställda får en grundläggande utbildning redan vid start, medan medarbetare i identifierade "högriskroller" tilldelas en särskild, fördjupad upplärning.

Informanternas beskrivningar visar samtidigt att informationssäkerhetsarbete inte enbart handlar om tekniska åtgärder eller utbildningsinsatser, utan även om hur organisationer förhåller sig till risk, säkerhet och verksamhetsnytta.

Organisationer balanserar mellan att upprätthålla en hög säkerhetsnivå och att behålla produktivitet och affärsfokus. Många beskriver ett skifte från ett traditionellt kontrollfokus till ett mer flexibelt, riskbaserat synsätt där säkerhet ses som hela organisationens ansvar, inte bara ett IT-problem.

En viktig utmaning är att få säkerhetsrutiner att bli en naturlig del av vardagen för medarbetarna, utan att de känns som ett hinder. IP2 reflekterar över att ramverk och standarder kan anses som omotiverande för medarbetare, och hen jämför detta med tidigare arbetsplatser där säkerhet kändes mer självklart:

> Det var så naturligt, du låste alltid datorn, du såg till att klassa dina dokument och information, det fanns i bakhuvudet, det var inte betungande. Det är lite dit jag vill komma, det ska vara en naturlig del, det ska inte vara betungande. Då måste man hela tiden jobba med de här sakerna. Då måste man hela tiden jobba med de här sakerna. Och jag menar, det är bra om man har ramverk och standarder, men det kan jag inte applicera på medarbetarna. Mitt team kan göra det, men medarbetarna har ingen lust att följa sådana bitar. (IP2, 00:34:28)

IP2 menar att det är enkelt att skapa strikta säkerhetsåtgärder i teorin, men i praktiken fungerar det inte. Man kan inte skydda allt och samtidigt ha en fungerande verksamhet. IP6 håller med och säger att det är viktigt att hitta en rimlig balans och vara beredd att acceptera vissa risker för att hålla kostnaderna nere.

Både IP1a och IP4 uttrycker kritik mot ett kontrollbaserat synsätt. IP1a menar att i motsats till "en checklista" (IP1a, Skriftlig komplettering, Ref 3.3) tolkar de cybersäkerhetslagens föreskrifter som en riktning och ett ramverk för att förstärka deras cybersäkerhetsarbete. IP4 beskriver hur organisationens tidigare säkerhetsarbete präglades av att pricka av långa listor med tekniska kontroller utan att medarbetarna egentligen förstod de bakomliggande riskerna. Detta förhållningssätt beskrivs ha lett till mycket arbete med potentiellt liten reell effekt. IP4 förklarar hur hen aktivt har valt att vända på detta perspektiv:

> Så jag har vänt på det. Och det är en liten, liten lista med kontroller. Och jag har sagt att det första vi ska fokusera på är att förstå vilka risker vi har. Och utifrån det måste vi välja vad vi behöver. (IP4, 00:03:54)

Som presenterat i 5.2.2 finns också en spänning mellan ekonomi och cybersäkerhet. Även om cybersäkerhet är intressant, vill man ofta hellre lägga pengar på sådant som utvecklar kärnverksamheten (IP2). Utmaningen är att följa reglerna utan att det går ut över produktiviteten.

IP5 beskriver också ett riskbaserat synsätt och ser cybersäkerhet som ett ständigt arbete med att hantera sannolikheter och risker. Målet är att skydda verksamheten mot stora avbrott (IP1a; IP5).

För att bli bättre förberedda menar informanterna att det är viktigt att öva praktiskt och regelbundet. IP2 säger att de nu testar sina disaster recovery-planer (detaljerade handlingplaner för oväntade händelser) två gånger om året för att hålla dem aktuella. IP2 tror också att framtiden kräver ännu mer avancerade tester, som penetrationstester, men framför allt att organisationen måste kunna tänka på nya sätt om en riktig cyberattack sker.

## 5.3 Extern kontext

### *5.3.1 Navigering i det regulatoriska landskapet*

IP4 upplever att NIS2 är den bästa typen av lagstiftning eftersom den säger att det säkerhetsarbete du gör ska vara i proportion till din verksamhets storlek och de risker du står inför. Detta gör lagstiftningen flexibel när det gäller hur man uppnår efterlevnad, även om det kan vara svårt eftersom det ställer krav på verksamheten att förstå sig själv.

Däremot upplevs de nationella kraven, särskilt MCF:s föreskrifter som varit ute på remiss, som oflexibla och otydligt formulerade. Bland annat menar IP1a att NIS2, i egenskap av EU-direktiv, tolkas alltför bokstavstroget i stället för att användas som en informationskälla för ändamålsenliga krav. Hen anser att intentionen som från början fanns i EU-direktivet har blivit "misshandlad" (IP1a, 01:35) och "finns inte kvar" (IP1a, 01:35:28); att MCF endast läser bokstäverna och avstår från att läsa mellan raderna. IP1a upplever att implementationen är mer omfattande än vad NIS2 egentligen kräver och menar att detta kan bero på att Sverige vill ligga i framkant när det gäller cybersäkerhet:

> Alltså som MCF ska göra det så extremt oflexibelt som det bara går liksom. Italien gjorde det, Finland har gjort det, de har ju tagit det på byggstövlarna och eftersom de gjorde det så måste ju vi vara bäst i klass... Så måste vi göra det ännu värre. Så tolkar jag det just nu (IP1a, 00:27:30)

Även IP3 och IP5 upplever att den svenska implementeringen av lagen är mer omfattande än den nödvändigtvis behöver vara enligt NIS2-direktivet. Denna syn skiljer sig från IP2:s, som upplever att den enda egentliga skillnaden från NIS2 är kraven på incidentrapportering.

Just dessa krav upplevs som särskilt svårtolkade. Det finns en osäkerhet kring vad som ska rapporteras, hur rapporteringen ska genomföras och vilka typer av incidenter som omfattas. Detta framgår av IP1a som beskriver svårigheter att tolka och omsätta kraven i praktiken. Osäkerheten blir särskilt tydlig i frågor om gränsdragning, där mindre incidenter problematiseras i relation till rapporteringskraven. Detta skapar oklarhet kring vad som är proportionerligt att rapportera.

I likhet med detta anser även IP2 att det är otydligt exakt vilka incidenter som bör rapporteras. I det stora hela har hen en positiv uppfattning om lagen, men hen anser att rapporteringsdelen är för svår. IP1a menar att enligt MCF:s föreskrifter ska alla incidenter rapporteras, men i praktiken går det inte. Ett trasigt etikettsystem (IP1a; IP1b) och spammejl (IP2; IP3) ges som exempel på incidenter som teoretiskt sett är inrapporteringsskyldiga händelser, men som de anser är oproportionerliga. Även andra incidenter där systemen redan har en hanteringsmekanism vid upptäckt nämns (IP2).

IP3 menar likaså att det är svårt att kvantifiera vad som är viktigt och vad som inte är, och att interna beslut om en incident ska rapporteras eller inte därför baseras på gissningar. Arbetet med tolkning anses vara överväldigande, liksom utredningarna som tillsätts för att besluta om "varje liten händelse" (IP3, 00:07:52). IP3:s uppfattning är dock att otydligheterna kommer att klarna upp med tiden.

Även IP5 tycker att kraven för incidentrapporteringen är otydliga och att de därför själva beslutar vilka incidenter de ska rapportera. Detta är dock något som IP6 är kritisk mot, eftersom hen menar att organisationen inte nödvändigtvis har mandat att bedöma vilka incidenter som är relevanta eller inte ur ett samhällsperspektiv.

Frågor om tolkningsutrymme och tydlighet i kraven förs även i dialog med tillsynsmyndigheterna. Bland informanterna medverkar IP1a, IP2 och IP5 i Samrådsgrupp Krisberedskapsplanering Av Livsmedelsförsörjning (SKAL), ett forum lett av Livsmedelsverket för samverkan mellan myndigheter och livsmedelskedjans aktörer för att säkerställa livsmedelsförsörjningen vid kriser och krig (Livsmedelsverket, 2025b). I detta forum förs bland annat samtal om cybersäkerhetslagen. Av de intervjupersoner som medverkar i denna grupp upplever samtliga att samarbetet och dialogen med Livsmedelsverket är bra. IP2 beskriver även SKAL som ett viktigt forum för erfarenhetsbyte mellan aktörer inom livsmedelsindustrin och menar att cybersäkerhetsrelaterade krav fortfarande är ”nytt för oss” (IP2, 00:17:39).

IP1a påpekar att det däremot är svårare att kommunicera med MCF: ”De står ju stick i stäv lite mot Livsmedelsverket … just nu.” (IP1a, 00:18:54) och menar att de har svårt att få igenom sina idéer. IP1a utvecklar detta genom att mena att Livsmedelsverket förstår ”hur det ska funka i verkligheten” (IP1a, 00:21:08), till skillnad från MCF. När det gäller MCF:s remisser är Livsmedelsverket nämligen inte sällan ense med livsmedelsföretagen och detta framgår i SKAL:s remissvar, men IP1a menar att MCF kör över dessa svar med motiveringen att ”så står det inte i lagen” (IP1a, 00:49:35).

I relation till frågor om mer sektorsanpassade föreskrifter skiljer sig informanternas uppfattningar åt. IP1a beskriver att både verksamhetsutövare och Livsmedelsverket försökt konkretisera hur de regulatoriska kraven kan anpassas efter olika praktiska situationer inom livsmedelssektorn: ”Det var precis det vi försökte göra
och det var precis det Livsmedelsverket också ville” (IP1a, 00:19:44). IP2 menar snarare att föreskrifterna i grunden bör vara branschöverskridande men menar samtidigt att olika verksamheter samtidigt kan behöva olika former av stöd och vägledning.

IP2 upplever likaså att Livsmedelsverket är enkla att samarbeta med och att ”det finns andra myndigheter som är svårare” (IP2, 01:01:54). Även IP5 upplever Livsmedelsverket som ett hjälpsamt organ. IP2 menar att vikten av just informationsdelningen mellan organisationer och myndigheter saknas i föreskrifterna.

Liknande forum, lett av motsvarande tillsynsmyndighet, finns i landet där IP4 är verksam. Där delas också regulatoriska uppdateringar och erfarenhetsutbyte mellan organisationerna. Bland annat delas information om incidenter som inträffat, något som enligt IP2 inte verkar vara på plats i svenska samverkansform.

Alla intervjupersoner deltar inte i SKAL och vissa har inte haft någon dialog med Livsmedelsverket överhuvudtaget angående cybersäkerhetslagen. IP3 motiverar detta med att hen upplever att deras organisation är ”så pass långt framme” (IP3, 00:36:58) och redan har en god förståelse för vad Livsmedelsverket förväntar sig av dem.

### 5.3.2 Branschsamverkan och erfarenhetsutbyte

Som presenterats ovan deltar flera av intervjupersonerna i samverkansforumet SKAL och IP4 i den motsvarande i landet där hen är verksam. Även som ovan beskrivet är delningen av information gällande inträffade incidenter, i jämförelse med landet där IP4 är verksam, delvis bristfällig i de svenska samverkansforumen. Denna skillnad beskrivs bland annat som en följd av internationella skillnader i lagar. I Sverige är det ett lagbrott att dela vissa typer av information som man delar där IP4 är verksam. Ett exempel på sådan information är IP-adresser som har identifierats som inblandade i cybersäkerhetsincidenter (IP2; IP4). IP2 menar att avsaknaden av informationsdelning hämmar det nationella säkerhetsarbetet (detta perspektiv utvecklas vidare i avsnitt 5.3.3, i relation till totalförsvaret).

Delningen av information mellan företag påverkas även av konkurrenslagen, en lag som som blockerar IP3:s intresse av att överhuvudtaget medverka i samverkansforum. IP3 beskriver att ”vi kan ju inte vara i kontakt med våra konkurrenter på det sättet för att konkurrenslagen säger att vi får ju inte ha för mycket informationsutbyte” (IP3, 00:34:59). IP3 menar vidare att deras advokatbyrå har avrått dem från detta med anledning av Konkurrensverkets tillsynsundersökningar som bedrivs i syfte att förhindra kartellbildning. Liknande upplever IP4, som är verksam utanför Sverige, men hen betonar att det gäller att hitta en balans, för samhällets bästa. På samma sätt menar IP2 att cybersäkerhetshoten kommer från främmande stater och att dessa riktar in sig på att slå ut hela livsmedelsindustrin snarare än specifika företag. På så vis konkurrerar inte företagen inom IT-området, utan hen menar att de jobbar ihop eftersom ”alla vi måste ju hjälpas åt” (IP2, 00:25:47) för att förhindra incidenter. Detta exemplifieras även av IP2 genom att referera till cyberattacken som drabbade Coop Sverige 2021:

> När Coop blev utsatta för den här attacken ... tjänar ju inte ICA mer pengar på det. Så att vi konkurrerar inte om det här området, utan snarare så att man kan samverka, dela och hjälpas åt (IP2, 00:26:09)

IP2 beskriver även att informationsdelning mellan verksamheter kan bidra till att identifiera gemensamma mönster i cyberattacker, exempelvis riktade mot specifika yrkesgrupper.

Denna poäng om att företag inte gynnas av andras bristande cybersäkerhet specificeras även av IP4: ”man konkurrerar inte om säkerhet” (IP4, 00:36:05).

Även om IP6 inte medverkar i SKAL, har hen deltagit andra sammanhang där företag diskuterar cybersäkerhetslagen och relaterade EU-regleringar, bland annat genom seminarier och kontinuerliga möten med moderbolaget. I dessa sammanhang har även ett bredare perspektiv på EU:s intentioner med den ökade regleringen, särskilt i relation till det rådande världsläget. Detta presenteras närmare i kategorin samhällsansvar och säkerhet.

### 5.3.3 Ojämna förutsättningar, delat samhällsansvar

IP3 upplever att regelverket inte tar hänsyn till organisationers olikartade behov av säkerhetsåtgärder, vilket står i linje med IP1a, IP2 och IP5:s syn på att organisationer tvingas använda främmande tekniker till följd av oflexibla krav (se 5.2.2). IP3 menar att alla har olika förutsättningar och att lagen därför inte är anpassad för alla. En anledning till att förordningarna ser ut på detta sätt anses bero på att MCF som stiftar dem ”ser inte hela bilden” (IP2, 00:57:53).

Skillnaden i förutsättningar syftas av de flesta intervjupersoner till skillnader i verksamheters storlek, kompetens, resurser och digital mognad, men IP6 tillägger att de även kan syfta till ledningens engagemang.

IP3 tror att särskilt mindre bolag kommer att få bekymmer och ger som exempel producenter som inte ens vet att de omfattas av cybersäkerhetslagen och menar att medvetandegörandet inte genomförts på ett proportionerligt sätt. Även IP2 menar att mindre organisationer kommer att få det svårare än de större organisationerna som, likt dem själva, har en IT-avdelning och IT-säkerhetsansvariga som kan hantera bördan. En del av utmaningen beskrivs som att enskilda personer sitter med arbetet. Detta ligger i linje med IP5:s uppfattning om att mindre företag, som ofta har färre resurser, har det svårare eftersom de saknar grupperingar som arbetar med dessa frågor. IP6 menar också att det förmodligen är mindre organisationer, företag med lägre kompetens och budget, som drabbas värst av lagkraven eftersom de ofta saknar den infrastruktur för att hantera detta som större organisationer redan har på plats.

Informanterna upplever att bristen i proportionalitet skapar en olikvärdig spelplan, delvis inom gruppen företag som omfattas av lagen men även på marknaden i sin helhet (IP1a). Ett perspektiv på det senare är att man anser att konkurrensen riskerar att bli snedvriden på grund av att företag som undkommer att omfattas av lagen inte behöver avsätta lika mycket resurser för efterlevnad:

> En tydlig faktor är att många mindre aktörer helt enkelt inte omfattas av lagen, eftersom de inte når upp till de omsättnings eller storlekskrav som anges. Det innebär att de kan fortsätta bedriva sin verksamhet utan samma krav på investeringar i styrning, dokumentation och tekniska säkerhetsåtgärder. Större aktörer inom samma sektor behöver däremot lägga betydande resurser på att uppfylla lagens krav. Ur ett säkerhetsperspektiv kan det vara logiskt, men ur ett konkurrensperspektiv finns det en risk för snedvridning när företag verkar på samma marknad men under olika regelverk. (IP1a, Skriftlig komplettering, Ref 4.1)

Graden av digital mognad inom verksamheten är annan förutsättning som skiljer sig mellan företag (IP1), och IP2 tror att det kan vara ”jättejobbigt” (IP2, 00:25:17) för de företag som saknar den kompetensen. Den digitala mognaden inom livsmedelssektorn beskrivs som mycket varierad, även inom enskilda verksamheter. Är kontoret ens arbetsplats anses man ha en hög mognad och vana inom IT, till skillnad från exempelvis ute i produktionen där ens enda digitala hjälpmedel kan vara en mobiltelefon (IP3). IP6 framhäver dock att digital mognad inte nödvändigtvis är synonymt med framgång compliance-mässigt, utan att ett lyckat arbete till stor del beror på den support man får från ledningen.

IP2 menar att samverkansforum är en stor tillgång för att lindra bristen på proportionalitet i lagkraven, delvis för mindre företag som saknar cybersäkerhetsavdelningar, men även för större organisationer som behöver stöd i att hantera olika krav. Som presenterat i föregående kategori menar hen att det inte finns någon konkurrens kopplad till IT-området utan att informationsdelning är kopplat till ett gemensamt samhällsansvar, vilket presenteras närmare i nästa kategori. Man hjälps åt organisationer emellan.

IP4 breddar perspektivet om proportionalitet och beskriver att NIS2 bygger på att ”det du gör ska ka vara proportionerligt i förhållande till storlek och vilka risker du har” (IP4, 00:04:36),

något som enligt hen är ”jätteenkelt och jättesvårt samtidigt” (IP4, 00:04:36). Även om det är relevant att ta hänsyn till detta vid utformningen av kraven, ser hen samtidigt ett annat perspektiv. Hen menar att det finns en anledning till att livsmedelssektorn har placerats under NIS2-direktivet och omfattas av omfattande lagkrav, nämligen den ökade geopolitiska oron. Attackeras man av fientliga stater med avancerade, specialiserade grupper spelar det ingen roll om antalet anställda är 50 eller 50 000 (IP4).

Den ökade geopolitiska oron kopplar även till livsmedelssektorns roll i totalförsvaret. IP2 beskriver att livsmedelsföretag idag har en central roll ur ett nationellt säkerhets- och beredskapsperspektiv. Hen menar att livsmedelsförsörjningen i stor utsträckning är beroende av privata verksamhetsutövare, då försvaret till skillnad från tidigare inte längre har några omfattande beredskapslager. Verksamheter som kan producera dricksvatten, lagerhålla produkter och upprätthålla leveranser beskrivs därför som en del av totalförsvaret. IP2 menar även att livsmedelsproduktion relativt snabbt kan ställas om för att tillhandahålla produkter anpassade för olika behov vid kris eller krig. Informanterna upplever även att det förändrade säkerhetsläget gjort det naturligt att livsmedelssektorn nu omfattas av cybersäkerhetslagstiftningen och betraktas som en samhällsviktig sektor.

Hur det gemensamma ansvaret organiseras och finansieras kan skilja sig åt beroende på land och ägarstruktur. IP4 ger ett exempel från där hen är verksam, och menar att många av de största livsmedelsföretagen där är kooperativ eller delvis statligt ägda:

> …så de har ofta en mer samhällsinriktad roll. Man talar också mycket om total beredskap och vikten av den privata sektorn. Och när man börjar ställa krav på distributionscentraler och så vidare, kommer det nog att ställas fler frågor om hur mycket ansvar eller hur mycket pengar som ska användas på samhällets vägnar. (IP4, 00:39:30)

Samhällsansvaret och rollen i totalförsvaret handlar inte bara om att distribuera livsmedel. När cybersäkerheten nu regleras måste organisationerna också tänka på globala hot. IP6 beskriver att det förändrade samhälls- och säkerhetsläget bidragit till en ökad förståelse för allvaret i cybersäkerhetsfrågor och gjort det lättare att driva sådana frågor inom verksamheten:

> Att man tar det som något tekniskt och det är problem och sådär. Men att man med detta, det positiva är ju att man får hjälp att driva de här frågorna, att man förstår att det är viktigt och varför och när man hör vad som händer i samhället, man förstår vad som kan hända (IP6, 00:09:48).

IP2 beskriver även att det förändrade säkerhetsläget kan innebära ökade behov av informationsdelning och samverkan mellan myndigheter och verksamhetsutövare inom livsmedelssektorn. Hen menar att myndigheter och verksamheter besitter olika typer av information och att ett ökat informationsutbyte skulle kunna bidra till att identifiera mönster och förebygga cyberrelaterade hot inom livsmedelssektorn som samtidigt kan få konsekvenser för samhällsförsörjningen i stort. IP2 beskriver de potentiella fördelarna med ett sådant informationsutbyte:

> … då kan vi också börja kolla på det. Och så får vi liksom, kan man fånga in och hitta mönster. Så att hela branschen kan samla datapunkter och sen så arbeta mot samma mål (IP2, 01:06:08).

# 6 Diskussion

## 6.1 Teknologisk kontext

### *6.1.1 Tekniska förutsättningar och säkerhetsanpassningar*

Empirin stödjer Bakers mening (2012) om legacy-system som trögrörliga tekniska strukturer som kräver omfattande anpassningar vid förändringar. Informanterna beskriver bland annat att sådana system är djupt integrerade i verksamhetsprocesser, vilket är en bidragande faktor till att de upplevs som svåra och kostsamma att ersätta. Detta ligger i linje med forskning som påvisar att äldre, proprietära lösningar och föråldrade operativsystem begränsar möjligheten till att implementera moderna säkerhetskontroller (Mosteiro-Sanchez et al. 2020; Makrakis et al. 2021), litteratur som även bekräftas av IP6s beskrivning av att implementationen blockeras på grund av gamla operativsystem. Det IP5 beskriver gällande att funktion har prioriterats framför säkerhet är ett kompletterande perspektiv på vad litteraturen menar att bristen på inbyggda säkerhetsfunktioner beror på, nämligen att OT-system tidigare isolerats nätverksmässigt (Makrakis, 2021). Ovan belyser en inneboende konflikt mellan operativ kontinuitet och modern cybersäkerhet. När systemen designades var isolering av system tillräckligt, men i dagens digitala landskap skapar denna historiska prioritering av funktion en konsekvens som kan vara både komplex och kostsam att hantera.

Empirin framhåller att säkerhetsarbetet i stället anpassas genom kompletterande lösningar, där skyddet utgörs av inneslutande strukturer genom exempelvis segmentering och kontroll av nätverkstrafik, något som IP1a benämner som en ”krockkudde”. Detta sammanfaller med hur Wai och Lee (2023) menar att det tekniska säkerhetsarbetet i legacy-system ser ut, nämligen att skyddet är arkitektoniskt inneslutande genom segmentering och nätverksövervakning, när systemet i sig inte kan anpassas. Detta skapar ett beroende av att de omslutande skydden fungerar felfritt, eftersom ett genombrott kan lämna dei sig sårbara systemen exponerade.

Som presenteras i empirin i den organisatoriska kontexten arbetar flera av organisationerna utefter standarder och ramverk såsom ISO 27001 och NIST CSF, även om de inte är certifierade. Arbetssätt utefter dessa ramar är förväntat enligt tidigare studier då ISO 27001 och NIST CSF anses som etablerade och globalt erkända (Culot et al. 2021; Salas-Riega et al. 2025). Syntesen beskriver nätverks- och mjukvarusäkerhet som en central kontrollkategori inom dessa ramverk, och att denna innefattar accesskontroll, övervakning och nätverksskydd, såsom segmentering och brandväggar (Tanjung et al. 2024). Som presenterats i litteraturgenomgången syftar en kombination av dessa skydd, tillsammans med exempelvis loggning, som “defense in depth” kombineras (Chandra et al. 2015). Även om IP6 beskriver det som att de använder lager ovanpå systemen vilket kan tolkas som en applicering av “defense in depth” för en starkare säkerhet, kontradikterar IP5 detta arbetssätt genom att mena att de inte gör det. IP5 uttrycker dock att detta innebär att systemen är känsliga, vilket sammanfaller med avsikten med “defense in depth” som ett förstärkt skydd (Chandra et al. 2015).

Relaterat till ovan presenterar empirin en förskjutning från egenutvecklade system mot externa, standardiserade system, vilket sammanfaller med identifierade trender som presenterats i litteratur gällande att organisationer migrerar från proprietära lösningar till

standardiserade molnplattformar (Hajra och Goel, 2025; Bhamare et al.2020; Nankya et al. 2023). Informanterna uppfattar att dessa upplevs ha bättre inbyggd säkerhetsfunktion och lättare säkerhetsuppdatering. Detta sammanfaller med argument i litteraturen gällande att leverantörer genom certifierade ramverk (ISO 27001) och automatiserade uppdateringar anses kunna hålla en högre säkerhetsnivå än enskilda organisationer (Khokrale, 2025).

Utöver att höja den rent tekniska säkerhetsnivån som intervjupersonerna och litteraturen beskriver, kan en förskjutning till leverantörer som strukturellt följer standarder, specifikt ISO 27001, dessutom ge en konkret skjuts gällande arbetet med efterlevnad av regulatoriska krav (Folorunso, 2024; Rakshan, 2025). Empirin tar dock inte upp några upplevda risker gällande det som litteraturen beskriver som leverantörslåsning (Hustad et al. 2021, Opara-Martins et al, 2016), vilket kan antyda en bristande medvetenhet i organisationernas strategiska riskanalys. Medan litteraturen betonar de långsiktiga ekonomiska och operativa riskerna med leverantörslåsning, tenderar empirin att fokusera på de omedelbara vinsterna i form av teknisk säkerhet, vilket kan leda till att inlåsningseffekter förbises i beslutsfattandet.

## 6.2 Organisatorisk kontext

### *6.2.1 Compliance: organisatorisk börda och kapacitet*

Empirin visar att cybersäkerhetslagen medför en påtaglig administrativ börda för organisationerna, inte enbart i form av ökad arbetsbelastning utan som en förskjutning av vad säkerhetsarbetet faktiskt består av. Fokus rör sig från att hantera säkerhetsproblem i praktiken mot att dokumentera och bevisa att arbetet genomförs, vilket bekräftar det Veigurs et al. (202) beskriver som compliance burden, där organisationer behöver avsätta omfattande resurser för att uppfylla administrativa krav på dokumentation, rapportering och uppföljning, med risk för att fokus förskjuts från faktisk säkerhetsförbättring till formalia.

Det är dock viktigt att skilja mellan börda kopplad till lagstiftningens syfte och börda kopplad till hur kraven konkretiserats i MCFs föreskrifter. IP1b:s oro för att resurser läggs på rapportering snarare än att lösa det faktiska problemet och IP3:s formulering om ”overhead på overheaden” (IP3, 00:31:03) pekar inte på ett motstånd mot regleringen som sådan utan på en upplevelse av att föreskrifternas utformning genererar administrativt arbete som inte nödvändigtvis stärker säkerheten. IP6 förstärker denna bild men tillägger att syftet med rapporteringen, att på samhälls-nivå skapa överblick över incidenter och möjliggöra varning till andra aktörer, är legitimt. Detta ligger i linje med den kritik som Svenskt Näringsliv (2025) och branschföreträdare i media (Svenska Dagbladet, 2025; Dagens Industri, 2026) har riktat mot MCF:s föreskrifter. Det är en distinktion som är central för hur compliance capability kan förstås: förmågan att uppnå långsiktig regulatorisk efterlevnad påverkas inte enbart av organisationens interna resurser, utan även av hur regulatoriska krav formuleras och vilken administrativ friktion de genererar (Veigurs et al. 2024).

Bördan är inte heller enbart resursmässig. Busetti och Scanni (2025) beskriver att otydlighet kring definitioner av rapporteringspliktiga incidenter och bedömningar av incidenters allvarlighetsgrad kan skapa variation i hur regulatoriska krav tolkas och omsätts i praktiken. IP3 beskriver hur oklarheten kring vad som är relevant och ska rapporteras i sig utgör en källa till administrativt merarbete. Bördan är således inte bara ett kvantitativt resursproblem utan

även ett tolkningsproblem, där organisationer själva måste lägga tid på att förstå vad som faktiskt förväntas av dem.

Detta är särskilt problematiskt i livsmedelssektorn, som genom NIS2 för första gången inkluderats som samhällsviktig sektor inom EU:s cybersäkerhetsreglering. Busetti och Scanni (2025) beskriver hur variationer i organisatorisk kapacitet påverkar förutsättningarna för regulatorisk implementering, vilket antyder att compliance burden riskerar att träffa hårdare i sektorer som saknar erfarenhet av liknande regulatoriska krav.

Empirin bekräftar sammantaget att compliance burden är en reell utmaning inom livsmedelssektorn, inte enbart resursmässig utan även tolkningsrelaterad, och att den primärt upplevs som ett problem med föreskrifternas utformning snarare än med lagstiftningens syfte. Detta indikerar att förutsättningarna för regulatorisk efterlevnad påverkas av hur krav formuleras i lika hög grad som av organisationernas interna kapacitet.

Parallellt med compliance burden framträder även skillnader i hur organisationerna själva uppfattar sin nuvarande compliance i relation till cybersäkerhetslagen. Informanternas beskrivningar av den egna organisationens beredskap speglar betydande skillnader i hur långt anpassningsprocessen har kommit. IP2 och IP3 beskriver sig ha kommit långt, där IP3 explicit lyfter det tidigare NIS-direktivet som en ”bra grundplåt” (IP3, 00:20:47) vilket antyder att tidigare erfarenheter av liknande regulatoriska krav kan underlätta anpassningen till nya krav. IP6 menar däremot att F6 befinner sig i ett tidigt skede och ifrågasätter om dess incidenthanteringsprocess är tillräckligt mogen, medan IP5 beskriver att F5 har god kontroll i dag men att cybersäkerhetslagen innebär ett utökat krav på att granska hela värdekedjan, inklusive leverantörernas cybersäkerhetsförmåga.

Variationen i upplevd beredskap kan förstås i ljuset av Busetti och Scanni (2025), som beskriver hur variationer i organisatorisk kapacitet och cybersäkerhetsmognad påverkar förutsättningarna för regulatorisk implementering. Detta indikerar att compliance inte är ett statiskt tillstånd utan ett löpande arbete som förändras i takt med att regulatoriska krav utvecklas, något som Racz et al. (2010) beskriver som centralt i ett GRC-perspektiv där kontinuerlig övervakning och uppföljning utgör kärnan i organisationers compliance-arbete.

Skillnaderna i informanternas beskrivningar av den egna organisationens beredskap antyder att organisationers förutsättningar för anpassning till nya regulatoriska krav i hög grad påverkas av tidigare erfarenheter av liknande regelverk och i vilken utsträckning relevanta processer och strukturer redan finns på plats.

### *6.2.2 Regulatoriska krav som intern förändringskraft*

Cybersäkerhetslagen tillför en extern auktoritet som förändrar de interna förutsättningarna för att driva igenom säkerhetsinitiativ. Att samtliga svenska informanter beskriver hur de kan luta sig mot lagkraven vid genomdrivande av beslut antyder att en sådan extern auktoritet reducerar behovet av intern förhandling, något som Herath och Rao (2009) beskriver i termer av hur formella mekanismer förändrar de incitament som styr medarbetares och ledningens beteende. IP1a illustrerar detta genom att beskriva hur man internt kan ”peka med hela handen” (IP1a, 01:32:02) mot lagkraven utan att någon diskussion krävs.

Empirin antyder att cybersäkerhetslagen fyller en legitimeringsfunktion som stärker interna aktörers mandat på ett sätt som rent interna initiativ inte förmår. Detta blir särskilt tydligt i

relation till det motstånd som informanterna beskriver vid försök att driva igenom säkerhetsinitiativ utan externt stöd.

Motståndet som informanterna beskriver tar sin grund i att säkerhetsinitiativ upplevs som kostsamma och resurskrävande utan att direkt bidra till kärnverksamheten. IP5 illustrerar detta med att initiativen inte bidrar till att organisationen ”säljer mer och tjänar pengar” (IP5, 00:11:41), och IP3 beskriver det som en ”jätteutmaning” (IP3, 00:15:13) att driva igenom interna initiativ. Busetti och Scanni (2025) beskriver hur resursbegränsningar och organisatorisk tröghet kan försvåra regulatorisk implementering och empirin antyder att samma mekanismer även försvårar genomdrivandet av interna initiativ. IP6 lyfter dock fram att lagkraven tillför externa konsekvenser, såsom straffavgifter och näringsförbud, vilket skapar en drivkraft som interna initiativ saknar och som motiverar organisationsledningen att agera.

IP4, som är verksam utanför Sverige, tillför ett kompletterande perspektiv och menar att inställningen till säkerhetsinitiativ inte nödvändigtvis kräver regulatorisk motivation, förståelsen för de verksamhetsmässiga konsekvenserna av att inte genomföra säkerhetsinitiativen kan vara tillräcklig. IP4 exemplifierar med att personal på fabriksnivå, trots att de befinner sig långt ifrån arbete med EU-regleringar, ”vet utmärkt väl vad en timmes driftstopp kostar och vad det innebär” (IP4, 00:30:15) vilket underlättar att motivera säkerhetsåtgärder. Detta relaterar till Herath och Rao (2009) som beskriver hur informella mekanismer såsom organisatoriska normer och individers upplevda betydelse av säkerhetsarbetet kan komplettera eller ersätta formella styrmekanismer. Samtidigt konstaterar IP4 att ju lägre mognad en organisation har, desto mer motiverande är regleringar, vilket kan förstås i ljuset av Busetti och Scanni (2025) som visar att variationer i organisatorisk kapacitet påverkar förutsättningarna för regulatorisk implementering. IP4 antyder även att lagkraven och verksamhetsförståelse snarare är kompletterande drivkrafter än konkurrerande, där behovet av det förstnämnda minskar i takt med att det sistnämnda ökar.

Empirin antyder att regulatoriska krav kan fylla en legitimerande funktion som underlättar genomdrivandet av säkerhetsinitiativ i organisationer där sådana initiativ annars möter motstånd, men att behovet av denna externa drivkraft varierar beroende på organisationens mognad och medarbetarnas förståelse för de verksamhetsmässiga konsekvenserna av bristande säkerhet.

Utöver att fungera som en legitimerande kraft för interna initiativ har cybersäkerhetslagen, enligt flera informanter, även fungerat som en drivkraft för säkerhetsarbete som organisationerna annars inte hade genomfört. IP4 uttrycker att lagen ”utan tvekan” (IP4, 00:12:05) har fungerat som en katalysator för organisationer som saknat ett tydligt säkerhetsarbete och IP2 menar att en konstruktiv effekt är att man tvingas se över sina system, vilket ses som ”bara positivt” (IP2, 01:08:50). IP5 beskriver hur säkerhetstänket har förändrats från ”nu gör vi det, och sen är det bra” (IP5, 00:16:13) till ett mer kontinuerligt arbete, vilket har inneburit en reell säkerhetsförbättring. Detta kan relateras till Busetti och Scanni (2025), som beskriver hur incidenthantering och efterföljande analys kan bidra till utveckling av organisationers cybersäkerhetsmognad och stärkt compliance capability över tid.

Inställningen till lagen är dock inte entydig. IP1a uttrycker att föreskrifternas detaljeringsgrad begränsar organisations handlingsutrymme och tvingar fram val av tekniker som

organisationen inte behärskar, på bekostnad av lösningar som skulle stärka säkerheten mer effektivt:

> Om vi hade fått lov att själva tänka ut hur vi ville lösa de här sakerna, om det var mer generellt skrivet, så hade vi kunnat lägga pengar på rätt saker. Vi hade kunnat bli bättre. Men som det är skrivet nu och de remisser som har varit ute är precis tvärtom. Det kommer att göra att vi måste välja tekniker som vi inte kan, som vi inte har behov av och som vi absolut inte vill använda i stället för att ta något annat som vi är duktiga på, som vi ser löser våra problem och som gör det säkrare. Men de får vi inte använda, för de stämmer inte med lagen. (IP1a, 00:51:21)

IP3 uttrycker liknande tankar och menar att oavsett om ”man har en cybersäkerhetslag eller rapporteringsskyldighet” (IP3, 00:11:03) eller inte så kommer man att skydda sitt företag och sin data. Detta antyder att för organisationer med hög mognad i sitt informationssäkerhetsarbete kan detaljstyrda föreskrifter upplevas som ett hinder snarare än ett stöd, ett mönster som speglar det Veigurs et al. (2024) beskriver om att regulatoriska krav kan bidra till compliance burden när de är utformade på ett sätt som inte tar hänsyn till organisationers varierande förutsättningar och befintliga säkerhetsarbete.

På längre sikt antyder empirin att regulatoriska krav inte enbart förändrar vad organisationer gör utan även hur roller och ansvar struktureras. IP5 beskriver hur säkerhetsrollen har förskjutits från att primärt handla om tekniskt skydd till att i allt högre grad omfatta organisatorisk systematik och dokumentation: ”du måste ha en systematik i arbetet, att det är dokumenterat, hur vi gör och hur vi arbetar” (IP5, 00:06:48). IP5:s beskrivning antyder att regulatoriska krav inte enbart påverkar vad organisationer gör utan även hur arbetet med informationssäkerhet förändras över tid.

Empirin visar sammantaget att cybersäkerhetslagens katalyserande effekt inte är entydig. För informanter som beskriver ett tidigare mindre utvecklat informationssäkerhetsarbete upplevs lagen som en välkommen drivkraft, medan informanter med ett mer utvecklat informationssäkerhetsarbete snarare upplever att föreskrifternas detaljeringsgrad begränsar handlingsutrymmet. Detta antyder att detaljstyrda krav riskerar att motverka sitt syfte i organisationer som redan har etablerade informationssäkerhetsstrukturer på plats.

### *6.2.3 Säkerhetsarbete: förhållningssätt och arbetssätt*

Gällande samordningen av informationssäkerhetsarbetet är ett återkommande mönster i empirin att det operativa ansvaret för att samordna och driva organisationens arbete med cybersäkerhetslagen i praktiken faller på IT-avdelningen, trots att frågorna berör hela organisationen. IP3 beskriver hur gränsdragningar mellan IT-säkerhet, fysisk säkerhet och regulatorisk efterlevnad ofta blir otydliga och bollas tillbaka till IT och IP5 betonar att IT-avdelningen tvingas initiera och driva processer trots en medvetenhet om att IT inte äger själva informationen. Detta kan relateras till Teichmann (2025) som framhåller att regulatorisk implementering förutsätter tydlig ansvarsfördelning och organisatorisk styrning och till Racz et al. (2010) som beskriver hur processer, roller och ansvar behöver struktureras upp för att möjliggöra kontinuerlig övervakning och uppföljning. Empirin antyder att just denna strukturering utgör en central utmaning i praktiken.

IT/OT-samordningen tillför en sektorsspecifik dimension. IP6 beskriver hur NIS2:s krav på segregering mellan IT och OT förutsätter ett samarbete med OT-sidan, som saknar egna resurser för NIS2-arbetet, vilket innebär att IT-avdelningen måste samordna arbetet utan att äga implementeringen. Livsmedelssektorn är i hög grad beroende av cyber-fysiska system där IT och OT är tätt integrerade, vilket innebär att samordningsutmaningarna inte enbart är organisatoriska utan även tekniskt betingade.

IP4 tillför ett kompletterande perspektiv genom att beskriva en centralt distribuerad modell där koncernen sätter kraven medan affärsenheterna ansvarar för genomförandet. Denna struktur hanterar samordningsproblemet på ett annat sätt än vad de svenska informanterna beskriver.

Ansvarsfördelningen för incidentrapportering illustrerar samordningsproblematiken ytterligare. IP3 beskriver oklarheter kring vem som faktiskt bär rapporteringsansvaret kontra vem som bara sammanställer incidentdata, medan IP5:s organisation hanterar detta genom en centraliserad modell där rapporteringen sköts centralt av IT: ”det ligger inte ute i verksamheten att någon ska rapportera in till den här inrapporteringsmyndigheten, utan det gör vi [centralt på IT]” (IP5, 00:43:06). Att organisationer löser detta på olika sätt indikerar att ansvarsfördelningen för incidentrapporteringen kräver aktiva strukturella val från organisationens sida.

Empirin indikerar att cybersäkerhetslagen lägger ansvaret för informationssäkerhet på organisationsledningen men att det operativa samordningsarbetet i praktiken kräver aktiva strukturella val som lagen inte föreskriver. Hur organisationer hanterar ansvarsfördelning, rapporteringsvägar och IT/OT-samordning varierar påtagligt, vilket antyder att compliance capability i den organisatoriska kontexten inte enbart handlar om resurser utan även om hur organisationer väljer att strukturera sitt informationssäkerhetsarbete.

En annan central fråga rör ledningens ansvar i arbetet med informationssäkerhet. Cybersäkerhetslagen innebär att det yttersta ansvaret för informationssäkerhet formellt placeras på organisationsledningen. IP6:s beskrivning av hur informationssäkerhet tidigare behandlats som en IT-fråga snarare än en organisationsövergripande fråga illustrerar varför detta upplevs som en betydelsefull förändring.

> det ligger ju liksom på IT-avdelningen, informationssäkerhet, vilket är korrekt. Men det som man alltid har fått kämpa med länge är just det här att det här är ju en angelägenhet för hela verksamheten. Det är ju inte liksom en IT-fråga som man bara dumpar hos IT-avdelningen och sen har man löst det. … Det jag tycker är intressant med NIS 2 är ju att man verkligen vill lyfta det och lägga ansvaret på ledningen och säga att det här är ert ansvar och ni kan inte komma undan. (IP6, 00:01:18)

IP4 tillför ett kompletterande perspektiv och menar att detta skifte är nödvändigt, utan budget, mandat och direkt kontakt med styrelsen riskerar informationssäkerhetsarbetet att stanna av oavsett hur kompetent den säkerhetsansvarige är. Detta kan relateras till Teichmann (2025) som beskriver att implementering av regulatoriska cybersäkerhetskrav förutsätter organisatorisk styrning och tydligt ledningsansvar, inte enbart tekniska eller juridiska lösningar.

Empirin visar dock att ett formellt ledningsansvar inte automatiskt innebär ett reellt engagemang. IP6 beskriver att det praktiska arbetet fortfarande tenderar att hamna på IT-avdelning och att övriga i ledningen förväntar sig att IT kan hantera det. Detta antyder ett gap mellan det ansvar lagen formellt tillskriver ledningen och hur ansvaret faktiskt fördelas i praktiken.

Att omsätta det formella ledningsansvaret i praktiken kräver aktiva åtgärder från organisationernas sida. IP6 illustrerar detta genom att beskriva hur hen aktivt arbetat med att medvetandegöra ledningen, bland annat genom en session där samtliga direktörer informerades om cybersäkerhetslagen, så att ingen kan hävda okunnighet. Detta antyder att lagens värde inte enbart ligger i att formellt fördela ansvar, utan i att skapa ett incitament som organisationer sedan måste omsätta i praktiken.

Hur detta omsätts i organisationernas praktiska arbete skiljer sig åt. Organisationernas säkerhetsarbete bygger i stor utsträckning på internationella ramverk och standarder, men ambitionsnivån och det praktiska genomförandet varierar påtagligt. Att flera organisationer arbetar mot ISO 27001 eller NIST CSF utan att vara certifierade antyder att ramverken primärt upplevs ha ett värde som strukturerande verktyg snarare än som formella krav att uppfylla.

Organisationernas förhållningssätt till standarder och certifieringar skiljer sig åt. IP1a menar att de inte ser nyttan med att "lägga den tiden" (IP1a, 01:00:22) på certifiering och föredrar en anpassad riskhantering, medan IP3 påpekar att leverantörskrav kopplade till ISO 27001 driver dem mot standarden trots avsaknad av certifiering. IP4 tillför ett kompletterande perspektiv genom att ha utvecklat en egen cyberkatalog baserad på CSF, vilket möjliggör kartläggning av styrning och ansvarsfördelning utan att vara bunden till en specifik standard. Att organisationer således arbetar mot liknande mål genom olika tillvägagångssätt antyder att vägen till ett strukturerat informationssäkerhetsarbete inte är entydig utan formas av verksamhetens specifika behov och förutsättningar. Att IP1a föredrar anpassad riskhantering framför certifiering medan IP3 drivs mot standarder av leverantörskrav snarare än egna val, kan relateras till Herath och Rao (2009) som beskriver hur compliance formas av både formella mekanismer såsom policys och kontrollsystem samt informella mekanismer såsom organisatoriska normer. Skillnaden IP1a och IP3 emellan speglar hur dessa mekanismer väger olika tungt i olika organisationer.

Kontinuitetsplaner utgör ett konkret exempel på hur informationssäkerhetsarbetet har fördjupats. IP1a beskriver att en sådan plan existerar men ännu inte är dokumenterad: "i huvudet på folk. Finns ju inte dokumenterat tyvärr. Utan det är ju det vi vill göra nu" (IP1a, 01:03:38), medan IP2 och IP5 menar att sådana planer finns på plats. Skillnaden mellan dessa organisationer illustrerar att systematisering av informationssäkerhetsarbetet befinner sig i olika stadier, och att dokumentation i sig utgör en del av det arbete som krävs för att omsätta compliance capability i praktiken.

Outsourcing och externa partners påverkar hur ansvaret för säkerhetsarbetet fördelas. IP2 beskriver exempelvis hur penetrationstester genomfördes när affärssystemet flyttades till en extern leverantörs molnlösning, vilket illustrerar att outsourcing inte innebär att det regulatoriska ansvaret överlåts. Detta kan relateras till Busetti och Scanni (2025), som beskriver hur begränsad intern kapacitet och resursbegränsningar kan försvåra regulatorisk implementering, och outsourcing framstår således som ett sätt att hantera sådana begränsningar utan att frånta organisationen ansvaret.

Utbildning och phishingkampanjer beskrivs av IP1, IP3 och IP6 som centrala delar av informationssäkerhetsarbetet. Att dessa insatser återfinns hos flera organisationer oberoende av varandra kan relateras till Herath och Rao (2009), som beskriver att medarbetares efterlevnad av informationssäkerhetspolicys utgör en central del av organisationers informationssäkerhetsarbete och att sådan efterlevnad påverkas av organisatoriska mekanismer såsom styrning, kontroll och social påverkan. Regelbundna utbildningar kan således förstås som ett sätt att bygga upp och upprätthålla sådana mekanismer i praktiken.

Variationen i hur organisationerna strukturerar sitt informationssäkerhetsarbete antyder att compliance capability inte byggs upp på ett enhetligt sätt, utan formas av organisationernas specifika förutsättningar, resurser och val. Gemensamt för samtliga organisationer är dock att informationssäkerhetsarbetet sträcker sig bortom tekniska åtgärder och i allt högre grad omfattar organisatoriska processer, dokumentation och medarbetarengagemang.

Utöver hur arbetet är organiserat framträder även ett mönster i hur informanterna förhåller sig till det. Spänningen mellan att upprätthålla en hög säkerhetsnivå och att behålla en fungerande verksamhet är ett återkommande tema. IP2 och IP6 beskriver båda hur informationssäkerhetsarbetet måste balanseras mot produktivitet och kostnader, och att det är nödvändigt att acceptera vissa risker för att verksamheten ska kunna fungera. Detta speglar en pragmatisk inställning där total säkerhet inte är ett realistiskt mål utan snarare ett kontinuerligt arbete med att hantera och prioritera risker.

IP1a uttrycker en explicit kritik mot ett kontrollbaserat förhållningssätt och beskriver hur de tolkar cybersäkerhetslagens föreskrifter som en riktning snarare än "en checklista" (IP1a, Skriftlig komplettering, Ref 3.3). Detta antyder att föreskrifterna upplevs ha ett värde som vägledning snarare än som en uppsättning krav att bocka av, och att ett riskbaserat förhållningssätt i vissa fall upplevs som mer ändamålsenligt för att faktiskt stärka säkerheten.

IP2:s vision om att säkerhetsrutiner ska bli en naturlig del av vardagen utan att upplevas som betungande illustrerar en ambition om att förankra informationssäkerhetsarbetet i organisationskulturen snarare än i formella krav. Detta kan relateras till Herath och Rao (2009), som beskriver att långsiktig efterlevnad förutsätter att organisationer förmår etablera en säkerhetskultur där informella mekanismer såsom normer och individers upplevda betydelse av det egna säkerhetsarbetet stödjer efterlevnaden.

Variationen i förhållningssätt antyder att compliance capability inte enbart handlar om att implementera tekniska kontroller eller följa föreskrifter, utan om organisationers förmåga att integrera informationssäkerhetsarbetet i verksamhetens processer och kultur på ett sätt som är hållbart över tid. Papazafeiropoulou och Spanaki (2016) beskriver att compliance capability förutsätter att processer, roller och ansvar struktureras för att möjliggöra kontinuerlig övervakning och uppföljning, och Racz et al. (2010) beskriver GRC som ett integrerat perspektiv där styrning, riskhantering och regulatorisk efterlevnad samordnas på ett sammanhängande sätt. Båda perspektiven speglar den ambition om integrerat och kulturförankrat säkerhetsarbete som informanterna ger uttryck för.

## 6.3 Extern kontext

### *6.3.1 Navigering i det regulatoriska landskapet*

Empirin visar att informanterna uppfattar graden av nationell avvikelse mellan cybersäkerhetslagen och NIS2-direktivet på olika sätt.

Detta ligger i linje med tidigare forskning som beskriver att NIS2-direktivet innehåller en relativt hög grad av flexibilitet och tolkningsutrymme, vilket kan bidra till variation i hur regelverket implementeras mellan medlemsstater beroende på nationella tolkningar, tillsynsstrukturer och regulatoriska förutsättningar (Veigurs et al. 2024; Teichmann, 2025).

Denna flexibilitet framgår även i IP4:s beskrivning av NIS2 som en flexibel och proportionerlig typ av lagstiftning, där säkerhetsåtgärder förväntas anpassas efter verksamhetens storlek och riskbild snarare än genom exakt specificerade lösningar. Samtidigt beskriver IP4 att denna flexibilitet ställer krav på organisationers egen förmåga att förstå och bedöma sina säkerhetsbehov, vilket indikerar att flexibiliteten i NIS2-direktivet kan förutsätta en viss grad av digital mognad och cybersäkerhetsmognad för att regulatoriska krav ska kunna tolkas och omsättas i praktiken.

Flera informanter upplever att den svenska implementeringen är mer omfattande än vad som krävs enligt direktivet, vilket i vissa delar kan indikera tendenser till gold-plating, där nationell implementering går längre än vad som är nödvändigt för att uppfylla EU-direktiv (Squintani, 2019). Detta blir särskilt tydligt i IP1a:s beskrivning av att NIS2-direktivets ursprungliga intention och flexibilitet upplevs ha försvagats genom MCF:s mer detaljstyrande nationella föreskrifter.

Samtidigt visar empirin att denna uppfattning inte delas av samtliga informanter, då vissa snarare upplever att skillnaderna främst rör incidentrapportering. Detta kan indikera att upplevelsen av regulatorisk avvikelse även påverkas av organisatoriska förutsättningar, erfarenheter och hur regelverket tolkas i praktiken.

Empirin indikerar därmed att den flexibilitet som NIS2-direktivet bygger på både kan möjliggöra proportionalitet och verksamhetsanpassning, men samtidigt skapa variation, tolkningsutrymme och osäkerhet kring hur regulatoriska krav konkretiseras och implementeras på nationell nivå. Detta tyder även på att nationella variationer i implementeringen kan uppfattas olika beroende på verksamheters organisatoriska förutsättningar och erfarenheter, oavsett om variationerna kan betraktas som gold-plating eller inte.

Informanternas beskrivningar visar att incidentrapportering utgör ett konkret exempel på de tolkningsutmaningar som kan uppstå när flexibla regulatoriska krav omsätts i praktiken. Informanternas beskrivningar indikerar att osäkerheten framför allt rör bedömningen av vilka incidenter som omfattas av rapporteringskraven samt hur dessa krav ska omsättas i praktiken.

Detta ligger i linje med Busetti och Scanni (2025), som beskriver att otydlighet kring definitioner av rapporteringspliktiga incidenter och bedömningar av incidenters allvarlighetsgrad kan skapa variation i hur regulatoriska krav tolkas och omsätts i praktiken. Informanternas beskrivningar tyder även på att osäkerheten inte enbart handlar om förståelsen

av regelverket, utan även om det praktiska ansvar som läggs på verksamheterna att själva avgöra när rapporteringsskyldighet föreligger. Detta illustreras tydligt genom att olika informanter problematiserar olika typer av incidenter i relation till rapporteringskraven. IP1a och IP1b lyfter exempelvis problem med etikettutskrifter, medan IP2 och IP3 beskriver spammejl och phishingförsök som incidenter som upplevs oproportionerliga att rapportera. IP5 beskriver samtidigt att de i praktiken själva behöver avgöra vilka incidenter som anses rapporteringsvärda.

Att flera informanter samtidigt beskriver osäkerhet kring incidentrapporteringen kan problematiseras i relation till Busetti och Scanni (2025), som beskriver incidentrapportering som en central del av cybersäkerhetsrelaterade regulatoriska krav. Informanternas beskrivningar indikerar samtidigt att betydande resurser och administrativt arbete behöver läggas på att tolka och bedöma vilka incidenter som faktiskt omfattas av rapporteringskraven.

Detta omfattar både bedömningen av vilka incidenter som är rapporteringspliktiga och den efterföljande regulatoriska hanteringen av sådana incidenter. Empirin ger därmed konkreta exempel på den compliance burden som Veigurs et al. (2024) beskriver i relation till implementeringen av NIS2-direktivet, särskilt genom omfattande krav på dokumentation, rapportering och regulatorisk uppföljning.

Den osäkerhet som beskrivs kring cybersäkerhetslagens krav tycks även öka betydelsen av dialog och samverkan mellan verksamhetsutövare och tillsynsmyndigheter. IP1a, IP2 och IP5, som medverkar i Livsmedelsverkets forum SKAL, beskriver exempelvis samarbetet med Livsmedelsverket som en viktig resurs i arbetet med regulatoriska frågor kopplade till cybersäkerhetslagen. SKAL är Livsmedelsverkets samrådsgrupp för krisberedskapsplanering inom livsmedelsförsörjningen och beskrivs som ett viktigt forum för dialog mellan myndigheter och verksamhetsutövare kring cybersäkerhetslagen och relaterade regulatoriska frågor.

Samtidigt beskriver framför allt IP1a en tydlig skillnad mellan Livsmedelsverkets och MCF:s arbetssätt, där Livsmedelsverket upplevs ha större förståelse för verksamheternas praktiska förutsättningar medan MCF i högre grad uppfattas fokusera på bokstavlig tolkning av regulatoriska krav. Empirin pekar därmed mot en spänning mellan sektorsspecifik verksamhetsförståelse och centraliserad regulatorisk styrning. Empirin ger även konkreta uttryck för det som Veigurs et al. (2024) beskriver kring hur nationella styrningsstrukturer påverkar implementeringen och tolkningen av cybersäkerhetsrelaterade regulatoriska krav. Flera informanter beskriver samtidigt att Livsmedelsverket och verksamhetsutövarna inom SKAL i vissa fall delar uppfattningar kring behovet av förändringar i MCF:s föreskrifter, men att dessa synpunkter ändå upplevs få begränsat genomslag i den slutliga regulatoriska utformningen.

Detta indikerar på att det finns olika uppfattningar kring hur cybersäkerhetsrelaterade regulatoriska krav bör konkretiseras och omsättas i praktiken inom olika verksamheter. Medan IP1a beskriver ett behov av att i större utsträckning anpassa regulatoriska krav efter praktiska situationer inom livsmedelssektorn, menar IP2 att föreskrifterna i grunden bör vara branschöverskridande. Skillnaderna mellan informanternas uppfattningar kan även relateras till Busetti och Scanni (2025), som beskriver att organisatoriska och sektorsspecifika förutsättningar påverkar hur cybersäkerhetsrelaterade regulatoriska krav förstås och omsätts i praktiken.

### 6.3.2 Branschsamverkan och erfarenhetsutbyte

Informanternas beskrivningar indikerar ett behov av informationsutbyte och samverkan mellan verksamhetsutövare i relation till cybersäkerhetsrelaterade hot och incidenter. Flera informanter uppger att det saknas formella strukturer för sådan samverkan utanför forum såsom SKAL, vilket ligger i linje med Veigurs et al. (2024), som beskriver att NIS2 saknar tydliga mekanismer för samverkan och informationsdelning mellan verksamhetsutövare, vilket innebär att sådant samarbete i stor utsträckning blir beroende av verksamhetsutövarnas egna initiativ. Detta kan innebära att verksamhetsutövare själva behöver initiera och upprätthålla forum för informationsutbyte och samverkan.

Både IP2 och IP4 beskriver också cybersäkerhet som ett område där verksamheter snarare behöver samverka än konkurrera. IP2 betonar exempelvis att ingen verksamhet gynnas av att en annan aktör inom livsmedelssektorn utsätts för en cyberattack och menar att verksamheter därför behöver samverka, dela information och hjälpas åt. IP2 beskriver även att informationsdelning kan bidra till att identifiera gemensamma mönster i cyberattacker och på så sätt stärka verksamheters chanser att identifiera och förebygga liknande incidenter. Detta visar även på att cybersäkerhet inte enbart uppfattas som en intern organisatorisk fråga utan även som en bredare sektors- och samhällsrelaterad fråga.

Flera informanter beskriver dock samtidigt att möjligheterna till informationsdelning påverkas av juridiska och regulatoriska begränsningar. IP3 beskriver exempelvis att konkurrensrättsliga aspekter och risker kopplade till kartellbildning påverkar organisationens vilja att delta i samverkansforum. Informanterna beskriver även att nationella regler kan begränsa möjligheterna att dela incidentrelaterad information såsom IP-adresser kopplade till cyberincidenter. Detta indikerar en möjlig paradox där informationsdelning och samverkan beskrivs som viktiga delar av cybersäkerhetsarbetet, samtidigt som juridiska och regulatoriska strukturer kan begränsa sådant informationsutbyte mellan verksamhetsutövare. Samtidigt syftar flera av dessa juridiska begränsningar i sig till att skydda andra samhälleliga och säkerhetsrelaterade intressen, såsom rättssäkerhet, konkurrensneutralitet och skyddet av känslig information. Empirin synliggör därmed hur cybersäkerhetsarbete kan präglas av avvägningar mellan olika regulatoriska och säkerhetsrelaterade intressen.

### 6.3.3 Ojämna förutsättningar, delat samhällsansvar

Busetti och Scanni (2025) beskriver att implementeringen av cybersäkerhetsrelaterade regulatoriska krav påverkas av variationer i organisationers compliance capability och organisatoriska förutsättningar, där faktorer såsom resursbegränsningar, kompetensbrist och varierande cybersäkerhetsmognad kan försvåra långsiktig compliance och incidenthantering. Detta framträder tydligt i informanternas beskrivningar av hur verksamheters storlek, resurser, kompetens, digitala mognad och ledningsengagemang påverkar möjligheterna att hantera cybersäkerhetsrelaterade lagkrav. Variationerna i organisatoriska förutsättningar och cybersäkerhetsmognad kan även relateras till att livsmedelssektorn först genom NIS2-direktivet inkluderats, medan andra sektorer sedan tidigare omfattats av NIS-direktivet.

Flera informanter beskriver exempelvis att mindre verksamheter riskerar att påverkas oproportionerligt av lagkraven, särskilt då de ofta saknar dedikerade cybersäkerhetsfunktioner, organisatoriska strukturer och resurser för att hantera regulatorisk implementering och långsiktig efterlevnad. Informanterna beskriver även att graden av digital mognad varierar både mellan och inom verksamheter, samtidigt som IP6 betonar att

ledningens engagemang kan vara avgörande för organisationers möjligheter att arbeta framgångsrikt med compliance. Detta stämmer även överens med Teichmann (2025), som beskriver att regulatorisk implementering inte enbart är en teknisk eller juridisk fråga utan även förutsätter organisatorisk styrning och ledningsansvar.

Informanternas beskrivningar indikerar samtidigt olika perspektiv på proportionalitet i relation till cybersäkerhetslagen. Medan flera informanter beskriver att lagkraven riskerar att påverka mindre verksamheter oproportionerligt, framhåller IP4 att NIS2 samtidigt bygger på en proportionalitetsprincip där säkerhetsåtgärder ska anpassas efter både verksamheters storlek och risknivå. Detta stämmer även överens med NIS2-direktivets indelning mellan väsentliga och viktiga verksamheter, där tillsyn och potentiella sanktionsavgifter differentieras mellan olika typer av verksamhetsutövare. IP4 beskriver dock detta som ”jätteenkelt och jättesvårt samtidigt”, vilket indikerar att bedömningen av vad som är proportionerliga säkerhetsåtgärder kan vara komplex i praktiken. Vad som uppfattas som proportionerliga säkerhetsåtgärder kan därmed variera mellan verksamheter med olika organisatoriska förutsättningar och nivåer av cybersäkerhetsmognad.

Busetti och Scanni (2025) framhåller att förutsättningarna för regulatorisk implementering påverkas av sektorspecifika förhållanden. Detta framträder även i informanternas beskrivningar av livsmedelssektorns roll i samhällsförsörjning, beredskap och totalförsvar.

Informanternas beskrivningar av det förändrade världsläget och det ökade behovet av cybersäkerhetsarbete kan relateras till EU:s ökade reglering inom informationssäkerhet och cybersäkerhet genom regelverk såsom GDPR, NIS-direktivet och NIS2-direktivet. Regelverken syftar till att harmonisera arbetet med informationssäkerhet, cybersäkerhet och motståndskraft inom samhällsviktiga verksamheter i EU. Detta framträder även i informanternas syn på livsmedelssektorns betydelse för samhällsförsörjning, nationell beredskap och totalförsvar, där inkluderingen av livsmedelssektorn i NIS2-direktivet uppfattas som naturlig till följd av sektorns samhällsviktiga funktion och ökade beroende av digitala system och informationsflöden.

Livsmedelssektorns roll i samhällsberedskap och totalförsvar tycks samtidigt kunna påverkas av verksamheters ägarstruktur och graden av samhälleligt ansvar inom sektorn, vilket framträder i IP4:s beskrivningar av hur många större livsmedelsföretag i hens kontext är kooperativ eller delvis statligt ägda. Även möjligheten att snabbt ställa om livsmedelsproduktion vid kris eller krig illustrerar hur sektorn inte enbart uppfattas som viktig ur ett ekonomiskt perspektiv, utan även som central för samhällets motståndskraft och beredskap. Detta framträder exempelvis i IP2:s beskrivning av att livsmedelsproduktion relativt snabbt kan anpassas för olika typer av behov vid kris eller krig.

Det förändrade säkerhetsläget tycks även ha bidragit till en ökad förståelse för allvaret i cybersäkerhetsfrågor och att cybersäkerhet inte längre uppfattas som en isolerad teknisk del av verksamheten, vilket framträder i IP6:s beskrivningar. IP2 menar att det förändrade säkerhetsläget sannolikt kommer innebära ökat informationsutbyte mellan myndigheter och verksamhetsutövare, vilket kan relateras till Busetti och Scanni (2025), som beskriver hur cybersäkerhetsrelaterade regulatoriska krav i ökande grad bygger på informationsdelning och samordning mellan organisationer och ansvariga myndigheter.

IP2 nämner även möjliga behov av säkerhetsklassning inom vissa roller i livsmedelssektorn, vilket kan förstås som en möjlig förlängning av det ökade fokus på cybersäkerhet,

samhällsberedskap och totalförsvar som cybersäkerhetslagen och NIS2-direktivet aktualiserar. Detta indikerar samtidigt att cybersäkerhetsrelaterade krav potentiellt kan påverka hur samhällsviktiga verksamheter organiseras och vilka ansvar, roller och säkerhetskrav som kopplas till vissa yrkesfunktioner. IP2 beskriver exempelvis hur livsmedelssektorn sannolikt kommer att få "ännu mer krav på oss, alltså som en del av totalförsvaret" (IP2, 00:14:22). Det är därmed inte osannolikt att det förändrade säkerhetsläget och ökade cybersäkerhetskrav över tid även kan bidra till nya former av ansvarsfördelning och organisatoriska säkerhetskrav inom samhällsviktiga verksamheter.

# 7 Slutsats

Detta kapitel sammanfattar studiens centrala fynd i relation till forskningsfrågan samt redogör för studiens bidrag. Avslutningsvis presenteras förslag på framtida forskning.

## 7.1 Slutsatser

Studien har undersökt följande forskningsfråga: *Hur präglas implementeringen av den svenska cybersäkerhetslagen hos stora verksamhetsutövare inom livsmedelssektorn?*

Organisationernas förutsättningar för implementering varierar påtagligt och påverkas i hög grad av befintliga säkerhetsstrukturer, tidigare arbete med regulatorisk efterlevnad och graden av ledningsengagemang. Organisationer som kommit längre i sitt implementeringsarbete beskriver anpassningen som ett fortsatt systematiseringsarbete, medan organisationer i ett tidigare skede står inför ett mer omfattande omställningsarbete. På det teknologiska planet tillkommer att legacy-system är djupt integrerade i verksamhetsprocesser och svåra att anpassa direkt, vilket innebär att skyddet sker genom omgivande arkitektur snarare än direkta anpassningar, samtidigt som en rörelse mot standardiserade externa system skapar bättre förutsättningar för att möta regulatoriska krav.

De utmaningar som framträder tydligast är inte primärt tekniska utan organisatoriska och regulatoriska. Vid tidpunkten för studiens genomförande hade de slutgiltiga föreskrifterna från MCF ännu inte fastställts, vilket innebär att organisationerna har förhållit sig till regulatoriska krav under pågående utformning. Compliance burden upplevs som reell men härrör inte från lagstiftningens syfte utan från hur kraven hittills konkretiserats, vilket tvingar organisationer att lägga resurser på att tolka och operationalisera vad som faktiskt förväntas av dem. På organisationsnivå framträder ett gap mellan det ansvar lagen formellt placerar på ledning och hur ansvaret fördelas i praktiken. Flera informanter upplever därtill tendenser till gold-plating, där MCF:s föreslagna föreskrifter uppfattas som mer detaljstyrande än vad NIS2-direktivet kräver.

Cybersäkerhetslagen medför samtidigt tydliga möjligheter. Lagen fungerar som en legitimeringskraft som reducerar intern friktion och tillför säkerhetsansvariga ett mandat de tidigare saknat, då initiativ som tidigare mötte motstånd kan drivas igenom med hänvisning till externa lagkrav. Flera informanter beskriver att lagen medfört konkreta förbättringar i det egna säkerhetsarbetet, exempelvis upprättandet av kontinuitetsplaner och systematiserade behörighetskontroller, vilket antyder att lagen haft en katalyserande effekt för organisationer där sådana strukturer tidigare saknades. Behovet av denna externa drivkraft varierar dock med hur välutvecklat organisationens informationssäkerhetsarbete är. För organisationer med mer välutvecklade informationssäkerhetsstrukturer upplevs detaljstyrda föreskrifter i vissa fall snarare som ett hinder för ett ändamålsenligt säkerhetsarbete.

Sammantaget antyder studiens fynd att förutsättningarna för att implementera cybersäkerhetslagen inom livsmedelssektorn formas av samspelet mellan organisationers interna kapacitet och hur regulatoriska krav formuleras och konkretiseras externt. Förmågan att uppnå en meningsfull regulatorisk efterlevnad avgörs således inte enbart av organisationernas interna resurser och strukturer, utan även i vilken utsträckning regelverket ger utrymme för ett säkerhetsarbete anpassat efter verksamhetens faktiska behov.

## 7.2 Studiens bidrag

Studien bidrar teoretiskt genom att visa att kombinationen av TOE-ramverket och compliance capability kompletterar varandra som analytiska verktyg vid studiet av regulatorisk implementering, där TOE strukturerar vilka faktorer som påverkar implementeringen och compliance capability förklarar hur organisationer hanterar dem. Empiriskt belyser studien hur cybersäkerhetsrelaterade regulatoriska krav tar sig uttryck i praktiken inom livsmedelssektorn, vilken genom NIS2-direktivet för första gången explicit inkluderas som samhällsviktig sektor inom EU:s cybersäkerhetsreglering. Studiens fynd indikerar även att föreskrifternas utformning och tydlighet påverkar organisationers förutsättningar för efterlevnad, vilket har implikationer för hur regulatoriska krav formuleras och kommuniceras.

## 7.3 Framtida forskning

Studien genomfördes nära inpå cybersäkerhetslagens ikraftträdande och vid en tidpunkt då MCF:s föreskrifter ännu inte fastställts, vilket innebär att implementeringsarbetet inom sektorn befinner sig i ett tidigt skede. Longitudinella studier som följer hur organisationers compliance-arbete utvecklas när föreskrifterna är på plats skulle därför ge en mer fullständig bild av implementeringsprocessen över tid.

Studiens urval avgränsas till stora verksamhetsutövare inom den svenska livsmedelssektorn. Empirin antyder att medelstora verksamhetsutövare påverkas oproportionerligt av lagkraven, varför framtida forskning med fördel kan undersöka hur dessa organisationer förhåller sig till cybersäkerhetslagen och vilka specifika utmaningar de möter.

Slutligen skulle jämförande studier mellan sektorer inom Sverige kunna belysa i vilken utsträckning de identifierade mönstren är specifika för livsmedelssektorn, medan jämförande

studier mellan medlemsstater inom EU skulle kunna belysa hur variationen i nationell implementering av NIS2 påverkar organisationers förutsättningar för efterlevnad.

# Referenser


Annosi, M. C., Brunetta, F., Capo, F., & Heideveld, L. (2020). Digitalization in the agri-food industry: The relationship between technology and sustainable development. Management Decision, 58(8), 1737–1757. https://doi.org/10.1108/MD-09-2019-1328

Baker, J. (2012). The technology–organization–environment framework. In: Dwivedi, Y.K., Wade, M.R. & Schneberger, S.L. (eds.) Information Systems Theory: Explaining and Predicting Our Digital Society. Springer.

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K. & Meskin, N. (2020). Cybersecurity for Industrial Control Systems: A Survey, Computers & Security, vol. 89, p.101677

Blue Institute. (2020). Livsmedelsindustrirapporten 2020. https://blueinstitute.se/wp-content/uploads/2020/12/Livsmedelsindustrirapporten2020.pdf

Boston Consulting Group (2020). How Digital Divides Health Care Providers. Boston Consulting Group. [online] 17 december. Tillgänglig på: https://www.bcg.com/publications/2020/how-health-care-providers-can-create-value-with-a-focused-digital-investment-strategy [Hämtad 2026-05-11].

Busetti, S., & Scanni, A. (2025). Evaluating incident reporting in cybersecurity: From threat detection to policy learning. Government Information Quarterly, vol. 42, article 102000, https://doi.org/10.1016/j.giq.2024.102000

Capgemini Research Institute. (2019). Championing data protection and privacy. Capgemini Research Institute. https://www.capgemini.com/at-de/wp-content/uploads/sites/11/2021/09/Report_GDPR_Championing_DataProtection_and_Privacy.pdf

Chandra, J.V., Challa, N. och Pasupuleti, S.K. (2015) 'Intelligence based Defense System to Protect from Advanced Persistent Threat by means of Social Engineering on Social Cloud Platform', Indian Journal of Science and Technology, 8(28), artikel-id: 63544.

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.

Culot, G., Nassimbeni, G., Podrecca, M. & Sartor, M. (2021). The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory-Based Research Agenda, The TQM Journal, vol. 33, no. 7, pp.76–105

Dagens industri (2026). MCF:s förslag försämrar cybersäkerheten [Debattartikel]. Publicerad 7 januari 2026. Tillgänglig på: MCF:s förslag försämrar cybersäkerheten

de Freitas, Titotto, de Andrade, & R. G. Lins. (2025). A Five-Step Cyber-Defence Model for Industry 4.0 Control Systems Integrating Iec 62443 and Iso 27000, in 2025 16th IEEE International Conference on Industry Applications (INDUSCON), 2025 16th IEEE International Conference on Industry Applications (INDUSCON), 14 October 2025, pp.743–750

Direktiv (EU) 2016/1148. Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå av säkerhet i nätverks- och informationssystem i hela unionen. Europaparlamentet, Europeiska unionens råd. EUR-Lex NIS-direktivet

Direktiv (EU) 2022/2555. Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet). Europaparlamentet, Europeiska unionens råd. EUR-Lex NIS2-direktivet

ENISA (2020). NIS Investments Report. Aten: European Union Agency for Cybersecurity. [online] Tillgänglig på: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20-%20NIS%20Investments%20Report.pdf.

Europeiska kommissionen (2020). Summary report on the open public consultation on the Directive on security of network and information systems (NIS Directive). Bryssel: European Commission. https://digital-strategy.ec.europa.eu/en/library/summary-report-open-public-consultation-directive-security-network-and-information-systems-nis

Europeiska unionen. (2026). Typer av rättsakter , Available Online: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_sv [Accessed 17 May 2026]

Folorunso, A., Mohammed, V., Wada, I. och Samuel, B., 2024. The impact of ISO security standards on enhancing cybersecurity posture in organizations. World Journal of Advanced Research and Reviews, 24(1), ss. 2582–2595. Tillgänglig via: https://doi.org/10.30574/wjarr.2024.24.1.3169 [Hämtad 18 maj 2026].

Förordning (EU) 2016/679. Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (GDPR). Europarlamentet, Europeiska unionens råd. EUR-Lex GDPR

Förordning (EU) 2019/881. Enisas (Europeiska unionens cybersäkerhetsmyndighet) certifiering av informations- och kommunikationsteknikens cybersäkerhet och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten). Europaparlamentet, Europeiska unionens råd. https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX:32019R0881

Hajra, A. och Goel, L. (2025) 'Cloud Migration Strategies for Legacy ERP Systemsn Challenges & Solution', International Journal for Research Publication and Seminar, 16(2), s. 169–175. doi: 10.36676/jrps.v16.i2.61.

Hustad, E., Sørheller, V., Jørgensen, E. och Vassilakopoulou, P. (2021). Moving enterprise resource planning (ERP) systems to the cloud: the challenge of infrastructural embeddedness. International Journal of Information Systems and Project Management. doi: 10.12821/ijispm080101.

Huth, D., Burmeister, F., Matthes, F., & Schirmer, I. (2020). Empirical results on the collaboration between enterprise architecture and data protection management during the implementation of the GDPR. In Proceedings of the 53rd Hawaii International Conference on System Sciences (HICSS). https://doi.org/10.24251/HICSS.2020.715

International Organization for Standardization. (2018). ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://www.iso.org/standard/73906.html

Kannelønning, K., & Katsikas, S. (2024). Deployment of cybersecurity controls in the Norwegian Industry 4.0. In Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES '24) (Article 188, pp. 1–8). ACM. https://doi.org/10.1145/3664476.3670896

Khokrale, R. (2025). Cybersecurity in ERP-Integrated Supply Chains: Risks and Mitigation Strategies. The Eastasouth Journal of Information System and Computer Science. doi: 10.58812/esiscs.v3i02.869

Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. Journal of Information Technology, 38(1), 16–44. https://doi.org/10.1177/02683962221141456

Livsmedelsverket (2025a). Definitioner och begrepp. (2026). , Available Online: https://www.livsmedelsverket.se/foretagande-regler-kontroll/sa-kontrolleras-ditt-foretag/nkp-webben/om-den-nationella-kontrollplanen/definitioner-och-begrepp/ [Accessed 18 May 2026]

Livsmedelsverket (2025b). SKAL - samrådsgruppen för beredskapsplanering. (2026). Available Online: https://www.livsmedelsverket.se/beredskap/skal-samradsgruppen-beredskapsplanering/ [Accessed 18 May 2026]

Livsmedelsverket (2026). Vägledning om verksamhetsutövare enligt cybersäkerhetslagen. https://www.livsmedelsverket.se/4911c0/globalassets/publikationsdatabas/vagledningar/vagledning-om-verksamhetsutovare-enligt-cybersakerhetslagen.pdf. [Hämtad 13 maj 2026].

Länsstyrelsen Stockholm (u.å.). Tillsyn av cybersäkerhet. https://www.lansstyrelsen.se/stockholm/samhalle/sakerhet-och-beredskap/tillsyn-av-cybersakerhet.html [Hämtad 2026-04-18].

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336. https://doi.org/10.1016/j.clsr.2019.06.007

MCFFS 2026:1. Myndigheten för civilt försvars föreskrifter om kriterier för att identifiera verksamhetsutövare enligt cybersäkerhetslagen. Myndigheten för civilt försvar. MCFFS 2026:1 PDF

Makrakis, G.M., Kolias, C., Kambourakis, G., Rieger, C. & Benjamin, J. (2021). Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents. IEEE Access, 9, ss. 165295–165325. doi: 10.1109/ACCESS.2021.3133348.

Mosteiro-Sanchez, A., Barcelo, M., Astorga, J. & Urbieta, A. (2020). Securing IIoT Using Defence-in-Depth: Towards an End-to-End Secure Industry 4.0, Journal of Manufacturing Systems, vol. 57, pp.367–378

Myndigheten för civilt försvar (2026). Så ser NIS2-regleringen ut, https://www.mcf.se/sv/amnesomraden/informationssakerhet-och-cybersakerhet/krav-och-regler-inom-informationssakerhet-och-cybersakerhet/nis-direktivet/cybersakerhetslagen-nis2/sa-ser-nis2-regleringen-ut/ [Accessed april 6th]

Myndigheten för samhällsskydd och beredskap (MSB). (2025). Föreskrifter om säkerhetsåtgärder och utbildning – remissversion.

Nankya, M., Chataut, R. & Akl, R. (2023). Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies, Sensors, vol. 23, no. 21, p.8840

Narayanan, M., Hafeez, M. A. & Munir, A. (2026). Encryption for Industrial Control Systems: A Survey of Application-Level and Network-Level Approaches in Smart Grids, Journal of Cybersecurity and Privacy, vol. 6, no. 1, p.11

NIST (2023). Guide to Operational Technology (OT) Security, NIST SP 800-82r3, Gaithersburg, MD: National Institute of Standards and Technology (U.S.), p.NIST SP 800-82r3, Available Online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf [Accessed 18 May 2026]

Njah, S., Danjou, C., Armellini, F., Beaudry, C. & Mosconi, E. (2026). A digital maturity model for assessing SMEs in the manufacturing sector. Digital Engineering, 9, 100084.

Oates, B. J., Griffiths, M., & McLean, R. (2022). Researching Information Systems and Computing. London: SAGE.

Opara-Martins, J., Sahandi, R. och Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. Journal of Cloud Computing, 5, pp. 1-18. doi: 10.1186/s13677-016-0054-z.

Papazafeiropoulou, A., & Spanaki, K. (2016). Understanding governance, risk and compliance information systems (GRC IS): The experts view. Information Systems Frontiers, 18(6), 1251–1263. https://doi.org/10.1007/s10796-015-9602-8

Proença, D., Vieira, R. & Borbinha, J. (2016). A maturity model for information governance. 11th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1–6.

Rakshan, V.J., 2025. ISO 27001: All-inclusive framework for information security management. Scientiarum: A multidisciplinary journal, 1(2), pp.5-11.

Rösch, D., Schuster, T., Waidelich, L., & Alpers, S. (2019). Privacy control patterns for compliant application of GDPR. In Proceedings of the 25th Americas Conference on Information Systems (AMCIS 2019). https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/27

Salas-Riega, J.L., Riega-Virú, Y., Ninaquispe-Soto, M. och Salas-Riega, J.M. (2025) 'Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats', International Journal of Advanced Computer Science and Applications, 16(6), s. 723–729.

Schmitz-Berndt, S., & Schiffner, S. (2021). Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR. International Review of Law, Computers & Technology, vol. 35, no. 2, pp. 101–115, https://doi.org/10.1080/13600869.2021.1885103

Seeba et al. (2025). Toward NIS2 compliance for multiple stakeholders with security level evaluation framework. Complex Systems Informatics and Modeling Quarterly, 45, 136–159. https://doi.org/10.7250/csimq.2025-45.07

Senna, P.P., Barros, A.C., Bonnin Roca, J. & Azevedo, A. (2023). Development of a digital maturity model for Industry 4.0 based on the technology-organization-environment framework. Computers & Industrial Engineering, 185, 109645.

Sharma, M. (2025) 'Workday's Approach to Secure and Compliant Cloud ERP Systems', arXiv. Preprint-id: 2511.02856. Tillgänglig via: https://arxiv.org/abs/2511.02856.

Shewale, V. (2025) 'Securing Legacy SCADA Systems: Practical strategies for the oil and gas industry', World Journal of Advanced Research and Reviews, 26(2), s. 341–346. doi: 10.30574/wjarr.2025.26.2.1575.

Sinha, A., Nguyen, T. H., Kar, D., Brown, M., Tambe, M., & Jiang, A. X. (2015). From physical security to cybersecurity. Journal of Cybersecurity, 1(1), 19–35. https://doi.org/10.1093/cybsec/tyv007

SFS 2025:1506. Cybersäkerhetslag. Försvarsdepartementet. https://rkrattsbaser.gov.se/sfst?bet=2025:1506 [Hämtad 2026-04-18].

Smetana, S., et al. (2021). Food supply chains as cyber-physical systems: A path for more sustainable personalized nutrition. Food Engineering Reviews, 13, 92–103.

Squintani L. Gold-Plating: A Misleading Overarching Concept. In: Beyond Minimum Harmonisation: Gold-Plating and Green-Plating of European Environmental Law. Cambridge Studies in European Law and Policy. Cambridge University Press; 2019:13-71.

Svenska Dagbladet (2025). MSB:s föreskrifter för cybersäkerhet kostar miljarder i onödan. Publicerad 8 december 2025. Tillgänglig på: artikeln på SvD

Svenskt Näringsliv. (2025). Remiss: Förslag till nya föreskrifter om säkerhetsåtgärder och utbildning enligt cybersäkerhetslagen.

https://www.svensktnaringsliv.se/sakomraden/digital-policy/remiss-forslag-till-nya-foreskrifter-om-sakerhetsatgarder-och-utb_1244763.html
Tanjung, D.F., Nurhayati, O.D. och Wibowo, A. (2024) 'Design Information Security in Electronic-Based Government Systems Using NIST CSF 2.0, ISO/IEC 27001: 2022 and CIS Control', International Journal of Innovative Science and Research Technology (IJISRT), 9(6), s. 523–530. doi: 10.38124/ijisrt/IJISRT24JUN1212.
Teichmann, F. (2025). Cybersecurity of critical infrastructure in Europe: The NIS2 directive in focus. International Cybersecurity Law Review, 6, 207–220. https://doi.org/10.1365/s43439-025-00154-4
Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. Computer Law & Security Review, 52, 105890. https://doi.org/10.1016/j.clsr.2023.105890
Veigurs, M., Lasmanis, T., & Romanovs, A. (2024). IT governance in critical sectors: Towards the NIS2 implementation. In 2024 IEEE 65th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS) (pp. 1–7). IEEE. https://doi.org/10.1109/ITMS64072.2024.10741938
von Solms, R. & van Niekerk, J. (2013). 'From information security to cyber security', Computers & Security, 38, pp. 97–102. https://doi.org/10.1016/j.cose.2013.04.004
Wai, E. & Lee, C. K. M. (2023). Seamless Industry 4.0 Integration: A Multilayered Cyber-Security Framework for Resilient SCADA Deployments in CPPS, Applied Sciences, vol. 13, no. 21, p.12008
Yerinde, A., et al. (2025). Cybersecurity in the food sector: Sector report. EFRA – Extreme Food Risk Analytics.
Zaguir, N. A., de Magalhães, G. H., & de Mesquita Spinola, M. (2024). Challenges and enablers for GDPR compliance: Systematic literature review and future research directions. IEEE Access, 12, 81608–81630. https://doi.org/10.1109/ACCESS.2024.3406724

# Appendix 1: Intervjuguide 1

**Inledning**
Mitt namn är (namn) och jag genomför denna intervju tillsammans med (namn) och (namn) som en del av vår kandidatuppsats som vi genomför som en del av vår utbildning på institutionen för informatik vid Ekonomihögskolan vid Lunds universitet. Studien avser undersöka hur storskaliga organisationer inom den svenska livsmedelssektorn förhåller sig till de krav som cybersäkerhetslagen medför.

**Etiska formalia**
Innan vi börjar med intervjun vill vi informera dig om följande:

- Ditt deltagande är frivilligt och du kan avbryta intervjun när som helst utan att ange skäl.
- Du kan välja att inte svara på enskilda frågor om du inte vill ge ett svar.
- Intervjun kommer att spelas in och transkriberas, men inspelningen används uteslutande för denna studies ändamål.

- Dina svar kommer att behandlas konfidentiellt. Om du önskar så kommer ditt namn att anonymiseras i uppsatsen.
- Du har rätt att ta del av transkriptet och godkänna din medverkan innan materialet används.

Samtycker du till att intervju spelas in och att dina svar används i studien?

## Intervjufrågor

**Bakgrund**

- Kan du kort beskriva din roll samt hur ditt ansvarsområde relaterar till informationssäkerhet?
- Hur har din roll och ditt arbete med informationssäkerhet förändrats i takt med att regulatoriska krav tillkommit över tid?

**Extern kontext**

- Hur uppfattar du de föreskriftsförslag som berör cybersäkerhetslagen, som hittills har presenterats av Myndigheten för Civilt Försvar (MCF), anser du att de föreslagna förändringarna kommer driva ert arbete mot en tydlig säkerhetsförbättring?
- Upplever du att cybersäkerhetslagens föreslagna krav skapar likvärdiga förutsättningar inom livsmedelssektorn, till exempel för aktörer med olika storlek eller varierande grad av digital mognad?

**Organisatorisk kontext**

- Hur arbetar organisationen idag med informationssäkerhet, finns det etablerade standarder eller ramverk som ni utgår ifrån (t.ex ISO/IEC 27001:2002 eller NIST's Cybersecurity Framework)?
- Hur har organisationen valt att förhålla sig till cybersäkerhetslagen internt, försöker ni redan nu tolka lagens intentioner och arbeta förberedande därefter eller väljer ni att avvakta tills ni vet med säkerhet vilka krav som lagen kommer ställa på er organisation?
- Hur organiseras och samordnas arbetet med informationssäkerhet mellan olika funktioner och avdelningar inom organisationen, och på vilket sätt påverkas denna organisering av cybersäkerhetslagen?

**Teknologisk kontext**

- Vilka, om några, av era system kommer att behöva genomgå tekniskt strukturella förändringar som en följd av cybersäkerhetslagen?
- Upplever du att era system generellt är anpassningsbara för säkerhetsförbättringar, och upplever du att det är någon skillnad i svårighet att införa organisationens egna säkerhetsinitiativ jämfört med externa regulatoriska krav?

# Appendix 2: Intervjuguide 2

**Inledning**
Mitt namn är (namn) och jag genomför denna intervju tillsammans med (namn) och (namn) som en del av vår kandidatuppsats som vi genomför som en del av vår utbildning på institutionen för informatik vid Ekonomihögskolan vid Lunds universitet. Studien avser undersöka hur storskaliga organisationer inom den svenska livsmedelssektorn förhåller sig till de krav som cybersäkerhetslagen medför.

**Etiska formalia**
Innan vi börjar med intervjun vill vi informera dig om följande:

- Ditt deltagande är frivilligt och du kan avbryta intervjun när som helst utan att ange skäl.
- Du kan välja att inte svara på enskilda frågor om du inte vill ge ett svar.
- Intervjun kommer att spelas in och transkriberas, men inspelningen används uteslutande för denna studies ändamål.
- Dina svar kommer att behandlas konfidentiellt. Om du önskar så kommer ditt namn att anonymiseras i uppsatsen.
- Du har rätt att ta del av transkriptet och godkänna din medverkan innan materialet används.

Samtycker du till att intervju spelas in och att dina svar används i studien?

**Intervjufrågor**

**Bakgrund**

- Kan du kort beskriva din roll och hur den relaterar till informations- eller cybersäkerhet?
- Hur har ditt arbete förändrats i takt med ökade regulatoriska krav kopplade till cybersäkerhet (t.ex. arbetsbelastning, dokumentation eller compliance-krav)?

**Extern kontext**

- Hur uppfattar du kraven i NIS2-direktivt? Tror du att de kommer leda till faktiska säkerhetsförbättringar i er organisation?
- Upplever du att NIS2 skapar likvärdiga förutsättningar inom livsmedelssektorn, oavsett organisationens storlek eller digitala mognad?

**Organisatorisk kontext**

- Hur arbetar ni idag med informationssäkerhet (t.ex. ISO 27001 eller NIST)?
- Hur har ni som organisation hittills förhållit er till NIS2-direktivet?
- Hur organiseras och samordnas informationssäkerhetsarbetet mellan olika funktioner och avdelningar inom organisationen, och på vilket sätt påverkas detta av NIS2?

**Teknologisk kontext**

- Vilka, om några, av era system kan behöva genomgå tekniska eller strukturella förändringar till följd av NIS2 Directive?

- Hur arbetar ni med att säkra äldre eller legacy-system i ljuset av NIS2? 3. Upplever du någon skillnad i svårighet mellan interna initiativ och krav kopplade till NIS2, exempelvis vad gäller implementering eller uppföljning?

# Appendix 3: AI-redogörelse

Verktyg: Whisper, Sunet Scribe, ChatGPT, Gemini, DeepL

**Transkribering**
Intervjuerna spelades in och transkriberades därefter med hjälp av de AI-baserade transkriberingsverktygen Sunet Scribe och Whisper.

**Översättning**
DeepL användes för översättning av IP4:s citat till svenska.

**Språkmodeller**
ChatGPT användes som stöd i skrivprocessen, bland annat för språkliga omformuleringar, strukturering av text, förbättring av akademiskt språk samt som diskussionsstöd vid utveckling och problematisering av resonemang kopplade till uppsatsens innehåll. Verktyget användes även som stöd vid disposition, formuleringar och tydliggörande av textavsnitt.

Författarna har själva författat uppsatsens text och endast använt AI-verktyg som stöd i arbetsprocessen. AI-verktygen har inte använts för att skapa referenser eller källhänvisningar. Samtliga referenser har identifierats och kontrollerats av författarna utifrån originalkällor. Författarna ansvarar fullt ut för uppsatsens innehåll, analyser, slutsatser och källhantering.