

# Internationella standarder och cybersäkerhet

Högskoleingenjörsutbildning i IT-ingenjör cybersäkerhet och digital infrastruktur

Ahmad Mossa

Eduardo Peña

Omar Al Zankha



HÖGSKOLAN I BORÅS

**Program:** IT-ingenjör - digital infrastruktur och cybersäkerhet.

**Svensk titel:** Internationella standarder och cybersäkerhet.

**Engelsk titel:** International standards and cybersecurity.

**Utgivningsår:** 2025

**Författare:** Ahmad Mossa, Eduardo Peña och Omar Al Zankah.

**Handledare:** Håkan Alm

**Examinator:** Carl Tinnsten.

**Nyckelord:** Cybersäkerhet, ISO 27001, ISO 27002, DevSecOps och DevOps.

---

## **Förord**

Stort tack till vår handledare Håkan Alm på Högskolan i Borås som har hjälpt och stöttat oss under arbetets gång. Vi vill också rikta ett stort tack till vår handledare på företaget och andra medarbetare som ställt upp på möten.

## Sammanfattning

Denna studie genomför en omfattande gapanalys av ett företags cybersäkerhetsarbete i förhållande till de internationella säkerhetsstandarderna ISO 27001 och ISO 27002. Syftet är att identifiera och kartlägga existerande brister samt ge konkreta och kvalitativa rekommendationer för att förbättra säkerhetsarbetet, särskilt inom ramen för intern mjukvaruutveckling. Studien analyserar säkerhetskontroller inom områdena säker utvecklingscykel, applikationssäkerhet, säker systemarkitektur och säker kodning, och undersöker hur dessa kan integreras effektivt i ett DevSecOps-ramverk.

Metodiskt tillämpas en kombinerad metodansats kvalitativ och kvantitativ, där data insamlas genom enkätundersökningar, semistrukturerade intervjuer och dokumentanalys. Resultaten visar tydligt att organisationen endast delvis uppfyller de säkerhetskrav som definieras av ISO-standarderna. Centrala brister identifierades inom säker kodning, systemarkitektur och applikationssäkerhet, samt inom organisatoriska områden såsom otydlig ansvarsfördelning och otillräcklig kompetensutveckling. Dessa brister påverkar negativt både cybersäkerhet och kvalitet i företagets mjukvaruutvecklingsprocesser.

För att adressera dessa problem föreslås åtgärder som inkluderar tydligare governance-modeller, regelbunden och strukturerad utbildning för utvecklare samt implementering av automatiserade säkerhetskontroller i utvecklingsprocesserna. Dessa förbättringar förväntas stärka kvaliteten i företagets mjukvaruprodukter samtidigt som cybersäkerheten förbättras markant. Studien bidrar därmed till en djupare förståelse för hur informationssäkerhet kan integreras effektivt i agila och kontinuerliga utvecklingsmiljöer.

## **Abstract**

This study performs a comprehensive gap analysis of an organization's cybersecurity efforts against the international standards ISO 27001 and ISO 27002. The primary objective is to identify existing compliance gaps and map critical improvement areas, providing actionable and qualitative recommendations specifically targeting cybersecurity and quality improvements in the context of internal software development. The analysis emphasizes key security controls within secure development life cycles, application security requirements, secure system architecture, and secure coding practices, exploring their effective integration within a DevSecOps framework.

Methodologically, the study applies a mixed methods qualitative and quantitative, gathering data through targeted surveys, semi-structured interviews, and extensive document reviews. Findings reveal significant gaps in meeting the security requirements stipulated by the ISO standards. Major deficiencies are observed in secure coding, system architecture, and application security, accompanied by organizational shortcomings such as unclear responsibility allocation and inadequate competence development. These issues negatively impact both cybersecurity and quality within the company's software development processes. To address these critical challenges, recommendations include establishing clearer governance structures, regular and structured training for developers, and implementing automated security controls within the development lifecycle. Such improvements are expected to significantly enhance the quality of the company's software products and strengthen overall cybersecurity posture. Consequently, the study contributes valuable insights into effectively embedding information security within agile and continuous development environments.

## Innehållsförteckning

<b>1. INTRODUKTION</b> .....	<b>1</b>
1.1 Bakgrund .....	2
1.2 Problemformulering .....	3
1.3 Syfte och frågeställningar .....	3
1.4 Avgränsningar .....	4
<b>2. TIDIGARE FORSKNING OCH TEORETISKA RAMVERK</b> .....	<b>6</b>
2.1 CIA-triaden (Konfidentialitet, Integritet, Tillgänglighet).....	6
2.2 Informationssäkerhet och ISO-standarder .....	7
2.2.1 ISO 27001 och dess krav på certifiering .....	7
2.2.2 ISO 27002:s säkerhetskontroller .....	8
2.3 Kvalitet & ledningssystem.....	8
2.4 Agila Metoder och Kvalitetssäkring .....	9
2.5 Agila ramverk.....	9
2.6 DevOps och DevSecOps .....	10
2.6.1 DevOps-principer.....	10
2.6.2 DevSecOps.....	11
2.7 ISO 27002-KONTROLLER I DevSecOps-KONTEXT.....	11
2.8 Säker utvecklingscykel.....	12
2.8.1 Säkerhetskrav för applikationer .....	12
2.8.2 Säker systemarkitektur och tekniska principer .....	12
2.8.3 Säker kodning .....	13
<b>3. METOD</b> .....	<b>14</b>
3.1 Kvantitativ och Kvalitativ metod .....	14
3.2 Litteraturstudie och tidigare forskning .....	15

<b>3.3</b>	<b>Metod urval .....</b>	<b>16</b>
3.3.1	Styrkor .....	17
3.3.2	Svagheter .....	18
<b>3.4</b>	<b>Forskningsdesign .....</b>	<b>18</b>
3.4.1	Granskning av ISO standarder: .....	19
3.4.2	Analys av FX dokument .....	19
3.4.3	Enkätundersökning.....	20
3.4.4	Målgrupp för enkätundersökningen .....	21
3.4.5	Utformning av enkäten .....	22
3.4.6	Enkätprocess.....	23
3.4.7	Intervjuer .....	23
3.4.8	Urvalskriterier för intervjuer .....	26
3.4.9	Studiens validitet och reliabilitet.....	27
<b>4.</b>	<b>RESULTAT.....</b>	<b>30</b>
<b>4.1</b>	<b>Empiriskt sammanhang och FX agilt arbetssätt .....</b>	<b>30</b>
<b>4.2</b>	<b>Presentation av enkätresultaten .....</b>	<b>31</b>
4.2.1	Säker utvecklingscykel .....	31
4.2.2	Säker systemarkitektur och tekniska principer .....	32
4.2.3	Säker kodning .....	32
4.2.4	Säkerhetskrav för applikationer .....	33
<b>4.3</b>	<b>Intervjuresultat: Agil transformation och cybersäkerhetsutmaningar i praktiken .....</b>	<b>33</b>
4.3.1	Varierande tolkningar av agila arbetssätt .....	34
4.3.2	Otydlig ansvarsfördelning och bristande styrning i cybersäkerhetsarbetet.....	35
4.3.3	Kulturella hinder och brist på ansvarskultur .....	36
<b>4.4</b>	<b>Gap-analys och de mest kritiska säkerhetskontroller som saknas .....</b>	<b>36</b>
<b>4.5</b>	<b>Sammanfattning av Resultat .....</b>	<b>38</b>
<b>5.</b>	<b>ANALYS .....</b>	<b>40</b>
<b>5.1</b>	<b>Analys av organisatoriska och metodologiska utmaningar .....</b>	<b>40</b>
<b>5.2</b>	<b>Implementering av agila och DevOps-baserade arbetssätt .....</b>	<b>40</b>

5.3	Kulturellt motstånd och kompetensgap.....	41
5.4	Styrningsbrister och ansvarsfördelning i komplexa IT-miljöer.....	41
5.5	Outsourcing och governance i cybersäkerhetsarbete .....	42
5.6	Brister i ansvarskultur och efterlevnad .....	42
5.7	Framtids förbättringar .....	43
5.8	Svar på forskningsfrågorna .....	44
<b>6.</b>	<b>DISKUSSION .....</b>	<b>46</b>
6.1	Diskussion av resultat.....	46
6.2	Diskussion av metod.....	48
6.3	Implikationer .....	50
6.3.1	Praktiska implikationer.....	50
6.3.2	Teoretiska implikationer.....	51
6.4	Slutsats.....	52
6.5	Förslag på vidare forskning .....	53
<b>7.</b>	<b>REFERENSER.....</b>	<b>55</b>
<b>8.</b>	<b>BILAGOR.....</b>	<b>59</b>
8.1	Bilaga 1 Enkätsvaren bara fullt implementerade kontroller för respektive kapitel i ISO 27002 .....	59
8.2	Bilaga 2 Kontroller som bedömts som delvis implementerade eller ej implementerade .....	66
8.3	Intervjufrågor:.....	83

Figur 1 Avgränsningar i studien.....	5
Figur 2 CIA-Trianden.....	6
Figur 3 Dessa faser upprepas i cykler (sprints), med kontinuerlig feedback och förbättringar.	9
Figur 4 Visualisering av identifieringsprocess av eventuella brister hos FX:s arbetsstruktur .	19
Figur 5 stegen i undersökningen .....	21
Figur 6 (DevOps) Iterativ livscykel för produktutveckling och drift. ....	31
Figur 7 Implementeringsdrad för säker utvecklingscykel. ....	32
Figur 8 Implementeringsdrad för säker systemarkitektur och tekniska principer .....	32
Figur 9 Implementeringsdrad för Säker kodning .....	33
Figur 10 Implementeringsdrad för Säkerhetskrav för applikationer .....	33
Figur 11 Implementeringsgrad av ISO 27002-kontroller i FX.....	37

Tabell 1 presenterar en översikt över de datainsamlingen från dokument som använts i studien, tillsammans med respektive syfte. ....	20
Tabell 2 redovisar det totala antalet svar som inkommit för varje enkät del. ....	23
Tabell 3 Översikt över genomförda intervjuer. ....	25
Tabell 4 Implementerad kontroller för säker utvecklingscykel i FX .....	59
Tabell 6 implementerad krav för systemarkitektur och tekniska principer i FX.....	59
Tabell 8 implementerad krav för Säkerhetskrav för applikationer i FX .....	60
Tabell 5 Översikt över implementeringsstatus för säkerhetskrav i olika ansvarsområden inom SDLC i FX.....	66
Tabell 7 Översikt över implementeringsstatus för säkerhetskrav i olika ansvarsområden inom Säker kodning i FX.....	72
Tabell 9 Översikt över implementeringsstatus för säkerhetskrav i olika ansvarsområden inom Säkerhetskrav för applikationer i FX. ....	77

## Terminologi

- **FX** – *Företag X* (alias för det studerade företaget, använt för anonymisering)
- **IEC** – *International Electrotechnical Commission* (Internationella elektrotekniska kommissionen)
- **ISO** – *International Organization for Standardization* (Internationella standardiseringsorganisationen)
- **ISMS** – *Information Security Management System* (ledningssystem för informationssäkerhet)
- **CIA** – *Confidentiality, Integrity, Availability* (Sekretess, integritet och tillgänglighet – grundprinciper för informationssäkerhet)
- **SDLC** – *Software Development Life Cycle* (programvarans utvecklingslivscykel)
- **CMMI** – *Capability Maturity Model Integration* (modell för processförbättring och mognadsbedömning)
- **DevOps** – *Development & Operations* (filosofi som förenar utveckling och drift i mjukvaruprocesser)
- **DevSecOps** – *Development, Security & Operations* (DevOps-praktik med integrerad säkerhet i hela utvecklingscykeln)
- **SaMD** – *Software as a Medical Device* (mjukvara avsedd att användas som medicinteknisk produkt)
- **RAID** – *redundant array of independent disks* (en teknik där flera hårddiskar kombineras till en enhet för att förbättra prestanda, ökad datakapacitet eller säkerhet genom redundans.)
- **CD/CI** – *Continuous Integration and Continuous Delivery* (metodik inom mjukvaruutveckling som möjliggör kortare utvecklingstider och förbättrad driftsäkerhet.)
- **ORS** – *Operational Room Solutions* (tillgänglighet av utrustning för cirjurer och patienter)
- **SAP** – *Systems, Applications and Products in Data Processing* (metodik som stödjer hantering och integrering av viktiga funktioner för företagets kontinuerligt drift)
- **SLA** – *Service Level Agreement* (med servicenivåavtal menas ett formellt avtal mellan en beställare och en leverantör)

- **FDA** – *Food Drugs Administration* (amerikanska myndigheten som ansvarar för att skydda folkhälsan genom att övervaka säkerhet och effektivitet för medicintekniska produkter, läkemedel och diagnostik.)

# 1. INTRODUKTION

Digitaliseringens framfart har medfört en kraftig ökning i användningen av datornätverk och molnbaserade system, vilket i sin tur har lett till nya sårbarheter och en mer komplex hotbild för organisationer. IT-utvecklingen möjliggör effektivare kommunikation, datalagring och affärsprocesser, innebär den även att potentiella angreppsytor expanderar. Dagens organisationer är ofta starkt beroende av sammankopplade nätverk, vilket gör att ett intrång i ett system snabbt kan sprida sig och påverka hela verksamheten. (Saeed, Altamimi, Alkayyal, Alshehri & Alabbad, 2023)

Informationssäkerhet är en kritisk resurs för organisationers överlevnad och konkurrenskraft, särskilt i en digitaliserad värld där hoten mot data ökar exponentiellt (Gerber & von Solms, 2008). Informationen utgör en central tillgång för organisationer, och brister i dess säkerhet kan innebära allvarliga hot, inte enbart mot verksamhetens integritet utan även mot dess fortsatta existens (Suorsa & Helo, 2024).

Följande studie fokuserar sig på anpassning av informationssäkerhetsarbetet för att upprätthålla ISO 27001-certifieringen under företags-X (FX) övergång process till intern mjukvaruutveckling (*in-house development*). FX, en global aktör med sina 8000 anställda, utgör ett exempel på denna utmaning. Även om ISO/IEC 27001 erbjuder ett robust ramverk för informationssäkerhet, saknas praktiska riktlinjer för dynamiska anpassningar (Suorsa & Helo 2024).

Bakgrunden belyser informationssäkerhetens betydelse och ISO 27001:s roll i organisationers säkerhetsarbete. Problemformuleringen adresserar utmaningarna med denna förändring samt behovet av en gapanalys för säkerställande av regelefterlevnad. Gap-analysen har använts som ett verktyg för att identifiera skillnader mellan organisationens nuvarande säkerhetsnivå och det önskade läget. Studien syftar till att utveckla en strukturerad metodik för att integrera ISO 27002:s erkända säkerhetskontroller i ett befintligt DevOps-system, med målet att omvandla detta till en DevSecOps-miljö, där specifika forskningsfrågor vägleder arbetet. Arbetet begränsas till relevanta delar av ISO 27002 för den interna utvecklingsverksamhet och certifieringens fortlevnad.

## 1.1 Bakgrund

Information är en av de viktigaste tillgångarna för en organisation, och brister i informationssäkerhet kan inte bara hota organisationens integritet utan även dess existens och rykta i marknad (Suorsa & Helo 2024). Incidenter som berör informationssäkerhet kan leda till både direkta kostnader, som dataförlust, och indirekta konsekvenser, som förlorat förtroende, därför alla organisationer strävar efter att säkerställa att känslig information skyddas mot obehörig åtkomst, förlust eller skada genom att implementera adekvata säkerhetsåtgärder (Guggenmos, Häckel, Ollig & Stahl 2022).

Denna studie fokuserar på implementeringen av informationssäkerhetshanteringssystem (ISMS) genom att tillämpa ISO/IEC 27001 som är en internationell standard för informationssäkerhetsledningssystem (ISMS). ISO/IEC 27001 är en internationell standard som tillhandahåller en strukturerad metod för att hantera säkerhetsrisker och skydda informations konfidentialitet, integritet och tillgänglighet (CIA) (ISO/IEC 27001:2022). Att behålla certifieringen inom ISO 27001 innebär för potentiella kunder att organisationen har processer som ökar datasäkerhet som i sin tur ökar tillit och förstärker affärsrelationer (Calder & Watkins 2024).

Trots standardens breda användning finns det en tydlig kunskapsbrist kring hur organisationer kan upprätthålla certifieringar vid större verksamhetsförändringar, såsom övergång till egen mjukvaruutveckling (*in-house development*) medföra särskilda svårigheter med att behålla organisationens säkerhetsarbete (Khan, Khan, Alzahrani & Ilyas 2022). Denna brist begränsar i sin tur organisationers förmåga att balansera innovation och regelefterlevnad. Standarden krävs för att säkerställa en enhetlig metodik för cybersäkerhet inom hela organisationen, inklusive alla dess globalt fördelade kontor.

Studien bidrar till fältet genom att utforska anpassningsprocesser för ISO 27002-kontroller i samband med organisatorisk förändring. Befintlig forskning på området har främst fokuserat på statiska implementeringar av säkerhetsstandarder, vilket har lämnat en kritisk lucka i förståelsen av hur informationssäkerhetslösningar kan utformas för att vara flexibla i en föränderlig miljö (Wu, Shi, Wu & Liu 2022). Genom att adressera denna brist strävar arbetet efter att ge både teoretiska och praktiska insikter för både akademien och industrin.

## **1.2 Problemformulering**

FX är certifierat enligt ISO 27001, men en nyligen genomförd förändring mot utveckling av egen mjukvara har skapat utmaningar för att upprätthålla informationssäkerheten enligt standardens krav. Denna förändring innebär ett kunskapsgap, det saknas tydliga riktlinjer för hur FX ska anpassa sina säkerhetsrutiner till det nya arbetssättet och samtidigt behålla ISO 27001 certifieringen. Kunskapsgapet påverkar inte bara FX:s interna processer utan även dess förmåga att garantera datasäkerhet och efterlevnad av branschregler. Om kraven inte uppfylls, kan det leda till allvarliga konsekvenser som potentiella säkerhetsincidenter, förlust av certifieringen och sänkt kundtillit.

DevOps kombinerar utveckling och drift för att snabba upp och automatisera mjukvaruleverans, medan DevSecOps lägger till säkerhet i DevOps-processen och integrerar den i varje steg. Genom att identifiera konkreta åtgärder som adresserar befintliga säkerhetsbrister bidrar studien inte enbart till att upprätthålla FX:s certifieringar, utan stimulerar även en bredare diskussion om hur organisationer kan överkomma utmaningar när de transformerar från DevOps till DevSecOps på liknande verksamheter.

I takt med att FX har övergått till intern utveckling av programvaror har det uppstått ett behov av att granska hur denna förändring påverkar befintliga säkerhetsstrukturer. Med utgångspunkt i detta genomförs en jämförelse mellan organisationens nuvarande arbetssätt och relevanta kontroller enligt ISO 27002, med hjälp av en gapanalys. Vidare studeras centrala dokument och processer relaterade till säkerhetspolicy, riskhantering och dataskydd för att identifiera potentiella sårbara områden. Avslutningsvis sammanställs ett antal åtgärdsförslag i syfte att stödja en mer ändamålsenlig anpassning till gällande standarder.

## **1.3 Syfte och frågeställningar**

Introduktionen till syftet kopplas till det tidigare identifierade problemet med att säkerställa regelefterlevnad inom informationssäkerhet, särskilt för FX:s in-house-mjukvaruutveckling. Dock finns det fortfarande ett forskningsgap när det gäller vägledning för hur företag ska agera när de expanderar sin produktionskapacitet och övergår till egenutvecklade mjukvarulösningar. Denna studie fokuserar att bidra till att fylla detta gap genom att undersöka vilka ytterligare ISO 27002-kontroller som blir relevanta när ett företag övergår till egen mjukvaruutveckling. Genom att använda FX som fallstudie analyseras hur dessa krav påverkar cybersäkerhetsarbetet i praktiken, och målet är att utveckla ett generellt ramverk eller modell som även andra organisationer kan använda vid liknande transformationsprocesser.

Genom att integrera ISO 27001 och ISO 27002-krav i ett DevOps-ramverk kan en hållbar DevSecOps-struktur skapas. Mot denna bakgrund formuleras syftet med denna uppsats enligt följande:

Syftet med detta arbete är att utforma ett strukturerat tillvägagångssätt för att fastställa informationssäkerhetskrav genom anpassning av ett DevOps-ramverk till ISO 27002, med fokus på säkerhetskontroller för in-house-utveckling. För att uppnå syftet har arbetet brutits ner i två forskningsfrågor. Den första forskningsfrågan (RQ1) identifierar kritiska organisatoriska barriärer för ISO 27001-efterlevnad i en DevSecOps-kontext, medan den andra (RQ2) fokuserar på operativa lösningar genom ISO 27002:s ramverk. Forskningsfrågorna formuleras enligt följande:

**RQ1:** Vilka organisatoriska hinder är mest kritiska för att upprätthålla ISO 27001-certifiering i en agil DevSecOps-miljö?

**RQ2:** Hur kan ISO 27002:s kontroller för säker utvecklingslivscykel, säker kodning, säkerhetskrav för applikationer och säker systemarkitektur användas för att identifiera och mäta implementeringsgap, samt effektivt integreras i en DevSecOps-modell?

## 1.4 Avgränsningar

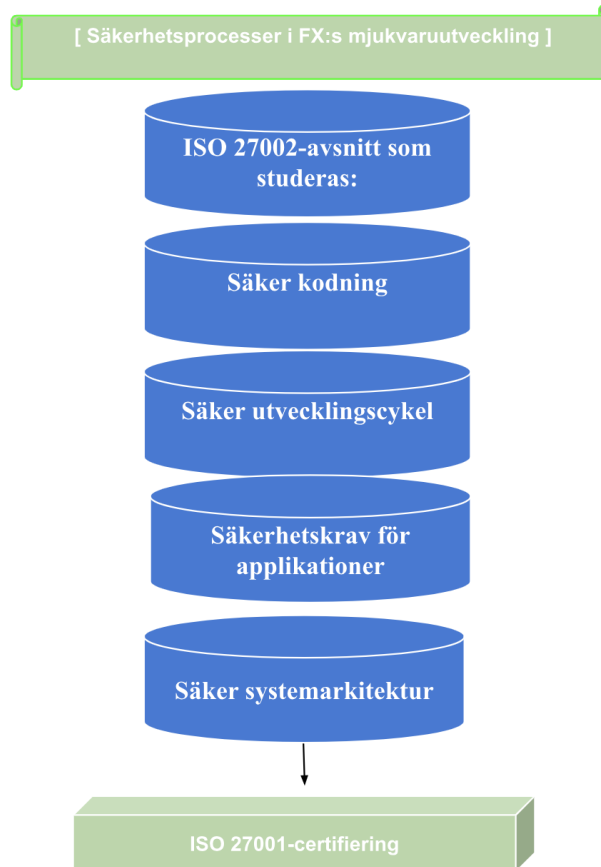
Avgränsningar definierar specifika gränser för studien. Dessa avgränsningar är förenade till fenomenet som undersöks och inte till praktiska begränsningar. Denna studie fokuserar på 4 huvudområden av sektioner av ISO 27002 som är direkt relevanta för FX:s interna arbetsstruktur inom mjukvaruutveckling samt bibehållandet av ISO 27001-certifieringen.

Studien inriktar sig främst på följande avsnitt i ISO 27002:

- Avsnitt 8.25 Säker utvecklingscykel: Integrering av säkerhet genom hela mjukvarulivscykeln, med dokumenterade processer för att förebygga säkerhetsproblem innan produkten når produktionsfasen.
- Avsnitt 8.26 Säkerhetskrav för applikationer: Definition och uppfyllande av säkerhetskrav, inklusive autentisering, åtkomstkontroller, loggning och kryptering, före utveckling och implementering.
- Avsnitt 8.27 Säker systemarkitektur: Säkerhet som en central del av systemarkitekturen för att skapa robust skydd mot framtida attacker.

- Avsnitt 8.28 Säker kodning: Följande av kodningsstandarder för att skydda mot vanliga sårbarheter, samt integration av kodgranskningsrutiner och utbildning i säker kodning för utvecklare.

Avgränsningarna visualiseras i Figur 1, där fokus läggs på specifika processteg relaterade till mjukvaruutveckling och säkerhetscertifiering.



*Figur 1 Avgränsningar i studien.*

## 2. TIDIGARE FORSKNING OCH TEORETISKA RAMVERK

Detta kapitel presenterar de teoretiska ramverk och begrepp som ligger till grund för studien. Syftet är att skapa en djupare förståelse för de utmaningar och möjligheter som uppstår när ett företag som FX övergår till intern mjukvaruutveckling (in-house development) samtidigt som det ska upprätthålla ISO 27001-certifieringen. Genom att integrera teorier om informationssäkerhet, agila metoder och projektledning kan en DevSecOps modell utvecklas för att säkerställa regelefterlevnad.

### 2.1 CIA-triaden (Konfidentialitet, Integritet, Tillgänglighet)

CIA-triaden är en central modell inom informationssäkerhet och består av tre grundläggande principer: Sekretess (Confidentiality), Integritet (Integrity) och Tillgänglighet (Availability). Dessa tre komponenter utgör en grundpelare för att säkerställa att information skyddas på ett effektivt och strukturerat sätt (Hussain, Abdullah, Humayun, Tavares & Jhanjhi 2022). Figur 2 visar hur dessa komponenter (sekretess, integritet och tillgänglighet) utgör en lika viktig roll för säkerhetsarbete inom ett företag.



Figur 2 CIA-Triangeln

*Sekretess:* Syftar till att begränsa tillgången till information så att endast behöriga användare kan läsa, ändra eller dela data. Detta innebär att obehörig åtkomst aktivt förhindras genom säkerhetsåtgärder som: Användarautentisering (användar-ID och lösenord), Åtkomstkontrollistor (ACL), Policybaserade säkerhetsrutiner. Genom att upprätthålla konfidentialitet säkerställs att känslig information förblir skyddad från läckage och missbruk (Hussain et al. 2022).

*Integritet:* Integritet fokuserar på att garantera att data förblir oförändrad under hela dess livscykel (Hussain et al. 2022). Detta inkluderar att förhindra obehöriga modifieringar samt säkerställa att data återspeglar sitt avsedda tillstånd. För att uppnå detta används metoder som: Datakryptering, Hashing för att verifiera dataäktenskap, Strikt hantering av filbehörigheter. En hög grad av dataintegritet är avgörande för att upprätthålla tillförlitligheten i informationssystemen.

*Tillgänglighet:* Innebär att information och system ska vara tillgängliga för behöriga användare när de behövs. Acceptabel tillgänglighet varierar beroende på organisationens behov – vissa verksamheter kräver nära nog 100 % driftstid, medan andra kan tolerera kortare avbrott. För att säkerställa tillgänglighet används åtgärder som, Regelbundet hårdvaruunderhåll, Nätverksoptimering, Systemuppdateringar och redundanslösningar (RAID).

Genom att balansera dessa tre principer kan organisationer bygga en robust säkerhetsarkitektur som skyddar både data och verksamhet. CIA-triaden fungerar som en grundläggande modell för att utforma och utvärdera informationssäkerhetsstrategier (Hussain et al. 2022).

## **2.2 Informationssäkerhet och ISO-standarder**

Internationella standardiseringsorganisationen (ISO) är en global organisation som utvecklar och publicerar internationella standarder. Dessa standarder täcker ett brett spektrum av områden, inklusive teknologi, säkerhet och miljö, och syftar till att säkerställa kvalitet, säkerhet och effektivitet i produkter och tjänster över hela världen. (Calder & Watkins 2024).

Detta examensarbete kommer att fokusera på ISO 27002, en internationell standard som beskriver krav och riktlinjer för hur organisationer, kan implementera ett effektivt informationssäkerhetsledningssystem (ISMS). Genom att följa ISO 27000-serien kan organisationer säkerställa att deras informationsresurser skyddas på ett strukturerat och lämpligt sätt (Suorsa & Helo 2024).

### **2.2.1 ISO 27001 och dess krav på certifiering**

Att uppnå ISO/IEC 27001-certifiering visar att en organisation har infört en acceptabel säkerhetsnivå, vilket kan stärka förtroendet hos kunder och intressenter. Enligt Kamil, Lund och Islam (2023) är ISO/IEC 27001 särskilt viktigt för att möta intressenters förväntningar på informationssäkerhet, särskilt inom privata organisationer i Sverige. Deras studie belyser hur

standarden bidrar till att skapa legitimitet och förtroende genom att tydligt definiera säkerhetsmål och krav (Kamil, Lund & Islam 2023).

### **2.2.2 ISO 27002:s säkerhetskontroller**

En av de största fördelarna med ISO 27002 är att dess semantiska kunskapsbas säkerställer att alla genererade beslutsalternativ överensstämmer med standardens krav samtidigt som de tar hänsyn till företagets specifika förutsättningar, såsom redan implementerade säkerhetsåtgärder (Fenz & Neubauer 2018). ISO 27002 erbjuder ett omfattande ramverk med riktlinjer och bästa praxis som täcker olika dimensioner av informationssäkerhet. Genom att använda standarden kan organisationer identifiera, bedöma och hantera säkerhetsrisker på ett strukturerat sätt. Detta stärker inte bara den operativa resiliensen genom att minska risken för säkerhetsincidenter, utan bidrar också till ökad förtroendebildning hos intressenter. Dessutom underlättar standarden efterlevnad av lagar, avtalsvillkor och andra regulatoriska krav. (Kamil, Lund & Islam 2023).

Även om ISO 27002 inte är en certifieringsbar standard, utgör den en central referenspunkt för implementering av ISO 27001, som däremot kan certifieras. ISO 27002 tilldelar varje säkerhetskontroll specifika attribut som underlättar val och anpassning av åtgärder. Det är viktigt att notera att ISO 27002, trots sitt värde som internationell standard, inte alltid hänger med i den snabba utvecklingen av IT-säkerhetshot. Detta innebär att vissa riktlinjer kan behöva kompletteras med ytterligare åtgärder för att hantera nya sårbarheter. Dessutom kräver många kontroller en helhetssyn, där åtgärder inom exempelvis åtkomstkontroll och nätverkssäkerhet bör samordnas för optimal effekt (Calder & Watkins 2024).

## **2.3 Kvalitet & ledningssystem**

En central del av kvalitetsstyrning är att kunna erbjuda olika typer av varor och tjänster med standardgaranti till ett specifikt ekonomiskt värde. Att framställa en vara av god kvalitet innebär ofta ett högre pris än vad som är uppenbar (Tonnquist 2024). IT-kvalitet kan definieras som ett systems eller en IT-lösningens förmåga att uppfylla användarnas behov och förväntningar. En väl genomtänkt systemarkitektur kan även minska risken för oväntade fel och underlätta framtida utveckling och uppgraderingar (Collin 2003).

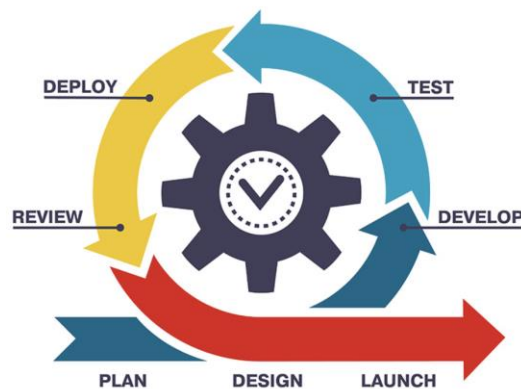
Kvalitet i projektarbetet; Den upplevda kvaliteten ska minst motsvara förväntningarna. Det är alltså intressenternas förväntningar, och då framför allt slutanvändarnas och de som direkt berörs av projektet, som är avgörande för om projektet anses lyckat eller inte. Vad som står i

projekt målet och kravspecifikationen spelar mindre roll om intressenternas förväntningar varit felaktiga. (Tonnquist 2024).

## 2.4 Agila Metoder och Kvalitetssäkring

2001 togs 'The Agile Manifesto' fram, ett dokument som syftar till att förbättra sätten mjukvaran utvecklas. (Görling 2009). Ett agilt team förväntas vara självständigt, styrande och organiserat, vilket också betyder att verksamheten skapar möjligheter där utrymme och flexibilitet ges till teamet. (Tonnquist 2024). Flera effekter kan nås genom att hålla ett kontinuerligt arbete gällande ökning av kvalitet medför att affärsrelationer, ekonomin inom verksamheten samt ökad efterfrågan är några av dessa positiva effekter (Harris, McDowell & Gibson, 2011).

Figur 3 visualiserar att även i agila metoder finns det vissa grundläggande faser, som utveckling och test, men dessa utförs iterativt snarare än linjärt.



Figur 3 Dessa faser upprepas i cykler (sprints), med kontinuerlig feedback och förbättringar.

## 2.5 Agila ramverk

Agil projektledning är en metod där traditionell projektmetodik kombineras med andra metoder för att skapa en mer flexibel och anpassningsbar arbetsprocess.

Projektmetodiken utgör ett ramverk som ger en helhetsbild av projektet, medan de agila metoderna styr hur arbetet organiseras, hur krav hanteras och hur projektets genomförande

struktureras. (Tonnquist 2024). I traditionella projektmodeller kan en otydlig kravbild innebära att projektet inte får starta, eftersom organisationen ofta vill minska risker genom att definiera alla krav i förväg. Med en agil metodik kan teamet i stället påbörja arbetet med de delar som redan är tydliga, samtidigt som kraven klargörs under projektets gång. Detta arbetssätt gör det

möjligt att driva projekt framåt utan att behöva ha en fullständig bild av slutresultatet från start, vilket kan vara en stor fördel i komplexa och föränderliga miljö (Gustavsson 2020).

## **2.6 DevOps och DevSecOps**

DevOps, en sammansättning av begreppen "Development" (utveckling) och "Operations" (drift), representerar en filosofi och en samling praktiker som syftar till att främja samarbete mellan dessa två traditionellt separata domäner inom mjukvaruutveckling. Målet är att skapa en mer effektiv och högkvalitativ livscykel för mjukvaruproduktion (Prates & Pereira 2025). DevSecOps är en utvidgning av DevOps, och den är ett modernt tillvägagångssätt för att integrera säkerhet i mjukvaruutveckling genom att införliva säkerhets principer och processer i hela utvecklingslivscykeln, från planering och design till utveckling, testning och drift (Lombardi & Fanton, 2023).

### **2.6.1 DevOps-principer**

Enligt Rajapakse, Zahedi, Babar och Shen (2022) kan DevOps definieras som ett tvärfunktionellt och samarbetsinriktat arbetssätt som strävar efter att automatisera och optimera processer för kontinuerlig leverans av nya programvaruversioner. Samtidigt betonas vikten av att säkerställa kvalitet, korrekthet och tillförlitlighet i leveransen.

DevOps förfinar principerna från Agile genom att implementera automatisering och kvalitetssäkring som en del av utvecklingsprocessen (Leite, Rocha, Kon, Milojevic & Meirelles 2020). Denna integration resulterar i en mer effektiv och högkvalitativ mjukvarulivscykel. Centralt för DevOps är flera nyckel principer, såsom kontinuerlig integration (CI), kontinuerlig leverans (CD) och kontinuerlig implementering (CD). Kontinuerlig integration innebär att utvecklare regelbundet, ofta dagligen, integrerar sina kodändringar i en gemensam huvudgren. Dessa ändringar valideras sedan genom automatiserade byggen och tester (Lombardi & Fanton 2023). Enligt Leite et al. (2020) följer DevOps-praktiker ofta CI/CD-modeller från kontinuerlig mjukvaruutveckling (Continuous Software Engineering, CSE), ett kunskapsområde inom mjukvaruutveckling som fokuserar på kontinuerlig rörelse i utvecklingsaktiviteter genom att definiera och tillämpa en uppsättning kontinuerliga praktiker. Kombinationen av dessa principer och praktiker minskar barriärer mellan utveckling och drift, samtidigt som det faciliterar kontinuerlig förbättring och innovation. Detta leder till en smidigare och responsiv utvecklingsprocess, där kvalitet och leveranshastighet är centrala målsättningar.

### 2.6.2 DevSecOps

Metoden bygger på DevOps-filosofin, där samarbete och automation är centrala element, men med ett särskilt fokus på att säkerhet inte ska behandlas som en separat fas utan vara en integrerad del av utvecklingsarbetet (Carter 2017). Traditionella tillvägagångssätt för mjukvarusäkerhet har ofta inneburit att säkerhetsgranskningar och tester sker i slutskedet av utvecklingscykeln, vilket leder till kostsamma korrigeringar och potentiella förseningar i produktlanseringen (Leite et al. 2020).

Carter (2017) betonar att detta kan resultera i en situation där säkerhetsrelaterade brister upptäcks först vid kvalitetskontroller, vilket i många fall leder till att säkerhetsproblem antingen ignoreras eller skjuts upp till framtida versioner. Genom att "skifta säkerheten åt vänster", vilket innebär att säkerhetskrav beaktas redan från början, snarare än att ses som en sista kontroll innan lansering, vilket leder till att utvecklingsprocessen kan säkerhetsaspekter identifieras och åtgärdas i ett tidigare skede, vilket minskar risken för allvarliga säkerhetsincidenter och potentiellt sänker kostnaderna för åtgärder i efterhand. DevSecOps förutsätter en kulturell omställning där säkerhetsteam, utvecklare och driftspersonal integrerar sina arbetsprocesser för att skapa en säker utvecklingsmiljö (Leite et al. 2020). I stället för att säkerhet ses som en begränsande faktor betonas ett inkluderande och samarbetsorienterat arbetssätt. Detta innebär att säkerhetsexperter stödjer utvecklingsteamerna genom utbildning och tillhandahållande av verktyg för säker kodning samt automatiserade säkerhetstester, vilket möjliggör en mer effektiv och proaktiv hantering av säkerhetsrisker (Carter 2017).

## 2.7 ISO 27002-KONTROLLER I DevSecOps-KONTEXT

Software Development Life Cycle (SDLC) är en systematisk process för att utveckla och underhålla mjukvara. Den består av olika faser som planering, design, implementering, testning och underhåll. Traditionella modeller som Waterfall och Agile har varit dominerande, men med den snabba teknologiska utvecklingen och ökande krav på snabbare leverans har nya metoder som DevOps och DevSecOps vuxit fram (Leite et al. 2020).

Dessa metoder fokuserar på att integrera utveckling och drift, samt att införliva säkerhet i tidiga stadier av utvecklingsprocessen.

*Här nedan redovisas fyra teoretiska aspekter från Cybersäkerhetskontroller med fokus på områden som rör studiens avgränsningar.*

## **2.8 Säker utvecklingscykel**

Modellen syftar till att fungera som en praktisk grund för företagsspecifika processer och arbetsmetoder, där hotmodellering, sårbarhetsanalyser och härledning av säkerhetskrav spelar en central roll på både system- och delsystemnivå (Dobaj, Macher, Ekert, Riel & Messnarz 2023). En viktig aspekt av modellen är dess fokus på proaktiv riskhantering, där hotanalys och säkerhetskrav definieras tidigt i utvecklingsprocessen. Detta säkerställer att cybersäkerhet integreras i hela produktlivscykeln – från koncept till driftsättning – vilket minskar risken för säkerhetsbrister i slutprodukten (Dobaj et al. 2023).

### **2.8.1 Säkerhetskrav för applikationer**

Applikationer utgör ofta en central del av en organisations IT-infrastruktur, då de hanterar och lagrar känsliga data. Därför är det avgörande att dessa system utformas med robusta säkerhetsåtgärder för att skydda både kundinformation och interna verksamhetsdata. Som säkerhetsarkitekt spelar man en nyckelroll i att definiera tydliga säkerhetsstandarder som utvecklingsteam kan följa vid design och implementering av applikationer (Young, Simos, Rodriguez & Diogenes 2023).

En kritisk aspekt är införandet av "säkra kodningspraxis", vilket innebär att undvika vanliga sårbarheter som injektionsattacker, felaktig autentisering och osäkra direktavbildningar. Genom att etablera riktlinjer för kodgranskning, säkerhetstestning och kontinuerlig sårbarhetshantering kan risken för intrång minimeras. Ytterligare bör applikationer utrustas med lämpliga säkerhetskontroller, såsom: Åtkomststyrning (RBAC, MFA), Datakryptering (både under överföring och lagring), Loggning och övervakning för tidig upptäckt av avvikelser. En proaktiv säkerhetsstrategi inkluderar även regelbundna penetrationstester och hotmodellering för att identifiera potentiella svagheter innan de utnyttjas (Young et al. 2023).

### **2.8.2 Säker systemarkitektur och tekniska principer**

IoT-teknik och distribuerade system används alltmer inom områden som fordonsindustri, logistik och sjukvård. En utmaning med dessa system är dock att IoT-enheter ofta har begränsad processorkraft och lagringskapacitet, vilket gör att användares medicinska data vanligtvis lagras på centraliserade tredjepartslösningar som kliniska databaser eller molnplattformar. Detta innebär att användare i många fall tager kontrollen över sina egna data, vilket kan leda till säkerhetsriskerna såsom dataläckage och enskilda felpunkter (Sharma, Moparthi, Namasudra, Shanmuganathan & Hsu 2022).

En framgångsrik säkerhetsarkitekt måste besitta en djup förståelse för cyber säkerhets principer, branschbästa praxis, nya hot trender och moderna säkerhetsteknologier. Genom att kombinera dessa kunskaper kan en säkerhetsarkitekt utforma robusta systemarkitekturer som skyddar organisationens känsliga information och digitala tillgångar mot cyberhot.

### 2.8.3 Säker kodning

Att säkerställa att säker kodning tillämpas redan under utvecklingsfasen är avgörande för att minimera sårbarheter i mjukvarusystem. Sensei är ett verktyg som framgångsrikt tillämpar säkra kodningsriktlinjer direkt i integrerade utvecklingsmiljöer (IDE) (De Cremer, Desmet, Madou & De Sutter 2020). Jämfört med traditionell statisk kodanalys erbjuder detta tillvägagångssätt flera fördelar:

- *Proaktiv säkerhet* – Verktyget identifierar och åtgärdar säkerhetsbrister i realtid under kodning, vilket gör det möjligt att hantera problem tidigt i mjukvarulivscykeln (SDLC).
- *Prestandaeffektivitet* – Eftersom verktyget inte kräver omfattande kontextanalys undviks de prestandaproblem som ofta uppstår vid traditionell statisk analys.
- *Snabbkorrigeringar* – Utvecklare erbjuds direktlösningar vid identifierade överträdelser, vilket påminner om en stavningskontroll under skrivande. En viktig aspekt av verktyget är dess anpassningsbarhet, vilket möjliggör skapande av projektspecifika regeluppsättningar. Detta underlättar kunskapsöverföring mellan säkerhetsexperter och utvecklare samt säkerställer att riktlinjerna är relevanta för den aktuella kodbasen. (De Cremer et al 2020).

### **3. METOD**

I detta kapitel redovisas den metodik som använts i studien, inklusive datainsamling, analysförfarande och motivering av metodval. Metoden har valts utifrån studiens syfte att genomföra en gap-analys av FX:s säkerhetskontroller i relation till relevanta delar av ISO 27002, med fokus på områden kopplade till intern systemutveckling. Gap-analysen har använts i syfte att belysa potentiella brister och förbättringsområden. För att besvara studiens frågeställningar har följande tillämpats: dokumentanalys, semistrukturerade intervjuer och en riktad enkätundersökning. Att göra intervju är en av de mest förekommande metoderna vid kvalitativa undersökningar, särskilt när syftet är att fördjupa förståelsen för en viss problemställning (Justesen & Mik-Meyer 2011). Inom ramen för studien genomfördes totalt nio intervjuer, vilka varierade mellan ostrukturerade och semistrukturerade format, med utvalda och relevanta medarbetare vid FX. Därtill analyserades interna dokument från organisationen, vilka är av särskild vikt då de speglar den aktuella verksamhetskontexten. Detta ger insyn i hur arbetet på FX är organiserat och reglerat, vilket bidrar till en djupare förståelse av studiens sammanhang.

#### **3.1 Kvantitativ och Kvalitativ metod**

Inom samhällsvetenskaplig forskning representerar kvantitativa och kvalitativa metoder två distinkta ansatser för att förstå och analysera verkligheten. Dessa metodologiska traditioner skiljer sig åt inte enbart i sina tekniska procedurer utan även i sina epistemologiska och ontologiska antaganden (Bryman, Nilsson, Clark, Foster & Sloan 2025).

Kvantitativa metoder kännetecknas av insamling och analys av numeriska data, vilket möjliggör statistisk bearbetning och identifiering av generella mönster inom det studerade området. Denna ansats syftar ofta till att ge en översiktlig bild av övergripande mönster (Justesen & Mik-Meyer 2011). Den kvantitativa metodens grundläggande antagande är att den sociala verkligheten är mätbar och kan undersökas med hjälp av strukturerade verktyg som ger kvantifierbar information. Denna data kan därefter analyseras med statistiska tekniker för att dra slutsatser (Jacobsen, Andersson & Holmberg 2024).

Kvalitativ metod fokuserar på att förstå sociala fenomen i deras naturliga kontext. Här präglas forskningsprocessen ofta av en induktiv och tolkande kunskapssyn, där fokus ligger på subjektiv mening och socialt konstruerade verkligheter (Bryman et al. 2025). Datainsamlingen

sker vanligtvis genom djupintervjuer, deltagande observation eller dokumentanalys, vilket möjliggör en nyanserad och kontextberoendeförståelse av det studerade fenomenet. Enligt Jacobsen, Andersson och Holmberg (2024) syftar den kvalitativa ansatsen inte primärt till att generalisera resultat, utan snarare till att bidra med djupgående insikter om specifika fall eller situationer.

Valet mellan kvantitativ och kvalitativ metod bör inte enbart styras av metodologiska preferenser, utan framför allt av forskningsfrågans karaktär. I vissa fall kan en kombination av båda ansatser, en så kallad metodtriangulering, erbjuda en mer heltäckande analys och öka forskningsresultatens trovärdighet (Bryman et al. 2025).

Studien använder en kombinerad metodansats för att undersökningen ska kunna belysa forskningsproblemet från både kvalitativa och kvantitativa perspektiv. Den kvalitativa delen syftar till att utforska deltagarnas upplevelser och hantering av säkerhetsfrågor inom FX genom djupintervjuer och dokumentanalys, vilket ger en kontextuell och nyanserad förståelse (Jacobsen, Andersson & Holmberg, 2024). Den kvantitativa delen analyserar i vilken utsträckning säkerhetsbrister förekommer genom enkätdata, vilket möjliggör identifiering av mönster och generaliseringar (Ejlertsson & Axelsson, 2014).

### **3.2 Litteraturstudie och tidigare forskning**

I denna studie har relevanta vetenskapliga publikationer identifierats genom systematiska sökningar i databasen Primo, med hjälp av sökord som direkt anknyter till rapportens syfte och forskningsfrågor, till exempel (ISO 27001, ISMS, DevSecOps). Ett medvetet urval har gjorts för att inkludera nyare och trovärdiga källor. Där valdes "peer reviewed" artiklar från Primo för att få vetenskapliga källor, och för att IT och informationssäkerhetsområdet karaktäriseras av en snabb teknologisk och regulatorisk utveckling väljas senaste litteratur. Äldre publikationer och ej peer reviewed litteratur har därmed uteslutits, i syfte att säkerställa att analysen vilar på vetenskapligt, verifierad och tillämpbar kunskap i förhållande till dagens komplexa cybersäkerhetslandskap.

Forskning inom informationssäkerhet har under de senaste åren i stor utsträckning fokuserat på hur ISO 27001 implementeras i olika typer av organisationer, samt vilka organisatoriska effekter denna standard medför. Införandet av ett ledningssystem för informationssäkerhet (ISMS) enligt ISO 27001 ofta leder till förbättrad struktur, tydligare roller, samt mer

systematiska processer för riskhantering (Kamil, Lund & Islam 2023). Certifieringen betraktas även som ett konkurrensmedel och ett sätt att uppnå extern legitimitet, särskilt inom branscher med höga regulatoriska krav.

Sådana förändringar innebär inte bara tekniska utmaningar utan kräver även att organisationen implementerar ytterligare säkerhetskrav, särskilt från ISO 27002, som behandlar praktiska kontrollåtgärder i mer detalj (Fenz & Neubauer 2018).

I takt med att fler företag rör sig mot en DevOps- eller DevSecOps-struktur uppstår även nya krav på integrering av säkerhet i hela utvecklingslivscykeln. Forskning har visat att traditionella ISMS-modeller inte fullt ut täcker de operativa och kontinuerliga aspekterna av modern mjukvaruutveckling (Rajapakse et al. 2022). DevSecOps har därmed identifierats som ett tillvägagångssätt som möjliggör en mer proaktiv och integrerad hantering av säkerhetskrav, men det saknas fortfarande etablerade ramverk för hur detta ska harmoniseras med ISO 27001 och ISO 27002 vid intern produktutveckling.

### **3.3 Metod urval**

Valet av metod bör utgå från undersökningens problemställning, eftersom det påverkar studiens tillförlitlighet. Det är därför nödvändigt att återvända till problemformuleringen och överväga vilken metod som på bästa sätt kan besvara forskningsfrågan (Jacobsen, Andersson & Holmberg 2024).

I denna studie har en kombinerad metodansats valts, där både kvalitativa och kvantitativa metoder kombineras för att på ett mångsidigt sätt belysa forskningsproblemet. Denna kombination är motiverad av behovet att dels få en djupgående förståelse för deltagarnas upplevelser och perspektiv, dels att kunna kvantifiera förekomsten av identifierade brister i säkerhetskontroller inom FX.

Den kvalitativa delen av studien syftar till att utforska komplexa sociala fenomen i deras naturliga kontext, vilket är särskilt relevant för att förstå hur aktörer inom FX upplever och hanterar säkerhetsfrågor. Genom metoder såsom djupintervjuer och dokumentanalys kan studien fånga de nyanserade och kontextbundna aspekter som är centrala för forskningsfrågan. Denna ansats möjliggör en rik och detaljerad förståelse av meningsskapande och sociala processer, vilket är avgörande för denna undersökning (Jacobsen, Andersson & Holmberg, 2024).

Den kvantitativa delen av studien syftar å sin sida till att kartlägga och analysera omfattningen av brister i säkerhetskontroller, exempelvis hur många sådana brister som förekommer och i vilken utsträckning (procentuellt) de påverkar verksamheten. För detta ändamål används enkäter som datainsamlingsmetod, vilket möjliggör en systematisk och strukturerad insamling av empiriska data från ett större antal respondenter. Enkäten ger därmed en kvantitativ grund för att identifiera mönster och generalisera resultat inom ramen för det studerade fältet (Ejlertsson & Axelsson, 2014).

Genom att kombinera dessa två metodansatser kan studien både förstå de bakomliggande mekanismerna och erfarenheterna (kvalitativa) samt erbjuda en överblick av utbredningen och omfattningen av säkerhetsrelaterade problem (kvantitativa). Detta ger en mer heltäckande bild av det komplexa fenomen som studien ämnar belysa.

### **3.3.1 Styrkor**

En central styrka är att metoden möjliggör en djupgående förståelse av situationen. Enligt Jacobsen, Andersson och Holmberg (2024) kvalitativa data kännetecknas av att vara öppna och nyansrika, vilket gör det möjligt att fånga komplexiteten i det studerade fenomenet, och kvalitativa ansatser har hög relevans då de ofta leder direkt till en djupare insikt om situationer eller processer. Flexibilitet är en av kvalitativ metods styrkor (Jacobsen, Andersson & Holmberg 2024). Det innebär att forskarna har möjlighet att justera både problemformulering och datainsamlingsstrategi under studiens gång. Forskningsprocessen är således inte strikt förutbestämd, utan kan anpassas efterhand som nya insikter uppstår, vilket gör den kvalitativa ansatsen särskilt lämplig för utforskande studier. En av de mest framträdande styrkorna med den kvalitativa metod som tillämpats i denna studie också är möjligheten till nära kontakt med respondenterna, vilket har skapat förtroende och ökat öppenheten i intervjuvaren (Jacobsen, Andersson & Holmberg 2024). Genom att låta samtalen formas utifrån deltagarnas egna erfarenheter snarare än en fast intervjuguide, kunde nyanserade och innehållsrika data samlas in.

Enkäten som datainsamlingsmetod har flera fördelar. Enligt Ejlertsson och Axelsson (2014) är enkäter särskilt lämpliga i vissa sammanhang, exempelvis när många personer ska nås på ett kostnadseffektivt sätt. En ytterligare styrka är att respondenterna kan besvara frågorna i sin egen takt och kontrollera relevanta fakta vid behov. I denna studie hade deltagarna två veckor på sig att besvara enkäten, vilket ökade möjligheten till välgrundade svar.

### **3.3.2 Svagheter**

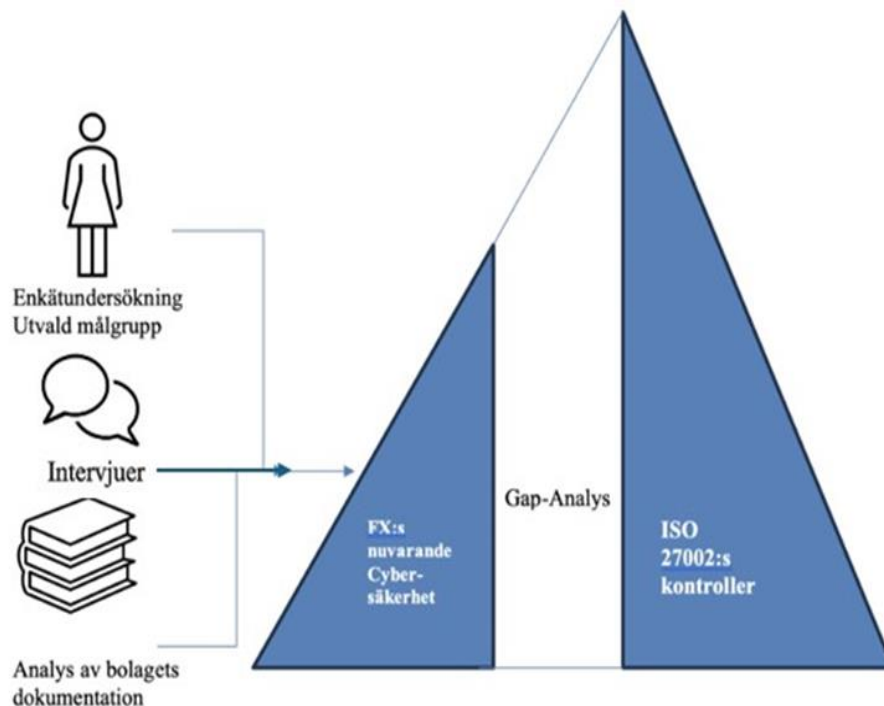
Med kvalitativa metoder är att de ofta är tids- och resurskrävande, särskilt när det gäller att samla in relevanta dokument och litteratur (Jacobsen, Andersson & Holmberg 2024). I denna studie kunde dock denna utmaning hanteras på ett effektivt sätt. Efter att ett sekretessavtal (NDA) undertecknats erhöll forskarna tillgång till det relevanta dokumentmaterialet från FX samt möjlighet att boka möten med berörda representanter inom organisationen. Vid behov kunde ytterligare kompletterande material begäras in, vilket bidrog till att underlätta och fördjupa datainsamlingen.

Jacobsen, Andersson och Holmberg (2024) pekar också på metodens komplexitet som en möjlig svaghet, det kan vara utmanande att tolka dokument korrekt, särskilt vid stora mängder kvalitativa data. I det här fallet upplevde forskarna vissa tolkningssvårigheter, vilket löstes genom återkoppling till FX för att få förtydliganden. En annan svaghet som nämns är metodens flexibilitet; även om den ofta ses som en fördel, kan den leda till känslan av att studien aldrig blir helt färdigställd, vilket kan skapa osäkerhet hos forskarna

## **3.4 Forskningsdesign**

Denna studie utgör en gap-analys med syftet att granska och bedöma de säkerhetskontroller som för närvarande tillämpas inom FX. Dessa kontroller omfattar både tekniska åtgärder och interna policyer som syftar till att upprätthålla en säker informationshantering inom organisationen. Genom att jämföra FX:s befintliga säkerhetsrutiner med de standardiserade riktlinjer som återfinns i ISO 27002, identifieras eventuella avvikelser, brister samt potentiella förbättringsområden i företagets övergripande arbete med informationssäkerhet.

Figur 4 illustrerar den systematiska metod som används för att utvärdera FX nuvarande cybersäkerhetsstatus. Tre primära datainsamlingsmetoder tillämpas: enkätundersökningar, semistrukturerade intervjuer och dokumentanalys. Data analyseras sedan genom en jämförelse med kraven i ISO 27002:s kontroller för att identifiera eventuella brister, vilket utgör själva gap-analysen.



Figur 4 Visualisering av identifieringsprocess av eventuella brister hos FX:s arbetsstruktur

### 3.4.1 Granskning av ISO standarder:

Som ett första steg genomfördes en sökning efter relevanta ISO-standarder via Svenska Institutet för Standarder (SIS). Eftersom tillgång till dessa standarder är kostnadsbelagd, kontaktades FX för att erhålla tillgång till de nödvändiga ISO dokument. En noggrann granskning av ISO 27001 och ISO 27002 genomfördes, med fokus på att extrahera säkerhetskontroller från relevanta kapitel. Dessa kontroller sammanställdes i en Excel fil som checklista, och sedan användes som underlag för att formulera frågor till enkäten.

### 3.4.2 Analys av FX dokument

För att fördjupa förståelsen av företagets DevOps-modell analyserades befintliga processer med fokus på att identifiera eventuella avvikelser i förhållande till krav i ISO 27001 och ISO 27002. Dessa gap dokumenterades systematiskt som underlag för möjliga förbättringsåtgärder. Det empiriska materialet har även legat till grund för utformningen av intervjufrågor och den efterföljande analysen, vilket i sin tur har resulterat i rekommendationer för att stärka efterlevnaden av gällande informationssäkerhetsstandarder.

Tabell 1 presenterar en översikt över de datainsamlingen från dokument som använts i studien, tillsammans med respektive syfte.

Typ	Dokumentsnamn	Beskrivning	Syfte
Dokument	<i>User Requirements Specification</i> (användarkrav)	Beskriver användarkraven och de funktionella förväntningarna på systemet.	Ge en översikt över användarkrav samt de funktionella förväntningarna på systemet.
Dokument	<i>Work Instruction</i> (arbetsinstruktioner)	Innehåller detaljerade instruktioner för arbetsprocesser och implementering av säkerhetsåtgärder.	Ge detaljerade instruktioner för arbetsprocesser och implementering av säkerhetsåtgärder.
Dokument	<i>Security in IT Solution Delivery</i> (säkerhet vid leverans av IT-lösningar)	Riktlinjer för att integrera säkerhetsåtgärder i utvecklings- och leveransprocessen av IT-lösningar	Ge riktlinjer för hur säkerhetsåtgärder kan integreras i utvecklings- och leveransprocesser.
Dokument	<i>DevOps and Agile Playbook</i> (riktlinjer för DevOps och agila metoder)	Policyer och metoder för att tillämpa DevOps och agila arbetssätt inom organisationen.	Identifiera policyer och metoder för att tillämpa DevOps och agila arbetssätt inom organisationen.
Dokument	ISO 27001	Internationell standard för hur man etablerar, implementerar, underhåller och förbättrar ett ledningssystem för informationssäkerhet (ISMS).	Förstå vilka krav som krävs för att uppnå certifiering enligt ISO 27001.
Dokument	ISO 27002	En uppsättning riktlinjer med säkerhetsåtgärder (kontroller) som stödjer ISO 27001, alltså <i>hur</i> man skyddar information i praktiken.	Identifiera vilka krav FX bör uppfylla inom intern mjukvara utveckling och informationssäkerhet.

### 3.4.3 Enkätundersökning

En enkätundersökning riktad till relevanta anställda inom FX genomfördes och syftet var att erhålla insikter om hur säkerhetskontrollerna efterlevs i praktiken, att kartlägga i vilken utsträckning dessa kontroller är implementerade inom organisationen och att bidra till att formulera intervjufrågor. Enkäten fokuserade på att identifiera aspekter av efterlevnaden för säkerhetskontroller.

Figur 5 illustrerar de grundläggande stegen i en forskningsprocess med fokus på enkätundersökningar. Processen inleds med att formulera syfte och problem – vad ska undersökas och varför. Därefter identifieras målgruppen och hur urvalet ska göras. Nästa steg är att utforma relevanta frågor för att samla in rätt information som analyseras genom bearbetning och tolkning. Slutligen publiceras resultaten så att de kan spridas och användas

vidare. Enligt (Ejlertsson & Axelsson 2014) säkerställer det systematisk och trovärdig forskningsprocess.



Figur 5 stegen i undersökningen

### 3.4.4 Målgrupp för enkätundersökningen

Målgruppen för enkätundersökningen definierades i samråd med FX:s [PhD & CISO / IT Director, Risk, Security and Compliance, and Global IT]. Baserat på hans rekommendationer riktades enkäten specifikt mot de roller inom organisationen som för närvarande har ansvar för följande centrala områden:

- Insikter om intern mjukvaruutveckling (Software Development In-House): Personer som är direkt involverade i utvecklingen av FX egna mjukvarulösningar.
- Insikter om operativ modell (Operating Model): Individer med kunskap om FX operativa processer och arbetsflöden.
- Insikter om arkitektur och inköpta applikationer (Architectural and Purchased Applications): Roller som arbetar med systemarkitektur och hantering av externa mjukvarulösningar.

- Insikter om allmän säkerhet (General Security): Personal med ansvar för övergripande säkerhetsfrågor och policyer.
- Insikter om mjukvaruunderhåll (Software Maintenance): Individer som är involverade i underhåll och uppdatering av befintliga mjukvarusystem.
- Insikter om Agile och DevOps (Agile and DevOps): Personer som arbetar med eller har kunskap om FX:s tillämpning av agila metoder och DevOps-principer.

Genom att rikta enkäten mot dessa specifika roller säkerställdes att respondenterna besitter den nödvändiga kompetensen och insikten för att ge relevanta och tillförlitliga svar.

### 3.4.5 Utformning av enkäten

Utformningen av frågor i ett frågeformulär kräver noggrant hänsynstagande till ett antal grundläggande principer, däribland vikten av språklig enkelhet och tydlighet i formuleringarna (Ejlertsson & Axelsson 2014). I enlighet med detta anpassades frågornas språkbruk efter målgruppen, och terminologi valdes med omsorg för att säkerställa att begreppen var väl förankrade i respondenternas kunskapsnivå och kontext.

(Ejlertsson & Axelsson 2014) betonar att frågor inte bör vara flertydiga, då en fråga som kan tolkas på flera sätt riskerar att generera svar som är svåra att tolka i efterhand. Om det är oklart hur respondenten har uppfattat en fråga, kan inte heller svaret ges en tillförlitlig analytisk betydelse.

Enkätens frågor utformades med fokus på att varje fråga skulle belysa en specifik aspekt av säkerhetskontrollerna, i syfte att undersöka deras aktuella tillämpning inom organisationen. Respondenterna ombads klassificera varje kontroll enligt fem fasta svarsalternativ: fullt implementerad (dokumenterad och genomförd), delvis implementerad, ej implementerad, ej tillämplig samt inte en del av min roll. För att fördjupa svaren och identifiera eventuella organisatoriska brister inkluderades även en öppen följdfråga: ”Om det inte finns en befintlig roll som kan ta ansvar för denna uppgift, föreslå en lämplig roll.” Denna del av enkäten syftade till att belysa behovet av nya roller eller ansvarsområden för att säkerställa att alla relevanta krav i ISO 27002 hanteras systematiskt.

Enkäten utformades och distribuerades med hjälp av Microsoft Forms. Frågeformuläret baserades på säkerhetskontroller från följande kapitel i ISO 27002: 8.25 säker utvecklingslivscykeln, 8.26 säkerhetskrav för applikationer, 8.27 säker systemarkitektur och

tekniska principer samt 8.28 säker kodning. En fullständig översikt av enkätfrågorna och svaret på dem återfinns i Bilaga 1 och Bilaga 2.

### 3.4.6 Enkätprocess

Som en del av datainsamlingen genomfördes fyra separata enkäter som syftade till att kartlägga kunskap och praxis inom olika områden av säker mjukvaruutveckling, och svaret ska bidra till att formulera intervjufrågor. Dessa områden inkluderade: Principer för säker systemarkitektur och systemutformning, Säker kodning, Säker systemutvecklingslivscykel, samt Säkerhetskrav för applikationer. Antalet svar varierade mellan 5 och 9, vilket återspeglar skillnader i de anställdas ansvarsområden och expertis inom respektive domän.

Fyra enkäter skickades via e-post till ett urval av tio respondenter som är studiens målgrupp. För att säkerställa att länkarna i e-postmeddelandet var autentiska och inte utgjorde någon form av phishing, inkluderades även FX IT-direktör i mejlet som en bekräftelse på legitimitet. Efter en vecka IT-direktören kontaktades för att påminna de anställda om att besvara enkäten. Efter ytterligare en vecka hade samtliga deltagare svarat på enkäten. Antalet svar varierade mellan de olika enkäterna, vilket kan förklaras av att varje respondent endast besvarade de delar som föll inom ramen för deras respektive ansvarsområde. Svaren sammanställdes och exporterades från Microsoft forms som Excel-filer för att senare användas som underlag för en gap-analys och formulera frågor för intervjuer.

*Tabell 2 redovisar det totala antalet svar som inkommit för varje enkät del och bort fall.*

Enkät	Antal svar	Bort fall
Principer för säker systemarkitektur och systemutformning	5	4
Säker kodning	6	3
Säker systemutvecklingslivscykel	8	1
Säkerhetskrav för applikationer	9	0

### 3.4.7 Intervjuer

Vid insamling av kvalitativa data finns det flera typer av intervjumetoder att välja mellan, beroende på studiens syfte och forskningsfrågor. De vanligaste formerna är strukturerade, ostrukturerade och semistrukturerade intervjuer. Strukturerade intervjuer kännetecknas av att forskaren använder ett fast frågeschema där frågorna ställs i en bestämd ordning och

formuleras på ett enhetligt sätt till samtliga respondenter. Fördelen med denna metod är att den ger hög jämförbarhet och är relativt enkel att analysera, men den begränsar också möjligheten att fånga nyanserade svar eller följa upp oväntade teman (Bryman et al. 2025).

Ostrukturerade intervjuer erbjuder stor flexibilitet. Här har forskaren inga i förväg bestämda frågor utan utgår i stället från några löst formulerade teman. Detta kan skapa utrymme för djupare och mer spontana samtal, men medför också en risk för att viktiga ämnen förbises och att analysen blir mer komplex (Justesen & Mik-Meyer 2011).

Semistrukturerade intervjuer kombinerar styrkorna från de två ovan nämnda metoderna och har därför blivit ett vanligt val i kvalitativ forskning. Denna metod innebär att forskaren använder en intervjuguide med öppna huvudfrågor som ger struktur, samtidigt som det finns möjlighet att anpassa frågorna utifrån samtalets gång. Fördelen med denna metod är att den möjliggör jämförbarhet mellan intervjuer samtidigt som forskaren har frihet att följa upp relevanta teman som uppstår under samtalet (Bryman et al. 2025). Den semistrukturerade intervjun är särskilt lämplig när forskaren eftersträvar en djupare förståelse för individers upplevelser, attityder och tolkningar (Jacobsen, Andersson & Holmberg 2024).

I denna studie har kvalitativa, semistrukturerade intervjuer använts som datainsamlingsmetod för att undersöka upplevda problem och hinder i informationssäkerhetshantering inom en organisation (FX), och för att komplettera svaren som forskarna fick från enkätundersökning. Utformningen av intervjufrågorna grundades i relevant vetenskaplig litteratur, där särskild vikt lades vid att formulera frågor som främjar reflektion och möjliggör nyanserade beskrivningar av respondenternas erfarenheter (Jacobsen, Andersson & Holmberg 2024). Intervjufrågorna utvecklades med stöd av en intervjuguide, som konstruerades för att vara tillräckligt strukturerad för att säkerställa jämförbarhet mellan intervjuerna, men samtidigt öppen nog för att fånga upp oväntade insikter. Dessutom låg resultaten från en tidigare enkätundersökning inom organisationen till grund för identifieringen av centrala teman, vilket bidrog till att göra frågorna kontextspecifika och empiriskt förankrade. Den semistrukturerade intervjun är särskilt lämplig i sammanhang där forskaren vill uppnå en djupare förståelse för individers uppfattningar och erfarenheter (Bryman et al. 2025). Metoden möjliggör en flexibel intervjuprocess där forskaren följer en intervjuguide med öppna huvudfrågor, men också kan avvika från denna för att följa upp intressanta teman som uppstår under samtalet (Justesen & Mik-Meyer 2011).

Tabellen nedan (se Tabell 3) redogör för genomförda intervjuer, inklusive datum, kön på deltagarna, yrkesroller, intervjutid samt intervjuform. Databasinsamlingen ägde rum mellan januari och april 2025 och omfattade totalt tio intervjuer, varav nio genomfördes via Microsoft Teams och en blev avbryt och skickade frågor via e-post i stället. Vid det första intervjutillfället träffade forskarna en representant från företaget. Syftet med mötet var att inledningsvis presentera företagets verksamhet samt att introducera den studie som ska genomföras. Under mötet erhöll forskarna även tillgång till relevanta dokument som bedömdes vara av betydelse för det fortsatta forskningsarbetet. Intervjuerna varierade i längd mellan 34 minuter och drygt 68 minuter. Deltagarna representerar ett brett spektrum av roller inom organisationen, däribland IT-direktörer, säkerhetsspecialister och applikationsägare, vilket bidrar till ett mångfacetterat perspektiv på organisationens projektmiljö.

Samtliga intervjuer utgick från en gemensam intervjuguide, utformad i enlighet med rekommendationer från Justesen, Mik-Meyer och Andersson (2011), där alla intervjupersoner fick besvara samma öppna huvudfrågor, se intervjufrågor i *bilaga 3*. Frågorna anpassades dock i viss mån efter respondenternas specifika roller och ansvar, för att säkerställa att svaren blev så relevanta som möjligt i förhållande till studiens syfte. Under intervjuerna tillämpades ett aktivt lyssnande för att kunna ställa adekvata följdfrågor och därigenom fördjupa förståelsen för de problem och hinder som informanterna beskrev, och alla intervjuer spelades in för att möjliggöra en noggrann analys och för att kunna sammanställa resultaten.

Metodens flexibilitet skapade utrymme för att intervjupersonerna kunde utveckla sina svar fritt och lyfta egna perspektiv och erfarenheter av informationssäkerhet, vilket bidrar till att generera ny kunskap och insikter inom det studerade området (Bryman et al. 2025).

*Tabell 3 Översikt över genomförda intervjuer.*

<b>Datum</b>	<b>Kön</b>	<b>Roll</b>	<b>Tid min:sek</b>	<b>Plats</b>
Tor 2025-01-23 11:00	<ul style="list-style-type: none"> <li>• Man</li> <li>• Man</li> <li>• Kvinna</li> </ul>	<ul style="list-style-type: none"> <li>• Operational and Application Security Specialist,</li> <li>• (PhD &amp; CISO / IT Director, Risk, Security and Compliance, and Global IT)</li> </ul>	57:05	Microsoft Teams (Inlednings möte)

		<ul style="list-style-type: none"> <li>External Contractor, Risk, Security and Compliance team</li> </ul>		
Mån 2025-03-03 11:00	<ul style="list-style-type: none"> <li>Man</li> <li>Kvinna</li> </ul>	<ul style="list-style-type: none"> <li>(PhD &amp; CISO / IT Director, Risk, Security and Compliance, and Global IT)</li> <li>External Contractor, Risk, Security and Compliance team</li> </ul>	54:37	Microsoft Teams
Tor 2025-04-10 11:00	<ul style="list-style-type: none"> <li>Man</li> </ul>	<ul style="list-style-type: none"> <li>IT Director</li> </ul>	41:44	Microsoft Teams
Tor 2025-04-10 13:00	<ul style="list-style-type: none"> <li>Man</li> <li>Man</li> </ul>	<ul style="list-style-type: none"> <li>Process Application Specialist</li> <li>IT Application Owner</li> </ul>	54:42	Microsoft Teams
Fre 2025-04-11 11:00	<ul style="list-style-type: none"> <li>Man</li> </ul>	<ul style="list-style-type: none"> <li>Operational and Application Security Specialist</li> </ul>	48:51	Microsoft Teams
Mån 2025-04-14 10:00	<ul style="list-style-type: none"> <li>Man</li> </ul>	<ul style="list-style-type: none"> <li>Solution Delivery Lead – ORS &amp; eCommerce</li> </ul>	50:36	Microsoft Teams
Mån 2025-04-14 13:00	<ul style="list-style-type: none"> <li>Man</li> </ul>	<ul style="list-style-type: none"> <li>Global IT Director Enterprise Architecture</li> </ul>	1:04:18	Microsoft Teams
Tis 2025-04-15 09:00	<ul style="list-style-type: none"> <li>Man</li> </ul>	<ul style="list-style-type: none"> <li>SAP Enterprise Architect</li> </ul>	1:08:06	Microsoft Teams
Ons 2025-04-16 09:00	<ul style="list-style-type: none"> <li>Man</li> </ul>	<ul style="list-style-type: none"> <li>AI ML Applied Research Scientist</li> </ul>	34:01	Microsoft Teams

### 3.4.8 Urvalskriterier för intervjuer

Att fastställa en lämplig urvalsstorlek är en återkommande utmaning inom både kvalitativ och kvantitativ forskning. Det är svårt att på förhand avgöra hur många respondenter som krävs för att uppnå teoretisk mättnad, det vill säga den punkt då ytterligare datainsamling inte tillför ny information. Enligt Bryman et al. (2025) menar vidare att om studiens syfte är att genomföra jämförelser mellan olika grupper exempelvis kön, ålder eller andra kategoriseringar krävs ett större och mer representativt urval.

Men studien är dock avsikten inte att jämföra olika grupper, utan snarare att få fördjupad insikt i en specifik kontext. För att besvara studiens frågeställningar har urvalet därför begränsats till individer med särskild kunskap och ansvarsområde om utveckling säkerhet och

säkerhetskontroller i FX. Det är alltså ett strategiskt urval där kompetens snarare än antal är avgörande. I linje med detta resonemang lyfter (Justesen & Mik-Meyer 2011) att en nära forskar–respondentrelation ofta är en fördel vid kvalitativa studier som syftar till att nå djupare förståelse, och att sådana studier ofta fungerar bäst med mindre urvalsgrupper.

I denna studie valdes att inledningsvis genomföra intervjuer med ett antal anställda inom FX som innehar nyckelroller i organisationens säkerhets- och utvecklingsarbete. Urvalet baserades på de svar som inkommit från den tidigare genomförda enkätundersökningen, där specifika områden identifierades som behövde fördjupas. Syftet med intervjuerna var att komplettera och förtydliga enkätsvaren, samt att samla in ytterligare information i syfte att uppnå datamättnad. Datainsamlingen avslutades i enlighet med principen om teoretisk mättnad, det vill säga när forskarna bedömde att ytterligare insamling inte längre tillförde ny information eller insikter (Bryman et al. 2025).

### **3.4.9 Studiens validitet och reliabilitet**

Validitet och reliabilitet utgör grundläggande begrepp för att bedöma en studies vetenskapliga trovärdighet. Dessa begrepp fungerar som kvalitetskriterier inom samhällsvetenskaplig forskning och är särskilt relevanta vid granskning av metodval och resultatens användbarhet (Jacobsen, Andersson & Holmberg 2024). Validitet avser i vilken utsträckning studien mäter det fenomen som den ämnar undersöka, det vill säga i vilken grad resultaten är giltiga i förhållande till studiens syfte och forskningsfrågor. Om validiteten är hög kan slutsatserna anses vara både relevanta och representativa för det undersökta området. Reliabilitet syftar på studiens stabilitet och upprepbarhet om samma metod används vid ett annat tillfälle, under liknande omständigheter, bör resultaten överensstämma. En studie med hög reliabilitet präglas av transparens, systematik och konsekvens i såväl datainsamling som analys (Justesen & Mik-Meyer 2011)

I denna studie har validiteten säkerställts genom en metodologisk triangulering där tre olika datakällor kombinerats: dokumentanalys, enkätundersökning och semistrukturerade intervjuer. Detta tillvägagångssätt har möjliggjort att olika perspektiv belyses och jämförs, vilket stärker slutsatsernas relevans och kontextuell.

Begreppsvaliditet är ofta den mest utmanande formen av validitet att uppnå vid utformningen av traditionella enkätundersökningar. För att säkerställa en hög begreppsvaliditet krävs djupgående förståelse för de teorier som enkätfrågorna avser att spegla. (Ejlertsson & Axelsson

2014). Även reliabiliteten är beroende av frågornas kvalitet, bristfälligt konstruerade frågor kan leda till betydande slumpvariation i svaren, vilket i sin tur försämrar mätningens tillförlitlighet (Ejlertsson & Axelsson 2014).

I den studien utformades enkätundersökningen med noggrant strukturerade frågor, direkt kopplade till säkerhetskraven i standarden ISO 27002. Svartalternativen kategoriserades för att möjliggöra en tydlig tolkning av svaren, och formulerades som: "Fullt implementerad (dokumenterat och implementerad)", "Delvis implementerat", "Ej implementerad ", "Ej tillämpligt" samt "Inte en del av min roll". Denna strukturering bidrog till att underlätta analysen och stärkte resultatens tillförlitlighet.

En fördel med enkätmetoden är dess förmåga att samla in data från ett större antal respondenter på ett relativt tidseffektivt sätt (Jacobsen, Andersson & Holmberg 2024). Detta möjliggör en övergripande kartläggning av hur säkerhetskrav implementerats inom olika delar av organisationen. En nackdel är dock att enkäter riskerar att ge ett begränsat djup och kan vara känsliga för tolkningsojämlikhet, särskilt om frågorna inte är helt entydiga eller anpassade till respondenternas olika kontextuella förhållanden (Ejlertsson & Axelsson 2014).

Under studien uppstod initialt en låg svarsfrekvens, vilket riskerade att påverka datainsamlingens omfattning negativt. Problemet hanterades genom att påminnelser skickades ut via FX IT-direktör, vilket resulterade i att samtliga respondenter inkom med svar inom den angivna tidsramen. Trots en viss försening bedöms datamaterialet ha uppnått både tillfredsställande bredd och djup.

Under analysfasen identifierades ytterligare en reliabilitetsutmaning. Vissa frågor genererade motsägelsefulla svar från olika respondenter inom samma organisation. Exempelvis kunde en respondent ange att ett visst säkerhetskrav var "Fullt implementerad", medan en annan bedömde samma krav som "Ej implementerad " eller "Delvis implementerat". För att förstå dessa diskrepanser genomfördes uppföljande intervjuer, där det framkom att respondenterna i många fall svarat utifrån sitt specifika ansvarsområde. Därmed kunde deras svar betraktas som korrekta utifrån det perspektiv de representerade. Detta belyser vikten av att i analysen beakta kontexten och den organisatoriska fördelningen av ansvar.

Samtliga intervjuer genomfördes digitalt via Microsoft Teams, vilket möjliggjorde inspelning på ett smidigt sätt. Valet av digitalt format grundades även i praktiska förhållanden då flera deltagare var verksamma i olika länder inom samma organisation, och efter deltagarnas önskemål.

Samtidigt är kvalitativa intervjuer resurskrävande både vad gäller tid och analysarbete. De är också känsliga för forskarens egna tolkningar, vilket kan påverka resultatens reliabilitet och trovärdighet (Jacobsen, Andersson & Holmberg 2024). För att minska risken för tolkningsojämlighet i analysarbetet tillämpades ett reflexivt förhållningssätt, där forskarna medvetet reflekterade över sin egen förförståelse och hur denna kunde påverka insamling och analys av data. Reflexivitet är centralt inom kvalitativ forskning, då det ökar insynen i forskningsprocessen och stärker trovärdigheten i resultaten (Justesen & Mik-Meyer 2011)

Dokumentanalys har även spelat en betydande roll i datainsamlingen. Genom att studera interna policyer och processdokument från FX kunde forskarna jämföra organisationens faktiska arbetsstruktur med relevanta ISO-krav. En fördel med dokumentanalys är att den tillhandahåller detaljerad och systematisk information som ofta är svår att fånga genom andra metoder. Dock noterades att vissa dokument var svårtolkade eller saknade tillräcklig detaljnivå, vilket krävde kompletterande tolkningar genom uppföljande intervjuer med ansvariga.

## 4. RESULTAT

Detta kapitel presenterar studiens resultat strukturerat enligt de fyra huvudområdena: säker utvecklingscykel, säker systemarkitektur, säker kodning samt säkerhetskrav för applikationer. Resultaten baseras på en omfattande empirisk datainsamling genom intervjuer och dokumentanalys. Kapitlet inleds med en översiktlig presentation av det empiriska sammanhanget och data, varefter detaljerade resultat presenteras i bilagor från enkät och sen resultat från intervjuer.

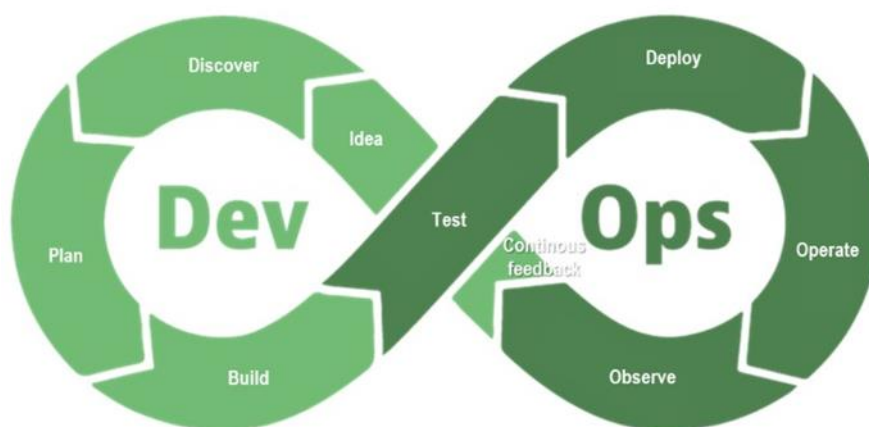
### 4.1 Empiriskt sammanhang och FX agilt arbetssätt

Studien genomfördes som en fallstudie på företaget FX, ett multinationellt företag med komplex IT-miljö bestående av cirka 600 officiella system och uppskattningsvis 3000 skugg-IT-system, vilket är IT-system, applikationer eller tjänster som används inom en organisation utan att vara godkända, kontrollerade eller hanterade av IT-avdelningen. Det kan inkludera allt från molntjänster (som Google Drive eller Dropbox) till sociala plattformar (som LinkedIn), AI-tjänster (som DeepSeek), eller till och med utländska webbplatser och appar, exempelvis ryska hemsidor som kan samla in eller behandla känsliga data. Även hårdvara eller programvara som anställda själva installerar för att lösa arbetsuppgifter utan IT:s vetskap räknas som Shadow IT. Datainsamlingen omfattade FX dokument analys, enkätundersökning och kvalitativa intervjuer med nyckelaktörer från olika delar av organisationen, inklusive IT Director, säkerhetsspecialister, IT arkitekter och utvecklare. Dessa representerade ett brett spektrum av roller och ansvarsområden, vilket möjliggjorde en helhetssyn på organisationens cybersäkerhetsstatus.

FX tillämpar ett agilt arbetssätt baserat på DevOps-principer. DevOps utgör en grundläggande komponent i FX operativa modell och påverkar i hög grad såväl organisationens arbetsprocesser som dess tjänsteleverans. Genom att integrera och automatisera moment relaterade till både systemutveckling och konfiguration (Development) samt IT-drift (Operations), syftar modellen till att öka effektiviteten och samtidigt förkorta systemutvecklingslivscykeln.

*Figur 6* illustrerar en agil DevOps-livscykel, där de olika processerna är kontinuerliga och ömsesidigt beroende, snarare än sekventiellt ordnade. I figuren återfinns ett antal centrala begrepp kopplade till produktutveckling och drift, såsom *Discover*, *Delay*, *Idea*, *Test*, *Continuous Feedback*, *Ops*, *Operate*, *Plan*, *Build* och *Observe*. Dessa begrepp representerar

olika faser och nyckelaktiviteter inom en samtida utvecklingsmiljö, där fokus ligger på ständig förbättring, återkoppling och tvärfunktionellt samarbete.



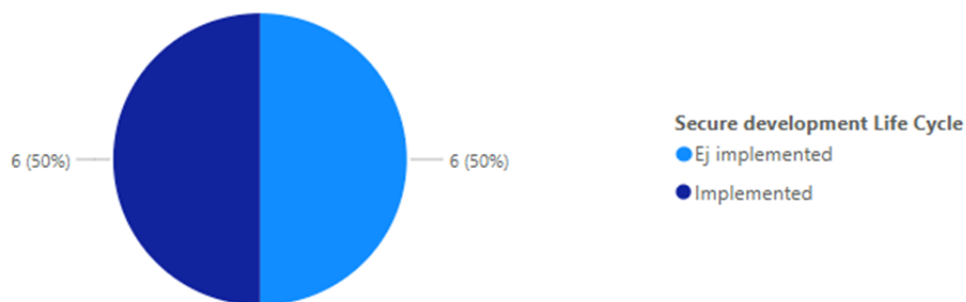
Figur 6 (DevOps) Iterativ livscykel för produktutveckling och drift.

## 4.2 Presentation av enkätresultaten

Resultaten presenteras inom ramen för fyra huvudsakliga kategorier, där varje kategori kompletteras med tabeller som visar hur utvalda kontroller enligt ISO 27002 har implementerats. I enkäten ombads respondenterna att ange sin yrkesroll samt att bedöma varje kontroll som fullt implementerad, delvis implementerad eller ej implementerad. För varje enskild kontroll redovisas vilka roller som bekräftat att implementeringen är fullständig, liksom eventuella skillnader i bedömning mellan olika respondenter. Tabeller som visar vilka kontroller som bedömts vara fullt implementerade enligt respektive kapitel i ISO 27002, tillsammans med enkätsvaren, återfinns i Bilaga 1. Kontroller som bedömts som delvis implementerade eller ej implementerade redovisas separat i Bilaga 2. I denna studie betraktas en kontroll som uppfylld om minst en respondent – utifrån sin roll – anger att den är fullt implementerad. Dessa resultat visualiseras även i form av diagram för att underlätta tolkningen.

### 4.2.1 Säker utvecklingscykel

Figur 7 illustrerar tillämpningen av säkerhetskrav i utvecklingslivscykeln. Här är fördelningen jämn, med 50 % (6 st) av kraven implementerade och 50 % (6 st) ej genomförda. Detta indikerar en delvis följd säkerhetsmetodik, men samtidigt en tydlig potential för ytterligare förbättringar.



Figur 7 Implementeringsgrad för säker utvecklingscykel.

#### 4.2.2 Säker systemarkitektur och tekniska principer

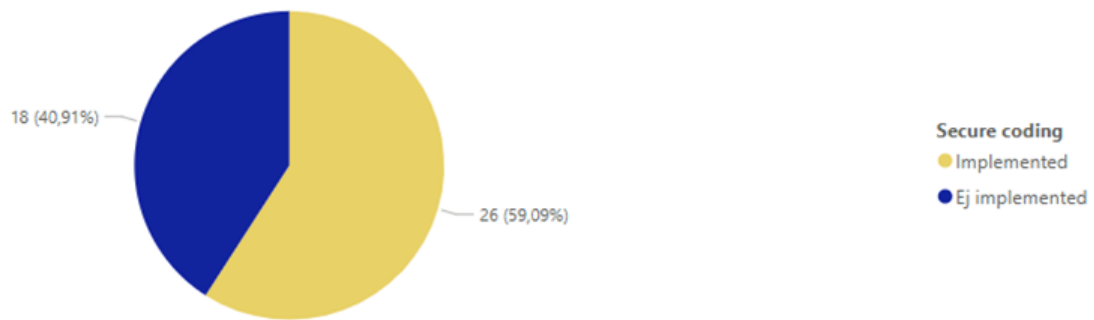
Figur 8 visar redovisar implementeringsgraden av säkerhetskrav relaterade till systemarkitektur och tekniska principer. Endast 23,33 % (7 st) av kraven är fullt implementerade, medan 76,67 % (23 st) ännu saknar implementering. Resultatet belyser ett betydande efterarbete för att uppnå efterlevnad enligt relevant säkerhetsstandarder. Diagrammet ger en tydlig översikt över nuvarande status i FX och belyser behovet av ytterligare arbete för att uppnå fullständig efterlevnad enligt ISO 27002.



Figur 8 Implementeringsgrad för säker systemarkitektur och tekniska principer

#### 4.2.3 Säker kodning

Figur 9 visar implementeringsgraden av säkerhetskrav från ISO 27002-standardens avsnitt om säker kodning inom FX. Enligt data har 40,91 % (18 st) av kraven fullföljts, medan 59,09 % (26 st) ännu inte implementerats. Resultatet indikerar att det finns utrymme för förbättringar när det gäller att tillämpa säker kodning enligt ISO 27002.



Figur 9 Implementeringsgrad för Säker kodning

#### 4.2.4 Säkerhetskrav för applikationer

Figur 10 presenterar implementeringsstatus för applikationssäkerhetskrav. Enligt data från enkät är endast 9,38% (3 st) av kraven fullt implementerade, medan majoriteten på 90,63% (29 st) fortfarande inte är genomförda. Denna stora skillnad indikerar ett betydande implementeringsgap när det gäller applikationssäkerhet. Resultaten understryker ett akut behov av att prioritera och åtgärda dessa säkerhetskrav för att uppnå en god säkerhetsnivå.



Figur 10 Implementeringsgrad för Säkerhetskrav för applikationer

### 4.3 Intervjuresultat: Agil transformation och cybersäkerhetsutmaningar i praktiken

I studien har semistrukturerade intervjuer genomförts med representanter från olika funktioner inom organisationen. De intervjuade personerna innehar varierande roller, ansvarsnivåer och tekniska expertisområden, vilket möjliggör en mångsidig belysning av ämnet.

Intervjuerna syftar även till att verifiera och komplettera de resultat som framkommit genom enkätundersökningen. Genom den semistrukturerade intervjumetodiken har det varit möjligt att anpassa frågorna efter varje respondents perspektiv, vilket har resulterat i mer nyanserade och

kontextuellt relevanta insikter. I det följande avsnittet presenteras centrala teman som framkommit i intervjumaterialet, med särskilt fokus på agila transformationsprocesser, cybersäkerhetsutmaningar samt ansvarsfördelning i en tekniskt komplex och distribuerad organisation.

#### 4.3.1 Varierande tolkningar av agila arbetssätt

Intervjuerna visar att förståelsen och tillämpningen av agila och DevOps-inspirerade arbetssätt skiljer sig markant mellan olika delar av företaget FX. Inom vissa team är det agila arbetssättet väl etablerat. En Solution Delivery Lead som leder arbete med front- och backend team, fokuserar på applikationsutveckling och DevOps, beskriver till exempel en tydlig uppdelning mellan frontend och backend-utveckling, där teamen arbetar parallellt men med nära samarbete:

*"Vi har olika team som jobbar med olika saker – portalen som kunden ser och backend. Vi jobbar mycket med andra team också."*

DevOps-modellen innebär här ett helhetsansvar för både utveckling och underhåll, vilket kräver tät kommunikation och hög grad av automatisering. Som respondenten uttrycker det:

*"Det primära ansvaret är applikationsutveckling och underhåll, alltså agil DevOps."*

Samtidigt finns exempel på verksamhetsdelar som fortfarande präglas av traditionella arbetsmodeller. SAP-verksamheten (*Systems, Applications and Products in Data Processing*) lyfts fram som ett område där det agila arbetssättet möter motstånd. En SAP Enterprise Architect som ansvarar för SAP – kärnsystemet för hela verksamheten, med cirka 2000 användare globalt, betonar behovet av struktur och kontroll:

*"Jag tror på agilt, men vi måste ha kontroll. Mitt team, till exempel – jag vill införa krav på struktur, och team som inte uppfyller kraven får inte utveckla för mig. Teamen som uppfyller krav får göra jobbet."*

Övergången till agila arbetssätt inom organisationen präglas av stora skillnader mellan teamen, vilket tyder på att förändringen saknar en enhetlig styrning. Flera respondenter lyfter behovet av en gemensam referensram, exempelvis en standardiserad agile playbook, för att minska fragmentering och skapa samsyn. Samtidigt framgår det att vissa anställda fortfarande arbetar enligt den traditionella Vattenfallsmodellen, vilket försvårar anpassningen till mer iterativa och självorganiserade arbetssätt som DevOps. Denna

kulturella tröghet kan påverka organisationens tekniska utveckling, och visar på behovet av tydlig vägledning och kompetensstöd i förändringsarbetet.

#### **4.3.2 Otydlig ansvarsfördelning och bristande styrning i cybersäkerhetsarbetet**

Flera intervjuer pekar på en genomgående osäkerhet kring vem som ansvarar för cybersäkerheten i olika delar av organisationen. En återkommande synpunkt är att kompetensförväntningarna är otydliga. Som en Solution Delivery Lead uttrycker det:

*"Det finns en gemensam känsla av otydlighet när det gäller hur hög kompetens inom cybersäkerhet borde det vara inom teamen."*

Denna otydlighet förvärras i molnbaserade miljöer där teknikutvecklingen sker snabbt, och teamen upplever att de saknar överblick över nya funktioner och säkerhetsinställningar. Respondenter menar att säkerhetsarbetet ofta förutsätter att någon annan har koll:

*"Vi jobbar mycket på Azure och cloud – det kommer nya saker hela tiden. Vi kan inte ha koll på det. Vi måste ha en expert som kollar upp sådana viktiga features."*

Ansvarsförskjutningen är tydlig även i relationen till externa leverantörer. Flera respondenter beskriver att säkerhetsarbetet är outsourcat och att företaget agerar som beställare snarare än ägare av processen. En Operational and Application Security Specialist förklarar:

*"All säkerhet, drift och övervakningscenter är outsourcade."*

Men när säkerheten inte är fullt integrerad i det interna arbetet, uppstår en risk att den betraktas som ett separat ansvar snarare än ett gemensamt uppdrag. Detta gäller även forsknings- och utvecklingsverksamheten, där en AI/ML-specialist uttrycker frustration över bristen på vägledning:

*"Vi har inga cybersäkerhetsriktlinjer. Det är upp till var och en att fördjupa sig i det de själva anser relevant."*

### 4.3.3 Kulturella hinder och brist på ansvarskultur

En tredje central tematik i materialet rör organisationens säkerhetskultur – eller bristen på en sådan. Respondenter från olika nivåer i företaget beskriver hur ansvar för säkerhet ofta skjuts över till centrala funktioner. Global IT Director förklarar:

*"Generellt tar vi för lite ansvar eftersom många vill att IT Director team ska äga ansvaret för säkerheten, vilket är en ohållbar situation."*

Detta speglar en bredare kultur där snabb leverans prioriteras över kvalitet och korrekthet. En SAP Enterprise Architect formulerar det tydligt:

*"Det gör för lite ont att göra fel. Den som levererar snabbt lyfts fram även om det är fel."*

Dessutom framkommer att efterlevnaden av säkerhetsrutiner ofta styrs av externa krav snarare än intern policy. System som omfattas av extern granskning hanteras mer noggrant än system utan sådana krav, vilket tyder på en selektiv säkerhetsmedvetenhet. Enligt Global IT Director:

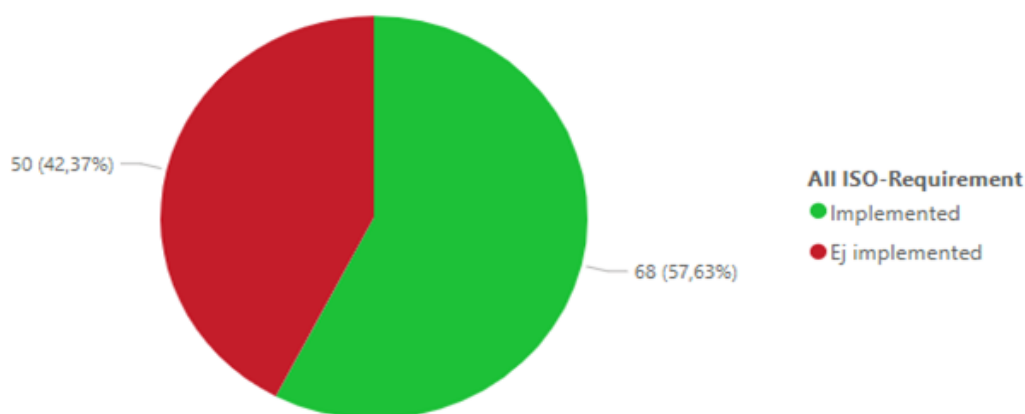
*"System som omfattas av extern validering [...] hanteras med hög strukturnivå. [...] Däremot saknas ofta formella säkerhetsrutiner för system som inte omfattas av sådan extern uppsikt."*

Sammantaget visar intervjuerna att det finns ett behov av en mer konsekvent och förankrad ansvarskultur för cybersäkerhet, där både struktur och ledarskap spelar en avgörande roll.

## 4.4 Gap-analys och de mest kritiska säkerhetskontroller som saknas

En empirisk analys har genomförts för att identifiera brister i FX:s nuvarande implementering av säkerhetskontroller enligt ISO 27002-standarderna. Studien avslöjar att ett betydande antal viktiga säkerhetsåtgärder inte är fullt ut implementerade eller helt saknas, vilket innebär allvarliga sårbarheter i organisationens cybersäkerhetsstrategi.

Enligt undersökningen omfattar ISO 27002 totalt 118 säkerhetskontroller som FX måste införa för att uppnå certifiering när verksamheten övergår till in-house-mjukvaruutveckling. Av dessa har endast en del implementerats. *Figur 11* visar fördelningen mellan implementerade och icke-implementerade ISO 27002-säkerhetskontroller i FX, där Av de totalt 118 kontrollerna är 68 (57,63%) implementerade, medan 50 (42,37%) ännu inte införts. En säkerhetskontroll bedömdes som fullt implementerad om den uppfylldes enligt målgruppens bedömning.



Figur 11 Implementeringsgrad av ISO 27002-kontroller i FX

Analysen framhäver att de icke-implementerade kontrollerna kan sammanfattas i fem kritiska brister. Dessa prioriteras och placeras inom ramen för DevSecOps-modellen, vilket presenteras i *Tabell 4* som visar prioriterade säkerhetskontroller för att stärka DevSecOps inom FX. Varje kontroll har tilldelats en prioritet, motiverats utifrån identifierade risker och kopplats till relevanta faser i utvecklingsprocessen. Syftet är att tydliggöra var insatser bör riktas för att förbättra säkerheten i mjukvaruleveransen. Dessa brister utgör centrala förbättringsområden för att säkerställa en robust säkerhetsarkitektur inför den kommande certifieringsprocessen.

Tabell 4 Säkerhetskontroller i DevSecOps deras prioritet och motivering

Säkerhetskontroller	Prioritet	Anledning	Placering i DevSecOps
Systematisk säkerhetstestning (exempelvis penetrationstester och kodgranskning)	Hög	Säkerhetstestning är avgörande för att identifiera sårbarheter innan systemet går i produktion. Bristen på detta ökar risken för exploatering av säkerhetsbrister, särskilt i en komplex IT-miljö som FX:s.	Testfasen (Continuous Testing).
Regelbunden utbildning i säker kodning för utvecklare	Hög	Kunskapsbristen bland utvecklare leder till att osäkra kodningspraxis används, vilket kan utnyttjas av angripare. Utbildning är en proaktiv åtgärd för att minska sådana risker.	Planeringsfasen (Plan) och Utvecklingsfasen (Code).

Tydlig ansvarsfördelning för säkerhetsfrågor	Hög	Studien visar att otydlig ansvarsfördelning leder till att säkerhetsåtgärder inte implementeras konsekvent. En tydlig roll- och ansvarsdefinition är nödvändig för att säkerställa ägarskap.	Alla faser, särskilt Planeringsfasen (Plan) och Övervakningsfasen (Monitor).
Automatiserad säkerhetskontinuitet i CI/CD-pipelinan	Medel	Automatisering saknas i flera delar av FX:s utvecklingsprocess, vilket gör säkerhetsarbetet manuellt och ineffektivt. Automatisering skulle öka hastigheten och tillförlitligheten.	Byggfasen (Build) och Driftsättningsfasen (Deploy).
Strukturerad hantering av tredjepartskomponenter (exempelvis bibliotek och ramverk)	Medel	FX använder många externa komponenter utan att systematiskt dokumentera eller uppdatera dem, vilket skapar säkerhetsrisker.	Utvecklingsfasen (Code) och Testfasen (Test)

#### 4.5 Sammanfattning av Resultat

Studiens resultat indikerar att FX uppvisar brister i flera centrala säkerhetskontroller enligt ISO 27002, vilket komprometterar organisationens kapacitet att hantera cybersäkerhetsrisker på ett effektivt sätt. För att adressera dessa brister krävs en särskild inriktning på de identifierade högprioriterade åtgärderna, inklusive säkerhetstestning, kompetensutveckling och en tydligare definition av ansvarsområden. Dessa åtgärder bör systematiskt integreras i samtliga faser av DevSecOps-modellen för att garantera en sammanhållen och kontinuerligt förbättrad säkerhetsprocess.

Betydande utmaning som framkommit är svårigheterna kring implementering av ISO-kontroller i samband med övergången från en traditionell DevOps-modell till en mer säkerhetsinriktad DevSecOps-ansats. Transformationen försvåras ytterligare av bristen på standardiserad kommunikation kring säkerhetskrav och ansvarsfördelning, vilket skapar osäkerhet inom både utvecklingsteam och ledning. Detta ställer krav på såväl tekniska anpassningar som kulturella förändringar inom organisationen.

En central insikt från studien är att säkerhetsarbetet inte kan begränsas till specifika funktioner eller avdelningar, utan måste genomsyra hela organisationskulturen. För att uppnå långsiktig efterlevnad av ISO-standarderna behöver FX därmed initiera en omfattande förändringsprocess som omfattar både tekniska lösningar och organisatoriska omställningar. Detta inkluderar men är inte begränsat till tydligare kommunikationsstrukturer, ett aktivt ledarskapsengagemang, en mer systematiskt dokumenterad ansvarsfördelning och höja anställda kunskap om cybersäkerhet genom riktade givande utbildningsinsatser. Endast genom en heltäckande ansats kan säkerhetsprinciperna bli en naturligt integrerad del av verksamheten snarare än en formell efterlevnadsövning.

## **5. ANALYS**

I detta kapitel analyseras studiens resultat i relation till tidigare forskning och teoretiska ramverk med syfte att bredda förståelsen av cybersäkerhetsutmaningar vid övergång till DevSecOps inom ramen för ISO 27002. Genom att använda gap-analys som metod har avståndet mellan organisationens nuvarande säkerhetsnivå och önskat tillstånd kartlagts, vilket tydliggör både brister och möjliga åtgärdsområden.

### **5.1 Analys av organisatoriska och metodologiska utmaningar**

Analysen av intervjuerna från olika delar av organisationen visar en komplex bild av hur agila metoder, DevOps och cybersäkerhetsarbete implementeras i praktiken. Det framgår tydligt att övergången från traditionella arbetsformer till agilt och DevSecOps präglas av såväl tekniska som kulturella utmaningar, vilket bekräftar tidigare forskning om transformation inom digitala miljöer (Leite et al. 2020; Carter 2017).

En ytterligare utmaning som framkom tydligt i intervjuerna och enkätundersökning är den begränsade förståelsen för ISO-standardernas krav bland respondenterna. Även om säkerhetsspecialister inom organisationen ofta har djupgående kunskap om ISO 27001 och ISO 27002, saknas det i många fall kompetens för att översätta dessa krav till tekniska implementationer i utvecklingsmiljön. Detta skapar ett glapp mellan formella regelverk och praktisk tillämpning, vilket också bekräftas i forskning om DevOps-säkerhet (Rajapakse et al. 2022). Detta kompetensgap försvårar integreringen av säkerhet i de vardagliga tekniska processerna, vilket gör att efterlevnaden riskerar att bli ytlig eller isolerad.

### **5.2 Implementering av agila och DevOps-baserade arbetssätt**

Flera respondenter beskriver en välintegrerad DevOps-struktur med tvärfunktionella team som ansvarar för både utveckling och underhåll. Denna modell återspeglar kärnan i DevOps-filosofin, där utveckling och drift samverkar i ett gemensamt ansvar över hela systemets livscykel (Rajapakse et al. 2022). Det kräver dock en kultur av transparens, automatisering och ständig återkoppling – något som endast delvis är realiserat i fallstudie.

Samtidigt framkommer i SAP-verksamheten en mer kontrollerad och hierarkisk syn på agilitet. Här betonas behovet av struktur och kontroll, vilket speglar en ofta förekommande konflikt i stora organisationer mellan självorganiserade team och krav på standardisering (Tonnquist

2024). Denna spänning indikerar att implementeringen av agila metoder måste anpassas till olika verksamhetsdelars mognadsgrad, vilket även lyfts fram av Gustavsson (2020).

### **5.3 Kulturellt motstånd och kompetensgap**

En central observation är det kulturella motståndet mot förändring, särskilt bland medarbetare med lång erfarenhet av traditionella arbetsmodeller. Respondenter beskriver hur införandet av agila och AI-drivna arbetssätt försvåras av invanda rutiner och låg förändringsvilja. Detta överensstämmer med vad Leite et al. (2020) kallar ”kulturell tröghet”, en av de största barriärerna vid övergång till DevSecOps.

Bristen av ett tydligt ägarskap för en agil playbook, i kombination med bristande kommunikation av standardiserade agila arbetssätt till leverans teams, har bidragit till fragmenterade och inkonsekventa arbetssätt inom organisationen. Det har i sin tur försvårat en enhetlig tillämpning av agila metoder i teamen. Detta förstärker tidigare forskning som betonar behovet av gemensamma ramverk för att undvika ineffektivitet och minskad samordning (Lombardi & Fanton, 2023).

### **5.4 Styrningsbrister och ansvarsfördelning i komplexa IT-miljöer**

Ett mönster i materialet handlar om bristande ansvarsfördelning och otillräckligt ledarskap. Flera av de intervjuade betonade att det ofta råder oklarhet kring vem som bär det operativa ansvaret för säkerhetskravens efterlevnad i utvecklingsprojekt. Denna osäkerhet riskerar att skapa brister i säkerhetsarbetet, särskilt i organisationer där säkerhet fortsatt betraktas som ett separat ansvarsområde snarare än en integrerad del av utvecklingskedjan. Tidigare forskning som genomfördes av Kitsios, Chatzidimitriou och Kamariotou (2023) understryker vikten av ledningsengagemang och tydlig styrning för att informationssäkerhet ska kunna bli en naturlig och långsiktig del av verksamheten.

Respondenternas beskrivningar av övergången några tjänster och system från molntjänster till lokala lösningar indikerar en osäkerhet kring hur ansvaret fördelas i samband med plattformsbaserade system. Denna osäkerhet är typisk för hybridmodeller, där ansvar för plattform och applikation är uppdelat mellan leverantör och organisation (Calder & Watkins, 2024). Bristen på tydlighet kring roller och mandat riskerar att försvaga säkerhetsstyrningen, vilket identifieras som ett kritiskt område inom systemarkitektur. Vidare saknas formella

cybersäkerhetsriktlinjer i forskningsnära funktioner. AI-forskare upplever att de själva måste tolka och implementera säkerhetsåtgärder, vilket kan leda till inkonsekvent tillämpning och ökad sårbarhet. Detta bekräftar Young et al. (2023), som betonar vikten av klara riktlinjer och stödverktyg för säker utveckling i avancerade tekniska miljöer.

## **5.5 Outsourcing och governance i cybersäkerhetsarbete**

Outsourcing av säkerhetsfunktioner innebär en betydande förskjutning av ansvar från intern IT till externa leverantörer. Respondenterna beskriver en modell som bygger på tillit till att leverantörer följer säkerhetsrutiner enligt certifieringsstandarder (till exempel ISO/IEC 27001). Även om detta kan vara effektivt i globala miljöer, betonar Fenz och Neubauer (2018) att intern uppföljning och kontroll är avgörande för att undvika säkerhetsluckor.

Att ansvaret för exempelvis backup och klienthantering ligger utanför den interna organisationen försvårar enhetlig kontroll och dokumentation. Som flera respondenter påpekar krävs tydliga avtal, servicenivåavtal (SLA) och kontrollmekanismer för att säkerställa att leverantörer lever upp till säkerhetskraven – ett synsätt som stöds av Suorsa och Helo (2023).

## **5.6 Brister i ansvarskultur och efterlevnad**

En återkommande utmaning är otydlig ansvarsfördelning och en svag ansvarskultur. Det råder oklarhet kring vilka säkerhetskunskaper som förväntas av olika team, och vem som har det yttersta ansvaret. Denna brist på tydlighet förstärks av frånvaron av standardiserade rutiner för cybersäkerhet – något som enligt ISO/IEC 27001:2022 är grundläggande för ett fungerande ISMS.

Dessutom beskriver flera respondenter en kultur där snabbhet prioriteras framför korrekthet. SAP-arkitektens observation att "det gör för lite ont att göra fel" visar på en belöningsstruktur som motverkar långsiktig efterlevnad och kvalitetskontroll. Detta står i kontrast till principerna inom DevSecOps, där säkerhet ska vara integrerad och kontinuerlig (Carter 2017).

Slutligen framgår att system som omfattas av extern granskning har högre efterlevnad än system utan regulatoriska krav. Detta mönster tyder på att säkerhetsarbete i hög grad drivs av externa incitament snarare än intern riskmedvetenhet, vilket minskar organisationens motståndskraft mot nya hot (Hussain et al. 2022).

## 5.7 Framtids förbättringar

Baserat på studiens resultat framgår ett tydligt behov av strukturerade förbättringsåtgärder för att stärka FX:s cybersäkerhetsarbete i samband med övergången till DevSecOps. Följande rekommendationer har formulerats för att adressera de brister som identifierats inom områdena ansvarsfördelning, kompetensförsörjning, systemstyrning och teknisk implementation.

För det första rekommenderas att organisationen utvecklar en övergripande säkerhetsstrategi med tydligt definierade roller och ansvarsområden. Studien visar att det idag råder oklarhet kring vilket team som bär ansvaret för cybersäkerhet, vilket försvårar samordningen av säkerhetsinitiativ. En strukturerad strategi, kompletterad med dokumenterade processer och beslutsvägar, kan bidra till att minska dessa gråzoner och stärka efterlevnaden av ISO 27002.

För det andra framkommer ett uttalat behov av satsningar på kompetensutveckling. Flera respondenter efterfrågar rekrytering av yngre medarbetare med vilja att utvecklas inom organisationen, samtidigt som nuvarande team ofta upplever hög arbetsbelastning och brist på stöd i säkerhetsfrågor. Cybersäkerhet ses i vissa fall som ett merarbete snarare än en integrerad del av arbetet, särskilt eftersom fokus i många projekt ligger på snabb produktleverans. Därför bör en kontinuerlig och rollanpassad utbildningsinsats införas, med särskilt fokus på säker kodning, testning och sårbarhetshantering. Regelbundna penetrationstester och kodgranskningar bör institutionaliseras som en del av det löpande arbetet, snarare än som punktinsatser.

Vidare rekommenderas också ett tydligare och mer strukturerat "Demand System" för hantering av utvecklingsbehov. Enligt flera respondenter tenderar nuvarande process att skapa en prioriteringsproblematik, där alla förfrågningar betraktas som akuta, vilket urholkar styrningen och försvårar effektiv resursfördelning. Ett förbättrat demandsystem skulle kunna skapa transparens och konsekvens i prioriteringsarbetet, vilket i förlängningen också gynnar säkerhetsrelaterade initiativ som annars riskerar att nedprioriteras.

En särskild utmaning utgörs av förekomsten av så kallad Shadow-IT. Enligt respondenter finns idag över 3000 okontrollerade system som hanteras utanför den formella IT-strukturen. För att hantera detta föreslås ett trestegsprogram: inventering och kategorisering av dessa system, beslut om integration eller avveckling baserat på riskbedömning, samt uppdatering av policyer för att förhindra att nya Shadow-IT-enheter uppstår i framtiden.

Slutligen rekommenderas en gradvis automatisering av säkerhetskontroller i CI/CD-pipelinen. Denna automatisering bör ske i etapper, med inledande fokus på de mest kritiska säkerhetsåtgärderna. En sådan implementering kommer att säkerställa en mer konsekvent och effektiv hantering av säkerhetsaspekter i utvecklingsprocessen.

Genom att systematiskt implementera dessa åtgärder kommer FX att kunna uppnå en högre grad av cybersäkerhet flexibilitet. En sådan utveckling är avgörande för att organisationen ska kunna hantera de alltmer komplexa säkerhetsutmaningarna i en digitaliserad verksamhetsmiljö. Långsiktigt kommer detta även att underlätta arbetet med att upprätthålla efterlevnaden av relevanta säkerhetsstandarder.

## 5.8 Svar på forskningsfrågorna

Det huvudsakliga målet med detta kapitel är att besvara studiens forskningsfrågor. Genom att koppla resultaten till de ursprungliga frågorna blir det möjligt att bedöma i vilken utsträckning syftet har uppnåtts.

Den första forskningsfrågan formulerades enligt följande:

### **RQ1: Vilka organisatoriska hinder är mest kritiska för att upprätthålla ISO 27001-certifiering i en agil DevSecOps-miljö?**

Studien identifierade tre övergripande kategorier av utmaningar:

**Organisatoriska:** Otydlig ansvarsfördelning och frånvaro av formella roller för säkerhetsarbete inom DevOps-team. Detta försvårar samordning och gör att säkerhet hamnar i skymundan.

**Tekniska:** Brist på verktygsintegration för säkerhetskontroller i CI/CD-flöden. Resultatet visar att utan automatiserade kontroller och testning lämnas säkerheten till manuella insatser, vilket är ineffektivt och sårbart.

**Kulturella:** Säkerhet ses som ett hinder snarare än en integrerad del av processen. Det finns en motvilja mot att prioritera säkerhet framför snabb leverans, vilket tyder på en otillräcklig medvetenhet inom organisationen om cybersäkerhetens betydelse. Detta speglar ett mönster utan en kulturell förändring blir tekniska åtgärder otillräckliga.

Den andra forskningsfrågan formulerades enligt följande:

**RQ2: Hur kan ISO 27002:s kontroller för säker utvecklingslivscykel, säker kodning, säkerhetskrav för applikationer och säker systemarkitektur användas för att identifiera och mäta implementeringsgap, samt effektivt integreras i en DevSecOps-modell?**

Analysen visar att kontrollerna i ISO 27002 – särskilt de som rör säker utvecklingslivscykel (8.25), säkerhetskrav för applikationer (8.26), säker systemarkitektur (8.27) och säker kodning (8.28) – är användbara som verktyg för gapanalys i DevSecOps-miljöer. Resultatet från enkäten visade att flera centrala säkerhetskontroller var bristfälligt implementerade: säker kodning var endast fullt implementerad i 43 % av fallen, medan säker systemarkitektur låg på 51 %. Genom att jämföra dessa resultat mot kontrollernas krav i ISO 27002 kunde konkreta brister identifieras, exempelvis avsaknad av kodgranskningsrutiner och svag dokumentation av säkerhetskrav. För att effektivt integrera dessa kontroller i DevSecOps säkerheten måste byggas in tidigt i utvecklingsprocessen ("shift-left") genom automatiserade kontroller och interna playbooks. Den praktiska nyttan blir tydlig i organisationer där utvecklingsteam arbetar parallellt – genom att strukturera kontrollpunkter i kodverktyg och pipelines kan säkerhetsnivån ökas utan att utvecklingstakten påverkas negativt

## 6. DISKUSSION

I detta kapitel diskuteras studiens resultat i relation till det uppställda syftet och forskningsfrågorna. Genom att tolka resultaten i jämförelse med tidigare forskning och det teoretiska ramverket belyses både förväntade och oväntade insikter. Vidare behandlas studiens metodval och hur dessa kan ha påverkat resultaten. Diskussionen omfattar även praktiska, teoretiska och sociala implikationerna av studiens slutsatser. Slutligen föreslås möjliga riktningar för vidare forskning som kan bygga vidare på de identifierade kunskapsluckorna.

### 6.1 Diskussion av resultat

Studien syftar till att identifiera och analysera gap i informationssäkerheten som uppstått i samband med företaget övergång från en traditionell DevOps-baserad utvecklingsmodell till ett mer säkerhetsinriktat DevSecOps-arbetsätt. I fokus har stått implementeringen av specifika kontroller från ISO 27002, med särskild inriktning på intern mjukvaruutveckling. Det huvudsakliga målet har varit att bedöma i vilken utsträckning dessa kontroller är etablerade, samt att belysa organisatoriska hinder som påverkar efterlevnaden av säkerhetskrav, särskilt med hänsyn till företagets ambition att bibehålla sin ISO 27001-certifiering.

Analysen visar att ISO 27002:s kontroller för säker utvecklingslivscykel, säkerhetskrav för applikationer, säker systemarkitektur och säker kodning, erbjuder en tydlig struktur för att kartlägga implementeringsgap i organisationens nuvarande säkerhetsarbete. Genom att kombinera kvantitativ-data från enkätundersökningen med kvalitativa insikter från intervjuer, har ett mönster identifierats där flera grundläggande säkerhetsprinciper – såsom kodgranskning, dokumenterad arkitekturstrategi och säker testmiljö – antingen saknas eller tillämpas inkonsekvent. Av de totalt 118 granskade kontrollerna återfanns bristande eller utebliven implementering i 50 fall, vilket utgör en betydande avvikelse från vad som krävs för att uppfylla ISO 27002-kontroller.

Dessa resultat överensstämmer med tidigare forskning som betonar vikten av ett omfattande tillvägagångssätt vid införandet av DevSecOps (Leite et al., 2020). De bekräftar att ett tekniskt ramverk, såsom ISO 27002, visserligen är en viktig grund för säker utveckling, men inte tillräckligt i sig självt. Säkerhetskontroller måste integreras i hela utvecklingscykeln och kompletteras med organisatorisk styrning och utbildning för att få fullt genomslag. I den studerade organisationen framträder i stället en fragmenterad bild, där utvecklingsteam ofta arbetar isolerat från säkerhetsfunktioner och där standardiserade arbetsätt saknas. Empiriska

data visar också att organisationens nuvarande utbildningssystem, såsom ILearn, främst uppfyller formella krav snarare än effektiv kompetensutveckling. Utbildningarna karakteriseras av en stark administrativ inriktning där dokumentation för myndigheter prioriteras framför faktiska läranderesultat.

Deltagarna upplever utbildningarna som pedagogiskt bristfälliga och meningslösa, då de inte leder till mätbar kunskapsförmedling. En tydlig avsaknad av systematisk uppföljning för att verifiera individuell inläring eller färdighetsutveckling observeras. I stället för att mäta verklig kompetens, fokuserar utvärderingen enbart på kvantitativa deltagandestatistik. Denna compliance-centrerade modell skapar en riskabel diskrepans mellan formella certifieringar och faktisk cybersäkerhetsmedvetenhet bland personalen. Detta indikerar ett behov av omstrukturering mot mer praktiskt orienterade utbildningsformer med integrerade kunskapsmätningar.

Resultaten visar att otydliga ansvarsområden, brist på formella rutiner och otillräcklig cybersäkerhetskompetens inom vissa team är organisatoriska hinder och centrala utmaningar. Detta bekräftas av flera respondenter som uttrycker osäkerhet kring vem som äger säkerhetsfrågorna, särskilt i en molnbaserad och distribuerad utvecklingsmiljö. Denna bild stämmer överens med Calder och Watkins (2024), som framhåller att ansvarsfördelning och intern styrning är avgörande för att ett ledningssystem enligt ISO 27001 ska vara hållbart och uppfylla krav för certifiering över tid.

Vidare visar resultaten att det råder skillnader i tolkning och tillämpning av säkerhetskrav beroende på teamens funktion och organisatoriska placering. En tydlig observation från studien är att säkerhetsarbetet inom organisationen i stor utsträckning verkar påverkas av yttre krav snarare än av en intern, konsekvent riskmedvetenhet. System som omfattas av extern granskning – exempelvis sådana som regleras av myndigheter eller kundkrav – uppvisar generellt sett en högre grad av efterlevnad. Däremot saknar många andra system, särskilt de med låg extern synlighet, formella säkerhetsrutiner och dokumenterade processer. Detta tyder på att säkerhetsnivån ofta avgörs av graden av granskning snarare än av systemets faktiska riskprofil.

Enligt Young et al. (2023) är sådana skillnader i tolkning och tillämpning av säkerhetskrav ett välkänt fenomen i större organisationer, där resurser ofta koncentreras till system som är föremål för extern kontroll, medan övriga system riskerar att hamna i skymundan.

Denna problematik förstärks av att endast 29 av totalt cirka 600 system – motsvarande 4,8 % – uppfyller kraven för att klassificeras som validerade. Det innebär att endast en liten andel av systemen inte bara tillämpar säkerhetsåtgärder, utan också har genomgått en formell och spårbar verifieringsprocess enligt fastställda kriterier. Diskrepansen mellan system som betraktas som "säkra" i vardaglig mening, och de som faktiskt är verifierat säkra enligt etablerade standarder, synliggör ett betydande gap i organisationens säkerhetsmognad. Detta understryker vikten av en enhetlig säkerhetsstrategi, där fokus ligger på intern riskhantering och systemets betydelse, i stället för att främst följa externa granskningsnivåer.

Organisatoriska kulturen är en viktig aspekt som framkommit i resultaten. Flera respondenter beskriver en belöningsmodell där snabb leverans värderas högre än korrekthet och dokumentation, vilket riskerar att skapa brister i säkerhetsarbetets legitimitet. Detta pekar på ett underliggande kulturellt problem där säkerhetsåtgärder inte integreras som en naturlig del av det dagliga utvecklingsarbetet. Det visar också att en lyckad DevSecOps-transformation kräver mer än teknik – det kräver ledarskap, kommunikation och en medveten satsning på ansvarskultur.

Resultaten bekräftar att de valda teoretiska ramverken ISO 27002 varit ändamålsenliga för studien. De har möjliggjort en systematisk identifiering av säkerhetsbrister och bidragit till förståelsen av de organisatoriska och kulturella utmaningar som påverkar implementationen. Dock har vissa komplexiteten, särskilt rörande kompetensutveckling, kulturell förändring och molnteknikens påverkan, visat sig ligga delvis utanför standardernas omedelbara räckvidd. Detta indikerar att framtida forskning bör inkludera komplementära modeller för organisatoriskt lärande och förändringsledning i samband med DevSecOps-transformationer.

## **6.2 Diskussion av metod**

Metoden som vald i studien möjliggjorde en triangulering av data, där enkätresultat kunde kompletteras och fördjupas genom intervjupersonernas perspektiv. Kombinationen av de har därmed bidragit till att ge både bredd och djup i resultatet, vilket är en styrka i fallstudier av detta slag (Bryman et al. 2025).

En styrka med den använda metoden var möjligheten till datatriangulering: enkäten gav kvantitativ information om hur respondenter upplever implementeringsgraden av olika

säkerhetskontroller, medan intervjuerna möjliggjorde fördjupade reflektioner kring orsakerna bakom dessa uppfattningar. Denna flerdimensionalitet anses enligt Justesen och Mik-Meyer (2011) vara en grundläggande förutsättning för att förstå sociala och organisatoriska fenomen i praktiken.

Samtidigt finns det vissa metodologiska begränsningar i studien som bör beaktas vid tolkningen av resultaten. Enkätundersökningen baseras i hög grad på respondenternas subjektiva bedömningar, vilket innebär att validiteten påverkas av deras individuella kunskapsnivå och tolkning av säkerhetsrelaterade begrepp. Utan kompletterande datakällor, såsom tekniska revisioner eller systemloggar, är det svårt att fastställa i vilken utsträckning uppgifterna speglar den faktiska efterlevnaden av säkerhetskrav.

Därtill har den organisatoriska och tekniska komplexiteten utgjort en utmaning. Med hundratals olika system i drift inom verksamheten, har det varit svårt att genomföra en heltäckande analys som inkluderar samtliga relevanta perspektiv. Detta gäller särskilt i en miljö där systemen förvaltas av olika team med varierande ansvar och mognadsgrad i säkerhetsarbetet. Denna fragmentering bidrar till att vissa resultat bör tolkas med viss försiktighet, särskilt när det gäller generalisering av mönster inom hela organisationen.

Även intervjudelen har sina svagheter. Urvalet av intervjupersoner var strategiskt men något begränsat till lednings, arkitektnivå och applikationsutvecklare vilket kan ha påverkat variationen i perspektiv. Röster från mer operativa roller, exempelvis systemutvecklare och testare, kunde ha tillfört värdefulla insikter om hur säkerhetsarbetet faktiskt genomförs i det dagliga arbetet. Justesen och Mik-Meyer (2011) betonar vikten av att lyssna till flera olika aktörers erfarenheter för att undvika en alltför ensidig bild av organisationens verklighet.

Valet av metod har också påverkat tolkningen av resultaten. Eftersom både enkät och intervjuer bygger på subjektiva utsagor snarare än teknisk verifiering, bör resultaten betraktas som indikationer på organisatoriska mönster och utmaningar snarare än absoluta mått på säkerhetsnivå. Som Jacobsen, Andersson och Holmberg (2024) påpekar, är detta en vanlig begränsning i samhällsvetenskaplig metodik, men samtidigt också ett värdefullt bidrag till förståelsen av organisatorisk praktik.

En ytterligare begränsning var den tidsmässiga ramar, där samtliga intervjuer genomfördes under en och samma vecka, vilket innebar att det inte fanns tillräckligt med tid för reflektion

och löpande förbättring av intervjuguiden mellan tillfällena. Med ett längre tidsspann hade analys och justering kunnat ske successivt, vilket sannolikt hade lett till mer nyanserade samtal och ett rikare datamaterial. Denna aspekt bör beaktas vid framtida liknande studier där kvalitativ datainsamling är central.

## **6.3 Implikationer**

Resultaten från denna studie har betydelse både för praktisk tillämpning i organisationer och för vidare forskning inom området informationssäkerhet och DevSecOps. I detta avsnitt diskuteras hur studiens slutsatser kan användas konkret, samt vilka bidrag den ger till teoretisk förståelse.

### **6.3.1 Praktiska implikationer**

Denna studie kan användas som ett verktyg för organisationer som befinner sig i en övergång från traditionell systemutveckling till DevSecOps och som samtidigt strävar efter att behålla ISO 27001 certifikat och uppfylla ISO 27002-kontroller. Genom att fokusera på hur specifika säkerhetskontroller är implementerade – eller inte implementerade – ger studien en strukturerad grund för att genomföra en intern gapanalys. Organisationer som vill identifiera svaga punkter i sin säkerhetsstruktur får genom studiens metod och resultat en praktisk vägledning för att analysera sitt nuläge i relation till internationella standarder.

Studien visar också att det inte räcker med att införa tekniska kontroller – det krävs även tydliga ansvarsfördelningar, fungerande kommunikationsvägar och utbildningsinsatser. Resultatet pekar på att säkerhetsarbetet i många fall hämmas av otydlighet kring roller och brist på samsyn mellan olika team. Detta är direkt tillämpbart för verksamheter som vill förbättra sin interna styrning inom cybersäkerhet. Ett konkret steg för företag är att skapa en organisationstäckande “agile playbook” som innehåller både tekniska riktlinjer och ansvarsmässiga ramar, anpassade för olika utvecklingsteam.

Vidare belyser studien behovet av kontinuerlig kompetensutveckling. Många medarbetare förväntas agera utifrån säkerhetskrav utan att ha tillgång till tillräckliga stödresurser. Organisationer kan använda dessa insikter för att strukturera utbildningsprogram och stödmaterial, särskilt riktade till utvecklare, produktägare och arkitekter, roller som är centrala

för att säker utvecklingslivscykel, säker kodning, säker systemarkitektur och säkerhetskrav för applikationer i praktiken

### **6.3.2 Teoretiska implikationer**

På teoretisk nivå visar denna studie hur ISO 27002 kan användas mer operativt i en DevSecOps-kontext. Tidigare forskning har visat att standarder ofta är abstrakta och svåra att omsätta i agila miljöer (Leite et al., 2020). Studien bidrar med ett konkret exempel på hur kontroller kan brytas ned och bedömas i praktiken, vilket stärker förståelsen för hur standardbaserade säkerhetsramverk kan tillämpas i moderna, snabbväxande utvecklingsmiljöer.

Samtidigt visar studien att organisatoriska faktorer – såsom kultur, ansvarskultur och belöningsystem – har stor påverkan på om säkerhetsåtgärder får genomslag. Studien lägger därmed grunden för vidare forskning om hur säkerhet kan integreras i agila arbetsformer på ett sätt som inte bara följer standarder, utan också fungerar i praktiken.

Utöver detta belyser studien hur internationellt verksamma företag, med distribuerade team och växande utvecklingsverksamhet, kan använda ISO 27002 som ett verktyg för att behålla en sammanhållen säkerhetsnivå i takt med att organisationen växer. Den modell som studien presenterar visar att en tydligt strukturerad gapanalys kan hjälpa globala företag att identifiera var säkerhetsansvar riskerar att falla mellan olika team, länder eller partners. Detta är särskilt relevant i skalbara miljöer där systemkomplexitet ökar snabbt, och där en gemensam referensram är nödvändig för att upprätthålla certifieringskrav och säkerhetsstandarder över tid och geografiska gränser.

Studien belyser även ett forskningsbehov inom företag som har en kombination av interna och externa IT-resurser där delar av IT-infrastrukturen, systemdriften eller säkerhetsansvaret hanteras av tredjepartsleverantörer, medan andra delar fortfarande styrs och ägs internt av organisationen. När delar av säkerhetsansvaret ligger hos externa leverantörer, samtidigt som organisationen behåller ansvaret för applikation och dataskydd, uppstår komplexa styrningsutmaningar. Detta är ett område där ISO-standarderna erbjuder begränsad vägledning, och där framtida studier kan bidra med nya teoretiska modeller för ansvarsfördelning och intern uppföljning.

## 6.4 Slutsats

Efter genomförd analys, diskussion och reflektion av de empiriska resultaten är det nu möjligt att dra en sammanfattande slutsats av denna studie. Syftet har varit att undersöka vilka gap som finns i implementeringen av ISO 27002:s säkerhetskontroller inom ett globalt företag som övergår från en DevOps-baserad utvecklingsmodell till ett mer säkerhetsinriktat DevSecOps-arbets sätt. Fokus har legat på att identifiera brister i säker utvecklingslivscykel, säkerhetskrav för applikationer, säker kodning och säker systemarkitektur, samt att belysa organisatoriska hinder som kan påverka förmågan att uppnå och behålla ISO 27001-certifiering i en agil utvecklingsmiljö.

I studien svarar forskarna på RQ1: Vilka organisatoriska hinder är mest kritiska för att upprätthålla ISO 27001-certifiering i en agil DevSecOps-miljö?

Resultaten visar att de mest kritiska organisatoriska hindren för att upprätthålla ISO 27001-certifiering i en agil DevSecOps-miljö är otydlig ansvarsfördelning och brist på en gemensam säkerhetskultur. Det visar också att trots tekniska ramverk som ISO 27001 och ISO 27002, är organisatoriska faktorer avgörande för ett sammanhållet säkerhetsarbete. Varierande kompetensnivåer och frånvaro av gemensamma arbetssätt försvårar säkerhetsintegrering i utvecklingscykeln. Detta understryker behovet av tydlig styrning, kontinuerlig kompetensutveckling samt tillgång till rätt resurser och stöd från ledningsnivå till utvecklingsteam

Studien svarar också på frågan RQ2: Hur kan ISO 27002:s kontroller för säker utvecklingslivscykel, säker kodning, säkerhetskrav för applikationer och säker systemarkitektur användas för att identifiera och mäta implementeringsgap, samt effektivt integreras i en DevSecOps-modell?

Där resultaten visar att ISO 27002:s kontroller för säker utvecklingslivscykel, säker kodning, säkerhetskrav för applikationer och säker systemarkitektur är praktiskt tillämpbara för att genomföra gapanalys i komplexa utvecklingsorganisationer. Studien visar att flera kritiska kontroller inom områden såsom kodgranskning, säkerhetsarkitektur, outsourcing och dokumentation av applikationssäkerhet inte är fullt implementerade. Genom att använda ISO 27002 som referensram kan dessa brister identifieras och mätas på ett strukturerat sätt. En effektiv integration i en DevSecOps-modell förutsätter dock att kontrollerna anpassas till agila arbetsformer och att de kontinuerligt följs upp inom ramen för en gemensam styrningsstruktur

Slutligen bidrar denna studie med en praktiskt användbar metod för att genomföra en säkerhetsbaserad gapanalys, men också med teoretiska insikter om samspelet mellan standarder, utvecklingsmodeller och organisation. Resultaten kan fungera som vägledning för andra företag som står inför liknande utmaningar, och som strävar efter att balansera snabb utveckling med hög informationssäkerhet i en global och skalbar miljö.

## **6.5 Förslag på vidare forskning**

Utifrån de resultat som framkommit i denna studie, finns flera områden som bör utforskas vidare i kommande forskning. Ett tydligt behov är att undersöka hur säkerhetskontroller enligt ISO 27002 kan operationaliseras i andra typer av organisationer och branscher än det fall som studerats här. Eftersom denna studie genomfördes inom ramen för ett specifikt företag med egen mjukvaruutveckling, vore det värdefullt att jämföra hur kontrollerna tillämpas i exempelvis offentlig sektor, SaaS-bolag eller organisationer med en mer distribuerad eller molnbaserad IT-infrastruktur.

Framtida forskning kan vara att undersöka hur organisationer kan utforma effektiva modeller för prioritering och resurstilldelning i komplexa utvecklingsmiljöer. I miljöer där flera intressenter konkurrerar om samma resurser, och där beställningar ofta klassificeras som högprioriterade oavsett faktisk kritikalitet, riskerar styrningen att förlora sin effektivitet. Det finns därmed ett behov av att utveckla och utvärdera strukturerade "demand management"-system som kan skapa tydliga kriterier för prioritering, samt bidra till en mer balanserad och förutsägbar resursplanering i teknikintensiva och agila organisationer.

Studien visar att fler respondenter efterfrågade anställning av yngre medarbetare med vilja att lära sig och växa inom organisationen. Dock upplever många en hög arbetsbelastning och att cybersäkerhet ses som en extra börda, särskilt eftersom kunderna främst fokuserar på produktleveranser snarare än säkerhetskrav. Därför framtida forskning bör även belysa hur kompetensförsörjning och arbetskultur påverkar organisationers förmåga att integrera cybersäkerhet i utvecklingsarbetet. I synnerhet finns behov av att undersöka hur rekrytering av nya medarbetare – särskilt yngre medarbetare med vilja att utvecklas – kan bidra till att stärka säkerhetskompetensen över tid. Samtidigt behöver studier granska hur hög arbetsbelastning och kundfokus på leveranstider påverkar uppfattningen om cybersäkerhet som en prioritet. Det är

angeläget att förstå hur organisatoriska incitament, kompetensutveckling och resursfördelning samverkar i skapandet av en långsiktigt hållbar säkerhetskultur.

Framtida forskning bör riktas mot att utveckla styrningsmodeller för hybrid IT-drift, där säkerhetsansvaret är uppdelat mellan interna team och externa leverantörer. I sådana miljöer uppstår ofta osäkerhet kring vilka roller som bär ansvar för olika delar av systemen, vilket kan leda till brister i kontroll och efterlevnad – särskilt i verksamheter som verkar under regulatoriska krav, exempelvis inom finans, hälsosektor eller tillverkningsindustri. Det finns ett behov av att närmare studera hur ansvar kan fördelas på ett transparent och spårbart sätt, inklusive vilken kompetens som krävs för olika roller, hur utbildningsbehov identifieras och hur kvaliteten i säkerhetsutbildningar kan följas upp över tid. En sådan forskningsinriktning skulle kunna bidra till en mer robust och hållbar styrning av cybersäkerhet i komplexa och distribuerade organisationer.

Studien identifierade behovet av ett starkare stöd för styrning i miljö som har en kombination av interna och externa IT-resurser, där organisationer förlitar sig på externa parter för delar av säkerhetsarbetet. Framtida forskning bör riktas mot att utveckla styrningsmodeller för hybrid IT-drift, där säkerhetsansvaret är uppdelat mellan interna team och externa leverantörer. I sådana miljöer uppstår ofta osäkerhet kring vilka roller som bär ansvar för olika delar av systemen, vilket kan leda till brister i kontroll och efterlevnad – särskilt i verksamheter som verkar under regulatoriska krav, exempelvis inom finans, hälsosektor eller tillverkningsindustri. Det finns ett behov av att närmare studera hur ansvar kan fördelas på ett transparent och spårbart sätt, inklusive vilken kompetens som krävs för olika roller, hur utbildningsbehov identifieras och hur kvaliteten i säkerhetsutbildningar kan följas upp över tid. En sådan forskningsinriktning skulle kunna bidra till en mer robust och hållbar styrning av cybersäkerhet i komplexa och distribuerade organisationer.

Dessutom framkom det i studien att organisatorisk kultur har stor betydelse för hur säkerhetskrav tolkas och efterlevs. Det finns därmed skäl att undersöka mer systematiskt hur belöningsystem, teamstruktur och ledarskap påverkar implementeringen av cybersäkerhet i agila utvecklingsmiljöer. En sådan studie skulle kunna bidra med värdefulla insikter om vilka incitament och styrformer som främjar säkerhetsmedvetande utan att motverka agilitet.

## 7. REFERENSER

- Bryman, A., Nilsson, B., Clark, T., Foster, L., & Sloan, L. (2025). *Brymans samhällsvetenskapliga metoder* (4 uppl). Liber.
- Calder, A. & Watkins, S. (2024). *IT Governance – An International Guide to Data Security and ISO 27001/ISO 27002* (8 uppl). IT Governance Publishing.
- Carter, K. (2017). Francois Raynaud on DevSecOps. *IEEE Software*, 34(5), 93–96. <https://doi.org/10.1109/MS.2017.3571578>
- Collin, B. (2003). *IT-kvalitet : verksamhets- & effektivitetsutveckling*. Studentlitteratur.
- De Cremer, P., Desmet, N., Madou, M., & De Sutter, B. (2020). Sensei: Enforcing secure coding guidelines in the integrated development environment. *Software, Practice & Experience*, 50(9), 1682–1718. <https://doi.org/10.1002/spe.2844>
- Dobaj, J., Macher, G., Ekert, D., Riel, A., & Messnarz, R. (2023). Towards a security-driven automotive development lifecycle. *Journal of Software: Evolution and Process*, 35(8). <https://doi.org/10.1002/smr.2407>
- Ejlertsson, G., & Axelsson, J. (2014). *Enkäten i praktiken: en handbok i enkätmetodik* (3 uppl). Studentlitteratur.
- Lombardi, F., & Fanton, A. (2023). From DevOps to DevSecOps is not enough. CyberDevOps: an extreme shifting-left architecture to bring cybersecurity within software security lifecycle pipeline. *Software Quality Journal*, 31(2), 619–654. <https://doi.org/10.1007/s11219-023-09619-3>
- Fenz, S. & Neubauer, T. (2018). Ontology-based information security compliance determination and control selection on the example of ISO 27002. *Information and Computer Security*, 26(5), 551–567. <https://doi.org/10.1108/ICS-02-2018-0020>

- Guggenmos, F., Häckel, B., Ollig, P. & Stahl, B. (2022). Security first, security by design, or security pragmatism – Strategic roles of IT security in digitalization projects. *Computers & Security*, 114, 102747. <https://doi.org/10.1016/j.cose.2022.102747>
- Gerber, M. & von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security*, 27(5–6), 124–135. <https://doi.org/10.1016/j.cose.2008.07.009>
- Gustavsson, T. (2020). *Agil projektledning* (4 uppl). Sanoma utbildning.
- Görling, S. (2009). *Att arbeta med IT-projekt* (1 uppl). Studentlitteratur.
- Harris, M. L., McDowell, W. C., & Gibson, S. G. (2011). Strategic relationships in a small business context: The impact of information quality and continuous quality improvement. *New England Journal of Entrepreneurship*, 14(2), 19–27. <https://doi.org/10.1108/NEJE-14-02-2011-B002>
- Hussain, K., Abdullah, A. B., Humayun, M., Tavares, J. M. R. S., & Jhanjhi, N. Z. (2022). *Information Security Handbook*. (1 uppl) <https://doi.org/10.1201/9780367808228>
- Jacobsen, D. I., Andersson, S., & Holmberg, J. (2024). *Hur genomför man undersökningar? : introduktion till samhällsvetenskapliga metoder* (3 uppl). Studentlitteratur.
- Justesen, L., Mik-Meyer, N., & Andersson, S. (2011). *Kvalitativa metoder : från vetenskapsteori till praktik* (1 uppl). Studentlitteratur.
- Kamil, Y., Lund, S., & Islam, M. S. (2023). Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden. *Information Systems and E-Business Management*, 21(3), 699–722. <https://doi.org/10.1007/s10257-023-00646-y>
- Khan, R. A., Khan, S. U., Alzahrani, M., & Ilyas, M. (2022). Security Assurance Model of Software Development for Global Software Development Vendors. *IEEE Access*, 10, 58458–58487. <https://doi.org/10.1109/ACCESS.2022.3178301>

- Leite, L., Rocha, C., Kon, F., Milojcic, D., & Meirelles, P. (2020). A Survey of DevOps Concepts and Challenges. *ACM Computing Surveys*, 52(6), 1–35. <https://doi.org/10.1145/3359981>
- Prates, L., & Pereira, R. (2025). DevSecOps practices and tools. *International Journal of Information Security*, 24(1), 11. <https://doi.org/10.1007/s10207-024-00914-z>
- Rajapakse, R. N., Zahedi, M., Babar, M. A., & Shen, H. (2022). Challenges and solutions when adopting DevSecOps: A systematic review. *Information and Software Technology*, 141, 106700. <https://doi.org/10.1016/j.infsof.2021.106700>
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors (Basel, Switzerland)*, 23(15), 6666-. <https://doi.org/10.3390/s23156666>
- Sharma, P., Moparthi, N. R., Namasudra, S., Shanmuganathan, V., & Hsu, C. (2022). Blockchain-based IoT architecture to secure healthcare system using identity-based encryption. *Expert Systems*, 39(10). <https://doi.org/10.1111/exsy.12915>  
<https://onlinelibrary-wiley-com.lib.costello.pub.hb.se/doi/full/10.1111/exsy.12915>
- Suorsa, M., & Helo, P. (2024). Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis. *Information Security Journal*, 33(3), 285–306. <https://doi.org/10.1080/19393555.2023.2270984>
- Tonnquist, B. (2024). *Projektledning* (9 uppl). Sanoma utbildning.
- Wu, W., Shi, K., Wu, C.-H. & Liu, J. (2022). Research on the impact of information security certification and concealment on financial performance: Impact of ISO 27001 and concealment on performance. *Journal of Global Information Management (JGIM)*, 30(3), 1–16. <https://doi.org/10.4018/JGIM.20220701.oa2>

Young, S., Simos, M., Rodriguez, G., & Diogenes, Y. (2023). Specify security requirements for applications. I Exam Ref SC-100 Microsoft Cybersecurity Architect. Pearson Education,Limited.

## 8. BILAGOR

### 8.1 Bilaga 1 Enkätsvaren bara fullt implementerade kontroller för respektive kapitel i ISO 27002

Tabell 4 Implementerad kontroller för säker utvecklingscykel i FX

Kontroll	Fullt implementerad
Separera utvecklings-, test- och produktionsmiljöer på ett tillfredsställande sätt för att säkerställa informationssäkerhet, förhindra obehörig åtkomst och skydda känslig information i utvecklings- och testmiljöer	IT Director IT Application Owner Process Application Specialist
Säkerhetskrav ska uttryckligen definieras och integreras under specifikations- och designfaserna i projekt	IT Application Owner Process Application Specialist
Definiera säkerhets kontrollpunkter i projekt för att säkerställa att säkerhetsåtgärder implementeras och granskas	IT Director
Säkra kataloger ska användas för att lagra och hantera källkod och konfigurationsfiler	Senior Manager, Advanced Analytics IT Application Owner
Konfigurera och hantera versionshanteringsystem för att säkerställa säkerheten och integriteten i kodändringar	Senior Manager, Advanced Analytics IT Application Owner
Licenskrav och alternativ ska utvärderas för att säkerställa kostnadseffektiva lösningar och undvika framtida licensproblem	Solution Delivery Lead – ORS & eCommerce IT Director

Tabell 5 implementerad krav för systemarkitektur och tekniska principer i FX

Kontroll	Fullt implementerad
Definiera specifika säkerhetsåtgärder som krävs för vissa verksamhetsprocesser (t.ex. kryptering av känslig information, kontroll av integritet och information vid digital signering)	Solution Delivery Lead – ORS & eCommerce
Tekniska principer för att säkra system bör integrering med organisations säkerhetsarkitektur	Solution Delivery Lead – ORS & eCommerce

Etablera teknisk säkerhetsinfrastruktur (t.ex. infrastruktur för kryptering med öppen nyckel [PKI], identitets och åtkomsthantering [IAM], förhindrande av dataläckage och dynamisk behörighetshantering),	Solution Delivery Lead – ORS & eCommerce
Organisationen säkerställer att förfrågningar till informationssystem krypteras från ändpunkt till ändpunkt	Solution Delivery Lead – ORS & eCommerce
Verifiera varje förfrågan till ett informationssystem, som om den hade kommit från ett öppet, externt nätverk, även om dessa förfrågningar kommer inifrån organisationen (dvs. inte per automatik lita på något innanför eller utanför organisationens perimeter).	Solution Delivery Lead – ORS & eCommerce  SAP Enterprise Architect
Använda metoder som bygger på principen om minsta möjliga behörighet samt dynamisk åtkomstkontroll. Detta omfattar att autentisera och godkänna informations eller systemförfrågningar baserat på kontextuell information, såsom autentiseringsinformation, användaridentiteter, uppgift om användarklient samt informationsklassning,	Solution Delivery Lead – ORS & eCommerce
Alltid autentisera den som kommer med en förfrågan och alltid validera förfrågningar till informationssystem på basis av information, inklusive autentiseringsinformation, användaridentiteter, data om användarklient samt informationsklassning, till exempel använd stark autentisering (t.ex. flerkontorsautentisering)	Solution Delivery Lead – ORS & eCommerce IT Director SAP Enterprise Architect

Tabell 6 implementerad krav för Säkerhetskrav för applikationer i FX

Kontroll	Fullt implementerad
Identifiera, specificera Säkerhetskrav för applikationer vid utveckling eller förvärv.	<ul style="list-style-type: none"> <li>IT Application Owner</li> <li>Process Application Specialist</li> </ul>
Fastställ säkerhetskrav för applikationer genom en riskbedömning med hjälp av specialister på informationssäkerhet	<ul style="list-style-type: none"> <li>IT Application Owner</li> <li>Process Application Specialist</li> </ul>
Utföra riskbedömning för applikationer som är tillgängliga via nätverk utsätts för ett antal nätverksrelaterade hot (t.ex. bedrägerier, avtalstvister eller röjande av information till allmänheten,	<ul style="list-style-type: none"> <li>IT Application Owner</li> <li>Process Application Specialist</li> </ul>

ofullständig överföring, felaktigstyrning av nätverkstrafik och obehörig ändring, duplicering eller återuppspelning av meddelanden).	
Detaljerade riskbedömningar och noggrant val av säkerhetsåtgärder som ofta krävs krypteringsmetoder för autentisering och säker överföring av data	<ul style="list-style-type: none"> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Tillitsnivå för entiteternas identitet (t.ex. genom autentisering)	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> <li>• IT Director</li> <li>• Senior Manager, Advanced Analytics</li> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Identifiering av vilken typ av information och klassningsnivå som applikationen ska behandla	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> <li>• IT Director</li> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Behov av att separera åtkomst och åtkomstnivå för data och funktioner i applikationen,	<ul style="list-style-type: none"> <li>• IT Director</li> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Författningskrav i den jurisdiktion där transaktionen skapas, behandlas, slutförs eller lagras	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Behov av skydd av personuppgifter för samtliga berörda parter,	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Krav på skydd av eventuell konfidentiell information	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> <li>• IT Application Owner</li> </ul>
Skydd av data under behandling, överföring och i vila	<ul style="list-style-type: none"> <li>• IT Director</li> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Behov av säker kryptering av kommunikationen mellan alla berörda parter	<ul style="list-style-type: none"> <li>• IT Director</li> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Automatiska säkerhetsåtgärder (t.ex. godkännandebegränsningar eller användning av tvåhandsprincip för godkännande),	<ul style="list-style-type: none"> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>

Säkerhetsåtgärder för utdata, med beaktande av vem som kan få åtkomst till utdata och godkännandeprocess för utdata	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Begränsningar av innehållet i fritextfält, eftersom dessa kan leda till okontrollerad lagring av konfidentiella uppgifter (t.ex. personuppgifter),	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> </ul>
Krav som härrör från verksamhetsprocess, såsom transaktionsloggning, övervakning och krav på oavvislighet,	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Felmeddelanden hantering	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> </ul>
Överväga vilken tillitsnivå parterna kräver för att lita på den andra partens angivna identitet	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> <li>• IT Director</li> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Överväga vilken tillitsnivå som krävs för integriteten i den information som utbyts eller behandlas samt mekanismer för att identifiera bristande integritet (t.ex. cyklisk redundanskontroll, hashning och digitala signaturer)	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Auktorisation avseende vem som kan godkänna innehåll i, utfärda eller signera viktiga transaktionsdokument	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Konfidentialitet, integritet, avsändarintyg och mottagarbevis för viktiga dokument samt oavvislighet (t.ex. avtal med koppling till upphandling och avtalsprocesser)	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> <li>• IT Application Owner</li> </ul>
Konfidentialitet och integritet för alla transaktioner (t.ex. beställningar, leveransadressuppgifter och kvittenser)	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> <li>• IT Application Owner</li> <li>• Process Application Specialist</li> </ul>
Krav på hur länge en transaktion ska hållas konfidentiell	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> </ul>
Försäkringskrav och andra avtalskrav	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> </ul>
Krav för att upprätthålla orderinformationens konfidentialitet och integritet	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> </ul>

Lämplig nivå för verifiering av betalningsinformation från kund	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> </ul>
Undvikande av förlust eller kopiering av information om transaktioner	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> </ul>
Lagring av transaktionsuppgifter utanför publikt tillgängliga miljöer (t.ex. på en lagringsplattform på organisationens intranät, så att den inte sparas och exponeras på elektroniska lagringsmedier som är direkt åtkomliga via internet)	<ul style="list-style-type: none"> <li>• Senior Manager, Advanced Analytics</li> </ul>
Säkerheten integreras och upprätthålls i hela processen för hantering av certifikat eller signaturer från början till slut då en betrodd utfärdare används (t.ex. för att utfärda och underhålla digitala signaturer eller digitala certifikat).	<ul style="list-style-type: none"> <li>• Solution Delivery Lead – ORS &amp; eCommerce</li> <li>• Senior Manager, Advanced Analytics</li> </ul>

Tabell 8 implementerad krav för Säker kodning i FX

Kontroll	Fullt implementerad
För tolkade språk exekvera kod på en server som inte är tillgänglig för användare och processer som använder den, med datalagrade i en skyddad databas.	Solution Delivery Lead – ORS & eCommerce Senior Manager, Advanced Analytics
Skydda administratörsåtkomst med hjälp av säkerhetsåtgärder, t.ex. principer för just-in-time-tilldelning och stark autentisering.	Solution Delivery Lead – ORS & eCommerce Senior Manager, Advanced Analytics
Konfigurera webbservrar för att förhindra katalogbläddring.	Solution Delivery Lead – ORS & eCommerce IT Director Senior Manager, Advanced Analytics
Utforma applikationskod att utgå från att den alltid är under attack	Solution Delivery Lead – ORS & eCommerce

Konfigurering av utvecklingsverktyg, t.ex. integrerade utvecklingsmiljöer (IDE), för att bidra till att skapa säker kod,	Solution Delivery Lead – ORS & eCommerce
Följa vägledning från leverantörer av utvecklingsverktyg och exekveringsmiljöer, enligt vad som är tillämpligt,	Solution Delivery Lead – ORS & eCommerce
Underhåll och användning av uppdaterade utvecklingsverktyg (t.ex. kompilatorer),	Solution Delivery Lead – ORS & eCommerce
Användning av kontrollerade utvecklingsmiljöer	Solution Delivery Lead – ORS & eCommerce
Användning av strukturerade programmeringsmetoder,	Solution Delivery Lead – ORS & eCommerce Senior Manager, Advanced Analytics
Dokumentation av kod och avlägsnande av programmeringsfel som kan göra det möjligt att utnyttja sårbarheter i informationssäkerheten,	Solution Delivery Lead – ORS & eCommerce Senior Manager, Advanced Analytics
Förbud mot att använda osäkra designlösningar (t.ex. användning av hårdkodade lösenord, ej godkända exempel på kod och ej autentiserade webbtjänster).	Solution Delivery Lead – ORS & eCommerce Senior Manager, Advanced Analytics
Utföra tester under och efter utveckling	Solution Delivery Lead – ORS & eCommerce
Utvärdera attacktyper och principen om minsta möjliga behörighet	Senior Manager, Advanced Analytics
Genomförd analys av de vanligaste programmeringsfelen och dokumentation som visar att dessa har hanterats.	Solution Delivery Lead – ORS & eCommerce
Uppdateringar bör paketeras och driftsättas på ett säkert sätt	Solution Delivery Lead – ORS & eCommerce
Hantera rapporterade sårbarheter i informationssäkerheten	Solution Delivery Lead – ORS & eCommerce
Logga fel och misstänkta attacker och loggarna bör granskas regelbundet för att göra de ändringar i koden som krävs,	Solution Delivery Lead – ORS & eCommerce
Skydda källkod mot obehörig åtkomst och manipulation (t.ex. genom användning av verktyg för konfigurationshantering, som normalt har funktioner som åtkomstkontroll och versionskontroll).	Solution Delivery Lead – ORS & eCommerce Senior Manager, Advanced Analytics
säkerställa att externa bibliotek hanteras (t.ex. genom att föra en förteckning över de bibliotek och biblioteksversioner som används) och regelbundet uppdateras med nya versioner,	Solution Delivery Lead – ORS & eCommerce
Välja, godkänna och återanvända av noggrant granskade komponenter, särskilt autentiserings och krypteringskomponenter	Solution Delivery Lead – ORS & eCommerce
Organisationer överväga externa komponenters licens, säkerhet och historik	Solution Delivery Lead – ORS & eCommerce

Säkerställa att program kan underhållas och spåras samt kommer från beprövade, välrenommerade källor.	Solution Delivery Lead – ORS & eCommerce
Säkerställa att utvecklingsresurser och artefakter har tillräckligt långvarig tillgänglighet.	Solution Delivery Lead – ORS & eCommerce
Möjligheten att få nödvändiga ändringar från leverantören i form av vanliga programuppdateringar	Solution Delivery Lead – ORS & eCommerce
Konsekvenser om organisationen blir ansvarig för framtida programvaruunderhåll till följd av förändringar,	Solution Delivery Lead – ORS & eCommerce
Kompatibilitet med annan programvara som används.	Solution Delivery Lead – ORS & eCommerce

## 8.2 Bilaga 2 Kontroller som bedömts som delvis implementerade eller ej implementerade

Tabell 7 Översikt över implementeringsstatus för säkerhetskrav i olika ansvarsområden inom SDLC i FX.

Kontroll	Delvis implementerad	Ej implementerad	Ej tillämplig
Separera utvecklings-, test- och produktionsmiljöer på ett tillfredsställande sätt för att säkerställa informationssäkerhet, förhindra obehörig åtkomst och skydda känslig information i utvecklings- och testmiljöer	Solution Delivery Lead – (ORS & eCommerce) External Contractor, supporting risk, security and compliance) Senior Manager, Advanced Analytics	Operational and Application Security Specialist)	
Programvaruutvecklingsmetoder ska innehålla vägledning och praxis för att integrera säkerhet genom hela utvecklingslivsrytmen	Solution Delivery Lead – (ORS & eCommerce) IT Application Owner External Contractor, supporting risk, security and compliance)	Global IT Director (Enterprise Architecture) Senior Manager, Advanced Analytics Process Application Specialist	Operational and Application Security Specialist Solution Delivery Lead – (ORS & eCommerce) IT Director
Etablera och följ säkra kodningsriktlinjer för varje programmeringsspråk som används i utvecklingen	Solution Delivery Lead – (ORS & eCommerce) IT Application Owner	Global IT Director (Enterprise Architecture) Process Application Specialist	Operational and Application Security Specialist IT Director Senior Manager, Advanced Analytics
Säkerhetskrav ska uttryckligen definieras och integreras under specifikations- och designfaserna i projekt	Solution Delivery Lead – (ORS & eCommerce) Operational and Application Security Specialist) Global IT Director (Enterprise Architecture) External Contractor, supporting risk, security and compliance)		IT Director Senior Manager, Advanced Analytics
Definiera säkerhetskontrollpunkter i projekt för att säkerställa att säkerhetsåtgärder implementeras och granskas	IT Application Owner Global IT Director (Enterprise Architecture)	Operational and Application Security Specialist) Process Application Specialist	Solution Delivery Lead – (ORS & eCommerce) Senior Manager, Advanced Analytics
Utvecklingsprocessen inkluderar system och säkerhetstestning, såsom	Solution Delivery Lead – (ORS & eCommerce)		IT Director Operational and Application Security Specialist

regressionstestning, kodskanning och penetrationstestning.	Global IT Director Enterprise Architecture IT Application Owner Process Application Specialist		Senior Manager, Advanced Analytics
Säkra kataloger ska användas för att lagra och hantera källkod och konfigurationsfiler	Global IT Director Enterprise Architecture Solution Delivery Lead – ORS & eCommerce	Process Application Specialist	IT Director Operational and Application Security Specialist
Konfigurera och hantera versionshanteringssystem för att säkerställa säkerheten och integriteten i kodändringar	Solution Delivery Lead – ORS & eCommerce External Contractor, supporting risk, security and compliance  Global IT Director Enterprise Architecture Process Application Specialist		IT Director Operational and Application Security Specialist
Utvecklare bör få regelbunden utbildning och ha den kunskap som krävs för att tillämpa bästa praxis för applikationssäkerhet	External Contractor, supporting risk, security and compliance Senior Manager, Advanced Analytics IT Application Owner	Solution Delivery Lead – ORS & eCommerce Process Application Specialist Process Application Specialist	IT Director Operational and Application Security Specialist
Utvecklare bör ha förmåga och verktyg för att förhindra, hitta och korrigera sårbarheter	Operational and Application Security Specialist Solution Delivery Lead – ORS & eCommerce IT Application Owner Process Application Specialist	IT Director	Senior Manager, Advanced Analytics
Licenskrav och alternativ ska utvärderas för att säkerställa kostnadseffektiva lösningar och undvika framtida licensproblem	Global IT Director Enterprise Architecture IT Application Owner	Process Application Specialist	Operational and Application Security Specialist
Organisationen bör försäkra sig om att leverantören uppfyller organisationens regler för säker utveckling, om utvecklingsarbetet utkontrakteras	Solution Delivery Lead – ORS & eCommerce IT Application Owner Process Application Specialist	Global IT Director Enterprise Architecture Operational and Application Security Specialist	IT Director Senior Manager, Advanced Analytics

Tabell 7 Översikt över implementeringsstatus för säkerhetskrav i olika ansvarsområden inom systemarkitektur och tekniska principer i FX.

<b>Kontroll</b>	<b>Delvis implementerad</b>	<b>Ej implementerad</b>	<b>Ej tillämplig</b>
Tekniska principer för att säkra system bör fastställas för, dokumenteras vid och tillämpas på utveckling av informationssystem.	Solution Delivery Lead – ORS & eCommerce Operational and Application Security Specialist SAP Enterprise Architect	IT Director Global IT Director Enterprise Architecture	
Tekniska principer för att säkra system bör beaktas alla delar av utformningsarbetet (verksamhet, data, applikationer och teknik).	Solution Delivery Lead – ORS & eCommerce IT Director Operational and Application Security Specialist SAP Enterprise Architect	Global IT Director Enterprise Architecture	
Ny teknologi bör analyseras med avseende på säkerhetsrisker och designen bör granskas utifrån kända attackmetoder.	Solution Delivery Lead – ORS & eCommerce IT Director Operational and Application Security Specialist Global IT Director Enterprise Architecture SAP Enterprise Architect		
Analys samtliga säkerhetsåtgärder som krävs för att skydda information och system mot identifierade hot	IT Director Operational and Application Security Specialist SAP Enterprise Architect	Global IT Director Enterprise Architecture	
Utvärdera säkerhetsåtgärdernas förmåga att förhindra, upptäcka eller hantera säkerhetsincidenter	Solution Delivery Lead – ORS & eCommerce IT Director Operational and Application Security Specialist SAP Enterprise Architect		
Definiera specifika säkerhetsåtgärder som krävs för vissa verksamhetsprocesser (t.ex. kryptering av känslig information, kontroll av integritet och information vid digital signering),	Operational and Application Security Specialist		IT Director

Definiera var och hur säkerhetsåtgärder ska tillämpas (t.ex. genom integrering med säkerhetsarkitektur och teknisk infrastruktur),	Solution Delivery Lead – ORS & eCommerce IT Director SAP Enterprise Architect	Operational and Application Security Specialist	
Säkerställa att enskilda säkerhetsåtgärder (manuella och automatiska) samverkar för att generera en integrerad uppsättning säkerhetsåtgärder.	Solution Delivery Lead – ORS & eCommerce IT Director	Operational and Application Security Specialist	
Tekniska principer för att säkra system bör tillämpas, där så behövs, på utkontrakterad utveckling av informationssystem med hjälp av avtal och andra bindande överenskommelser mellan organisationen och den leverantör till vilken utkontrakteringen sker.	Solution Delivery Lead – ORS & eCommerce SAP Enterprise Architect	Operational and Application Security Specialist	IT Director
Organisationen bör säkerställa att leverantörernas metoder för säker utveckling är anpassade till organisationens behov.	Solution Delivery Lead – ORS & eCommerce IT Director SAP Enterprise Architect	Operational and Application Security Specialist	
Tekniska principer för att säkra system bör integrering med organisations säkerhetsarkitektur	IT Director SAP Enterprise Architect	Operational and Application Security Specialist Global IT Director Enterprise Architecture	
Etablera teknisk säkerhetsinfrastruktur (t.ex. infrastruktur för kryptering med öppen nyckel [PKI], identitets och åtkomsthantering [IAM], förhindrande av dataläckage och dynamisk behörighetshantering),	IT Director Operational and Application Security Specialist		
Tekniska principer för att säkra system bör beakta organisationens förmåga att utveckla och stödja vald teknik,	Solution Delivery Lead – ORS & eCommerce Operational and Application Security Specialist		IT Director
Tekniska principer för att säkra system balanserar kostnad, tid och komplexitet för att uppfylla säkerhetskraven.	Solution Delivery Lead – ORS & eCommerce IT Director Global IT Director Enterprise Architecture SAP Enterprise Architect	Operational and Application Security Specialist	
Anpassa tekniska principer för att säkra system med bästa befintlig god praxis och standarder för säkerhetsteknik.	Solution Delivery Lead – ORS & eCommerce IT Director SAP Enterprise Architect	Operational and Application Security Specialist	

Tekniska principer för att säkra system och fastställda tekniska rutiner bör regelbundet ses över för att säkerställa att de på ett verkningsfullt sätt bidrar till förbättrad säkerhet i utvecklingsprocessen.	Solution Delivery Lead – ORS & eCommerce IT Director	Operational and Application Security Specialist Global IT Director Enterprise Architecture SAP Enterprise Architect	
Tekniska principer för att säkra system och fastställda tekniska rutiner bör ses över regelbundet för att säkerställa att de förblir aktuella när det gäller att bekämpa nya potentiella hot och fortsätter vara tillämpliga när den teknik och de lösningar som används utvecklas.	Solution Delivery Lead – ORS & eCommerce IT Director	Operational and Application Security Specialist SAP Enterprise Architect	
Tillämpa tekniska principer för att säkra system på utformning eller konfiguration av en rad olika metoder som t.ex. (feltolerans, segregering (t.ex. genom virtualisering eller containeranvändning), teknik för att förhindra manipulation)	Solution Delivery Lead – ORS & eCommerce IT Director SAP Enterprise Architect	Operational and Application Security Specialist	
Använd säkra virtualiseringsmetoder för att förhindra störningar mellan applikationer som körs på samma fysiska enhet, och ifall en virtuell instans av en applikation komprometteras av en angripare Påverkas endast denna instans, inte andra applikationer eller data.	Operational and Application Security Specialist	Global IT Director Enterprise Architecture	Solution Delivery Lead – ORS & eCommerce IT Director SAP Enterprise Architect
Använd teknik för att förhindra manipulation för att upptäcka manipulering av Informationsbehållare oavsett om dessa har fysisk form (t.ex. ett inbrottslarm) eller logisk form (t.ex. en datafil)	Operational and Application Security Specialist		Solution Delivery Lead – ORS & eCommerce IT Director
Tekniska principer för att säkra system bör tillämpning av principer för säker systemarkitektur, t.ex. ”inbyggd säkerhet”, ”flernivåskydd”, ”säkerhet som standard”, ”standardnekande”, ”säkerhet vid fel”, ”lita inte på indata från externa applikationer”, ”säkerhet vid driftsättning”, ”utgå från ett intrång”, ”minsta möjliga behörighet”, ”användbarhet och hanterbarhet” och ”minsta möjliga funktionalitet”,	Solution Delivery Lead – ORS & eCommerce IT Director Operational and Application Security Specialist SAP Enterprise Architect	Global IT Director Enterprise Architecture	

Genomförde en säkerhetsorienterad designöversyn för att bidra till att identifiera säkerhetsrelaterade sårbarheter, säkerställa att säkerhetsåtgärder specificeras samt uppfylla säkerhetskrav,	Operational and Application Security Specialist	Solution Delivery Lead – ORS & eCommerce IT Director SAP Enterprise Architect	
Dokumentation och formell bekräftelse av säkerhetskontroller som inte helt uppfyller kraven (t.ex. på grund av att säkerhetskrav kringgås),	Solution Delivery Lead – ORS & eCommerce IT Director SAP Enterprise Architect	Operational and Application Security Specialist Global IT Director Enterprise Architecture	
Härdning av system för att minska sårbarheter och minimera attackytan i enlighet med säker systemteknik.	Solution Delivery Lead – ORS & eCommerce IT Director SAP Enterprise Architect	Operational and Application Security Specialist	
Organisationen bör utgå från att det redan har skett ett intrång i organisationens informationssystem och därför inte enbart förlita sig på nätverkets säkerhetsperimeter	Solution Delivery Lead – ORS & eCommerce SAP Enterprise Architect	IT Director Operational and Application Security Specialist Operational and Application Security Specialist Global IT Director Enterprise Architecture	
Tillämpa strategin ”aldrig lita på och alltid verifiera” för åtkomst till informationssystem.	Solution Delivery Lead – ORS & eCommerce IT Director SAP Enterprise Architect	Operational and Application Security Specialist Global IT Director Enterprise Architecture	
Organisationen säkerställer att förfrågningar till informationssystem krypteras från ändpunkt till ändpunkt	IT Director SAP Enterprise Architect	Operational and Application Security Specialist Global IT Director Enterprise Architecture	
Verifiera varje förfrågan till ett informationssystem, som om den hade kommit från ett öppet, externt nätverk, även om dessa förfrågningar kommer inifrån organisationen (dvs. inte per automatik lita på något innanför eller utanför organisationens perimeter).	IT Director	Operational and Application Security Specialist Global IT Director Enterprise Architecture	
Använda metoder som bygger på principen om minsta möjliga behörighet samt dynamisk åtkomstkontroll. Detta omfattar att autentisera och godkänna informations eller systemförfrågningar baserat på kontextuell information, såsom autentiseringsinformation, användaridentiteter, uppgift om användarklient samt informationsklassning,	IT Director SAP Enterprise Architect	Operational and Application Security Specialist Global IT Director Enterprise Architecture	

Alltid autentisera den som kommer med en förfrågan och alltid validera förfrågningar till informationssystem på basis av information, inklusive autentiseringsinformation, användaridentiteter, data om användarklient samt informationsklassning, till exempel använd stark autentisering (t.ex. flerfaktorautentisering)	Operational and Application Security Specialist Global IT Director Enterprise Architecture		
--	--	--	--

Tabell 8 Översikt över implementeringsstatus för säkerhetskrav i olika ansvarsområden inom Säker kodning i FX.

Kontroll	Delvis implementerad	Ej implementerad	Ej tillämplig
Organisationen inrätta organisationsövergripande processer för en god styrning i fråga om säker kodning.		Solution Delivery Lead – ORS & eCommerce Operational and Application Security Specialist Senior Manager, Advanced Analytics	IT Director
Tillämpa och fastställa en säker minimibaslinje.	AI ML applied research scientist	Solution Delivery Lead – ORS & eCommerce Operational and Application Security Specialist Senior Manager, Advanced Analytics	IT Director
Utöka säkra kodningsprocesser och styrning till programvarukomponenter från tredjeparter och programvara med öppen källkod.	Solution Delivery Lead – ORS & eCommerce IT Director AI ML applied research scientist	Operational and Application Security Specialist Senior Manager, Advanced Analytics	IT Director
Övervaka omvärldshot samt aktuell rådgivning och information om sårbarheter i programvara ständig förbättring och fortbildning för organisationens principer för säker kodning	Solution Delivery Lead – ORS & eCommerce IT Director	Operational and Application Security Specialist Senior Manager, Advanced Analytics	
Säkerställa ständig förbättring för att verkningsfulla rutiner för säker kodning införs för att möta den snabbt föränderliga hotbilden.	Solution Delivery Lead – ORS & eCommerce	Operational and Application Security Specialist Senior Manager, Advanced Analytics	IT Director

Säkerställa att säkerhetsrelevant kod anropas när så krävs och kan motstå manipulation.	Solution Delivery Lead – ORS & eCommerce	Operational and Application Security Specialist	IT Director Senior Manager, Advanced Analytics
För tolkade språk exekvera kod på en server som inte är tillgänglig för användare och processer som använder den, med datalagrade i en skyddad databas.	AI ML applied research scientist	Operational and Application Security Specialist	IT Director
Skydda administratörsåtkomst med hjälp av säkerhetsåtgärder, t.ex. principer för just-in-time-tilldelning och stark autentisering.	Operational and Application Security Specialist AI ML applied research scientist		IT Director
Konfigurera webbservrar för att förhindra katalogbläddring.	Operational and Application Security Specialist AI ML applied research scientist		
Utforma applikationskod att utgå från att den alltid är under attack.	IT Director AI ML applied research scientist Senior Manager, Advanced Analytics	Operational and Application Security Specialist	
Utforma kritiska applikationer så att de kan stå emot interna fel. Till exempel kan utdata från en komplex algoritm kontrolleras så att de ligger inom vissa gränser innan de används i en applikation som är kritisk, t.ex. ur ett säkerhetsperspektiv eller ekonomiskt perspektiv.	Solution Delivery Lead – ORS & eCommerce IT Director Operational and Application Security Specialist Senior Manager, Advanced Analytics		
Åtgärda sårbarheter i webbapplikationer orsakade av dålig design och kodning (t.ex. databasinjektioner och webbkodinjektioner).	Solution Delivery Lead – ORS & eCommerce IT Director Operational and Application Security Specialist AI ML applied research scientist Senior Manager, Advanced Analytics		
Organisations specifika förväntningar och godkända principer för säker kodning som ska användas både internt och vid utkontrakterad kodutveckling	AI ML applied research scientist Senior Manager, Advanced Analytics	Solution Delivery Lead – ORS & eCommerce Operational and Application Security Specialist Global IT Director Enterprise Architecture	IT Director
Vanliga och historiska metoder för kodning samt fel som ger upphov till sårbarheter i	AI ML applied research scientist	Operational and Application Security Specialist	Solution Delivery Lead – ORS & eCommerce IT Director

Informationssäkerheten			Senior Manager, Advanced Analytics
Konfigurering av utvecklingsverktyg, t.ex. integrerade utvecklingsmiljöer (IDE), för att bidra till att skapa säker kod		Operational and Application Security Specialist AI ML applied research scientist	IT Director Senior Manager, Advanced Analytics
Följa vägledningar från leverantörer av utvecklingsverktyg och exekveringsmiljöer, enligt vad som är tillämpligt	AI ML applied research scientist Senior Manager, Advanced Analytics	Operational and Application Security Specialist	IT Director
Underhåll och användning av uppdaterade utvecklingsverktyg (t.ex. kompilatorer)	Operational and Application Security Specialist AI ML applied research scientist Senior Manager, Advanced Analytics		IT Director
Utvecklarnas kvalifikationer vad gäller att skriva säker kod	Solution Delivery Lead – ORS & eCommerce Operational and Application Security Specialist	AI ML applied research scientist Senior Manager, Advanced Analytics	IT Director
Säker design och arkitektur, inklusive hotmodellering,	Solution Delivery Lead – ORS & eCommerce AI ML applied research scientist Senior Manager, Advanced Analytics	Operational and Application Security Specialist Global IT Director Enterprise Architecture	IT Director
Standarder för säker kodning, och i tillämpliga fall föreskriva att de ska användas	Solution Delivery Lead – ORS & eCommerce AI ML applied research scientist Senior Manager, Advanced Analytics	Operational and Application Security Specialist Global IT Director Enterprise Architecture	IT Director
Användning av kontrollerade utvecklingsmiljöer.	AI ML applied research scientist	Operational and Application Security Specialist Global IT Director Enterprise Architecture Senior Manager, Advanced Analytics	IT Director
Överväga metoder för säker kodning som är specifik för de programspråk och de tekniker som används	Solution Delivery Lead – ORS & eCommerce AI ML applied research scientist Senior Manager, Advanced Analytics	Operational and Application Security Specialist	IT Director
Användning av säkra programmeringsmetoder, t.ex. parprogrammering, refaktorisering, sakkunnig granskning,	Solution Delivery Lead – ORS & eCommerce AI ML applied research scientist	Operational and Application Security Specialist	IT Director Senior Manager, Advanced Analytics

säkerhetsiterationer och testdriven utveckling,			
Användning av strukturerade programmeringsmetoder	AI ML applied research scientist	Operational and Application Security Specialist	IT Director
Dokumentation av kod och avlägsnande av programmeringsfel som kan göra det möjligt att utnyttja sårbarheter i informationssäkerheten	AI ML applied research scientist	Operational and Application Security Specialist	IT Director
Förbud mot att använda osäkra designlösningar (t.ex. användning av hårdkodade lösenord, ej godkända exempel på kod och ej autentiserade webbtjänster).	IT Director AI ML applied research scientist	Operational and Application Security Specialist	
Utföra tester under och efter utveckling	AI ML applied research scientist Senior Manager, Advanced Analytics	Operational and Application Security Specialist	IT Director
Använd statisk testning av applikationssäkerhet för att identifiera sårbarheter i programvara.	Solution Delivery Lead – ORS & eCommerce	Operational and Application Security Specialist Senior Manager, Advanced Analytics	IT Director AI ML applied research scientist
Utvärdera attacktyper och principen om minsta möjliga behörighet	Solution Delivery Lead – ORS & eCommerce IT Director Operational and Application Security Specialist AI ML applied research scientist		
Genomförd analys av de vanligaste programmeringsfelen och dokumentation som visar att dessa har hanterats	AI ML applied research scientist	Operational and Application Security Specialist Senior Manager, Advanced Analytics	IT Director
Uppdateringar bör paketeras och drifställas på ett säkert sätt	IT Director Operational and Application Security Specialist AI ML applied research scientist Senior Manager, Advanced Analytics		
Hantera rapporterade sårbarheter i informationssäkerheten	IT Director Operational and Application Security Specialist AI ML applied research scientist	Senior Manager, Advanced Analytics	
Logga fel och misstänkta attacker och loggarna bör granskas regelbundet för att göra de ändringar i koden som krävs,		Operational and Application Security Specialist AI ML applied research scientist Senior Manager, Advanced Analytics	IT Director

Skydda källkod mot obehörig åtkomst och manipulation (t.ex. genom användning av verktyg för konfigurationshantering, som normalt har funktioner som åtkomstkontroll och versionskontroll).	AI ML applied research scientist	Operational and Application Security Specialist	IT Director
Säkerställa att externa bibliotek hanteras (t.ex. genom att föra en förteckning över de bibliotek och biblioteksversioner som används) och regelbundet uppdateras med nya versioner,	AI ML applied research scientist Senior Manager, Advanced Analytics	Operational and Application Security Specialist	IT Director
Välja, godkänna och återanvända av noggrant granskade komponenter, särskilt autentiserings och krypteringskomponenter	Operational and Application Security Specialist Senior Manager, Advanced Analytics	Global IT Director Enterprise Architecture AI ML applied research scientist	IT Director
Organisationer överväga externa komponenters licens, säkerhet och historik	IT Director Operational and Application Security Specialist AI ML applied research scientist Senior Manager, Advanced Analytics	Global IT Director Enterprise Architecture	
Säkerställa att program kan underhållas och spåras samt kommer från beprövade, välrenommerade källor	IT Director AI ML applied research scientist Operational and Application Security Specialist Global IT Director Enterprise Architecture Senior Manager, Advanced Analytics		
Säkerställa att utvecklingsresurser och artefakter har tillräckligt långvarig tillgänglighet.	Operational and Application Security Specialist AI ML applied research scientist Senior Manager, Advanced Analytics		IT Director
Överväga risken för att inbyggda säkerhetsåtgärder och integritetsprocesser komprometteras	Solution Delivery Lead – ORS & eCommerce Operational and Application Security Specialist Senior Manager, Advanced Analytics	AI ML applied research scientist	IT Director
Huruvida leverantörens samtycke ska inhämtas	Operational and Application Security Specialist		Solution Delivery Lead – ORS & eCommerce IT Director

			AI ML applied research scientist Senior Manager, Advanced Analytics
Möjligheten att få nödvändiga ändringar från leverantören i form av vanliga programuppdateringar	IT Director Operational and Application Security Specialist		AI ML applied research scientist Senior Manager, Advanced Analytics
Konsekvenser om organisationen blir ansvarig för framtida programvaruunderhåll till följd av förändringar,	Operational and Application Security Specialist Senior Manager, Advanced Analytics		IT Director AI ML applied research scientist
Kompatibilitet med annan programvara som används.	IT Director Operational and Application Security Specialist Global IT Director Enterprise Architecture AI ML applied research scientist Senior Manager, Advanced Analytics		

Tabell 9 Översikt över implementeringsstatus för säkerhetskrav i olika ansvarsområden inom Säkerhetskrav för applikationer i FX.

<b>Kontroll</b>	<b>Delvis implementerad</b>	<b>Ej implementerad</b>	<b>Ej tillämplig</b>
Identifiera, specificera Säkerhetskrav för applikationer vid utveckling eller förvärv.	Solution Delivery Lead – ORS & eCommerce IT Director Operational and Application Security Specialist External Contractor, Risk, Security and Compliance team AI ML applied research scientist Senior Manager, Advanced Analytics		
Fastställ säkerhetskrav för applikationer genom en	Solution Delivery Lead – ORS & eCommerce IT Director		

riskbedömning med hjälp av specialister på informationssäkerhet	Operational and Application Security Specialist External Contractor, Risk, Security and Compliance team AI ML applied research scientist		
Utföra riskbedömning för applikationer som är tillgängliga via nätverk utsätts för ett antal nätverksrelaterade hot (t.ex. bedrägerier, avtalstvister eller röjande av information till allmänheten, ofullständig överföring, felaktigstyrning av nätverkstrafik och obehörig ändring, duplicering eller återuppspelning av meddelanden).	IT Director AI ML applied research scientist	Operational and Application Security Specialist External Contractor, Risk, Security and Compliance team	Senior Manager, Advanced Analytics
Detaljerade riskbedömningar och noggrant val av säkerhetsåtgärder som ofta krävs krypteringsmetoder för autentisering och säker överföring av data	IT Director Operational and Application Security Specialist External Contractor, Risk, Security and Compliance team AI ML applied research scientist		Senior Manager, Advanced Analytics
Tillitsnivå för entiteternas identitet (t.ex. genom autentisering)	Operational and Application Security Specialist AI ML applied research scientist		
Identifiering av vilken typ av information och klassningsnivå som applikationen ska behandla	Operational and Application Security Specialist	AI ML applied research scientist Senior Manager, Advanced Analytics	
Behov av att separera åtkomst och åtkomstnivå för data och funktioner i applikationen,	Solution Delivery Lead – ORS & eCommerce Operational and Application Security Specialist AI ML applied research scientist		
Motståndsförmåga mot skadliga attacker eller oavsiktliga störningar (t.ex. skydd mot buffertöversvämning eller SQL-injektioner)	Solution Delivery Lead – ORS & eCommerce IT Director Operational and Application Security Specialist IT Application Owner Process Application Specialist	Senior Manager, Advanced Analytics	AI ML applied research scientist

Författningskrav i den jurisdiktion där transaktionen skapas, behandlas, slutförs eller lagras	IT Director Operational and Application Security Specialist AI ML applied research scientist		Senior Manager, Advanced Analytics
Behov av skydd av personuppgifter för samtliga berörda parter,	IT Director Operational and Application Security Specialist AI ML applied research scientist		Senior Manager, Advanced Analytics
Krav på skydd av eventuell konfidentiell information	IT Director Operational and Application Security Specialist AI ML applied research scientist		Senior Manager, Advanced Analytics
Skydd av data under behandling, överföring och i vila	Solution Delivery Lead – ORS & eCommerce Operational and Application Security Specialist AI ML applied research scientist Senior Manager, Advanced Analytics		
Behov av säker kryptering av kommunikationen mellan alla berörda parter	Solution Delivery Lead – ORS & eCommerce Operational and Application Security Specialist AI ML applied research scientist Senior Manager, Advanced Analytics		
Säkerhetsåtgärder för indata, inklusive kontroller av integritet och validering av indata	Solution Delivery Lead – ORS & eCommerce. IT Director Operational and Application Security Specialist AI ML applied research scientist Senior Manager, Advanced Analytics IT Application Owner Process Application Specialist		
Automatiska säkerhetsåtgärder (t.ex. godkännandebegränsningar eller	Solution Delivery Lead – ORS & eCommerce	Operational and Application Security Specialist	IT Director Senior Manager, Advanced Analytics

användning av tvåhandsprincip för godkännande),	AI ML applied research scientist		
Säkerhetsåtgärder för utdata, med beaktande av vem som kan få åtkomst till utdata och godkännandeprocess för utdata.	IT Director Operational and Application Security Specialist AI ML applied research scientist		Senior Manager, Advanced Analytics
Begränsningar av innehållet i fritextfält, eftersom dessa kan leda till okontrollerad lagring av konfidentiella uppgifter (t.ex. personuppgifter)	Operational and Application Security Specialist AI ML applied research scientist IT Application Owner Process Application Specialist		IT Director Senior Manager, Advanced Analytics
Krav som härrör från verksamhetsprocess, såsom transaktionsloggning, övervakning och krav på oavvislighet	IT Director Operational and Application Security Specialist AI ML applied research scientist		Senior Manager, Advanced Analytics
Krav som härrör från andra säkerhetsåtgärder (t.ex. gränssnitt för loggning och övervakning eller system för detektering av informationsläckage)	Solution Delivery Lead – ORS & eCommerce IT Director Operational and Application Security Specialist AI ML applied research scientist IT Application Owner	Senior Manager, Advanced Analytics	
Felmeddelanden hantering	IT Director Operational and Application Security Specialist AI ML applied research scientist Senior Manager, Advanced Analytics IT Application Owner Process Application Specialist		
Överväga vilken tillitsnivå parterna kräver för att lita på den andra partens angivna identitet	Operational and Application Security Specialist AI ML applied research scientist		Senior Manager, Advanced Analytics
Vilken tillitsnivå som krävs för integriteten i den information som utbyts eller behandlas samt	Operational and Application Security Specialist AI ML applied research scientist		IT Director Senior Manager, Advanced Analytics

mekanismer för att identifiera bristande integritet (t.ex. cyklisk redundanskontroll, hashning och digitala signaturer),			
Auktorisation avseende vem som kan godkänna innehåll i, utfärda eller signera viktiga transaktionsdokument	Operational and Application Security Specialist AI ML applied research scientist		IT Director Senior Manager, Advanced Analytics
Konfidentialitet, integritet, avsändarintyg och mottagarbevis för viktiga dokument samt oavvislighet (t.ex. avtal med koppling till upphandling och avtalsprocesser)	Operational and Application Security Specialist AI ML applied research scientist		IT Director Senior Manager, Advanced Analytics
Konfidentialitet och integritet för alla transaktioner (t.ex. beställningar, leveransadressuppgifter och kvittenser)	Operational and Application Security Specialist AI ML applied research scientist		IT Director Senior Manager, Advanced Analytics
Krav på hur länge en transaktion ska hållas konfidentiell	Operational and Application Security Specialist AI ml applied research scientist		IT Director Senior Manager, Advanced Analytics IT Application Owner Process Application Specialist
Försäkringskrav och andra avtalskrav	Operational and Application Security Specialist AI ML applied research scientist		IT Director Senior Manager, Advanced Analytics IT Application Owner Process Application Specialist
Krav för att upprätthålla orderinformationens konfidentialitet och integritet	Operational and Application Security Specialist		IT Director AI ML applied research scientist Senior Manager, Advanced Analytics IT Application Owner Process Application Specialist
Lämplig nivå för verifiering av betalningsinformation från kund	Operational and Application Security Specialist		IT Director AI ML applied research scientist Senior Manager, Advanced Analytics IT Application Owner

			Process Application Specialist
Undvikande av förlust eller kopiering av information om transaktioner	Operational and Application Security Specialist		IT Director AI ML applied research scientist Senior Manager, Advanced Analytics IT Application Owner Process Application Specialist
Lagring av transaktionsuppgifter utanför publikt tillgängliga miljöer (t.ex. på en lagringsplattform på organisationens intranät, så att den inte sparas och exponeras på elektroniska lagringsmedier som är direkt åtkomliga via internet),	Operational and Application Security Specialist		Solution Delivery Lead – ORS & eCommerce IT Director AI ML applied research scientist IT Application Owner Process Application Specialist
Säkerheten integreras och upprätthålls i hela processen för hantering av certifikat eller signaturer från början till slut då en betrodd utfärdare används (t.ex. för att utfärda och underhålla digitala signaturer eller digitala certifikat).	Operational and Application Security Specialist		IT Director AI ML applied research scientist IT Application Owner Process Application Specialist

## 8.3 Intervjufrågor:

Inledande fråga:

- Är det okej att jag spelar in ljudet från intervjun i syfte att underlätta analysen?

**Om teamets struktur och samarbete:**

1. Kan du beskriva hur ert team är organiserat?
2. Hur många personer arbetar i teamet?
3. Hur ser ert samarbete ut med andra IT-funktioner eller IT-relaterade avdelningar inom organisationen?

**Om implementation av processer:**

4. Varför tror du att vissa processer är fullt implementerade, medan andra inte är det?
5. Vad anser du krävs för att en process ska bli fullt implementerad?

**Om arbetssätt och rutiner:**

6. Hur arbetar ni i teamet – följer ni ett agilt arbetssätt eller något annat ramverk?
7. När ni får nya krav eller processer som ska integreras – hur anpassar ni era rutiner för att möta detta?

**Om förbättringar och ideala lösningar:**

8. Om du fick fria händer, hur skulle du vilja implementera en process eller ett arbetssätt?
9. Ur ditt perspektiv, hur skulle en ideal lösning se ut för att uppnå högsta möjliga cybersäkerhet?

**Avslutande:**

10. Tack för din medverkan – finns det något du vill tillägga, kommentera eller dela med dig av?

*Not: Frågorna är av semistrukturerad karaktär och kan komma att anpassas under intervjutillfället beroende på respondentens svar och samtalets riktning.*



# HÖGSKOLAN I BORÅS

Besöksadress: Allégatan 1 · Postadress: 501 90 Borås · Tfn: 033-435 40 00 · E-post: [registrator@hb.se](mailto:registrator@hb.se) · Webb: [www.hb.se](http://www.hb.se)