FSPOS

Tillgångsförvaltning av informations- och IKT-tillgångar

Kravbild och principer

2025-01-07

AG Analys

Sammanfattning

Aktörer inom finansiell sektor förväntas ha kontroll över de risker som är förknippade med verksamheten. För att uppnå detta behöver en aktör ha god kännedom om sin verksamhet och vad den utgörs av, annars kan riskanalysen bli bristfällig samt att otillräckliga säkerhetsåtgärder implementeras.

Denna promemoria beskriver hur systematisk tillgångsförvaltning möjliggör kontroll över verksamhetens risker. Fokus för promemorian är informations- och IKT-tillgångar då dessa är avgörande för att aktörer inom den finansiella sektorn ska kunna erbjuda sina tjänster. Systematisk förvaltning av informations- och IKT-tillgångar underlättar riskhantering och är grundläggande för att kunna implementera och övervaka nödvändiga säkerhetsåtgärder och kontroller. Systematisk tillgångsförvaltning sker under tillgångarnas hela livscykel och bygger på identifiering, kartläggning, klassificering och dokumentation av tillgångar, samt att tillgångsägare identifieras och riskhantering av tillgångar genomförs.

Tillgångsförvaltning bidrar till ökad förmåga att förebygga och hantera incidenter och kriser. Denna förmåga är helt avgörande för att kunna hindra, och minska påverkan från, exempelvis cyberattacker, vilket är en viktig del i organisationens generella beredskapsarbete.

1 Inledning

Den finansiella sektorns digitalisering har inneburit stora möjligheter men också risker rörande informationssäkerhet och tillgänglighet av finansiella tjänster. Riskerna avser olika typer av it-incidenter, omedvetna och medvetna, där de senare inkluderar incidenter som cyberrelaterad brottslighet och statsunderstödda antagonistiska angrepp.[1] Hotbilden inom informations- och cybersäkerhetsområdet i sektorn blir alltmer sofistikerad och komplex.[2] Det försämrade säkerhetspolitiska läget är en av anledningarna till detta. Den finansiella sektorn är samhällsviktig och därmed ett möjligt mål för de som vill skada Sverige.

För att tillhandahålla finansiella tjänster, vilka är centrala för ett fungerande samhälle, är information samt informations- och kommunikationsteknologi (IKT) en förutsättning. Den komplexa hotbilden, tillsammans med ökande komplexitet i de finansiella aktörernas it-miljöer och organisationer, bidrar till att skyddet av informations- och IKT-tillgångar[3] blir alltmer avgörande, men också mer utmanande. Detta återspeglas bland annat av ökade krav på riskhantering i nya regleringar som exempelvis EU-förordningen om digital operativ motståndskraft för finanssektorn (DORA-förordningen).

Att ha kontroll över verksamhetens risker är centralt i lagstiftningen av den finansiella sektorn. Genom att systematiskt hantera tillgångarna i en organisation underlättas arbetet med riskhantering, detta då tillgångsförvaltning ger en förståelse för verksamhetens tillgångar och de risker och sårbarheter de förknippas med. För informations- och IKT-tillgångar specifikt ses tillgångsförteckningen som grundläggande för att kunna implementera och övervaka lämpliga säkerhetsåtgärder och kontroller.[4]

Tillgångsförvaltning av informations- och IKT-tillgångar kan bidra till att stärka beredskapen inom den finansiella sektorn då arbetet möjliggör en ökad förmåga att hantera incidenter, cyberhot och andra störningar som kan påverka säkerheten i det finansiella systemet. Denna förmåga har blivit en strategisk fråga, inte bara för verksamheten som sådan, utan också för den nationella säkerheten.

1.1 Syfte

Syftet med denna promemoria är att ge den finansiella sektorns aktörer en ökad förståelse för tillgångsförvaltning som en viktig del i arbetet med informations- och cybersäkerhet. Fokus är att sätta tillgångsförvaltning i sitt sammanhang, belysa relevanta utmaningar samt översiktligt beskriva kravbilden inom den finansiella sektorn. Promemorian avser även att beskriva principer, i form av processer och angreppssätt, för hur en aktör inom den finansiella sektorn kan ta sig an arbetet med tillgångsförvaltning med fokus på informationstillgångar och IKT-tillgångar.

Målet är att promemorian ska stärka sektorns förståelse för, och förmåga att, arbeta systematiskt med tillgångsförvaltning och, som en följd av detta, även bidra till att stärka sektorns beredskap. Med ökad förståelse, tillsammans med de i promemorian presenterade utgångspunkterna för

---

[1] *Finansinspektionen 2022. Förstärkt digital motståndskraft hos företag i den finansiella sektorn. Dnr 22-10015.*

[2] *Svenska Bankföreningen 2024. Hotbildsbedömning för Sveriges banker.*

[3] *I denna promemoria omnämns både informationstillgångar och IKT-tillgångar för att återspegla de begrepp som används i flertalet regleringar inom finanssektorn, inklusive Digital Operational Resilience Act (DORA).*

[4] *Deane & Kraus, 2021. The Official (ISC)² CISSP CBK Reference.*

arbetet med tillgångsförvaltning, är målet även att underlätta för intresserade aktörer att påbörja eller fördjupa sitt arbete inom området.

1.2 Avgränsning

Tillgångförvaltning berör organisationens alla tillgångar. Denna promemoria avgränsas dock till att fokusera på tillgångsförvaltning av informationstillgångar och IKT-tillgångar, vilka i sin tur avgränsas till tillgångar som relaterar till informationshantering och teknologi såsom data, programvara och hårdvara.

Analysen av krav i lagar, förordningar och föreskrifter (kapitel 3.1) omfattar de viktigaste kraven som är tillämpliga inom Sverige och Europa. Varje enskild aktör behöver genomföra sin egen analys av regelverken, anpassad till den egna verksamheten.

Promemorian är inte ett metodstöd för hur en organisation ska arbeta med tillgångsförvaltning för att uppfylla kraven i de lagar och regelverk som reglerar området. I stället ska promemorian ses som ett stöd i arbetet med tillgångsförvaltning, med fokus på informationstillgångar och IKT-tillgångar.

1.3 Genomförande

Promemorian har tagits fram genom en litteraturstudie samt med stöd av en referensgrupp bestående av representanter från olika delar av den finansiella sektorn. Litteraturstudien innefattar lagar, förordningar, föreskrifter och regelverk relevanta för den finansiella sektorn med bäring på frågor kopplade till informations- och cybersäkerhet. Även standarder som exempelvis ISO 27001, ISO 31000, ISO 55000, NIST Cybersecurity Framework och CIS Critical Security Controls har analyserats.

2 Tillgångsförvaltning

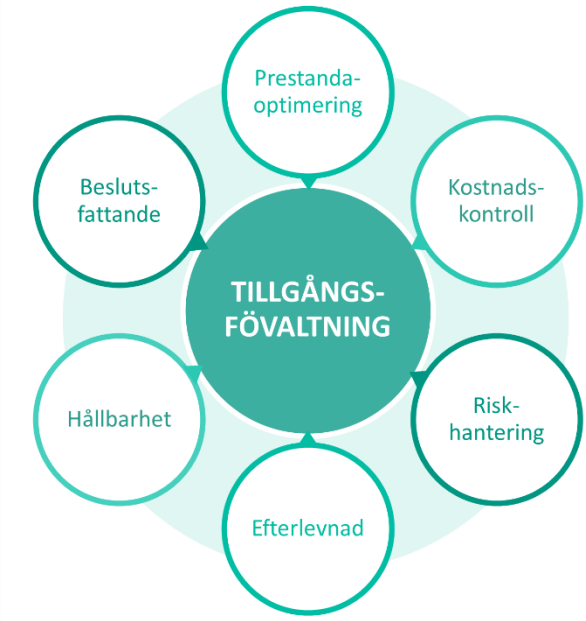
Tillgångsförvaltning, på engelska *asset management*, är enligt ISO 55000 det systematiska och samordnade arbetet för att realisera värde från tillgångar.[5] Tillgångsförvaltning innebär att effektivt och hållbart hantera en organisations tillgångar under deras livscykel. Med tillgångar avses här fysiska, finansiella, immateriella och humana tillgångar som har potentiellt eller faktiskt värde för organisationen. Inom immateriella tillgångar inryms bland annat tillgångar som tjänste- och processtillgångar men också tillgångar som exempelvis kundregister och data.

Tillgångsförvaltning är en viktig del i en organisations strategiska arbete, med syfte att bland annat bidra till förbättrad:[6]

[5] *ISO 55000:2024(en) Asset management — Overview, principles and terminology, kap.3.1.*

[6] *Bild baserat på illustration från International Organization for Standardization ISO (hämtad: 2024-08-20) samt text från Institute of Asset Management, IAM (2024) Asset management – an anatomy version 4 sida 22.*

- ***Prestandaoptimering*** – genom att säkerställa tillgångars effektivitet och pålitlighet vilket möjliggör för en maximerad produktivitet.
- ***Kostnadskontroll*** – genom att säkerställa en effektiv förvaltning av tillgångarna under deras livscykel genom planering, underhåll och förnyelse.
- ***Riskhantering*** – genom att säkerställa att risker kopplade till tillgångar identifieras, bedöms och hanteras, kan tillgångarna skyddas.
- ***Efterlevnad*** – genom att säkerställa att förvaltning av tillgångar följer gällande lagar, förordningar, direktiv, standarder etc.
- ***Hållbarhet*** – genom att säkerställa att miljö- och sociala frågor hanteras inom ramen av förvaltningen.
- ***Beslutsfattande*** – genom att säkerställa att välgrundade beslut fattas på tillförlitliga data och analyser av tillgångars prestanda och tillstånd.



Figur 1. Tillgångsförvaltningens bidrag i verksamheten.

2.1 *Tillgångsförvaltning som del i beredskapsarbetet*

Arbetet med tillgångsförvaltning kan bidra positivt i en organisations beredskapsarbete, både med avseende på incidenter, fredstida kriser och vid höjd beredskap, se figur 2. Detta eftersom tillgångsförvaltning syftar till att ge en systematisk och detaljerad förståelse för en organisations tillgångar. Genom att ha en tydlig överblick och kontroll över sina tillgångar underlättas organisationens arbete att systematiskt identifiera och hantera risker kopplade till tillgångarna, oavsett om de är materiella eller immateriella. Tillgångförvaltningen möjliggör en proaktiv hantering av risker då de tillgångar som är mest utsatta för hot kan identifieras och skyddsstrategier och riskminimerande åtgärder kan sättas in.

Figur 2. Tillgångsförvaltning som del i beredskapsarbetet.

Arbetet med tillgångsförvaltning innebär även att tillgångar och deras beroenden identifieras, vilket möjliggör en effektiv kontinuitetshantering då planering för att minimera effekter av störningar och kriser underlättas. Tillgångsförvaltning kan också ge stöd till utvecklingen av robusta beredskapsplaner, exempelvis genom att säkerställa redundans för nyckelresurser och backupsystem för data. När en incident eller kris inträffar kan systematisk tillgångsförvaltning vara till nytta vid hanteringen då en uppdaterad tillgångsförteckning möjliggör för en organisation att snabbt kunna förstå vilka system och resurser som är påverkade, samt vilka resurser som finns tillgängliga för att stötta krishanteringen.

Det är inte bara inom risk-, kris- och kontinuitetshantering som tillgångsförvaltning bidrar med nytta. För organisationer med verksamhet som omfattas av Säkerhetsskyddslag (2028:585) ger systematisk tillgångsförvaltning värdefulla indata till säkerhetsskyddsanalysen. Verksamhetsutövaren ska i sin analys identifiera de skyddsvärden som finns i den säkerhetskänsliga verksamheten, vilka bland annat kan inkludera säkerhetsskyddsklassificerade uppgifter samt anläggningar, objekt, system, egendom och andra tillgångar som är av betydelse för Sveriges säkerhet.[7]

Sammantaget innebär detta att tillgångsförvaltning bidrar till organisationens beredskapsarbete, ett arbete som syftar till att snabbare kunna anpassa sig vid en förändring eller kris. Detta innebär även att tillgångsförvaltning bidrar till organisationens arbete med civilt försvar och i planeringen för hur organisationen ska verka under höjd beredskap.

3 Tillgångsförvaltning av informations- och IKT-tillgångar

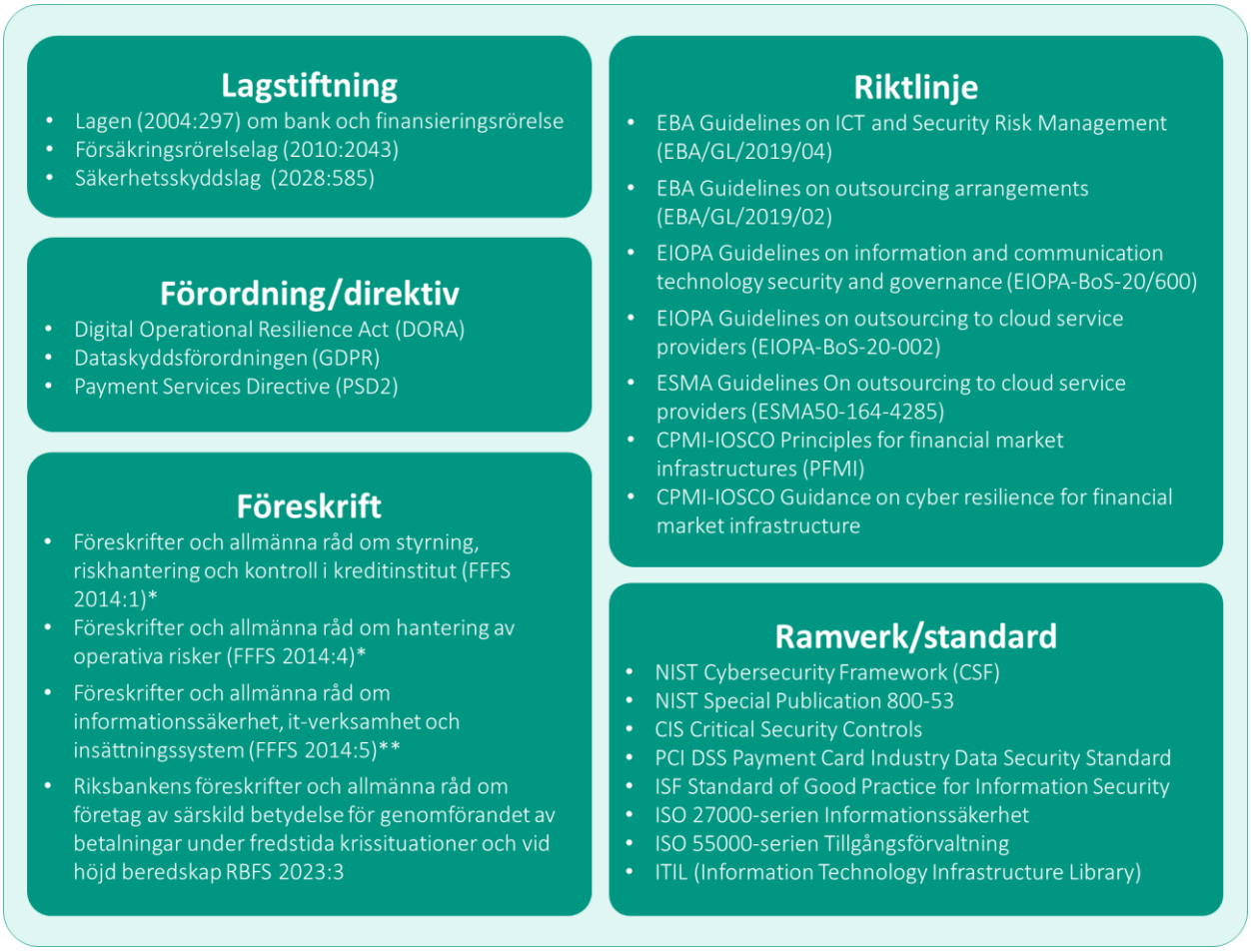
Inom den finansiella sektorn är informationstillgångar och IKT-tillgångar centrala för att verksamheten ska kunna bedrivas och finansiella tjänster tillhandahållas. Dessa tillgångar omfattar allt från känsliga kunddata och finansiell information till digitala system och plattformar som möjliggör datalagring och kommunikation. Att arbeta systematiskt med förvaltning av dessa tillgångar är avgörande ur flera perspektiv; affärsmässigt, regulatoriskt och beredskapsmässigt.

Det finns flera lagar och regelverk som syftar till att säkerställa att finansiella aktörers informationstillgångar och IKT-tillgångar skyddas mot risker som exempelvis dataintrång, cyberattacker eller avbrott. De senaste åren har regelverkens omfattning vuxit för att möta de krav och förväntningar som finns på den finansiella sektorns förmåga att skydda sina digitala tillgångar och sina kunders integritet, samt förmågan att säkerställa systemens tillgänglighet och säkerhet. Att omfattningen av regelverken vuxit är en följd av en allt komplexare digital miljö men också en ökad hotbild mot den finansiella sektorn.

3.1 Krav, riktlinjer och standarder

Krav på hantering av informations- och IKT-tillgångar ställs i lagar, förordningar, föreskrifter och riktlinjer riktade mot finanssektorn. Utöver dessa finns ett antal ramverk och standarder för hur man kan och bör arbeta med förvaltning av dessa tillgångar. För denna promemoria har de lagar, förordningar, föreskrifter, riktlinjer och standarder som presenteras i figur 3 analyserats. Se även Appendix A för en mer ingående beskrivning av respektive dokument.

[7] *PMFS 2022:1, Säkerhetspolisens föreskrifter om säkerhetsskydd, 2 kap. 3 §.*



*Figur 3. Lagar, regelverk och standarder som analyserats avseende förvaltning av informations- och IKT-tillgångar. *Ny version är på remiss och väntas antas i januari 2025. ** Föreskriften kommer att utgå i januari 2025.*

Ordet *tillgångsförvaltning* används sällan eller inte alls i de regelverk som analyserats. I stället ställs krav på att aktörer bland annat ska:

…ha kontroll över de risker som dess rörelse är förknippad med.[8]

… identifiera alla informationstillgångar och IKT-tillgångar […]. De ska kartlägga informationstillgångarnas och IKT-tillgångarnas konfiguration samt länkarna och det ömsesidiga beroendet mellan de olika informationstillgångarna och IKT-tillgångarna.[9]

Det första exemplet, att ha kontroll över sina risker, är återkommande i alla lagar, förordningar, föreskrifter och riktlinjer. För att en organisation ska ha kontroll över sina risker krävs en systematisk hantering av dess tillgångar.

Det andra exemplet är hämtat från DORA, men skrivningar med samma innebörd återfinns i majoriteten av de förordningar, föreskrifter och riktlinjer som analyserats för denna promemoria. Bland annat riktlinjerna från Europeiska Bankmyndigheten (EBA) och Europeiska försäkrings- och tjänstepensionsmyndigheten (EIOPA) ställer dessa krav och går steget längre då de även

[8] *Lagen (2004:297) om bank och finansieringsrörelse, 6 kap. 2 §.*

[9] *DORA-förordningen. Digital Operational Resilience Act (DORA), kapitel 2 artikel 8(4).*

kravställer att tillgångsförvaltning ska ske systematiskt genom hela tillgångens livscykel.[10] Skrivningarna innebär att aktörerna behöver arbeta med tillgångsförvaltning av sina informations- och IKT-tillgångar. Tydligt är att identifiering och hantering av tillgångar är centralt för efterlevnad av gällande lagar och regelverk.

I arbetet med informations- och cybersäkerhet underlättar det att utgå från en etablerad standard. Vilken standard som är bäst lämpad beror på organisationen och dess förutsättningar. Gemensamt för de flesta standarder för tillgångsförvaltning är att de bygger på principer om livscykelhantering och riskhantering av tillgångar, samt lyfter vikten av att integrera tillgångsförvaltning i organisationens strategiska arbete.

3.2 Utmaningar och förutsättningar inom den finansiella sektorn

Inom den finansiella sektorn finns flera utmaningar och förutsättningar som måste beaktas och som kan påverka arbetet med förvaltning av informationstillgångar och IKT-tillgångar. Nedan presenteras några av dessa.

- ***Dynamiska hotlandskap:*** Att identifiera, bedöma och hantera cyberhot mot organisationens IKT-tillgångar kan vara en betydande utmaning där många faktorer påverkar. Utmaningen förstärks av cyberhotens ständiga utveckling och komplexiteten i moderna it-miljöer.

- ***Komplexa organisationer:*** I takt med att organisationen växer, särskilt för organisationer verksamma i flera länder, ökar risken att organisationen inte har kontroll över tillgångarna. Organisationer inom finanssektorn kan omfatta dotterbolag, filialer, tredjepartsleverantörer, entreprenörer, tillfälligt anställda med flera, även inom andra jurisdiktioner/regioner. Det innebär utmaningar kring identifieringen av tillgångar och att dess skydd följer organisationens beslutade baslinje.

- ***Komplex lagstiftning:*** Mängden regleringar och lagstiftningar inom finanssektorn har ökat de senaste åren, inte minst inom informations- och cybersäkerhetsområdet. Flertalet av dessa är både omfattande och komplexa. Därför bör organisationer ha en kontinuerlig omvärldsbevakning och analys av lagar och regler som rör hantering av informationstillgångar. Detta bör även kompletteras med intern revision för att tillse efterlevnad.

- ***Komplex it-miljö:*** Organisationer hanterar normalt en bred variation av IKT-tillgångar, från fysiska servrar till molntjänster och mobila enheter. Sambanden mellan dessa tillgångar kan vara komplexa. Varje tillgångskategori har dessutom sina unika hanteringskrav, vilket försvårar möjligheten att behålla en enhetlig översikt och kontroll.

- ***Ökat beroende av tredjepartsleverantörer:*** Flertalet utmaningar följer av det ökade beroendet av tredjepartsleverantörer inom IKT-området, exempelvis övervakning av leverantörskedjor och förvaltning av tillgångar som hanteras av dessa leverantörer. Organisationer bör därför tillse att regulatoriska och kontraktuella säkerhetskrav överförs

[10] *EBA (2019) Guidelines on ICT and Security Risk Management (EBA/GL/2019/04), avsnitt 55. EIOPA (2020) Guidelines on information and communication technology security and governance (EIOPA-BoS-20/600) avsnitt 45.*

till tredjepartsleverantörer[11] samt att baslinjer för säkerhet möts av dessa. En ytterligare utmaning är finanssektorns monoberoende[12] av vissa tjänsteleverantörer som kan få mycket omfattande konsekvenser för samhället vid en störning.

- ***Användning av molntjänster:*** Användandet av molntjänster kan ha positiva effekter för den enskilda organisationen men kan samtidigt skapa nya säkerhetsrisker. Att tillgångsförvalta molntjänster kan vara utmanande och medför därför särskilda krav vid upphandling av dessa tjänster. ESMA och EIOPA har utställt särskilda rekommendationer och riktlinjer vid utkontraktering av molntjänster[13]. Dessa tillsammans med relevanta kontroller i befintliga ramverk och tekniska lösningar[14] kan användas för att hantera risker som uppstår vid användning av molntjänster.

- ***Datalokalisering (geografisk plats för lagring av data):*** Organisationer med verksamhet i flera länder kan omfattas av flera dataskyddslagar samt kundkrav som kan innefatta datalokalisering. Ett exempel är GDPR som medför krav på hantering och lagring av personuppgifter. Följaktligen behöver risker med gränsöverskridande dataflöden hanteras, vilka bland annat kan uppstå vid användning av molntjänster.

- ***Dold it eller skugg-it (eng: shadow IT):*** Tillgångar som inte har identifierats och godkänts av en central funktion är en utmaning för organisationer. Exempel på dold it är SaaS-tjänster som affärsverksamheten på eget initiativ köper in och använder på ett okontrollerat sätt. Dold it kan begränsa möjligheten till konfigurationshantering och förändringsledning för organisations tillgångar. Inkorrekt konfigurationshantering medför risken att tillgångar inte möter organisationens beslutade baslinje[15] för säkerhet och därigenom ökar sårbarheten för hot. Brister i förändringsledning ökar risken för okontrollerade förändringar av programvaru- och hårdvarutillgångar, vilket kan få negativ påverkan på produktionsmiljöer.

- ***Datakvalitet:*** Uppdaterad och pålitlig dokumentation om varje tillgång är avgörande för en tillförlitlig tillgångsförvaltning. Även relationer mellan tillgångar måste vara dokumenterade. Inkonsekvent eller ofullständig information om tillgångar och dess relationer riskerar att leda till felaktiga beslut som påverkar it-miljöns prestanda och säkerhet.

- ***Snabb teknisk utveckling:*** Den snabba tekniska utvecklingen innebär att IKT-tillgångar blir föråldrade (når *end-of-life* status) i en accelererande takt. Att balansera behovet av uppdateringar genom exempelvis förlängda (och ibland kostsamma) supportavtal med att maximera tillgångarnas värde har därför blivit en växande utmaning. Investeringar i ny teknik kan innebära höga kostnader och strategiska överväganden.

---

[11] *DORA, kapitel 2 artikel 30, ställer krav på hur kontraktsmässiga arrangemang för användning av IKT-tjänster bör utformas.*

[12] *Monoberoende innebär att vara beroende av en specifik digital tjänst eller produkt som saknar konkurrerande alternativ och är unik på marknaden.*

[13] *ESMA (2021). Guidelines On outsourcing to cloud service providers (ESMA50-164-4285), EIOPA (2020). Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002).*

[14] *Säkerhetförmedling för molnåtkomst (CASB), utökad identifiering och svar (XDR), dataförlustskydd (DLP) är några exempel.*

[15] *En baslinje är en uppsättning säkerhetskrav, granskade och godkända, för hela eller delar av organisationen eller ett system.*

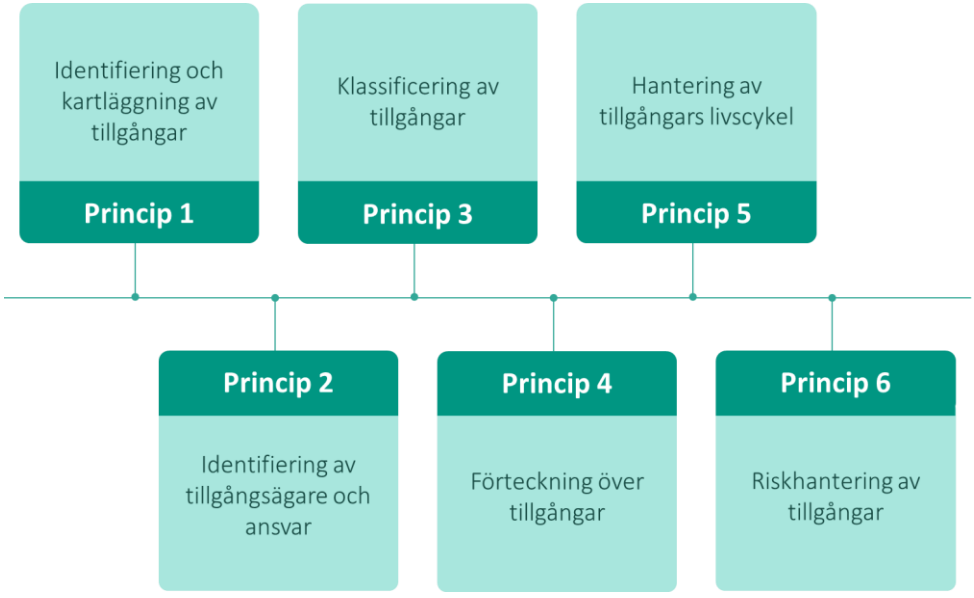
- ***Artificiell intelligens (AI):*** Användningen av AI inom finanssektorn har ökat snabbt de senaste åren, särskilt för prognoser och analyser av stora datamängder. AI kan även automatisera många grundläggande bankärenden som betalningar, insättningar, överföringar och kundtjänstförfrågningar. Detta ställer helt nya krav på förvaltningen av organisationens informationstillgångar då dessa kan ligga till grund för inlärning av olika AI-modeller.

- ***Begränsade resurser:*** Effektiv livscykelhantering av tillgångar kräver betydande resurser och teknisk kompetens. Då organisationens resurser alltid är begränsade krävs en noggrann resursplanering, vilket innebär att identifiera, prognostisera och allokera resurser i verksamheten för att kunna upprätthålla en modern och säker it-miljö.

4 Övergripande principer för tillgångsförvaltning

Aktörer inom finanssektorn bör arbeta både strategiskt och systematiskt för att åstadkomma en tillfredsställande riskhantering och för leva upp till de regulatoriska krav som ställs på deras tillgångsförvaltning. Det är av största vikt att detta arbete integreras med verksamhetens övriga arbete med att uppnå digital operativ motståndskraft. För att lyckas med detta bör aktörerna utgå från en etablerade standard för tillgångsförvaltning.

Detta avsnitt beskriver sex övergripande principer för tillgångsförvaltning, se figur 4. Principerna bygger på tillämpliga ramverk och standarder inom finanssektorn, exempelvis ISO 27001, ISO 31000, ISO 55000, NIST SP 800-53, NIST SP 1800-5, CIS CSC, ISF SoGP med flera. Principerna ska i första hand betraktas som ett stöd och vägledning i arbetet att uppnå en effektiv tillgångsförvaltning. Observera att efterlevnad av de beskrivna principerna inte innebär att samtliga regulatoriska krav som ställs på aktörer inom finanssektorn är uppfyllda.



Figur 4. Övergripande principer för effektiv tillgångsförvaltning

Principerna är applicerbara för alla typer av tillgångar, även om detta PM i första hand fokuserar på informationstillgångar och IKT-tillgångar. Principerna bör implementeras i organisationen i den angivna ordningen.

Princip 1: Identifiering och kartläggning av tillgångar

Det första steget i effektiv tillgångsförvaltning är en noggrann identifiering av aktörens samtliga skyddsvärda informationstillgångar och IKT-tillgångar som stödjer verksamhetsfunktioner och stödprocesser, följt av en kartläggning av dess inbördes beroenden. Skyddsvärda tillgångar innefattar (men är inte begränsade till):

- Informationstillgångar[16]
    - ***Data*** – Enskild data eller datamängder, dvs. gruppering av information som del av en informationstillgång, exempelvis en eller flera tabeller i en databas.
    - ***Information*** – Utgör den bearbetade, organiserade och strukturerade formen av data och kan bestå av en eller flera datamängder.
    - ***Kunskap*** – Immateriella tillgångar som exempelvis kunskap behöver skyddas och upprätthållas över tid. Enskilda individer (eller roller) kan besitta särskild kunskap som är avgörande för verksamheten och som därmed behöver hanteras genom exempelvis kontinuitetshantering.

- IKT-tillgångar[17]
    - ***Programvarutillgångar*** – Inkluderar alla mjukvaruapplikationer och mjukvaruplattformar, operativsystem, mjukvarulicenser etc.
    - ***Hårdvarutillgångar*** – Inkluderar bärbara datorer, stationära datorer, servrar, arbetsstationer, nätverksutrustning, kommunikationsutrustning, lagringsenheter (stationära och flyttbara), kringutrustningar, etc. Här ingår även mobiltelefoner, surfplattor och andra mobila enheter.
    - ***Fysiska tillgångar*** – Inkluderar kontor, datahallar och andra byggnader som är nödvändiga för att upprätthålla verksamheten. Här ingår även klimatanläggningar, brandsläckning, passersystem, passerkort, nyckelbrickor etc.

Identifiering av tillgångar är delvis ett manuellt arbete som kan vara tidskrävande. Arbetets komplexitet ökar ju större organisationen är. Tekniska hjälpmedel finns, exempelvis verktyg för *Asset Discovery* som automatiskt upptäcker och varnar när oidentifierade programvarutillgångar eller hårdvarutillgångar försöker få tillgång till nätverket. Organisationer bör även arbeta systematiskt med förändringsledning så att identifiering av nya tillgångar upprätthålls vid alla förändringar i IKT-miljön.

Efter identifiering bör tillgångarnas inbördes beroenden kartläggas. Kartläggningen omfattar samtliga beroenden mellan aktörens verksamhetsfunktioner/stödprocesser och dess informationstillgångar, samt mellan informationstillgångar och underliggande IKT-tillgångar. Som stöd i denna kartläggningsprocess kan MSB:s *Vägledning för processorienterad informationskartläggning*[18] användas. Vid kartläggning av tillgångar bör även beroenden gentemot

---

[16] *DORA, kap. 1 artikel 3, definierar informationstillgång som "En samling materiell eller immateriell skyddsvärd information".*

[17] *DORA, kap. 1 artikel 3, definierar IKT-tillgång som "En programvaru- eller maskinvarutillgång i nätverks- och informationssystemen som används av den finansiella entiteten".*

[18] *MSB (2012). Vägledning för processorienterad informationskartläggning, Publ.nr MSB493.*

personal, uppdragstagare och tredje parter samt beroenden av andra interna och externa system och processer beaktas i syfte att kunna hantera de informationstillgångar som stödjer deras kritiska verksamhetsfunktioner och stödprocesser.

Princip 2: Identifiering av tillgångsägare och ansvar

Tillgångsägare för varje informationstillgång och IKT-tillgång bör identifieras och tilldelas. Genom att tilldela roller inom organisationen ägarskap för tillgångar under hela deras livstid kan organisationen säkerställa att informationen i dess verksamhetsfunktioner och stödprocesser ges rätt skydd. Tillgångsägaren ansvarar för att klassificera tillgången samt säkerställa att tillgången uppfyller de säkerhetskrav som följer klassificeringen.

Informationstillgångar ägs av informationsägaren. Beroende på organisationens storlek och hur identifieringen och kartläggningen av informationstillgångar har strukturerats kan följande roller behöva utses som komplement till informationsägare:

- ***Dataägare*** *(eng: Data Owner)* – äger en eller flera datamängder (gruppering av information som del av en informationstillgång). Ansvaret gäller klassificering, skydd, användning och kvalitet av datamängder.

- ***Dataansvarig, dataföreståndare*** *(eng: Data Steward)* – ansvarar för de data som en organisation har. Ansvaret gäller att data är korrekta, aktuella, användbara och fullständiga. Rollen sammanfaller delvis med dataförvaltare.

- ***Dataförvaltare*** *(eng: Data Custodian)* – Har ett tekniskt ansvar för data. Ansvaret gäller sådant som datalagring, dataöverföring, dataskydd, backup och andra tekniska processer för hantering av data.

För IKT-tillgångar finns flertalet modeller för styrning och förvaltning. I traditionell bemärkelse är ITIL och PM3 vanligt förekommande förvaltningsmodeller och omfattar roller för ägandeskap på strategisk, taktisk och operationell nivå. Oavsett förvaltningsmodell bör organisationen utse ett tydligt ägarskap för alla typer av IKT-tillgångar (programvarutillgångar, hårdvarutillgångar och fysiska tillgångar).

Princip 3: Klassificering av tillgångar

När kartläggningen är slutförd bör samtliga informationstillgångar och IKT-tillgångar klassificeras med avseende på kritikalitet[19], det vill säga dess skyddsvärden hos organisationen. Vid klassificering bör hänsyn tas till skyddsbehovet utifrån konfidentialitet, riktighet och tillgänglighet hos tillgångarna, se exempelvis MSB:s metodstöd för systematiskt informationssäkerhetsarbete[20]. Lämpliga nivåer för klassificering[21] kan vara:

---

[19] *Benämningen kritikalitet härstammar från EBA Guidelines on ICT and Security Risk Management och EIOPA Guidelines on information and communication technology security and governance.*

[20] *MSB (2024). Metodstödet för systematiskt informationssäkerhetsarbete, Klassning av information. Hämtad: 2024-11-19.*

[21] *Nomenklatur och modell för klassificering skiftar mellan olika organisationer. NIST SP 800-53 föreslår nivåerna hög-medelstor-låg påverkan medan MSB Vägledning för processorienterad informationskartläggning föreslår nivåerna mycket allvarlig-allvarlig-lindrig påverkan.*

- Hög påverkan
- Medelstor påverkan
- Låg påverkan

Klassificering möjliggör gruppering av tillgångar baserat på utvalda kriterier vilket underlättar vid bedömning av risker och beslut om lämpliga skyddsnivåer. Klassificering innebär även att organisationen kan prioritera underhållsinsatser, fördela resurser effektivt och fatta välgrundade beslut om strategier för tillgångsförvaltning.

Princip 4: Förteckning över tillgångar

När samtliga informationstillgångar och IKT-tillgångar har identifierats, kartlagts, tilldelats ägare och klassificerats bör en förteckning över dessa tillgångar upprätthållas. Förteckningen över tillgångar bör vara korrekt, uppdaterad, konsistent och överensstämma med övriga register i syfte att upprätthålla tillgångarnas skyddsbehov och tydliggöra ägarskap.

Därutöver bör förteckningen över IKT-tillgångar:

- lagra konfigurationen av IKT-tillgångar samt länkar och inbördes beroenden mellan olika IKT-tillgångar för att möjliggöra en korrekt konfigurationshantering och förändringsledning,[22] samt
- vara tillräckligt detaljerad för att möjliggöra snabb identifiering av en IKT-tillgång och dess lokalisering, säkerhetsklassificering och ägarskap. Inbördes beroenden mellan olika tillgångar bör dokumenteras som hjälp vid hantering av säkerhetsincidenter och operativa incidenter, bland annat it-attacker.[23]

Användning av särskild programvara för tillgångshantering (*eng: Asset Management Software*) kan underlätta dokumentation och hantering av organisationens samtliga tillgångar, samt efterlevnad av företagets säkerhetspolicys, lagkrav, regulatoriska krav och tillsynskrav. Denna typ av programvara gör det möjligt att hålla förteckningen över tillgångar uppdaterad över tid och därigenom optimera utnyttjande och kostnader för underhåll och säkerhet.

Att ha en uppdaterad och fullständig förteckning av sina tillgångar är grundläggande för att kunna implementera och övervaka nödvändiga säkerhetsåtgärder och kontroller.[24] Därutöver bör kontroller införas så att nya tillgångar identifieras, kartläggs och förs in i tillgångförteckningen när ny information skapas eller vid anskaffning av IKT-tillgångar (se vidare princip 5).

Princip 5: Hantering av tillgångars livscykel

Varje tillgång i organisationen har en livscykel. Denna livscykel skiljer sig något beroende på typ av tillgång. Livscykelhantering innebär en strategisk och systematisk process för att hantera tillgångar från början till slut. Aktörer inom finanssektorn bör utveckla och införa en tydlig process för informationstillgångars och IKT-tillgångars livscykelhantering. Även säkerheten

---

[22] *EBA (2019). Guidelines on ICT and Security Risk Management (EBA/GL/2019/04), avsnitt 53.*

[23] *EBA (2019) Guidelines on ICT and Security Risk Management (EBA/GL/2019/04), avsnitt 54. EIOPA (2020) Guidelines on information and communication technology security and governance (EIOPA-BoS-20/600), avsnitt 44.*

[24] *Deane & Kraus, 2021. The Official (ISC)² CISSP CBK Reference.*

måste upprätthållas genom hela livscykeln. Det innefattar att informationstillgångarna skyddas och IKT-tillgångarna säkras från nya hot och sårbarheter, samt att risker identifieras och hanteras under hela livscykeln.

Hantering av informationstillgångars livscykel (*eng: Information Lifecycle Management – ILM*) omfattar strategier, processer och verktyg i syfte att upprätthålla en centraliserad styrning (inklusive master data-hantering) och uppfylla regulatoriska krav, exempelvis inom dataskydd (GDPR). ILM skapar de förutsättningar som krävs för att kunna upprätthålla informationens skyddsvärden genom hela livscykeln, även när informationen förändras (och därigenom klassificeringen av informationen). Detta uppnås genom tydliga hanteringsregler för varje fas genom livscykeln. Hanteringsreglerna varierar beroende på hur informationen har klassificerats. Informationstillgångars livscykel innefattar följande faser:

- ***Skapande*:** Organisationen skapar och genererar kontinuerligt ny information, antingen manuellt eller automatiskt.

- ***Lagring:*** All information som skapas, används eller förändras måste lagras på ett säkert sätt.

- ***Användning:*** Användare i organisationen läser, granskar, ändrar eller på annat sätt manipulerar informationen. Information kan även processas automatiskt.

- ***Delning:*** Informationen delas till användare inom eller utanför organisationen. Vid delning måste rätt säkerhetsåtgärder användas, exempelvis kryptering.

- ***Arkivering:*** Information behöver arkiveras av regulatoriska skäl eller för framtida bruk.

- ***Radering:*** Överflödig information bör raderas då den kan utgöra riskexponering för obehörig åtkomst samt bidra till onödiga kostnader för lagring.

Hantering av IKT-tillgångars livscykel (*eng: Asset Lifecycle Management – ALM*) omfattar strategier, processer och verktyg i syfte att upprätthålla drift, säkerhet och kostnadskontroll hos dessa tillgångar under hela dess livstid. Användning av ALM är avgörande för att maximera värdet av IKT-investeringar, säkerställa att tekniska resurser matchar organisationens nuvarande och framtida behov samt uppfyller regulatoriska krav inom sektorn. ALM hjälper organisationen att hitta potentiella problem och förbättringsområden hos enskilda IKT-tillgångar, samt fatta välgrundade beslut gällande underhåll, reparationer, uppgraderingar och utbyte. IKT-tillgångars livscykel innefattar följande faser:

- ***Planering:*** Inkluderar identifiering av krav, riskanalys, selektering av lämpliga tillgångar samt bedömning av finansiella och operationella förutsättningar.

- ***Anskaffning:*** Inköp eller leasing av tillgångar, vilket inkluderar avtal för att uppfylla samtliga kravställningar för drift, underhåll och säkerhet.

- ***Utrullning:*** Installation, konfiguration och driftsättning av tillgångar i syfte att dessa fungerar som förväntat och är integrerade med organisationens system och processer.

- ***Användning:*** Omfattar den dagliga användningen av tillgångar för att utföra dess avsedda funktioner och uppfylla organisationens operativa behov. Regler måste finnas för tillåten användning i syfte att tillgångarna skyddas, används och hanteras på lämpligt sätt. Processer måste finnas vid återlämnande av tillgångar då anställning, uppdrag eller avtal ändras eller upphör.

- ***Underhåll:*** Löpande underhåll, reparationer, uppgraderingar och utbyte av tillgångar för att säkerställa dess tillförlitlighet, tillgänglighet och säkerhet samtidigt som driftstopp och kostnader minimeras.

- ***Avveckling:*** Avyttring, försäljning eller avaktivering av tillgångar när dessa inte längre behövs eller har nått slutet av sin nyttjandeperiod.

Processen för livscykelhantering bör stöttas med kontroller som möjliggör identifiering och kartläggning av IKT-tillgångar vid till exempel anskaffning. Kontrollerna kan även tillse att tillgångsförteckningen hålls uppdaterad vid till exempel avveckling av en IKT-tillgång.

Princip 6: Riskhantering av tillgångar

Organisationen bör genomföra regelbundna riskbedömningar i syfte att utvärdera potentiella hot mot organisationens informationstillgångar och IKT-tillgångar med hänsyn till faktorer som informationens känslighet, sårbarheter i it-miljön, potentiell inverkan av dataintrång men även medarbetarnas utbildning och kunskap inom området. Den sammanvägda bedömningen av risker underlättar för organisationen att besluta om lämpliga informationssäkerhetsstrategier och skyddsnivåer för organisationens tillgångar.

Riskhantering av tillgångar är avgörande för att upprätthålla tillgångarnas prestanda och erhålla rätt skydd. Följande aktiviteter är centrala i riskhanteringsprocessen:

- ***Analysera sårbarheter:*** Underrättelser om cyberhot som mottagits från forum och källor för informationsutbyte bör användas. Sårbarhetsanalys och penetrationstester är exempel på metoder för att identifiera och analysera sårbarheter.

- ***Hotmodellering:*** Interna och externa hot bör identifieras och analyseras genom exempelvis hotmodellering och scenarioanalys.

- ***Riskidentifiering:*** Riskscenarier bör beskrivas utifrån analyserade hot och sårbarheter.

- ***Konsekvensanalys:*** Den potentiella konsekvensen av olika riskscenarier bör analyseras med hänsyn till faktorer som dataförlust, ekonomisk förlust, minskat förtroende, avbrott i verksamheten, samt legala och regulatoriska krav. En genomförd konsekvensanalys i enlighet med *FSPOS Vägledning för kontinuitetshantering*[25] underlättar för att förstå påverkan vid dataförlust och avbrott i verksamheten.

- ***Riskvärdering och prioritering:*** En värdering bör göras för varje identifierad risk baserat på dess sannolikhet och konsekvens. Värderingen kan visualiseras i en riskmatris och

[25] *FSPOS (2024). Vägledning för kontinuitetshantering, v. 6.0*

syftar till att bedöma om en risk kan accepteras eller måste hanteras. Riskvärdering hjälper även till att prioritera bland åtgärderna. De allvarligaste riskerna (hög sannolikhet och/eller hög konsekvens) bör åtgärdas först.

- ***Riskhantering och strategier:*** Lämpliga strategier för hantering av risker bör beslutas. Dessa ligger till grund för att införa lämpliga säkerhetsåtgärder och kontroller[26] i syfte att skydda tillgångarna mot identifierade hot och sårbarheter.

- ***Identifiering av riskägare:*** En riskägare bör utses till varje risk med ansvar för att risken hanteras och säkerhetsåtgärder införs.

- ***Dokumentation och rapportering:*** Ett riskregister som dokumenterar alla identifierade risker och dess hantering bör upprätthållas. Resultaten av riskbedömningen bör rapporteras regelbundet till relevanta intressenter, inklusive ledningsgrupp och informations- och cybersäkerhetsteam.

- ***Granska och uppdatera:*** Effektiviteten av införda säkerhetsåtgärder bör övervakas kontinuerligt. Riskbedömningen bör granskas och uppdateras regelbundet för att återspegla förändringar i hotbilden, affärsprocesserna och it-miljön.

[26] *Flertalet kontrollramverk (ISO 27001, NIST SP 800-53, NIST SP 1800-5, CIS CSC, ISF SoGP, m.fl.) innehåller lämpliga kontroller för tillgångshantering. Några exempel på sådana kontroller är hantering av tillgångars åtkomsträttigheter, övervakning av tillgångar och hantering av incidenter och återställning.*

5 Avslutande reflektion

Denna promemoria har analyserat regulatoriska krav på tillgångsförvaltning inom den finansiella sektorn. Det är tydligt att det försämrade säkerhetspolitiska läget tillsammans med en alltmer komplex digital väld, där finansiella system och aktörer är starkt sammankopplade, ökar både kraven och förväntningarna på finansiella aktörers förmåga att förebygga och hantera incidenter och kriser.

Centralt i de krav som ställs på aktörer inom finansiell sektor är att de förväntas ha kontroll över de risker som är förknippade med verksamheten. För att uppnå kontroll över risk måste en aktör ha god kännedom om sin verksamhet och vad den utgörs av. Har aktören inte denna kännedom ökar sannolikheten att riskanalysen blir ofullständig och att den efterföljande riskhanteringen blir bristfällig. Systematisk tillgångsförvaltning blir således grundläggande för riskhanterings-processen och införandet av säkerhetsåtgärder. Eftersom finansiell verksamhet är beroende av informations- och IKT-tillgångar är förvaltningen av dessa väsentlig för aktörer inom sektorn.

Tillgångsförvaltning innebär ett arbetssätt för en systematisk hantering av tillgångar genom hela deras livscykel. De principer för tillgångförvaltning som presenteras i denna promemoria ger en aktör möjlighet att närma sig systematisk tillgångsförvaltning av informations- och IKT-tillgångar baserat på krav och riktlinjer inom sektorn. Det finns flera ramverk och standarder för tillgångsförvaltning, vilka många gånger kompletteras med ramverk för säkerhetsåtgärder och kontroller. Säkerhetsåtgärder och kontroller är nödvändiga för att skydda verksamhetens tillgångar, och därmed verksamheten som sådan, varför arbetet med att implementera dessa inte ska förbises.

Tillgångsförvaltning beskrivs generellt inte som en del av beredskapsarbetet i en organisation; dess viktiga bidrag till processer som bland annat risk-, kris och kontinuitetshantering påvisar dock tillgångsförvaltningens relevans för beredskapsarbetet och byggandet av en motståndskraftig organisation. I en tid där hotbilden mot den finansiella sektorn ökar från flera håll behöver sektorns aktörer således arbeta med systematisk tillgångsförvaltning av alla sina tillgångar, bland dem sina informations- och IKT-tillgångar.

Referenser

Deane & Kraus, 2021. *The Official (ISC)² CISSP CBK Reference*, (Cissp: Certified Information Systems Security Professional) 6th Edition

European Banking Authority, EBA (2019). *Guidelines on ICT and Security Risk Management* (EBA/GL/2019/04)

European Insurance and Occupational Pensions Authority, EIOPA (2020). *Guidelines on information and communication technology security and governance* (EIOPA-BoS-20/600)

European Insurance and Occupational Pensions Authority, EIOPA (2020). *Guidelines on outsourcing to cloud service providers* (EIOPA-BoS-20-002)

European Securities and Markets Authority, ESMA (2021). *Guidelines On outsourcing to cloud service providers* (ESMA50-164-4285)

Finansinspektionen (2022). *Förstärkt digital motståndskraft hos företag i den finansiella sektorn.* Dnr 22-10015

FSPOS (2024). *Vägledning för kontinuitetshantering, v. 6.0*

Förordning 2022/2554 (DORA-förordningen). *Europaparlamentets och rådets förordning (eu) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn*.

ISO 55000:2024 (2024). *Asset management — Overview, principles and terminology*

Institute of Asset Management (2024). *Asset management – an anatomy*, version 4

International Organization for Standardization, ISO (2024). *Illustration* Hämtad: 2024-08-20

MSB (2024). *Metodstödet för systematiskt informationssäkerhetsarbete, Klassning av information.* Hämtad: 2024-11-19

MSB (2012). *Vägledning för processorienterad informationskartläggning*, Publ.nr MSB493

PMFS 2022:1 *Säkerhetspolisens föreskrifter om säkerhetsskydd*

SFS 2004:297 *Lag om bank och finansieringsrörelse*

Svenska Bankföreningen (2024). *Hotbildsbedömning för Sveriges banker*

APPENDIX A – Krav, riktlinjer och standarder

Lagstiftning	Kort beskrivning	Relevans för tillgångsförvaltning
Lagen (2004:297) om bank och finansieringsrörelse	Denna lag innehåller bestämmelser för att driva bank- och finansieringsrörelse.	Kraven som ställs på informations- och cybersäkerhet utgår från 6 kap. 2 § Riskhantering, som säger att ”Ett kreditinstitut ska identifiera, mäta, styra, internt rapportera och ha kontroll över de risker som dess rörelse är förknippad med.”
Försäkringsrörelselag (2010:2043)	Försäkringsrörelselagen innehåller regler om bildandet av, verksamheten i och tillsynen över svenska försäkringsföretag.	I försäkringsrörelselagen ställs krav på ett försäkringsföretags system för riskhantering. Systemet ska bland annat omfatta operativa risker (10 kap. 7 §).
Säkerhetsskyddslag (2028:585)	Denna lag innehåller krav på åtgärder som syftar till att skydda uppgifter som är av betydelse för Sveriges säkerhet.	Krav ställs på informationssäkerhet i syfte att säkerhetsskyddsklassificerade uppgifter ska skyddas samt förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet (2 kap. 2 §).
Förordning/direktiv	**Kort beskrivning**	**Relevans för tillgångsförvaltning**
Digital Operational Resilience Act (DORA)	En EU-förordning för effektiv och övergripande hantering av digitala risker i syfte att stärka den finansiella sektorns motståndskraft mot cyberhot.	I DORA ställs krav på finansiella entiteters tillgångsförvaltning, bland annat i kapitel 2 artikel 8(4), där det anges att finansiella entiteter ska ”identifiera alla informationstillgångar och IKT-tillgångar, inbegripet sådana på fjärrplatser, nätverksresurser och maskinvaruutrustning, och kartlägga de som anses vara kritiska. De ska kartlägga informationstillgångarnas och IKT-tillgångarnas konfiguration samt länkarna och det ömsesidiga beroendet mellan de olika informationstillgångarna och IKT-tillgångarna.”
Dataskyddsförordningen (GDPR)	GDPR syftar till att harmonisera skyddet av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter.	I GDPR avsnitt 2 artikel 32 kravställs bland annat förmågan att fortlöpande säkerställa personuppgifters konfidentialitet, riktighet och tillgänglighet samt motståndskraften hos de system och tjänster som behandlar personuppgifter.
Payment Services Directive (PSD2)	PSD2 är EU:s andra betaltjänstdirektiv och reglerar konton och betalningar för både företag och privatpersoner.	I PSD2 artikel 95(1) ställs krav på att betaltjänstleverantörerna inrättar en ram för att ”hantera operativa risker och säkerhetsrisker, med anknytning till de betaltjänster som de tillhandahåller. Som en del av denna ram ska betaltjänstleverantörerna fastställa och upprätthålla effektiva incidenthanteringsförfaranden, inbegripet för upptäckt och klassificering av allvarliga operativa incidenter och säkerhetsincidenter”.

Föreskrift	Kort beskrivning	Relevans för tillgångsförvaltning
Föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut* (FFFS 2014:1) **ny version är på remiss och väntas antas i januari 2025*	Föreskriften innehåller bestämmelser om hur ett företag ska genomföra styrning, riskhantering och kontroll.	FFFS 2014:1 kravställer bland annat att företag ska ha ändamålsenliga it-system och rutiner för att skydda konfidentialitet, riktighet och tillgänglighet i sin information (2 kap. 2 §) samt ramverk för riskhantering (5 kap. 1 §).
Föreskrifter och allmänna råd om hantering av operativa risker* (FFFS 2014:4) **ny version är på remiss och väntas antas i januari 2025*	Föreskriften innehåller bestämmelser om hur ett företag ska hantera sina operativa risker.	FFFS 2014:4 kravställer bland annat att företag i sitt säkerhetsarbete ska identifiera vilka tillgångar och värden som ska skyddas (5 kap. 7 §). Föreskriften hänvisar till FFFS 2014:5 för bestämmelser om informationssäkerhet samt hantering av it-system.
Föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem** (FFFS 2014:5) ***kommer utgå i januari 2025*	Föreskriften innehåller bestämmelser om hur ett företag ska hantera informationssäkerhet, it-verksamhet och insättningssystem.	FFFS 2014:5 kravställer bland annat att företag ska arbeta strukturerat och metodiskt med informationssäkerhet genom att använda sig av ett ledningssystem (2 kap. 1 §). Föreskriften kravställer även att företag ska se till att dess it-system är tillräckligt säkra i förhållande till arten hos den information som hanteras i systemen (3 kap. 1 §), samt att det ska finnas dokumentation över varje enskilt system som är av betydelse för verksamheten (3 kap. 5 §).
Riksbankens föreskrifter och allmänna råd om företag av särskild betydelse för genomförandet av betalningar under fredstida krissituationer och vid höjd beredskap RBFS 2023:3	Föreskriften innehåller bestämmelser om hur verksamheter som är av särskild betydelse för genomförandet av betalningar under fredstida krissituationer och vid höjd beredskap ska planera och förbereda samt utbilda och öva.	RBFS 2023:3 kravställer att företagets planering och förberedelse ska säkerställa att företaget har tillgång till den informationsteknik och information som behövs för att upprätthålla verksamheten (4 §), under fredstida krissituationer och vid höjd beredskap.
Riktlinje	**Kort beskrivning**	**Relevans för tillgångsförvaltning**
EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04)	Riktlinjerna innehåller krav på informationssäkerhet, inklusive cybersäkerhet, i den mån informationen förvaras i it-system.	Riktlinjerna ställer krav på att kartlägga informationstillgångar ”som stödjer finansinstitutets verksamhetsfunktioner och stödprocesser såsom IKT-system, personal, uppdragstagare och tredje parter samt beroenden av andra interna och externa system och processer” (avsnitt 16).

		Identifierade informationstillgångar ska klassificeras med avseende på kritikalitet (avsnitt 17). Vid klassificering ska hänsyn tas till konfidentialitets-, integritets- och tillgänglighetskraven. Det ska även finnas ett tydligt tilldelat ansvar för informationstillgångarna (avsnitt 18). Vidare ställs krav på att ”upprätthålla en uppdaterad förteckning över sina IKT-tillgångar (bl.a. IKT-system, nätenheter, databaser osv.). Förteckningen över IKT-tillgångar ska lagra konfigurationen av IKT-tillgångar samt länkar och inbördes beroenden mellan olika IKT-tillgångar för att möjliggöra en korrekt konfigurerings- och ändringshanteringsprocess” (avsnitt 53). ”Förteckningen över IKT-tillgångar ska vara tillräckligt detaljerad för att möjliggöra snabb identifiering av en IKT-tillgång och dess lokalisering, säkerhetsklassificering och ägarskap. Inbördes beroenden mellan olika tillgångar bör dokumenteras som hjälp vid hantering av säkerhetsincidenter och operativa incidenter, bl.a. IT-attacker” (avsnitt 54). Krav ställs även på att ”övervaka och hantera livscyklerna för IKT-tillgångar för att säkerställa att de även fortsättningsvis uppfyller och stödjer verksamhetskraven och riskhanteringskraven”. Övervakningen syftar även till att avgöra huruvida IKT-tillgångar stöds av externa eller interna leverantörer och utvecklare, samt ”huruvida alla relevanta fixar och uppgraderingar tillämpas med utgångspunkt i dokumenterade processer. Risker som härrör från föråldrade eller ickestödda IKT-tillgångar bör bedömas och genomgå riskreducering” (avsnitt 55).
EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)	Riktlinjerna innehåller krav på interna styrningsarrangemang och riskhantering vid utkontraktering.	Riktlinjerna ställer krav på att bedöma hur utkontrakteringslösningar potentiellt påverkar den operativa risken (avsnitt 64). Relevanta funktioner och därmed förknippade uppgifter och system ska definieras och klassificeras vad gäller känslighet och de säkerhetsåtgärder som krävs, i syfte att kunna bedöma risker och besluta om en lämplig skyddsnivå (avsnitt 68).
EIOPA Guidelines on information and communication technology security and governance (EIOPA-BoS-20/600)	Riktlinjerna innehåller krav för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik.	Riktlinjerna ställer krav på att ”göra och regelbundet uppdatera en kartläggning av sina affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar) för att identifiera deras betydelse och ömsesidiga beroendeförhållanden beträffande IKT-risker och säkerhetsrisker” (avsnitt 17a). Identifierade tillgångar (t.ex. informationstillgångar och IKT-tillgångar) ska klassificeras utifrån kritikalitet, skyddskraven för konfidentialitet, integritet och tillgänglighet ska bedömas, samt tillgångsägare ska identifieras (avsnitt 17b). Vidare ställs krav på att ha en uppdaterad förteckning över sina IKT-tillgångar. ”Förteckningen över IKT-tillgångar bör vara tillräckligt detaljerad för att möjliggöra

		snabb identifiering av en IKT-tillgång och dess lokalisering, säkerhetsklassificering och äganderätt" (avsnitt 44). Krav ställs även på att övervaka och hantera livscykeln för IKT-tillgångar för att säkerställa att de uppfyller och stöder verksamhetskraven och riskhanteringskraven. Det ska kontrolleras att "IKT-tillgångarna stöds av deras leverantörer eller interna utvecklare och att alla relevanta fixar och uppgraderingar tillämpas med utgångspunkt i en dokumenterad process. De risker som härrör från föråldrade eller icke-stödda IKT-tillgångar bör bedömas och genomgå riskreducering. Avvecklade IKT-tillgångar bör bearbetas och bortskaffas på ett säkert sätt" (avsnitt 45).
EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002)	Riktlinjerna innehåller krav för uppdragsavtal med molntjänstleverantörer.	Riktlinjerna ställer krav på att bedöma hur utkontrakteringslösningar potentiellt påverkar den operativa risken (avsnitt 30). Relevanta funktioner och därmed förknippade uppgifter och system ska definieras och klassificeras vad gäller känslighet och de säkerhetsåtgärder som krävs, i syfte att kunna bedöma risker och besluta om en lämplig skyddsnivå (avsnitt 31b).
ESMA Guidelines On outsourcing to cloud service providers (ESMA50-164-4285)	Riktlinjerna innehåller krav för uppdragsavtal med molntjänstleverantörer.	Riktlinjerna ställer krav på att strategier för utkontraktering av molntjänster är i linje med bland annat verksamhetens strategier för IKT och riskhanteringsprocess, inklusive hantering av IKT, informationssäkerhet och operativa risker (avsnitt 12). Riktlinjen ställer även krav på hur avtal med molntjänstleverantörer bör utformas med hänsyn till bland annat datalokalisering, informationssäkerhet, personuppgifter samt incident-, kris- och kontinuitetshantering (avsnitt 28).
CPMI-IOSCO Principles for financial market infrastructures (PFMI)	Riktlinjerna fastställer 24 principer som måste följas av alla FMI:er.	Tillgångsförvaltning av informations- och IKT-tillgångar kravställs genom riktlinjerna för riskhantering och informationssäkerhet. FMI:er ska ha ett övergripande ramverk för riskhantering (princip 3), robusta system för att hantera och minimera operationell risk (princip 17) genom att säkerställa användning av lämpliga system, policys, processer, och kontroller liksom systematiskt arbete med kontinuitetshantering.
CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure	Dessa riktlinjer är tillägg till PFMI avseende cyberresiliens.	Riktlinjen kravställer förvaltning av informationstillgångar med utgångspunkt i att en stark cyberresiliens är avhängig kunskap om tillgångarna, deras processer, beroenden och system. Informationstillgångar och relaterade tillgångar ska identifieras och klassificeras i en logg som regelbundet ska granskas och uppdateras (3.2). Utöver detta ska även beroenden ska identifieras (3.3). Riktlinjen lägger även emfas på att cyberresiliens är beroende av effektiva säkerhetskontroller och system, varför krav ställs att FMI:er konsekvent ska upprätthålla en stark ICT-kontrollmiljö (4.2). Utöver detta kravställs att kris- och kontinuitetsplaner stödjer skydd, och om behov återupprättande, av tillgångars integritet, tillgänglighet och konfidentialitet (6.2).

Ramverk/standard	Kort beskrivning	Relevans för tillgångsförvaltning
NIST Cybersecurity Framework (CSF)	NIST CSF är en uppsättning krav för att hjälpa organisationer att minska sina cybersäkerhetsrisker genom att bättre upptäcka, reagera på och förhindra cyberattacker.	NIST CSF ställer krav på tillgångsförvaltning i steget för identifiering, där organisationen förväntas inventera fysiska system och hårdvara (ID.AM-1), mjukvaruplattformar och applikationer (ID.AM-2), kartlägga kommunikation och dataflöden (ID.AM-3), katalogisera externa informationssystem (ID.AM-4), prioritera tillgångar (ID.AM-5), samt utse ägandeskap och ansvar (ID.AM-6).
NIST Special Publication 800-53	NIST SP 800-53 är en informationssäkerhetsstandard med säkerhetskontroller för informationssystem.	NIST SP 800-53 innehåller detaljerade säkerhetskontroller för tillgångsförvaltning i syfte att uppfylla kraven enligt NIST CSF.
CIS Critical Security Controls v.8 (CIS CSC)	CIS CSC är en uppsättning av bästa praxis för att skydda en organisation från cyberattacker.	Ramverket introducerar 18 kritiska kontroller, med tillhörande säkerhetsåtgärder, för ökad cybersäkerhet. CSC tar sin utgångpunkt i inventering av hårdvaru- och mjukvarutillgångar (kontroll 1 och 2), framtagande av processer och teknologi för att identifiera, klassificera och skydda information och data (kontroll 3), samt säker konfigurering av hårdvaru- och mjukvarutillgångar säkerställas (kontroll 4). Ramverket innefattar även kontroller som åtkomstkontroll (kontroll 6), kontinuerlig hantering av sårbarheter relaterade (kontroll 7) samt incidenthantering (kontroll 17).
PCI DSS Payment Card Industry Data Security Standard	PCI DSS är en säkerhetsstandard som syftar till att skydda betalningskortsdata.	Standarden kravställer tillgångsförvaltning, bland annat genom inventering och klassificering av tillgångar (2.4) samt åtkomstkontroll (7.1/8) och skydd av kritiska informationstillgångar och IKT-tillgångar (6.1) samt kortdata (3.4).
ISF Standard of Good Practice for Information Security (ISF SoGP)	Standard of Good Practice for Information Security är en standard för informationssäkerhet.	Standarden tillhandahåller ett ramverk med för att upprätthålla och förbättra informationssäkerhet. Standarden omfattar informationssäkerhetskontroller och informationsriskrelaterad vägledning samt god praxis som täcker tillgångsförvaltning av informationstillgångar i form av krav på bland annat inventering, klassificering, skydd och livscykelhantering av informationstillgångar.
ISO 27000-serien Informationssäkerhet	ISO 27000-serien är en standard för informationssäkerhet, cybersäkerhet och dataskydd.	Standarden tillhandahåller ett ramverk för att etablera, implementera, underhålla och ständigt förbättra ett ledningssystem för informationssäkerhet. Ett ledningssystem för informationssäkerhet implementerat enligt denna standard är ett verktyg för riskhantering, cyberresiliens och operationell excellens.
ISO 55000-serien Tillgångsförvaltning	ISO 55000-serien är en standard för tillgångshantering inom alla typer av organisationer, för alla typer av tillgångar.	Standarden tillhandahåller ett ramverk för att etablera, implementera, underhålla och förbättra ett tillgångshanteringssystem. Standarden täcker olika aspekter, inklusive tillgångsförvaltningspolicy, -strategi, mål och process för tillgångsförvaltning.

ITIL (Information Technology Infrastructure Library)	ITIL är ett ramverk för best practice inom it-tjänstehantering (ITSM) och it-tillgångsförvaltning (ITAM).	Ramverket tillhandahåller bland annat en vägledning för it-tillgångsförvaltning med fokus på att hantera och optimera användningen av en organisations it-tillgångar, detta inkluderar bland annat kartläggning av tillgångar och risk- och livscykelhantering. It-tillgångsförvaltningen integreras inom ITIL med andra processer såsom incidenthantering, förändringsledning och konfigurationshantering.