UPPSALA UNIVERSITET

UFV 2021/1794

Informationssäkerhetsarbete

Internrevisionsrapport

Fastställd av Konsistoriet 2021-12-14

Innehållsförteckning

Sammanfattning

Internrevisionen har granskat om informationssäkerhetsarbetet inom universitetet bedrivs systematiskt och riskbaserat och i enlighet med interna styrdokument och krav som Myndigheten för samhällsskydd och beredskap (MSB) via föreskrifter ställer på statliga myndigheter. Granskningen har särskilt inriktats mot att undersöka hur arbetet är utformat och hur det styrs, följs upp och rapporteras. Därutöver har informationssäkerhetsarbete på fyra institutioner undersökts genom granskning av tillämpningen av rutinerna för informationsklassificering och riskhantering.

Internrevisionens sammanfattande bedömning av *utformningen och styrningen av informationssäkerhetsarbetet* är att det finns ett förbättringsbehov rörande systematik, effektivitet och följsamhet mot regler och rutiner i flera av de delar av arbetet som granskats, bl.a. när det gäller strukturerad och systematisk planering och samordning samt stöd. Det finns även behov av att ytterligare förtydliga ansvar och/eller arbetsuppgifter för vissa roller i informationssäkerhetsarbetet.

Internrevisionen ser vidare stora förbättringsbehov vad avser *uppföljning, utvärdering och rapportering av informationssäkerhetsarbetet* (även i relation till kraven i MSB:s föreskrifter). Exempelvis uppföljning av om arbetet svarar mot ledningens målsättning och utvärdering av om regler, rutiner och arbetssätt är implementerade och tillämpas på avsett sätt inom universitetet.

Även beträffande systematiken i *genomförandet av informationssäkerhetsarbete vid institution* bedömer internrevisionen att ett stort förbättringsbehov föreligger (också här i relation till MSB:s krav). Detta gällande att universitetet som myndighet ska säkerställa att den information som universitetet ansvarar för informationsklassificeras och riskbedöms och att skydd utformas för den. Från granskning av fyra institutioner framkommer att informationsklassificering och riskhantering genomförs i olika omfattning med varierande systematik. Ingen av de granskade institutionerna har rutiner som säkerställer en systematisk klassificering av de informationsmängder som de är informationsägare av. Universitetets rutiner bedöms således inte vara tillfredsställande implementerade.

Trots det hittills genomförda arbetet med informationsklassificering och riskbedömning vid institutionerna och trots de stödjande insatser som genomförts för att underlätta för institutioner i arbetet, bedömer internrevisionen att det kvarstår ett omfattande arbete innan följsamhet i förhållande till MSB:s krav på att information som universitetet äger ska vara informationsklassificerad och riskbedömd, kan anses vara uppnått.

Då granskningsresultatet visar på brister lämnar internrevisionen ett antal rekommendationer till rektor, i syfte att förbättra den interna styrningen och kontrollen och för att informationssäkerhetsarbetet ska kunna uppnå en högre grad av systematik, effektivitet och följsamhet med interna styrdokument och MSB:s föreskrifter.

1 Bakgrund

Informationssäkerhetsarbete syftar till att säkerställa att informationstillgångarna i verksamheten skyddas. Säker hantering av information är av vikt vid utförande av all verksamhet både inom universitetet och vid andra organisationer. Informationssäkerhetsarbete är en del av det dagliga arbetet, men i statlig verksamhet finns krav på att det ska utföras systematiskt, ha sin grund i identifierade risker och dokumenteras.[1]

Ansvar för informationssäkerhetsarbetet följer inom universitetet det delegerade verksamhetsansvaret, vilket innebär att den som är ansvarig för en verksamhet också är ansvarig för dess informationssäkerhetsarbete. Prefekten är således ansvarig för informationssäkerheten vid sin institution. Säkerhetschefen, som tillika är universitetets informationssäkerhetschef, samordnar universitetets informationssäkerhetsarbete bl.a. med hjälp av Enheten för informationssäkerhet, som arbetar stödjande och rådgivande gentemot institutioner och övriga delar av organisationen.

För att uppnå säker hantering av information ska, som en del av det systematiska och riskbaserade informationssäkerhetsarbetet, informationsklassificering och riskbedömning utföras. Detta görs genom att bedöma informationens skyddsvärde utifrån säkerhetsaspekterna *konfidentialitet* (skydd mot obehörig åtkomst), *riktighet* (skydd mot obehöriga förändringar) *och tillgänglighet* (tillgänglig för behöriga när den ska användas). Därefter analyseras hur informationen ska komma att hanteras och om system och andra informationstillgångar lever upp till en tillräcklig nivå av säkerhet för informationen.

Informationsklassificering och riskbedömning är grundläggande aktiviteter i ett systematiskt och riskbaserat informationssäkerhetsarbete, och en förutsättning för att kunna utforma en skyddsnivå för informationen som är väl avvägd i förhållande till informationens betydelse för verksamheten. I enlighet med revisionsplanen genomför internrevisionen en granskning i syfte att undersöka om universitetets informationssäkerhetsarbete bedrivs på ett systematiskt och riskbaserat sätt.

2 Syfte och omfattning

Det övergripande syftet med granskningen är att undersöka och bedöma om den interna styrningen och kontrollen är betryggande vad avser universitetets informationssäkerhetsarbete. Granskningen har inriktats mot att bedöma om informationssäkerhetsarbetet inom universitetet bedrivs systematiskt och riskbaserat och i enlighet med interna och externa regelverk såsom MSB:s.[2]

[1] MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6). Definitioner: *Information/-mängd* innefattar all elektronisk, pappersbaserad, muntlig eller på annat sätt lagrad eller kommunicerad information (UFV 2018/211). *Informationstillgångar* omfattar såväl informationen som de resurser (system – hård-/mjukvara – och kommunikationslösningar) som används för att hantera informationen (UFV 2017/93). *Informationssäkerhet* avser säkerhet för informationstillgångar avseende bevarande av konfidentialitet, riktighet och tillgänglighet hos informationen (MSBFS 2020:6 §3).

[2] Enligt MSBFS 2020:6 4§ ska myndigheten bedriva ett *systematiskt* och *riskbaserat* informationssäkerhetsarbete med stöd av standarderna ISO 27001:2017 och 27002:2017 och enligt 6§ ska myndigheten säkerställa att informationssäkerhetsarbetet är

Granskningen fokuserar särskilt på följande områden:

- Utformning och styrning av informationssäkerhetsarbetet (regler & rutiner, ansvarsfördelning & målsättning samt kompetens & stöd)
- Genomförande av informationssäkerhetsarbetet (informationsklassificering och riskhantering)
- Uppföljning och rapportering av informationssäkerhetsarbetet (uppföljning & utvärdering samt rapporteringsrutiner)

Granskningen av genomförandet av informationssäkerhetsarbetet har inriktats på arbete som bedrivs vid institutioner. Vid granskningen av de övriga områdena – utformning och styrning samt uppföljning och rapportering – berörs främst det universitetsövergripande informationssäkerhetsarbetet. Informationssäkerhetsarbete som bedrivs inom ramen för de s.k. e-förvaltningsområdena och intendenturerna har inte granskats.

Granskningen utgår från krav som MSB via föreskrifter ställer på statliga myndigheters informationssäkerhetsarbete, d.v.s. informationssäkerhet i ett brett perspektiv, och har inte inriktats mot rutiner som avser informationstyper som regleras i särskilda regelverk såsom Dataskyddsförordning (GDPR) eller säkerhetsskyddslagstiftning. Granskningen omfattar inte heller IT-tekniska säkerhetsåtgärder i informationssystem eller rutiner/lösningar för hantering och lagring av forskningsdata.

Granskningen har genomförts genom dokumentstudier och intervjuer med prefekter och medarbetare inom forskning och administration vid fyra institutioner; Institutionen för cell- och molekylärbiologi, Institutionen för folkhälso- och vårdvetenskap, Institutionen för kemi – Ångström och Sociologiska institutionen.[3] Därutöver har universitetets säkerhetschef tillika informationssäkerhetschef samt chef och informationssäkerhetssamordnare vid Enheten för informationssäkerhet vid Säkerhetsavdelningen intervjuats. Även universitetets dataskydds-ombud vid Juridiska avdelningen, chefen för Avdelningen för universitetsgemensam IT (UIT) och chefen för Enheten för arkitektur och integration vid UIT har intervjuats. Företrädare för projektet FAIRdriktning vid Planeringsavdelningen har också bidragit med information.

2.1 Revisionsfrågor

För att uppnå syftet kommer följande revisionsfrågor att besvaras:

- Är universitetets informationssäkerhetsarbete utformat i enlighet med kraven i MSB:s föreskrifter, med fokus på regler & rutiner, ansvar & målsättning, kompetens & stöd samt uppföljning & rapportering?
- Tillämpas universitetets regler och rutiner för informationssäkerhetsarbete inom organisationen så att informationssäkerhetsarbetet vid institutioner och andra delar av organisationen bedrivs systematiskt och riskbaserat?

systematiskt och riskbaserat genom arbetssätten informationsklassning, riskbedömning, identifiera behov av säkerhetsåtgärder och utvärdera säkerhetsåtgärderna och vid behov anpassa skyddet.

[3] I urvalet av institutioner har en variation eftersträvats vad avser vetenskapsområdestillhörighet. Intervjuerna har i huvudsak genomförts under maj, juni och augusti 2021. Granskningen är genomförd av internrevisorerna Madelene Norsell (granskningsledare) och Pia Frölen.

- Vilken uppföljning och utvärdering gör universitetet av att regler och rutiner tillämpas och att informationssäkerhetsarbetet fungerar på avsett sätt inom organisationen?
- Finns rapporteringsrutiner som säkerställer att universitetsledningen får information om huruvida målsättningen med informationssäkerhetsarbetet nås och eventuella hinder för detta, t.ex. brister avseende om regler och rutiner tillämpas på avsett sätt?

2.2 Risker

Ett bristfälligt informationssäkerhetsarbete riskerar leda till att risker och hot mot universitetets information och informationstillgångar inte identifieras och hanteras. Detta kan i sin tur innebära negativa konsekvenser för bevarande av informationens konfidentialitet, riktighet och tillgänglighet. Om inte säkerhetsnivån är i överensstämmelse med informationens känslighet och betydelse för verksamheten kan det exempelvis få negativa konsekvenser såsom:

- Otillräckligt skydd av information och/eller informationstillgångar, med följden att information t.ex. känsliga personuppgifter, forskningsdata eller information med hög skyddsnivå, går förlorad, modifieras eller kommer obehöriga till del. [4]
- Störningar och avbrott i verksamheten så att utbildning, forskning och övrig verksamhet inte kan genomföras på ett effektivt och ändamålsenligt sätt.
- Att förtroendet för universitetets utbildning och forskning skadas.

2.3 Bedömningskriterier

Med bedömningskriterier avses de regler eller normer som bildar underlag för internrevisionens bedömningar och rekommendationer. Granskningen tar sin utgångspunkt i och bedömningar görs utifrån myndighetsförordningens krav om att verksamheten ska bedrivas på ett sätt så att bl.a. effektivitet, regelefterlevnad och god hushållning med medel uppnås samt högskoleförordningens krav på att det vid universitetet ska finnas en intern styrning och kontroll som fungerar på ett betryggande sätt. [5]

Bedömningar görs därutöver främst utifrån bl.a.:

MSBFS 2020:6 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (som baseras på standarderna ISO 27001:2017 och 27002:2017). [6]

Ledningssystem för informationssäkerhet (LIS), UFV 2017/651 (reviderade 2018-08-01).

Riktlinjer för säkerhetsarbetet vid Uppsala universitet UFV 2009/1929 (beslutade 2010-02-09).

Rutiner för informationssäkerhet vid Uppsala universitet UFV 2017/93 (reviderade 2021-03-29).

Rutiner för informationssäkerhet – riskhantering UFV 2018/211 (reviderade 2018-06-15).

Arbetsordning för universitetsförvaltningen vid Uppsala universitet UFV 2018/1183.

[4] Vid felaktig hantering av personuppgifter riskeras sanktionsavgifter.

[5] 3§ Myndighetsförordningen (2007:515) och 2 kap. 2§ högskoleförordningen (SFS 1993:100).

[6] MSBFS 2020:6 4§ Myndigheten ska bedriva informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav och SS-EN ISO/IEC 27002:2017 Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder eller motsvarande.

3 Informationssäkerhetsarbete vid universitetet

Universitetet är liksom andra organisationer beroende av information för att kunna utföra sin verksamhet och hanterar dagligen en mängd information inom utbildnings- och forskningsverksamheten. För att kunna skydda informationen och de informationssystem (hård- och mjukvara) och kommunikationslösningar som hanterar den, är ett effektivt och systematiskt informationssäkerhetsarbete betydelsefullt.

MSB ger, sedan 2009, ut föreskrifter med krav på hur statliga myndigheters informationssäkerhetsarbete ska utformas och bedrivas, och som universitetet har att förhålla sig till. Enligt kraven ska statliga myndigheters informationssäkerhetsarbete utföras systematiskt, ha sin grund i identifierade risker och dokumenteras. Universitetet har fastställt interna rutiner för informationssäkerhet baserade på MSB:s krav. Rutinerna syftar till att utgöra en grund för hur informationssäkerhetsarbetet vid universitetet ska utföras och anger säkerhetskrav som ställs på all behandling av information vid universitetet.

Information finns i olika former, t.ex. i digital och pappersbaserad form. Den förvaras, lagras och delas på olika sätt, t.ex. via molntjänster, på servrar, bärbara datorer, USB-minnen och externa hårddiskar. Ibland förvaras och lagras de ”fysiskt” i skrivbordslådor och hyllor på arbetsrum, i källarförråd eller andra förvaringslokaler. Vidare finns det information som är extra skyddsvärd, bl.a. information som omfattas av sekretess, innehåller känsliga personuppgifter, är licensskyddad eller verksamhetskritisk såsom t.ex. forskningsdata som samlats in över lång tid och/eller inte är möjlig att återskapa.

Vad gäller ansvaret för genomförande av informationssäkerhetsarbetet inom universitetet följer detta det delegerade verksamhetsansvaret, d.v.s. linjeorganisationen. Säkerhetsavdelningen ansvarar för universitetets systematiska informationssäkerhetsarbete och till säkerhetschefens ansvar hör t.ex. samordning, utveckling och uppföljning av arbetet, utformning och förvaltning av interna regelverk samt insatser för att stödja verksamheten inom området.

Informationssäkerhet är som beskrivits ovan ett brett arbetsområde och inkluderar även IT-säkerhet i form av arbete med att utforma tekniska säkerhetsåtgärder i t.ex. informationssystem, nätverk, kommunikationslösningar och annan infrastruktur som hanterar informationen. Inom Enheten för informationssäkerhet vid Säkerhetsavdelningen finns medarbetare som arbetar med båda inriktningarna. Granskningen fokuserar dock i det följande på de delar, av MSB:s föreskrifter om informationssäkerhet för statliga myndigheter, som avser utformning, styrning, genomförande, uppföljning och rapportering av informationssäkerhetsarbete, och inte på IT-tekniska säkerhetsåtgärder i informationssystem.

4 Iakttagelser och resultat från granskningen

I kapitel 4 redogörs för iakttagelser och bedömningar som gjorts under granskningen. [7] Rapporteringen är i huvudsak avvikelsebaserad vilket innebär att sådana iakttagelser som vi bedömer som brister eller risker beskrivs.

4.1 Utformning och styrning av informationssäkerhetsarbetet

Granskningen av utformning och styrning av informationssäkerhetsarbetet har inriktats mot områdena regler och rutiner, ansvarsfördelning och målsättning samt kompetens och stöd.

4.1.1 Regler och rutiner

Granskningen visar att universitetsövergripande regler, riktlinjer och rutiner för hur informationssäkerhetsarbetet ska bedrivas, inklusive en informationssäkerhetspolicy, finns upprättade. Styrdokumenten har dock upprättats över tid, vilket innebär att det finns diskrepans i ordalydelse och sakinnehåll mellan dokumenten.

Styrande dokument, i form av regler och riktlinjer, samt rutiner och arbetssätt är viktiga delar av den interna styrningen och kontrollen, för att tydliggöra hur informationssäkerhetsarbetet inom universitetet ska bedrivas och för att stödja och underlätta för de i verksamheten som ska genomföra arbetet.

Enligt MSB:s föreskrifter ska interna regler och arbetssätt finnas upprättade för informationssäkerhetsarbetet. Myndigheten ska säkerställa att det finns en informationssäkerhetspolicy, av vilken bl.a. ledningens målsättning med informationssäkerhetsarbetet ska framgå. [8]

I universitetets mål- och regelsamling och på medarbetarportalens sidor om informationssäkerhet, återfinns universitetsgemensamma regler, riktlinjer och rutiner, kopplat till informationssäkerhetsarbete och skydd av information och informationstillgångar. De tre övergripande styrdokumenten som är tänkta att styra informationssäkerhetsarbetet är:

- *Riktlinjer för säkerhetsarbete*
  Omfattar övergripande riktlinjer även för universitetets informationssäkerhetsarbete, och utgör tillsammans med ett antal riktlinjer och rutiner specifikt inriktade mot olika delar av informationssäkerhetsarbetet, grunden för utformningen och styrningen av arbetet med informationssäkerhet och riskhantering. [9]

[7] Iakttagelserna bygger huvudsakligen på uppgifter som inhämtats vid intervjuer och baseras därmed på de intervjuades beskrivningar av det egna arbetet och/eller institutionens/avdelningens rutiner för informationssäkerhetsarbetet.
[8] MSBFS 2020:6 5§.
[9] Riktlinjer för säkerhetsarbete, UFV 2009/1929. Utöver de styrdokument som nämns här i avsnittet, finns ett antal rutiner som relaterar till informationssäkerhetsområdet t.ex. Rutiner för informationssäkerhet – riskhantering UFV2018/211, Rutiner för säker informationshantering UFV 2018/668, Rutiner för anskaffning och drift av IT-system UFV 2020/2599, Rutiner för säker hantering av mobila enheter och portabla lagringsmedia UFV2018/1675, Rutin för hantering av behörigheter UFV 2018/1170, Rutin för lösenordshantering UFV 2013/1490.

- *Rutiner för informationssäkerhet*
  Utgör universitetets informationssäkerhetspolicy, som i linje med kraven i MSB:s föreskrifter bl.a. anger ledningens övergripande *målsättning* med informationssäkerhetsarbetet samt föreskriver att arbetet ska *omfatta all behandling av information vid universitetet* och *tydliggör ansvarsfördelning* för arbetet. [10]
- *Ledningssystem för informationssäkerhet (LIS)*
  Beskriver med utgångspunkt i MSB:s föreskrifter samt ISO-standarder hur informationssäkerhetsarbetet vid universitetet ska styras och utföras. [11]

Internrevisionen noterar att universitetets styrdokument för informationssäkerhetsarbetet är upprättade över tid (*Riktlinjer för säkerhetsarbetet* upprättade 2009/2010), vilket innebär att de i viss mån skiljer sig i ordalydelse och sakinnehåll mellan dokumenten. Detta gäller exempelvis beskrivning av säkerhetschefens ansvar och den övergripande målsättningen med informationssäkerhetsarbetet.

Under granskningen har internrevisionen noterat förbättringsbehov som institutioner har framfört under intervjuerna. Ett av dessa är behovet av att styrande och stödjande dokument men även informationsmaterial och löpande informationsgivning, t.ex. e-postutskick, översätts till engelska då det inte är ovanligt med engelskspråkiga medarbetare i t.ex. forskningsprojekten. Enligt Säkerhetsavdelningen har ett översättningsarbete initierats och är pågående. Internrevisionen noterar att vissa av styrdokumenten redan är översatta till engelska. [12] Ett annat utvecklingsbehov som lyfts fram vid institutionsintervju är att styrdokument, t.ex. rutiner och instruktioner, i högre grad bör utformas och struktureras utifrån ett användar-/målgruppsperspektiv för att uppnå bättre förankring inom organisationen. [13]

4.1.2 Ansvarsfördelning och målsättning

Granskningen visar att det finns ett behov av att ytterligare förtydliga ansvar och/eller arbetsuppgifter för vissa roller i informationssäkerhetsarbetet. Detta gäller informations-säkerhetssamordnarna, informationsägare samt den som är ”utsedd att leda och samordna” universitetets informationssäkerhetsarbete (säkerhetschefen). Därtill ser internrevisionen ett behov av att utifrån ledningens övergripande målsättning, formulera konkreta mål samt vidareutveckla rutiner för strukturerad och systematisk planering, samordning och uppföljning av universitetets informationssäkerhetsarbete.

[10] Rutiner för informationssäkerhet, UFV 2017/93, utgör, enligt dokumentet, universitetets informationssäkerhetspolicy. Enligt MSBFS 2020:6 5§ ska myndigheten säkerställa att det finns en informationssäkerhetspolicy där ledningens *målsättning* med och inriktning för informationssäkerhetsarbetet framgår”. Den ska även ”*tydliggöra* myndighetsledningens och den övriga organisationens *ansvar*, inklusive den eller de som utses att leda och samordna informationssäkerhetsarbetet, och informationssäkerhetsarbetet ska utformas så att det omfattar ”*all behandling av information* som myndigheten ansvarar för”.

[11] Ledningssystem för informationssäkerhet (LIS), UFV 2017/651.

[12] Styrdokumenten Ledningssystem för informationssäkerhet (LIS), Rutiner för informationssäkerhet samt en instruktion för hur informationsklassificering går till, är redan översatta till engelska.

[13] Det har framkommit synpunkter att styrande dokument, t.ex. rutiner och instruktioner som kräver åtgärder av chefer/medarbetare inom organisationen, inte alltid upplevs vara utformade på ett sätt som är användarvänligt och lätt att ta till sig. Det riskerar leda till brister i tillämpning av rutiner om t.ex. texten är svårbegriplig med facktermer och/eller om inte användar-/målgrupp som de vänder sig till framgår tydligt – inklusive vad man förväntas vidta för åtgärd, när och varför.

MSB:s föreskrifter ställer krav på hur statliga myndigheters informationssäkerhetsarbete ska utformas och styras. Som beskrivits tidigare ska ledningens målsättning med och inriktning för informationssäkerhetsarbetet framgå av informationssäkerhetspolicyn. Därutöver ska myndigheten tydliggöra myndighetsledningens och övriga organisationens ansvar – inklusive ansvar för den som är utsedd att leda och samordna informationssäkerhetsarbetet.[14] Den som utses att leda och samordna bör ges en oberoende, kravställande och granskande roll. Därtill bör myndigheten tydliggöra vilka befattningar som är informationsägare, d.v.s. ansvariga för att säkerställa att information skyddas på avsett sätt.[15]

Vad avser ledningens målsättning med universitetets informationssäkerhetsarbete så framgår, i linje med MSB:s föreskrifter, en övergripande målsättning i *Rutiner för informationssäkerhet*, d.v.s. i informationssäkerhetspolicyn: ”Universitetets informationstillgångar ska vara skyddade på ett säkert sätt med avseende på tillgänglighet, riktighet och konfidentialitet. Arbetet med informationssäkerhet ska sträva efter att balansera risker – trolig frekvens och konsekvenser – mot kostnader för skyddsåtgärder”. [16] Internrevisionen har efterfrågat dokumentation som kan visa på en strukturerad och systematisk planering, samordning och uppföljning som omfattar universitetets informationssäkerhetsarbete. Exempelvis genom plan som åskådliggör konkretiserade mål och strategier, prioriteringar på kort och lång sikt samt ett målinriktat arbete med aktiviteter med angivelse om ansvariga samt tidpunkt för när de ska vara genomförda och som man kan följa till uppföljning och utvärdering av måluppfyllnad.[17] Vid intervjuer med Säkerhetsavdelningen framgår att de dokument som finns i anslutning till området är Säkerhetsavdelningens verksamhetsplan och Risk- och sårbarhetsanalysen. Internrevisionen har dock av dessa dokument inte kunnat utläsa konkreta mål för universitetets informations-säkerhetsarbete. [18] Det går inte heller att uttyda ett strukturerat och systematiskt arbetssätt vad avser planering, samordning och uppföljning såtillvida att det tydligt går att följa från mål till strategier, prioriteringar och aktiviteter vidare till uppföljning av pågående aktiviteter/arbete och utvärdering i förhållande till målen.

Internrevisionen noterar i sammanhanget att det inte heller inom ramen för universitetsförvaltningens verksamhetsplan finns uppdrag avseende universitetsövergripande informationssäkerhetsarbete/kopplade till Säkerhetsavdelningens ansvarsområde. [19]

[14] MSBFS 2020:6 5 §.

[15] MSBFS 2020:6 allmänt råd till 5 §.

[16] *Rutiner för informationssäkerhet*, UFV 2017/93.

[17] ISO 27001 6.2 förtydligar vad avser Informationssäkerhetsmål och planering för att uppnå dem: "Organisationen ska upprätta informationssäkerhetsmål för relevanta funktioner och nivåer. När organisationen planerar för att uppnå målen ska den avgöra, bl.a.: vad som ska göras, vem som ska ansvara, när det ska vara genomfört och hur resultaten ska utvärderas.” Dokumenterad information om informationssäkerhetsmålen ska bevaras.

[18] Säkerhetsavdelningens verksamhetsplan för 2021, 2021-02-10. I verksamhetsplanen beskrivs Säkerhetsavdelningens organisation/roll med stort fokus inriktat mot e-förvaltning – ” Säkerhetsavdelningen har en rådgivande och samordnande roll inom e-förvaltningsorganisationen vad gäller informationssäkerhet, kravanalys samt uppföljningar” och ”långsiktiga mål för e-området Säkerhet” anges. Internrevisionen noterar att det dock inte beskrivs mål eller roll för samordning gentemot övriga områden/universitetsövergripande informationssäkerhetsarbete, dock framgår prioriteringar som går utanför e-förvaltningen.

[19] Verksamhetsplan för universitetsförvaltningen 2021, UFV 2020/1852.

.

Vad avser ansvarsfördelning och organisering av informationssäkerhetsarbetet inom universitetet, är detta beskrivet i flera av de interna styrdokumenten.[20] Det framgår att arbetet med att upprätthålla informationssäkerheten är fördelat på flera roller på olika nivåer i organisationen. Utgångspunkten är att ansvar för informationssäkerhetsarbetet, enligt *Rutiner för informationssäkerhet* (d.v.s. informationssäkerhetspolicyn), följer universitetets linjeorganisation. Rektor har det övergripande ansvaret för informationssäkerhetsarbetet och ett kontrollansvar att utförandet följer det delegerade ansvaret. [21] Vid varje institution är, enligt *Riktlinjer för säkerhetsarbete,* prefekten ansvarig för säkerheten inklusive delområdet informationssäkerhet. [22] Chefer inom universitetet ansvarar för att information om informationssäkerhetsarbetet sprids, att resurser avsätts, att medarbetare ges tillräcklig kunskap och att de arbetsmetoder som används bidrar till god informationssäkerhet. Medarbetare i sin tur ska följa de regler och riktlinjer som universitetet beslutat om. Beträffande ansvar för utförande av operativa informationssäkerhetsuppgifter, noterar internrevisionen att informationsägarrollen, som enligt råden till MSB:s föreskrifter är central och bör tydliggöras, inte finns definierad i universitetets informationssäkerhetspolicy.

Säkerhetsavdelningen är den avdelning som, enligt universitetsförvaltningens arbetsordning, ansvarar för ”universitetets systematiska informationssäkerhetsarbete”.[23] Vad gäller MSB:s krav om att myndigheten ska ha någon ”utsedd att leda och samordna informationssäkerhets-arbetet”, så är chefen för Säkerhetsavdelningen enligt delegationsordningen tillika informationssäkerhetschef och den som enligt Säkerhetsavdelningen svarar upp mot MSB:s krav. [24] Säkerhetschefens ansvar beskrivs i flera av de interna styrdokumenten, dock med något olika omfattning mellan dokumenten. Av *Riktlinjer för säkerhetsarbetet* framgår att säkerhets-chefen samordnar och är stödjande och rådgivande. Av *Rutiner för informationssäkerhet* omfattar ansvaret också där samordning och stöd men i tillägg även bl.a. utveckling och uppföljning av informationssäkerhetsarbetet. Under granskningen har internrevisionen noterat att det, vid Säkerhetsavdelningen, upplevs otydligt vad uppgiften att ”leda och samordna” mer specifikt omfattar och hur långt det ansvaret sträcker sig inom organisationen, särskilt vad avser den uppföljande och granskande roll som lyfts fram i råden till MSB:s föreskrifter.

Inom säkerhetsavdelningen finns Enheten för informationssäkerhet. Enhetens medarbetare, inklusive två informationssäkerhetssamordnare, är enligt uppgift säkerhetschefens ”förlängda arm” och resurser i de stödjande delarna av arbetet med att ”leda och samordna” informationssäkerhetsarbetet. Enhetens ansvarsområde innefattar enligt delegationen till enhetschefen ett stödjande uppdrag i förhållande till universitetets verksamheter kopplat till området informations- och IT-säkerhet. [25]

[20] *Riktlinjer för säkerhetsarbete*, UFV 2009/1929, *Rutiner för informationssäkerhet*, UFV 2017/93. *Ledningssystem för informationssäkerhet* (LIS), UFV 2017/651.

[21] *Rutiner för informationssäkerhet*, UFV 2017/93.

[22] *Riktlinjer för säkerhetsarbete*, UFV 2009/1929. Av *Prefektens uppgifter och beslutanderätter*, UFV 2011/619, framgår prefektens ansvar för att regelverk följs inom organisationen.

[23] Arbetsordning för universitetsförvaltningen vid Uppsala universitet, s. 22 och 14, UFV 2018/1183 (fastställd 2019-01-14).

[24] Av Delegationer från universitetsdirektören vid Uppsala universitet, s. 7, UFV 2020/1218, framgår att chefen för Säkerhetsavdelningen tillika är informationssäkerhetschef och får fatta beslut om systematiska informationssäkerhetsarbetet.

[25] Enligt delegation från säkerhetschefen till enhetschefen innefattar enhetens ansvarsområde att stödja universitetets verksamheter genom att tillhandahålla relevanta kompetenser och resurser för utveckling och förvaltning av effektiva och enhetliga lösningar kopplade till området informations- och IT-säkerhet”.

Även informationssäkerhetssamordnarnas verksamhet är inriktad på att ge råd och stöd till prefekter/chefer och medarbetare i informationssäkerhetsarbetet inom institutioner och andra delar av organisationen. Av intervjuerna vid Enheten för informationssäkerhet framgår att uppföljning, utvärdering och kontroll, t.ex. av om arbetssätten fungerar ute i verksamheten eller om regler och rutiner avseende informationssäkerhetsarbete är implementerade och efterlevs på avsett sätt inom organisationen, inte uppfattas ingå i enhetens uppdrag och arbetsuppgifter.

Internrevisionen noterar i sammanhanget att informationssäkerhetssamordnarnas uppdrag och arbetsuppgifter inte är formaliserade. Det saknas arbetsbeskrivning, instruktion eller liknande som beskriver deras arbetsuppgifter och verksamhet. Arbetet består dock av stödjande insatser bl.a. att hålla utbildningar, genomföra informationsinsatser och workshops inom organisationen, metod-/rutinutveckling avseende informationssäkerhet/-arbete m.m. Det stödjande arbetet gentemot verksamheten är enligt samordnarna i hög grad efterfrågebaserat. Det styrs inte på ett tydligt strukturerat eller systematiskt sätt, t.ex. med utgångspunkt i de delar av organisationen där behov eller brister i informationssäkerhetsarbetet särskilt har identifierats eller utifrån planer med mål, aktiviteter, prioriteringar m.m. formulerade för arbetet.

Beträffande samordning av universitetets informationssäkerhetsarbete finns, i tillägg till vad som redan beskrivits ovan, ytterligare roller i informationssäkerhetsarbetet där samverkan dem emellan är av vikt. Dataskyddsombudets verksamhet är exempelvis nära relaterad till informationssäkerhetsarbetet, då personuppgifter är en informationstyp med särskilda krav på skydd enligt Dataskyddsförordningen. [26] Dataskyddsombudets ansvar beskrivs i informationssäkerhetspolicyn. Även Avdelningen för universitetsgemensam IT är nära relaterad och ska enligt universitetsförvaltningens arbetsordning ”samverka i arbetet med informationssäkerhet” - det finns dock inte beskrivet vad som ingår i deras roll i förhållande till informationssäkerhetsarbete eller på vilket sätt samverkan ska ske. [27] Den samverkan som sker mellan dessa och Säkerhetsavdelningen sker främst som del av den löpande verksamheten eller i vissa fall i projektform.

Vid intervjuer framgår dock att det finns en informell grupp för operativ samverkan och informationsutbyte där representanter för Säkerhetsavdelningen, Avdelningen för universitetsgemensam IT samt dataskyddsombudet ingår. Under granskningen har internrevisionen vid flera av intervjuerna gjort noteringar som indikerar på bristande samordning, bl.a. kopplat till prioriteringar samt upplevda otydligheter i vad som ingår i avdelningarnas uppdrag och roller. Internrevisionen noterar att det inte finns någon gemensam målsättning för samverkansarbetet med tydliggjorda prioriteringar på kort och lång sikt. Kopplat till samverkan har även institutioner som intervjuats under granskningen, framfört att det inte alltid är tydligt vilken del av organisationen som ansvarar för olika informations-säkerhetsrelaterade frågor och vem de ska vända sig till i olika ärenden. [28]

[26] EU:s Dataskyddsförordning (GDPR).

[27] Därtill pågår enligt uppgift olika typer av utvecklingsinsatser som drivs av andra delar av organisationen och som i vissa avseenden har koppling till koordinering av informationssäkerhetsarbete. FAIRd-riktningsprojektet vid Planeringsavdelningen samt det s.k. datakontoret som utgörs av den operativa gruppen inom projektet FAIRd-riktning och dit forskare ska kunna vända sig vid frågor om forskningsdata, har lyfts som exempel.

[28] Det har framförts behov av en tydlig ingång för frågor och stöd i anslutning till olika delar inom informationssäkerhets-området. I dagsläget finns risk att man vid frågor vänder sig till personliga kontakter.

4.1.3 Kompetens och stöd

Granskningen visar att universitetet tillhandahåller utbildning, information och stöd inom informationssäkerhetsområdet. Dock är systematiken begränsad vad avser hur det ska säkerställas att chefer/medarbetare med roller/uppgifter i informationssäkerhetsarbetet, t.ex. informationsägare på institutioner/motsvarande, har tillräcklig kompetens för att utföra uppgifterna.

Att upprätthålla och utveckla kompetens hos personal som hanterar information och/eller har uppgifter i informationssäkerhetsarbetet samt att utforma det stöd som behövs i arbetet, är förutsättningar för ett effektivt informationssäkerhetsarbete och för att information ska kunna behandlas och skyddas på ett säkert sätt, vilket framhålls i MSB:s föreskrifter. [29] Myndigheten ska säkerställa att personal med utpekade roller i informationssäkerhetsarbetet har tillräcklig kompetens för att kunna utföra sina arbetsuppgifter samt utveckla kompetensen, bl.a. genom utbildning och informationsinsatser. Myndigheten ska även avgöra vilket stöd som behöver utformas för utförandet av informationssäkerhetsarbetet samt säkerställa att stödet utvärderas och vid behov anpassas. [30]

Även i universitetets interna styrdokument framhålls personalens kompetens som en viktig förutsättning för informationssäkerhetsarbetet. [31] Chefer inom universitetet ansvarar för att medarbetare ges tillräcklig kunskap inom området. [32]

Inom universitetet erbjuds olika former av kompetensförstärkande och stödjande aktiviteter som syftar till att upprätthålla och utveckla kompetensen kopplat till informationssäkerhetsområdet. Exempel på sådana aktiviteter är internutbildning – både lärarledda kurser och digitala s.k. nanokurser – och informations- och stödmaterial på medarbetarportalens webbplats för informationssäkerhet. Vidare genomförs informationsinsatser, workshops och andra typer av mer praktiskt inriktat stöd och vägledning, bl.a. inom ramen för Enheten för informationssäkerhets stödjande verksamhet. [33]

Av intervjuer med Säkerhetsavdelningen framgår att behov av ytterligare kompetens- och stödinsatser fångas i den löpande verksamheten, bl.a. vid informationssäkerhetssamordnarnas kontakter med institutioner eller i samband med *Risk- och sårbarhetsanalysen*. När behov har identifierats upplevs det dock, enligt Säkerhetsavdelningen, vara en utmaning att nå ut till institutionerna med information, utbildning och annat stöd. Detta är även en risk som uppmärksammats och kommunicerats i risk- och sårbarhetsanalysen under flera års tid. Risken förstärks, enligt samordnarna, genom att det vid institutioner och andra delar av organisationen

[29] MSBFS 2020:6 9 § p 4 och 5.

[30] MSBFS 2020:6 5 § p 4 och 5.

[31] *Riktlinjer för säkerhetsarbete*, UFV 2009/1929.

[32] *Rutiner för informationssäkerhet*, UFV 2017/93 .

[33] Enligt informationssäkerhetssamordnarna fick informationssäkerhetsfrågor ett uppsving i samband med införandet av GDPR och det fokus på skydd av personuppgifter som Dataskyddsförordningen ställer krav på. Samordnarna och dataskyddsombudet samarbetade vid utformning av rutiner, genomförde gemensamma informationsinsatser mm.

oftast inte finns någon administrativ stödroll/kontaktpersoner/funktionsansvariga för informationssäkerhet. [34]

Av intervjuer med institutionerna framgår att tre av institutionerna har tagit del av stödjande aktiviteter anordnade av informationssäkerhetssamordnarna, bl.a. workshops, och är positiva till den typen av verksamhetsnära praktiskt stöd. Flera av institutionerna understryker vikten av just verksamhetsnära stöd och möjligheter till specialanpassat stöd. [35] Detta då verksamheter och forskning skiljer sig kraftigt åt mellan olika vetenskapsområden/institutioner och kan lyda under olika externa, till och med internationella, krav. Det framkommer vidare att någon institution upplever att universitetets rutiner och lösningar riktas till ”likformade” verksamheter och att de därför riskerar bli alltför generella för att utgöra ett stöd. Den risk som framförs är att institutioner då måste rekrytera egen kompetens, skaffa egna lösningar mm vilket kan innebära avvikelser från regler och dubbla kostnader och suboptimering utifrån ett universitetsövergripande perspektiv.

Internrevisionen noterar också att institutionerna har begränsad systematik vad gäller att medarbetare/informationsägare ska ha/ges relevant och tillräcklig kunskap, t.ex. via utbildning, inom informationssäkerhetsområdet. Någon institution har dock introduktion av nya medarbetare som inkluderar informationssäkerhetsfrågor. Ett förbättringsområde som lyfts är att kommunikationen av vilka utbildningar som finns mer aktivt behöver riktas till olika målgrupper. Likaså behöver information som skickas till institutionerna bli tydligare och förmedlas i förhållande till mottagare. Någon institution upplever både informationsutskick, rutiner och riktlinjer vara mer eller mindre svårbegripliga och att budskapet inte alltid är tillräckligt tydligt. Det upplevs svårt att uppfatta vad syftet är, om det krävs en åtgärd och vem som i så fall ska göra vad, när och varför.

Det har även framkommit förbättringsbehov vad avser att information i anslutning till informationssäkerhetsområdet, som ges på olika förvaltningsavdelningars webbplatser på medarbetarportalen, inte anses vara enhetlig och samordnad. Webbsidor för olika områden har olika utseenden och systematik/koncept för hur information förmedlas.

Internrevisionen noterar även att systematisk utvärdering (och vid behov anpassning) av om de kompetensförstärkande, stöd- och informationsinsatserna som universitetet erbjuder är tillräckliga och svarar mot behov i verksamheten och interna och externa krav, inte genomförs sammantaget på universitetsövergripande nivå.

4.1.4 Bedömning

Granskningen visar att universitetsövergripande styrande och stödjande dokument för hur informationssäkerhetsarbetet ska bedrivas inom universitetet finns upprättade. Internrevisionen har noterat att styrdokumenten har upprättats över tid och att det finns diskrepans i lydelse och sakinnehåll mellan dokumenten. Styrdokumenten bör därför ses över samlat och harmoniseras. För att ytterligare öka möjligheterna att nå fram med styrdokumentens budskap och i förlängningen förbättra tillämpning av dem, bör dokumenten ses över och struktureras utifrån

[34] Två av institutionerna som intervjuats planerar dock för införande av sådana ”samordnare/kontaktpersoner” med särskilt uppdrag t.ex. att samordna informationssäkerhetsarbete inom institutionen och att bevaka området och upprätthålla kompetens.
[35] Institutioner har även framfört behov av råd och stöd i deras arbete med att upparbeta systematiska rutiner.

ett användar-/målgruppsperspektiv. Det översättningsarbete avseende styrdokumenten som påbörjats bör med fördel fortsätta då många medarbetare vid institutionerna är engelskspråkiga.

Internrevisionen konstaterar vidare att universitetet, i linje med kraven i MSB:s föreskrifter, har en beslutad informationssäkerhetspolicy, av vilken övergripande målsättning för och ansvarsfördelning och organisering framgår. I linje med föreskrifterna har universitetet även utsett säkerhetschefen till informationssäkerhetschef att leda och samordna informationssäkerhetsarbetet. Internrevisionen har under granskningen noterat en upplevd otydlighet vad uppgiften ”att leda och samordna” inkluderar och hur långt ansvaret sträcker sig inom organisationen. Internrevisionen bedömer att det finns risk att uppgifter såsom uppföljning, utvärdering och kontroll av regelefterlevnad hamnar mellan stolarna. Otydligheten riskerar även att leda till att samordningen av informationssäkerhetsarbetet inom universitetet inte blir effektiv.

Beträffande ansvarsfördelning och organisering av informationssäkerhetsarbetet i övrigt, visar granskningen att arbetet med att upprätthålla informationssäkerheten är fördelat på flera roller på olika nivåer inom organisationen. Det finns ett behov av att förtydliga vissa av rollerna. Utöver rollen ”att leda och samordna” behöver även rollen som informationsägare samt informationssäkerhetssamordnarnas roll och arbetsuppgifter beskrivas tydligare.

För att möjliggöra ett i högre grad målinriktat och effektivt informationssäkerhetsarbete inom universitetet, ser internrevisionen ett behov av att utifrån ledningens övergripande målsättning, formulera konkreta mål samt vidareutveckla rutiner för strukturerad och systematisk strategisk planering och samordning av informationssäkerhetsarbetet. Det finns även ett behov av att utveckla samverkansarbetet mellan berörda parter vid universitetsförvaltningen, bl.a. så arbetet samordnas och styrs utifrån gemensam målsättning och tydliggjorda prioriteringar. Därtill har förbättringsmöjlighet noterats i fråga om systematiken vad gäller hur det ska säkerställas att medarbetare/informationsägare inom institutioner och andra delar av organisationen ska ges relevant och tillräcklig kunskap/stöd, t.ex. via utbildning, inom informationssäkerhetsområdet.

4.2 Genomförande av informationssäkerhetsarbete vid institution

4.2.1 Informationsklassificering och riskhantering

Granskningen visar att informationsklassificering och riskhantering avseende informationssäkerhet genomförs i olika omfattning och med varierande systematik vid de institutioner som granskats. Ingen av de intervjuade institutionerna har rutiner som säkerställer att informationsklassificering genomförs systematiskt av de informationsmängder som institutionen är informationsägare av. Universitetets rutiner för informationsklassificering tillämpas i begränsad utsträckning vid de granskade institutionerna och bedöms således inte vara implementerade på ett tillfredsställande sätt inom delar av universitetets organisation.

Statliga myndigheter ska, enligt krav i MSB:s föreskrifter, bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av etablerade ISO-standarder. [36] Detta ska

[36] MSBFS 2020:6 4 § Informationssäkerhetsarbetet ska bedrivas med stöd av ISO-standarderna 27001:2017 och 27002:2017.

myndigheten säkerställa bl.a. genom att informationsklassificering och riskbedömning ska ske av den information som myndigheten ansvarar för. [37]

Informationsklassificering och riskbedömning är grundläggande aktiviteter i ett systematiskt och riskbaserat informationssäkerhetsarbete, och en förutsättning för att kunna utforma en skyddsnivå för informationen som är väl avvägd i förhållande till informationens betydelse för verksamheten. Internrevisionen har valt att undersöka tillämpningen av den här rutinen i syfte att bedöma systematik och riskbasering, men även då det är en aktivitet som är obligatorisk att genomföra för alla institutioner och andra verksamheter som äger information. Dessutom är klassificeringen grund för de övriga delarna av det systematiska informationssäkerhetsarbetet – att identifiera åtgärder för hur informationen ska skyddas och vid behov anpassa skyddet. [38]

Universitetets rutiner och modell för informationsklassificering beskrivs i *Rutiner för informationssäkerhet – riskhantering,* vilken även inkluderar instruktioner och mallar som stöd för det praktiska genomförandet.[39] Av rutinerna framgår att det är informationsägaren, d.v.s. den del av organisationen som äger informationen, som ska genomföra klassificering. Vid universitetet följer, som tidigare beskrivits, ansvaret för informationssäkerhet det delegerade verksamhetsansvaret. Vid institutioner innebär det att prefekten är ansvarig för informationssäkerheten och ofta även informationsägare till den information som institutionen ansvarar för. Prefekten är därmed även ansvarig för att informationsklassificering genomförs för t.ex. informationsmängder kopplat till institutionens forskningsprojekt/-studier. [40]

Informationsklassificering innebär att institutionen systematiskt ska gå igenom och klassificera och riskbedöma institutionens olika informationsmängder/-typer utifrån säkerhetsaspekterna *konfidentialitet, riktighet* och *tillgänglighet.* [41]

Informationsklassificering är på så sätt ett led i systematisk riskhantering, vilket är grunden för såväl förebyggande säkerhetsarbete som intern styrning och kontroll. Genom att klassificera informationen och medvetandegöra vilka risker som finns i institutionens informations-hantering, ökar möjligheterna att begränsa riskerna och styra hur informationen ska skyddas. Exempelvis genom att reflektera utifrån hur information i specifika forskningsprojekt/-studier ska behandlas och förvaras, om och hur den ska delas med olika samarbetspartners, kanske till

[37] MSBFS 2020:6 6 § definierar informationsklassificering som att myndigheten ska ”klassa sin information avseende konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få” och riskbedömning som ”identifiera, analysera och värdera risker för sin information”. Utifrån dessa identifieras behov av och införs säkerhetsåtgärder, vilka sen ska utvärderas och skyddet av informationen ska anpassas därefter.

[38] Rutiner för informationssäkerhet – riskhantering, UFV2018/211, avsnitt 5, t.ex. kravanalys, riskanalys och åtgärder..

[39] Rutiner för informationssäkerhet – riskhantering, UFV2018/211, bl.a. avsnitt 7.3 och bilagorna 2 & 6. Då granskningen här är inriktad på tillämpning av rutiner vid institutionerna, så beskrivs de utifrån institutionsperspektiv, men normalt gäller samma regler och rutiner även för informationssäkerhetsarbete som utförs vid intendenturer och inom e-förvaltningsorganisationen.

[40] Av Rutiner för informationssäkerhet, UFV 2017/93 framgår ”Ansvaret för genomförande och tillsyn av informationssäkerheten följer det delegerade verksamhetsansvaret (ordinarie linjeansvar)”. Av Rutiner för informationssäkerhet – riskhantering, UFV2018/211 framgår ”Informationsklassificering genomförs av den organisation som äger informationen.” och det framgår av definitionerna att det med organisation avses en organisatorisk enhet, t.ex. institution, projekt.

[41] Informationssystem som innehåller homogen information som används på liknande sätt av många institutioner, t.ex. Raindance med redovisningsinformation och Ladok med studieadministrativ information, klassas universitetsgemensamt inom ramen för e-förvaltningsområden. Detta för att underlätta så att inte varje institution var för sig ska behöva lägga tid på att klassa samma informationstyper i parallella processer. Rutiner för informationssäkerhet – riskhantering, UFV2018/211.

och med delas med eller transporteras till partners och lärosäten internationellt. [42] Dessutom bidrar rutinen till att skapa förståelse hos medarbetare som arbetar med informationen om vilket skydd som krävs för olika informationstyper/-mängder. Något som är extra bra att ha kännedom om t.ex. inför start av en forskningsstudie eller introduktion av nyanställda.

Av granskningen framgår att informationsklassificering och riskbedömning/-hantering kopplat till skydd av information genomförs i olika omfattning och med varierande systematik mellan de institutioner som ingått i granskningen. Ingen av de intervjuade institutionerna har rutiner som säkerställer att informationsklassificering genomförs systematiskt av de informationsmängder som institutionen är informationsägare av. Intervjuer och studier av dokumentation av utförda informationsklassificeringar visar att vid tre av de intervjuade institutionerna har klassificering genomförts, dock endast för begränsade delar av institutionens informationsmängder. [43] Exempelvis har det skett endast för ett fåtal av institutionens forskningsprojekt/-studier, inom endast en viss del av institutionen, inför upphandling eller utveckling av en särskild informationstillgång. Vid en av institutionerna som granskats har vi inte kunnat identifiera att informationsklassificering genomförts, i enlighet med universitetets regelverk, överhuvudtaget. Enligt institutionen har det, i den mån det förekommit strukturerade aktiviteter liknande informationsklassificering, föranletts av externa krav, t.ex. att forskningsprojekt finansierat av EU och Vetenskapsrådet krävt datahanteringsplan eller att särskilda krav ställts i anslutning till forskningssamarbeten med externa parter.

Även vid en annan institution lyfts exempel där forskningsprojektet medvetet valt att hellre tillämpa externa samarbetspartners informationssäkerhetskrav och regler, då partnerns regler uppfattats som tydligare och mer vägledande, och därför enklare att anamma och tillämpa än universitetets. [44]

Efter genomförd informationsklassificering ska resultatet enligt universitetets rutiner dokumenteras med hjälp av tillhandahållna mallar och skickas in till Säkerhetsavdelningen. [45] I det fall informationsklassificeringen genomförs inför anmälan av personuppgiftsbehandling ska den även biläggas anmälan när den upprättas i diariesystemet W3D3. [46] Det har dock framkommit under granskningen att rutinen att rapportera resultaten av genomförda informationsklassificeringar till Säkerhetsavdelningen tillämpas i låg utsträckning. [47]

[42] Olika informationsmängder/-typer inom t.ex. en institution, ett forskningsprojekt, är av varierande karaktär och behöver hanteras och skyddas på olika sätt beroende på hur den används. Viss information är mer känslig, värdefull eller kritisk utifrån ett verksamhetsperspektiv än annan. Viss information utsätts för större risk beroende på hur den hanteras, förvaras och delas.

[43] En av institutionerna beskriver ett arbetssätt för sitt informationssäkerhetsarbete som bedöms vara i högre grad systematiskt än de andra intervjuade institutionerna. Två av institutionerna planerar, som beskrivits tidigare, även för införande av specifika ”samordnare/kontaktpersoner” med särskilt uppdrag t.ex. att samordna informationssäkerhetsarbete inom institutionen och att bevaka området och upprätthålla kompetens.

[44] Internationella forskningsprojekt/-samarbeten med utländska lärosäten nämns som exempel då den externa samarbetspartnerns krav och regler uppfattats tydligare och därför varit styrande.

[45] Rutiner för informationssäkerhet – riskhantering, UFV2018/211, bl.a. avsnitt 7.3 och bilagorna 2 & 6. Resultatet från genomförda informationsklassificeringar kommer efterfrågas i samband med institutionernas årliga återrapportering gällande informationssäkerhet och dokumentation/en kopia av den genomförda klassificeringen ska skickas till Säkerhetsavdelningen.

[46] Enligt instruktioner till det webbaserade formuläret för anmälan av personuppgiftsbehandling. Sedan införande av GDPR tillämpas rutin att informationsklassificering ska genomföras innan anmälan av personuppgiftsbehandling och bifogas anmälan.

[47] I de fall informationsklassificeringarna genomförts med stöd av informationssäkerhetssamordnarna har ofta dokumentationen kommit Säkerhetsavdelningen till del på det sättet. Enligt samordnarna har dock rapportering/dokumentation

Vid intervjuerna med Säkerhetsavdelningen framkommer att inte heller de systematiskt begär in uppgift om och dokumentation från de informationsklassificeringar och kravanalyser m.m. som institutionerna genomfört. Enligt uppgift har det förekommit, i vissa fall när institutioner kontaktat Säkerhetsavdelningen med frågor om hur de ska rapportera resultatet från informationsklassificeringarna, att Säkerhetsavdelningens budskap varit att de inte behöver rapportera eller sända in dokumentationen. Detta med motiveringen att det viktigaste är att institutionen/projektet har genomfört klassningen – inte att den kommer Säkerhetsavdelningen till del. Dessutom framgår vid intervjuerna med Enheten för informationssäkerhet, att deras uppdrag inte omfattar att följa upp och kontrollera att institutionerna efterlever regler och rutiner samt att de försöker undvika att uppfattas som kontrollinstans. Detta innebär att det inte heller finns någon lägesbild av i vilken utsträckning rutinerna för informationsklassificering är implementerade och efterlevs.

Internrevisionen noterar i övrigt att ingen av institutionerna som intervjuats uppger sig ha kompenserande rutiner för riskanalys, som på annat sätt säkerställer att bedömning, analys och hantering av risker kopplat till skydd av institutionens information genomförs. Tre av institutionerna anger att de bidragit med information till den universitetsgemensamma risk- och sårbarhetsanalysen, dock utan att underliggande riskanalysarbete internt inom institutionen genomförts. [48]

4.2.2 Bedömning

Internrevisionen konstaterar att universitetet har fastställda universitetsövergripande rutiner för informationsklassificering med tillhörande instruktioner och mallar som stöd. Granskningen visar dock att rutinen tillämpas i begränsad utsträckning vid de granskade institutionerna.

Informationsklassificering och riskbedömning/-hantering kopplat till skydd av information genomförs i olika omfattning och med varierande systematik. Ingen av de intervjuade institutionerna har rutiner som säkerställer att de informationsmängder-/typer som institutionen är informationsägare av informationsklassificeras eller riskbedöms på ett systematiskt sätt. Institutionerna har inte heller kompenserande rutiner som säkerställer att informationsmängderna riskbedöms på annat sätt. Detta kan medföra att risker inte uppmärksammas och hanteras. Internrevisionen har även noterat att rutinen att resultatet av genomförda informationsklassificeringar ska rapporteras till Säkerhetsavdelningen tillämpas i låg utsträckning, vilket kan innebära att information om risker inte kommer Säkerhetsavdelningen till kännedom och att institutionen inte kan ges stöd i hanteringen.

Internrevisionen gör den sammantagna bedömningen att universitetets regler och rutiner för informationsklassificering och riskhantering tillämpas i begränsad utsträckning vid de granskade institutionerna och bedöms således inte vara implementerade på ett tillfredsställande sätt inom delar av universitetets organisation. Detta trots att krav på informationsklassificering i myndigheter har ställts sedan MSB:s föreskrifter infördes 2009. Att det vid universitetet inte

i övrigt inkommit från endast ett fåtal (handfull) institutioner/forskargrupper/projekt. Rutin för att begära in/säkerställa att dokumentation sänds in finns inte. När informationsklassificering genomförts inför anmälan av personuppgiftsbehandling ska den bifogas anmälan i diariesystemet W3D3.

[48] Institutionerna som lämnat uppgifter till risk- och sårbarhetsanalysen uppger att uppgiftslämnandet vid dessa tillfällen inte ha föregåtts av underliggande/förberedande riskanalysarbete internt inom institutionen.

genomförs uppföljning eller utvärdering av om arbetssätt fungerar eller i vilken utsträckning rutinerna är implementerade och efterlevs inom organisationen är inte heller tillfredsställande.

Universitetet som myndighet ska enligt MSB:s föreskrifter säkerställa att informationsklassificering och riskbedömning av information genomförs. Mot bakgrund av detta och då informationsklassificering och riskbedömning är grundläggande delar av ett systematiskt informationssäkerhetsarbete och utgångspunkt för att kunna utforma skydd för universitetets information, anser internrevisionen att det är angeläget att i högre grad prioritera arbetet med att implementera dessa rutiner inom organisationen. Internrevisionen ser ett behov av att ett sådant implementeringsarbete måste drivas, samordnas och stödjas på ett strukturerat och systematiskt sätt från universitetsövergripande håll.

4.3 Uppföljning och rapportering av informationssäkerhetsarbetet

4.3.1 Uppföljning och utvärdering

Granskningen visar på brister vad avser strukturerad och systematisk uppföljning och utvärdering av universitetets informationssäkerhetsarbete, exempelvis vad gäller uppföljning av om ledningens målsättning med arbetet är uppfylld och utvärdering av om universitetets regler, rutiner och arbetssätt motsvarar behoven, är implementerade och tillämpas på avsett sätt inom universitetets organisation.

Uppföljning och utvärdering är viktiga delar av ett systematiskt informationssäkerhetsarbete och intern styrning och kontroll, då det bidrar till att ge en lägesbild av om t.ex. målsättningarna för arbetet är uppfyllda, rutiner tillämpas och arbetet fungerar på avsett sätt, vilket i förlängningen ger ett underlag för att vidareutveckla och förbättra arbetet.

Uppföljning av att informationssäkerhetsarbetet svarar mot myndighetsledningens målsättning och inriktning ska, enligt MSB:s föreskrifter, göras minst en gång per år genom sammanställning och analys av resultatet av genomförda:

- utvärdering av innehåll i interna regler, arbetssätt och stöd och vid behov anpassning,
- informationsklassificeringar,
- riskbedömningar,
- utvärdering av säkerhetsåtgärder,
- utvärderingar av att interna regler, arbetssätt och stöd används på avsett sätt. [49]

Uppföljningen av myndighetens informationssäkerhetsarbete bör, enligt MSB:s föreskrifter, vidare hållas samman av den eller de som utsetts att leda och samordna informationssäkerhetsarbetet vid myndigheten. [50] Utvärdering enligt första punkten ovan bör ske genom interna kontroller, granskningar, interna och externa revisioner eller motsvarande. Interna regler och arbetssätt bör tydliggöra hur och när utvärdering ska ske. [51]

[49] MSBFS 2020:6 14 §.
[50] MSBFS 2020:6 Allmänt råd till 14 §.
[51] MSBFS 2020:6 Allmänt råd till 5 §.

Under granskningen har internrevisionen noterat att krav på uppföljning framgår av flera av universitetets interna styrdokument kopplat till informationssäkerhetsområdet, dock med varierande ordalydelser. [52] I den senaste uppdateringen av *Rutiner för informationssäkerhet* har uppföljning och efterlevnad fått en mer framträdande plats i styrdokumentet jämfört med tidigare, t.ex. nya skrivningar som inkluderar att säkerhetschefen ansvarar för uppföljning av informationssäkerhetsarbetet och att informationssäkerhetsarbetet årligen ska följas upp för att säkerställa att det bedrivs i enlighet med universitetets regler och riktlinjer m.m. Där framgår även att universitetets dataskyddsombud ska övervaka den interna efterlevnaden av Dataskyddsförordningen och universitetets strategi för skydd av personuppgifter. [53]

Internrevisionen har under granskningen efterfrågat dokumentation från genomförda uppföljningar, analyser, utvärderingar, GAP-analys, granskningar, kontroll av regelefterlevnad och liknande material vad avser universitetets informationssäkerhetsarbete. Detta i syfte att undersöka om uppföljning och utvärdering i enlighet med kraven i MSB:s föreskrifter genomförs med systematik och regelbundenhet samt om det finns dokumentation som gör det möjligt att följa resultatet av dessa till följdbeslut om åtgärder och återrapportering av om åtgärderna gett effekt.

Vid intervjuerna med Säkerhetsavdelningen framgår att *Risk- och sårbarhetsanalysen*, som årligen sammanställs och föredras för rektor och konsistoriet, utgör samlingsdokument för uppföljning av säkerhetsarbetet och omfattar risker och sårbarheter m.m. även inom informationssäkerhetsområdet. [54] Internrevisionen noterar dock att den inte visar om ledningens målsättning uppfylls eller om regler och rutiner efterlevs och tillämpas på avsett sätt. Vid sidan av risk- och sårbarhetsanalysen genomför Säkerhetsavdelningen, enligt uppgift, inte andra typer av systematiska uppföljningar av informationssäkerhetsarbetet. Det finns t.ex. inte någon dokumenterad GAP-analys som visar konsekvenser för universitetets informations-säkerhetsarbete i förhållande till den nya versionen av MSB:s föreskrifter som började gälla 1 oktober 2020, så att det går att följa bedömd påverkan och prioriterade åtgärder och status. [55]

Vad gäller risk- och sårbarhetsanalysen som uppföljningsdokument, har internrevisionen även noterat bristande systematik i de efterföljande stegen. Detta då resultat och identifierade brister inte på ett tydligt och systematiskt sätt går att följa till vilka konkreta åtgärder som beslutats till följd av resultatet. Det saknas t.ex. en åtgärds-/handlingsplan med angivelser om beslutade åtgärder och dess prioriteringsordning, ansvarig för att vidta åtgärderna, tidplan för när de ska vara genomförda och återrapporterade. Internrevisionen har även noterat att det inte heller sker återkoppling av resultatet av analysen tillbaka till de institutioner som bidragit med enkätsvar.

Av intervjuer med Säkerhetsavdelningen framgår vidare att den uppföljning som i praktiken genomförs, bl.a. inom ramen för risk- och sårbarhetsanalysen, i låg utsträckning omfattar information från det informationssäkerhetsarbete som utförs vid institutionerna. [56] Enligt

[52] Jämför Ledningssystem för informationssäkerhet (LIS) UFV 2017/651 avsnitt 7, Riktlinjer för säkerhetsarbetet, UFV 2009/1929 avsnitt 5 med Rutiner för informationssäkerhet, UFV 2017/93, uppdaterad 2021-03-29, avsnitt 4.2 och 4.14.

[53] Rutiner för informationssäkerhet, UFV 2017/93, uppdaterad 2021-03-29, avsnitt 4.2 och 4.14.

[54] Rapport från risk- och sårbarhetsanalys 2020, UFV 2020/2000, 2020-12-15.

[55] Enligt MSBFS 2020:6 6 § ska myndigheten utvärdera säkerhetsåtgärder och vid behov anpassa skyddet av information. I arbetet ingår att genomföra en GAP-analys. Vidare ska informationssäkerhetsarbetet dokumenteras.

[56] Uppgifter inhämtas från institutionerna via en enkät som tillställs samtliga institutioner. Avseende den risk- och sårbarhetsanalys som genomfördes 2020 omfattade enkäten endast två huvudfrågor kopplat till informationssäkerhetsområdet – *Används system/IT-tjänster som anskaffats i egen regi, t.ex. i forskningsarbetet, och har i så fall anskaffningen föregåtts av*

informationssäkerhetssamordnarna ingår inte uppföljning och kontroll, t.ex. av om regler och rutiner är implementerade och tillämpas på avsett sätt inom institutionerna, i deras uppdrag. Med hänvisning till ”resursläget” uppger de att de inte har förutsättningar för att genomföra sådan uppföljning inom ramen för de två befattningar som samordnarfunktionen utgör. Informationssäkerhetssamordnarna får dock genom sina stödjande aktiviteter, t.ex. vid besök, workshops m.m. succesivt ökad insyn i institutionernas informationssäkerhetsarbete.

Vid intervjun med universitetets dataskyddsombud framgår vidare, att det inte heller inom ramen för denna tillsynsfunktion, görs uppföljning och kontroll av om institutioner och andra delar av organisationen efterlever Dataskyddsförordningen eller om de hanterar information med personuppgifter på ett sätt så att de skyddas utifrån informationssäkerhetsaspekter.

4.3.2 Rapporteringsrutiner

Granskningen visar på brister vad avser formaliserade rapporteringsrutiner för att systematiskt hålla rektor/universitetsledningen informerad om informationssäkerhetsarbetet.

Rapportering och återkoppling till myndighetsledningen, som ytterst ansvarar för informationssäkerheten, t.ex. om hur informationssäkerhetsarbetet fungerar och om målsättningarna med arbetet nås, är en del av det systematiska informationssäkerhetsarbetet och en förutsättning för att kunna besluta om förbättringsåtgärder.

Myndighetsledningen ska, enligt MSB:s föreskrifter, informera sig om i vilken utsträckning införda säkerhetsåtgärder motsvarar myndighetens behov, allvarliga risker som inte åtgärdats och övriga hinder för att uppnå ledningens målsättning med informationssäkerhetsarbetet. [57] Bedömningen av övriga hinder bör inkludera brister avseende interna regler och arbetssätt, tilldelning av ansvar och resurser m.m. [58]

ISO-standarden 27001:2017 förtydligar vidare att en s.k. ledningens genomgång, bör genomföras med planerade intervall för att säkerställa att ledningssystemet för informationssäkerhet fortsatt är tillräckligt, lämpligt och ger avsedd verkan. Ledningens genomgång ska kunna resultera i beslut rörande eventuella behov av ändringar i ledningssystem och andra förbättringar. [59]

Av universitetets interna styrdokument framgår, i linje med vad MSB föreskriver ovan, att universitetsledningen ska informera sig om informationssäkerhetsarbetet, om införda säkerhetsåtgärder motsvarar behoven och om hinder för att uppnå ledningens målsättning med informationssäkerhetsarbetet föreligger. [60] Det framgår även av styrdokument att periodisk

informationsklassificering och kravanalys? och Finns det kännedom om det utbud av centrala IT-tjänster som tillhandahålls av UIT och datakontoret?. Enligt dokumentation från informationssäkerhetssamordnarna var svarsfrekvensen 85% (institutioner).

[57] MSBFS 2020:6 15 §.

[58] MSBFS 2020:6 Allmänt råd till 15 §.

[59] ISO 27001/2017 s. 8-9.

[60] Rutiner för informationssäkerhet, UFV 2017/93, avsnitt 4.2.

rapportering av hur informationssäkerhetsarbetet fungerar i verksamheten med avseende på uppsatta mål, praktisk erfarenhet och efterlevnad i huvudsak utförs av säkerhetsavdelningen. [61]

Av intervjuerna med Säkerhetsavdelningen framgår att *Risk- och sårbarhetsanalysen* är huvuddokument även för den rapportering som årligen sker till rektor och konsistoriet. I övrigt genomförs inte ledningsgenomgångar eller annan systematisk rapportering där rektor, eller ansvarskedjan i övrigt, får rapport om måluppfyllnad vad avser informationssäkerhetsarbetet, eventuella hinder för detta, om arbetssätten fungerar och om regler och rutiner efterlevs och tillämpas på avsett sätt inom universitetet. Rapporteringskulturen mellan säkerhetschefen (i rollen som informationssäkerhetschef) och ledningen i form av rektor och universitetsdirektör är istället, sedan tillbaka i tiden, präglad av informella muntliga kontakter på ad hoc basis. Internrevisionen har följaktligen inte heller kunnat ta del av skriftliga rapporter, beslut eller annan dokumentation där man tydligt och på ett systematiskt sätt kan följa rapportering av nuläge till beslut om säkerhetsåtgärder/vidareutveckling, åtgärdsplan och återrapportering av om åtgärderna fått effekt. Enligt Säkerhetsavdelningen finns dock tankar på att bygga ut rapporteringen så att den blir strukturerad och mer frekvent.

4.3.3 Bedömning

Granskningen visar på brister vad avser strukturerad och systematisk uppföljning, utvärdering och rapportering av det informationssäkerhetsarbete som bedrivs inom universitetet. Exempelvis gäller detta uppföljning och rapportering av om ledningens målsättning med arbetet är uppfylld och utvärdering av om universitetets regler, rutiner och arbetssätt motsvarar behoven, är implementerade och tillämpas på avsett sätt inom universitetets organisation.

Den uppföljning och rapportering som årligen sker genom risk- och sårbarhetsanalysen uppges i låg grad omfatta en lägesbild av det informationssäkerhetsarbete som bedrivs på institutioner. Internrevisionen ser att det finns en risk att risk- och sårbarhetsanalysen endast har en begränsad funktion vad avser systematisk strategisk planering och uppföljning av informationssäkerhetsarbetet inom universitetet, på grund av bristande systematik i de efterföljande stegen. Avsaknad av åtgärds-/handlingsplan med angivelser om prioriteringsordning, ansvarig och tidplan för genomförande och återrapportering, leder till att resultat och identifierade brister inte på ett tydligt och systematiskt sätt går att följa till vilka konkreta åtgärder som beslutats till följd av resultatet. Risken förstärks av att det inte heller sker någon återkoppling av resultatet av risk- och sårbarhetsanalysen tillbaka till institutioner som medverkat i enkäten.

Bristen på strukturerad och systematisk uppföljning och utvärdering av det informationssäkerhetsarbete som bedrivs riskerar att begränsa möjligheterna till ett effektivt förbättringsinriktat arbetssätt. Därmed riskeras gå miste om information som skulle kunna användas till att på ett effektivare sätt inrikta stöd och andra resurser samt styra och samordna arbetet i övrigt.

För att uppnå ett systematiskt och effektivt informationssäkerhetsarbete är det av vikt att arbetet styrs, planeras och genomförs, men internrevisionen ser det som angeläget att det även följs upp, utvärderas och rapporteras för att möjliggöra ett framåtriktat, systematiskt och effektivt arbete med att upprätthålla och vidareutveckla skyddet av universitetets information.

[61] Riktlinjer för säkerhetsarbetet – Ledningssystem för informationssäkerhet (LIS), UFV 2017/651, avsnitt 7 Utvärdering av prestanda (övervakning mätning, analys och utvärdering, internrevision, ledningens genomgång).

5 Sammanfattande bedömning och rekommendationer

Internrevisionen har granskat och bedömt om informationssäkerhetsarbetet inom universitetet bedrivs systematiskt och riskbaserat och i enlighet med interna styrdokument och krav som MSB via föreskrifter ställer på statliga myndigheter. Granskningen har särskilt inriktats mot att undersöka hur informationssäkerhetsarbetet är utformat och hur det styrs, följs upp och rapporteras. Därutöver har genomförande av informationssäkerhetsarbete på fyra institutioner undersökts genom granskning av tillämpningen av rutinerna för informationsklassificering och riskhantering.

Internrevisionens sammanfattande bedömning av *utformningen och styrningen av informationssäkerhetsarbetet* är att det finns ett förbättringsbehov rörande systematik, effektivitet och följsamhet mot regler och rutiner i flera av de delar av arbetet som granskats, bl.a. samordning, planering och stöd. Det finns även ett behov av att ytterligare förtydliga ansvar och/eller arbetsuppgifter för vissa roller i informationssäkerhetsarbetet.

Internrevisionen ser vidare stora förbättringsbehov vad avser *uppföljning, utvärdering och rapportering av informationssäkerhetsarbetet* (även i relation till kraven i MSB:s föreskrifter). Exempelvis uppföljning av om arbetet svarar mot ledningens målsättning och utvärdering av om regler, rutiner och arbetssätt är implementerade och tillämpas på avsett sätt inom universitetet.

Även beträffande systematiken i *genomförandet av informationssäkerhetsarbete vid institution* bedömer internrevisionen att ett stort förbättringsbehov föreligger (också här i relation till MSB:s krav). Detta gällande att universitetet som myndighet ska säkerställa att den information som universitetet ansvarar för informationsklassificeras och riskbedöms och att skydd utformas för den. Från granskning av de fyra institutionerna framkommer att informationsklassificering och riskhantering genomförs i olika omfattning med varierande systematik. Ingen av de granskade institutionerna har rutiner som säkerställer att informationsklassificering genomförs systematiskt av de informationsmängder som de är informationsägare av. Universitetets rutiner bedöms således inte vara tillfredsställande implementerade.

Trots det hittills genomförda arbete med informationsklassificering och riskbedömning vid institutioner och trots de stödjande insatser som genomförts för att underlätta för institutioner i arbetet, bl.a. inom ramen för informationssamordnarnas verksamhet, bedömer internrevisionen att det kvarstår ett omfattande arbete innan följsamhet i förhållande till MSB:s krav på att information som universitetet äger ska vara informationsklassificerad och riskbedömd, kan anses vara uppnått.

För att förbättra den interna styrningen och kontrollen så att universitetets informationssäkerhetsarbete ska kunna bedrivas med en högre grad av systematik och effektivitet samt i enlighet med interna styrdokument och MSB:s föreskrifter, rekommenderar internrevisionen rektor att:

- Förtydliga ansvar och/eller arbetsuppgifter för vissa roller i informationssäkerhetsarbetet, inklusive:
    - den som är ”utsedd att leda och samordna” universitetets informationssäkerhetsarbete,
    - informationssäkerhetssamordnarna vid Säkerhetsavdelningen samt
    - informationsägarna.
- Tillse att personal med arbetsuppgifter/roll i informationssäkerhetsarbetet, bl.a. informationsägare vid institutioner, har relevant och tillräcklig kunskap och kompetens.
- Utvärdera inriktning för och dimensionering av de stödjande resurserna, inklusive informationssäkerhetssamordnarnas verksamhet, i syfte att tillse att de ges förutsättningar för utförande av insatser som svarar mot risk och behov i verksamheten.
- Utveckla samverkansarbetet mellan berörda parter vid universitetsförvaltningen, bl.a. så att arbetet samordnas och styrs utifrån gemensam målsättning och tydliggjorda prioriteringar samt att information ges på ett samordnat och enhetligt sätt.
- Införa rutiner för strukturerad och systematisk planering och samordning av informationssäkerhetsarbetet inom universitetet, samt att utifrån ledningens övergripande målsättning formulera konkreta mål som kan utgöra grund för ett målinriktat arbete.
- Prioritera arbetet med att implementera universitetets rutiner för informationssäkerhet, inklusive informationsklassificering och riskhantering, vid institutioner/motsvarande, samt tillse att kompetens och stöd för arbetet motsvarar verksamhetens behov.
- Införa rutiner för strukturerad och systematisk uppföljning, utvärdering och rapportering av informationssäkerhetsarbetet, och som även inkluderar uppföljning av mål och utvärdering av att regler, arbetssätt och stöd tillämpas och används på avsett sätt.
- Se över och uppdatera styrdokumenten för informationssäkerhetsarbetet samlat, i syfte att harmonisera dem innehållsmässigt.

Madelene Norsell	Sven Jungerhem
Internrevisor/granskningsledare	Internrevisionschef