Stockholms universitet

PM
2021-02-02

Dnr:
SU FV-1.1.6-0295-20

Maria Pilbark Brenner
Internrevisionschef
Internrevisionen

Styrelsemöte 19 februari 2021

Internrevisionsrapport - Informationssäkerhet

Bakgrund

I enlighet med Internrevisionsplan för 2020 (Dnr: SU FV-1.1.6-0562-19) har internrevisionen granskat Stockholms universitets informationssäkerhetsarbete. Granskningen har genomförts av PwC på uppdrag av internrevisionen och PwCs iakttagelser och rekommendationer har sammanställts i en internrevisionsrapport.

Till PwCs granskningsrapport bifogas internrevisionens missiv. Av missivet framgår en översiktlig sammanfattning av granskningsresultatet samt internrevisionens rekommendationer.

Förslag till styrelsens beslut

Styrelsen beslutar

- Att lägga ärendet till handlingarna.

Bifogade dokument

- Internrevisionsrapport Informationssäkerhet (Dnr: SU FV-1.1.6-0295-20)
- Internrevisionens missiv

Stockholms universitet Besöksadress Telefon:
E-post: maria.pilbark.brenner@su.se

Stockholms universitet

2020-11-30 Dnr SU FV-1.1.6-0295-20

Maria Pilbark Brenner
Internrevisionen

Stockholms universitet – granskning av informationssäkerhet

Bakgrund och syfte

2017 utförde Internrevisionen, med hjälp av PwC, en granskning av informationssäkerhet (Dnr SU FV-1.1.6-0267-17). Avrapportering till universitetsstyrelsen skedde i maj 2017 och i samband med detta fattade styrelsen beslut om ett antal åtgärder utifrån rektors yttrande. I enlighet med internrevisionsplanen för 2020 har Internrevisionen återigen gett PwC i uppdrag att granska Stockholms universitets (SU) informationssäkerhet. Det övergripande syftet med granskningen har varit att utvärdera SUs interna styrning och kontroll av åtgärdsarbetet utifrån 2017 års granskning.

Resultat av granskningen

PwCs granskning visar att en handlingsplan för att genomföra beslutade informationssäkerhetsåtgärder togs fram under perioden februari – mars 2019. Granskningen av handlingsplanen, och den interna styrningen och kontrollen av arbetet utifrån denna, har identifierat ett antal observationer. Observationerna beskrivs på ett övergripande sätt i nedanstående punkter. För en fullständig beskrivning av observationerna hänvisas till PwCs rapport.

- Handlingsplanen omfattar inte på ett fullständigt sätt den typ av långsiktiga strategiska informationssäkerhetsåtgärder, för SU som helhet, som styrelsen beslutade om 2017. Handlingsplanen lägger stor vikt vid it-säkerhetsåtgärder, inom ramen för IT-avdelningen. Dessa åtgärder är viktiga för informationssäkerheten, men är endast en del av de åtgärder som behöver vidtas för att säkra ett strategiskt och systematiskt informationssäkerhetsarbete inom hela SU.

- Det finns brister i handlingsplanens ändamålsenlighet då åtgärder, ansvar och tidplaner i flera fall uttrycks på ett så pass övergripande sätt att de inte bedöms ge tillräckliga förutsättningar för en effektiv styrning, uppföljning och återrapportering av åtgärdsarbetet.

- Det saknas rutiner/arbetssätt som säkerställer att hinder och utmaningar i åtgärdsarbetet fångas upp och omhändertas på ett proaktivt sätt.

- Nuvarande återrapportering av åtgärdsarbetet bör stärkas och behovsanpassas i större grad. Kraven bör förtydligas avseende vad som ska rapporteras, av vem, till vem, kvalitetssäkringsåtgärder samt med vilken frekvens rapportering ska ske.

Stockholms universitet

Baserat på ovanstående observationer är PwCs sammanfattande bedömning att den interna styrningen och kontrollen av universitetets åtgärdsarbete är otillfredsställande.

Genomförda intervjuer visar att även verksamheten själv har identifierat brister i åtgärdsarbetet och att man anser att det långsiktiga och systematiska informationssäkerhetsarbetet inom SU som helhet inte har kommit så långt som man önskat. De huvudsakliga skälen till detta uppges vara att verksamheten har tvingats prioritera ett mer operativt arbete kopplat till exempelvis IT-säkerhet och implementering av rutiner med anledning av den nya Dataskyddsförordningen. Även personalförändringar och resursbrist har lyfts som orsaker till identifierade brister och förseningar. I syfte att stärka och effektivisera arbetet har ett antal åtgärder vidtagits under 2020, vilka återges på ett översiktligt sätt i PwCs rapport. Verksamheten har dock gjort bedömningen att ett ännu mer omfattande omtag krävs för att säkra ett effektivt informationssäkerhetsarbete framåt. I avvaktan på att formerna för detta omtag ska sättas har åtgärdsarbetet nu pausats helt enligt uppgift.

Internrevisionen ser positivt på att ett omtag planeras då detta bedöms kunna ge ökade förutsättningar för ett mer ändamålsenligt och effektivt åtgärdsarbete framgent. Med detta som utgångspunkt rekommenderar Internrevisionens att planerat omtag genomförs skyndsamt. Vidare rekommenderar Internrevisionen att PwCs rekommendationer omhändertas inom ramen för planerat omtag. PwCs rekommendationer omfattar i huvudsak följande punkter:

- Överse befintlig handlingsplan och säkerställ fullständighet. Handlingsplanen bör kompletteras med åtgärder som säkrar ett systematiskt informationssäkerhetsarbete för hela universitet, i enlighet med styrelsens beslut 2017.

- Överväg att skapa en särskild handlingsplan för långsiktiga strategiska åtgärder avseende informationssäkerhet. Denna kan kompletteras med den mer operativa och detaljerade handlingsplan som föreligger idag.

- Överse befintlig handlingsplan och säkerställ ändamålsenlighet, dvs bryt ner åtgärder, ansvar och tidplan till en nivå som ger förutsättningar för effektiv intern styrning och kontroll av åtgärdsarbetet löpande under året.

- Etablera rutiner som säkerställer att relevanta styrdokument avseende informationssäkerhetsarbetet, och beslutad handlingsplan, förankras på alla nivåer inom universitetet.

- Etablera rutin/arbetssätt som bidrar till att hinder och utmaningar i åtgärdsarbetet identifieras och hanteras på ett proaktivt sätt, exempelvis genom regelbundna riskanalyser.

- Identifiera relevanta intressenter/beslutsfattare från hela universitetet, fastställ vilken information de bör ta del av och utarbeta rutiner som säkerställer en behovsbaserat och

Stockholms universitet

systematisk återrapportering. Integrera statusrapporteringen med redan befintliga rapporteringsstrukturer där detta är möjligt, exempelvis i tertialrapportering och riskrapportering.

- Tydliggör övergripande ansvar för SUs informationssäkerhet, både avseende åtgärdsarbete samt strategiskt och systematiskt informationssäkerhetsarbete över tid. I det fall ansvaret delegeras bör detta tydligt framgå av Besluts- och delegationsordning för Stockholms universitet. Tilldelat ansvar bör även speglas i mandat och rapporteringsvägar.

För en fullständig beskrivning av utförd revision, observationer, risker och rekommendationer hänvisar Internrevisionen till PwCs rapport.

Maria Pilbark Brenner
Internrevisionschef

Stockholms universitet – Granskning av informationssäkerhet

November 2020

Kvalitetsansvarig
Nils Jeppsson
Ansvarig granskare
Niklas Ljung
Gransknings deltagare
Anton Andersson

Sammanfattande bedömning

Öhrlings PricewaterhouseCoopers AB (“PwC, vi”), organisationsnummer 556029- 6740, har enligt ramavtal (SU FV-2.2.2-1739-20) om internrevisionstjänster för Stockholms universitet, organisationsnummer 202100-3062 genomfört “Granskning av informationssäkerhet”.

Det övergripande syftet med denna granskning har varit att utvärdera den interna styrningen och kontrollen av universitets åtgärdsarbete utifrån tidigare genomförda revisioner och utvärderingar.

Den sammanfattande bedömningen (för definition se bilaga 3) av det granskade området är:

Otillfredsställande

Den sammanfattande bedömningen bygger på att utförd granskning har identifierat tre (av fem) revisionsfrågor med risknivå mycket hög, en revisionsfråga med risknivå hög samt en revisionsfråga där bedömning av risknivå inte är applicerbar.

Revisionsfrågor med risknivå mycket hög avser:

- Är beslutad handlingsplan för SU:s informationssäkerhetsarbete fullständig utifrån de iakttagelser tidigare granskningar har identifierat?
- Är den interna styrningen och kontrollen av åtgärdsarbetet ändamålsenligt strukturerad för att säkerställa att ett effektivt arbete bedrivs på hela universitetet?
- Sker systematisk och kvalitetssäkrad återrapportering av arbetet med, och effekten av, handlingsplanen till universitetsstyrelsen och andra beslutsfattare/intressenter?

Revisionsfrågor med risknivå hög avser:

- Finns det processer som säkerställer att hinder och utmaningar i arbetet fångas upp och omhändertas?

Revisionsfrågor där bedömning av risknivå inte är applicerbar:

- Finns det processer som anpassar handlingsplanen utifrån ändrade förutsättningar?

2020-11-20

Nils Jeppsson
Kvalitetsansvarig

Niklas Ljung
Ansvarig granskare PwC

Innehållsförteckning

1 Inledning

1.1 Bakgrund och syfte

Internrevisionen genomförde en granskning av Stockholms universitets informationssäkerhet 2017. Utöver denna internrevision har Stockholms universitet på eget initiativ även genomfört en utvärdering av IT- och informationssäkerhet samt penetrationstestgranskningar. Under 2019 beslutade Stockholms universitet att en handlingsplan skulle tas fram för att arbeta med att åtgärda identifierade brister inom IT- och informationssäkerhetsområdena.

Det övergripande syftet med denna internrevisionsgranskning är att utvärdera den interna styrningen och kontrollen av det åtgärdsarbete som genomförs med anledning av tidigare revisioner/utvärderingar, detta gör vi genom att besvara följande 5 revisionsfrågor:

- Är beslutad handlingsplan för SU:s informationssäkerhetsarbete fullständig utifrån de iakttagelser tidigare granskningar har identifierat?
- Är den interna styrningen och kontrollen av åtgärdsarbetet ändamålsenligt strukturerad för att säkerställa att ett effektivt arbete bedrivs på hela universitetet?
- Finns det processer som säkerställer att hinder och utmaningar i arbetet fångas upp och omhändertas?
- Sker systematisk och kvalitetssäkrad återrapportering av arbetet med, och effekten av, handlingsplanen till universitetsstyrelsen och andra beslutsfattare/intressenter?
- Finns det processer som anpassar handlingsplanen utifrån ändrade förutsättningar?

1.2 Metod

Vårt tillvägagångssätt bygger på intervjuer och dokumentanalys där vi utgår ifrån syftet med granskningen och de revisionsfrågor som internrevisionen vid Stockholms universitet har definierat för granskningen. Respektive revisionsfråga bryts ned i ett antal mer detaljerade frågor och dokumenteras i ett granskningsprogram. Frågeställningarna fokuserar på arbetet med handlingsplanen som finns för att åtgärda de informationssäkerhetsbrister som har identifierats under tidigare granskningar på Stockholms universitet. Totalt kommer 10-12 intervjuer att genomföras med koppling till universitets informationssäkerhetsarbete.

PwC kvalitetssäkrar granskningen genom avstämning och faktagranskning av iakttagelser med de intervjuade personerna samt genom intern kvalitetsgranskning av rapporten som helhet. Granskningen sammanfattas sedan i en revisionsrapport med iakttagelser och rekommendationer där revisionsbevis struktureras i enlighet med de identifierade iakttagelserna. För att möjliggöra god spårbarhet och uppföljning kommer iakttagelser och rekommendationer struktureras enligt överenskommelse med Internrevisionen vid Stockholms universitet.

Granskningen omfattar styrande dokument, processer, rutiner samt kontroller inom Stockholms universitet och har inte till syfte att utvärdera hela Stockholms universitet detaljerade informationssäkerhetsarbete, utan det är Stockholms universitets informationssäkerhetsarbete i enlighet med revisionsfrågorna som granskats.

1.3 Begreppsdefinitioner

Under granskningen har PwC utgått från nedan beskrivna tankesätt vad gäller IT-säkerhet och informationssäkerhet som bygger på MSB:s begreppsutredning.

- **Informationssäkerhet** fokuserar på att skydda alla typer av information och informationstillgångar från att hamna i orätta händer, förvanskas eller förstöras. Däri innefattas t ex IT-miljö, men även dokument i pappersform samt andra typer av fysiska tillgångar så som labblokaler, personal, kemikalier och för verksamheten kritiska leverantörer.
- **IT-säkerhet** är det samlade begreppet för att skydda elektronisk information med fokus på IT-miljö, IT-system, datorer, servrar och IT-infrastruktur. IT-säkerhet är en komponent av informationssäkerheten, som syftar till att skydda digital information.
- Det finns flera definitioner av ordet **cybersäkerhet/cyber security**, men de har alla gemensamt att cybersäkerhet består av ett ökande antal verktyg, riskhanteringsmetoder, teknik, utbildning och best praxis teorier för att skydda nätverk, enheter, program och data från attacker eller obehörig åtkomst.

Nedan följer exempel på andra relevanta aktörers definitioner av begreppen.

Datainspektionen:

”**Informationssäkerhet** handlar framför allt om att hindra information från att läcka ut, förvanskas och förstöras. Det handlar också om att rätt information ska finnas tillgänglig för rätt personer, och i rätt tid. Information ska inte kunna hamna i orätta händer och missbrukas.”

MSB:

”**Informationssäkerhe**t är de åtgärder som vidtas för att förhindra att information: görs tillgänglig för eller i övrigt kommer obehöriga till del (konfidentialitet), förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning (riktighet), och information ska kunna utnyttjas i förväntad utsträckning och inom önskad tid (tillgänglighet).”

SU Institutionen för data- och systemvetenskap:

“**IT-säkerhet**, säkerhet beträffande skydd av IT-system och dess data syftande till att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation.”

”**Informationssäkerhet**, säkerhet beträffande skydd av informationstillgångar syftande till att upprätthålla önskad sekretess, riktighet och tillgänglighet (även spårbarhet och oavvislighet) för desamma.”

”**Datasäkerhet**, säkerhet beträffande skydd av datorsystem och dess data syftande till att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling. Datasäkerhet kan betraktas som synonymt med den något vidare termen IT-säkerhet vilken dock även innefattar säkerhet i samband med dator- och telekommunikation (s.k. kommunikationssäkerhet).”

2 Handlingsplan - bakgrund och nuläge

Nedan följer en kort redogörelse för Stockholms universitets åtgärdsarbete fram till idag med anledning av tidigare iakttagelser som gjorts avseende IT- och informationssäkerhet.

I maj 2017 genomfördes en internrevision av universitetets informationssäkerhet. Arbetet rapporterades i rapporten ”Övergripande granskning av informationssäkerhetsarbetet på Stockholms universitet” (Dnr SU FV-1.1.6-0267-17). Med anledning av internrevisionsrapporten beslutade styrelsen vid samma tillfälle om ett antal åtgärder som föreslogs i rektors yttrande, bl.a. att ge IT-avdelningen i uppdrag att utveckla en praktisk vägledning och en genomförandeplan för institutioner och förvaltningsavdelningar i syfte att efterleva universitetets policy och riktlinjer för informationssäkerhet.

Under 2017 - 2018 initierade även verksamheten själva externa utvärderingar av universitets informationssäkerhet samt två penetrationstester för att skaffa sig en tydligare bild av informations- och IT-säkerheten.

I februari 2019 fattade universitetsdirektören beslut om att ge IT-avdelningen i uppdrag att utarbeta en konkret handlingsplan för hur universitetets informationssäkerhet framdeles ska formeras. En sådan handlingsplan utarbetades under perioden februari - mars 2019 och avrapporterades därefter till universitetsdirektören den 29 mars. Handlingsplanens syfte var att ta fram förbättringsåtgärder baserat på en sammantagen analys från samtliga revisioner, utvärderingar och penetrationstester under 2017–2018, samt en incident som också inträffade under den aktuella tidsperioden.

Under 2018 sker ett stort implementeringsarbete av nya rutiner med anledning av ikraftträdandet av den nya Dataskyddsförordningen. I samband med detta är universitetets Informationssäkerhetschef utsedd till tf Dataskyddsombud. Ett nytt Dataskyddsombud rekryterades och tillträdde tjänsten 2019.

Under 2019 skapades en operativ enhet för IT-/informationssäkerhet för Stockholms universitet (”IT-säkerhetsteamet”) med syfte att driva och stödja hela Stockholms universitet i IT- och informationssäkerhetsfrågor. Enheten var initialt placerad på infrastruktursektionen och här var även Informationssäkerhetschefen organiserad.

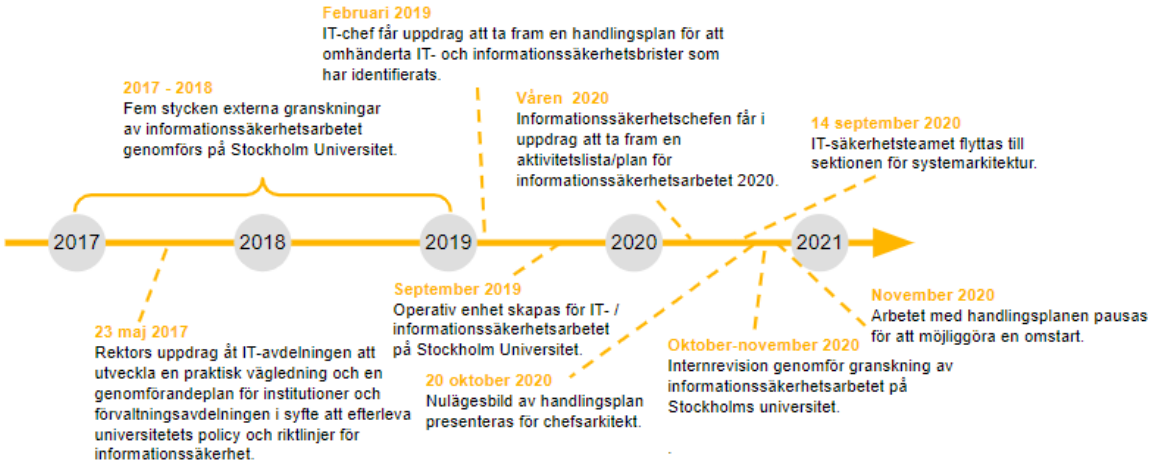
I maj 2020 initierades en organisationsförändring inom IT-avdelningen och den 14 september 2020 flyttas IT-säkerhetsteamet till sektionen för arkitektursektionen (tillhör IT-avdelningen). Syftet med flytten av gruppen var att effektivisera arbetet med handlingsplanen som enligt uppgift hade gått långsamt, bl.a. pga. att infrastrukturfrågor hade prioriterats framför IT- och informationssäkerhetsfrågor. Att lägga IT-säkerhetsteamet tillsammans med portföljområdesarkitekter (tillhör IT-avdelningen) bedöms som tydligare och ge förutsättningar för ett effektivare arbete. Enligt uppgift pågår just nu även en utredning avseende universitetets säkerhetsorganisation i sin helhet, där informationssäkerhetsområdet ingår.

Under våren 2020 får informationssäkerhetschefen i uppdrag av chefen för IT-avdelningen att ta fram en aktivitetslista/plan för informationssäkerhetsarbetet under 2020.

Efter omorganisationen i september 2020 initierar chefsarkitekten en genomgång av arbetet med handlingsplanen för att få en nulägesbild att arbeta vidare efter. Denna genomgång presenteras för chefsarkitekten den 20 oktober 2020. För att få bättre styrning och kontroll på det fortsatta arbetet med handlingsplanen beslutas att arbetet ska bedrivas som projekt enligt PPS modellen och inte i linjeverksamheten. Projektledare ska rapportera löpande till projektets styrgrupp. Chefsarkitekten ingår i styrgruppen och ansvarar för att rapportera handlingsplanens status till chefen för IT-avdelningen och universitetsdirektören.

Arbetet med handlingsplanen har dock pausats under november 2020 på grund av identifierade brister i analysen och handlingsplanen. Man avser att göra ett omtag av arbetet med handlingsplanen

för att säkerställa att den fångar upp alla IT- och informationssäkerhets aspekter samt för att etablera en tillfredsställande styrning och uppföljning av arbetet.



3 Identifierade observationer och risker

3.1 Revisionsfråga 1

Är beslutad handlingsplan för SU:s informationssäkerhetsarbete fullständig utifrån de iakttagelser tidigare granskningar har identifierat?

1.1 Ofullständig handlingsplan	
Observation	Handlingsplanen tillsammans med aktivitetslistan för informationssäkerhet omhändertar inte åtgärder som på ett fullständigt sätt hanterar • alla de observationer/risker som framkommit i tidigare granskningar/utvärderingar • rektorns beslut om åtgärder med anledning av internrevisionens rapport från 2017 (yttrande daterat 2017-05-23, Dnr SU FV 1.1.6-0267-17). • Åtgärder som syftar till att säkra informationssäkerhet på universitetet som helhet
Risk	Risk att strategiskt informationssäkerhetsarbete på övergripande nivå ej genomförs och att informationssäkerhet för universitetet som helhet därmed ej säkras på ett tillfredsställande sätt. En ofullständig handlingsplan ökar risken för att nödvändiga åtgärder i syfte att hantera identifierade brister i informationssäkerhetsarbetet inte vidtas på önskvärt sätt. Brister i informationssäkerheten kan leda till exempelvis obehörigt intrång, förlust av data/information, skadat anseende och förlorade intäkter.
Rekommendation	Överse befintlig handlingsplan och säkerställ att den tar höjd för samtliga identifierade brister och rektorns beslut om åtgärder. I de fall åtgärder ej vidtas bör detta framgå tydligt, tillsammans med förklaring till att risken/observationen ej hanteras. Vid översyn av handlingsplanen kan verksamheten överväga att skapa en särskild handlingsplan för långsiktiga strategiska åtgärder avseende informationssäkerhet. Denna kan kompletteras med den mer operativa och detaljerad handlingsplan som föreligger idag. En sådan uppdelning kan även vara fördelaktig vid återrapportering av status till olika nivåer inom organisationen.

Utökad beskrivning av observation 1.1

Internrevisionsrapporten från 2017 "Övergripande granskning av informationssäkerhetsarbete på Stockholms universitet" föranledde ett yttrande där rektor bland annat beslutade följande:

- "Uppdra åt IT-avdelningen att utveckla en praktisk vägledning och en genomförandeplan för institutioner och förvaltningsavdelningar i syfte att efterleva universitetets policy och riktlinjer för informationssäkerhet."
- "Utreda hur informationssäkerhetsarbetet och förbättringsåtgärder effektivt kan följas upp. I det sammanhanget bör även informationssäkerhetsfunktionens resurser samt ansvarsfördelning mellan institutioner, IT-avdelningen och den övriga centrala förvaltningen utredas".

Genomförd granskning visar att nuvarande handlingsplan ej omfattar åtgärder som tydligt kopplar till ovanstående beslut. Revisionen har heller ej kunnat spåra, varken genom dokumentstudier eller intervjuer, de dokument som specificeras av rektorns beslut, dvs en praktisk vägledning och genomförandeplan för institutioner och förvaltningsavdelningar.

Revisionen har heller inte kunnat identifiera åtgärder som tydligt syftar till att säkra införandet av ett universitetsövergripande ledningssystem för informationssäkerhet. Åtgärder har i stor utsträckning fokuserats kring IT-säkerhet och IT-enhetens arbete, exempelvis på åtgärder är " Införa SULIS[1] anvisningar i IT-avdelningens förvaltning" och "Ta helhetsgrepp över IT-säkerhet på SU".

[1] Stockholms universitets ledningssystem för informationssäkerhet.

PwC noterar att informationssäkerhetschefens nuvarande organisatoriska placering inom IT-avdelningen kan vara en av flera bidragande orsaker till att ett myndighetsövergripande och strategiskt informationssäkerhetsperspektiv inte omhändertas av handlingsplanen på ett tillfredsställande sätt. Enligt uppgift pågår just nu en utredning av Säkerhetsorganisationens utformning, där informationssäkerhetschefens placering ingår.

Vidare kan PwC konstatera att för de observationer/iakttagelser som ej hanteras av handlingsplanen saknas det en förklaring till varför de inte inkluderas, eller beskrivning av hur de eventuellt omhändertas på annat sätt.

Revisionsfråga 1 - Övergripande bedömning

Baserat på ovanstående observationer är vår sammanfattade bedömning att handlingsplanen ej är fullständig och revisionsfråga 1 har riskklassificerats som: **Mycket hög**.

3.2 Revisionsfråga 2

Är den interna styrningen och kontrollen av åtgärdsarbetet ändamålsenligt strukturerad för att säkerställa att ett effektivt arbete bedrivs på hela universitetet?

2.1 Handlingsplanens utformning är ej ändamålsenlig	
Observation	Handlingsplanens nuvarande utformning bedöms inte ge tillräckliga förutsättningar för en effektiv styrning, kontroll och rapportering av åtgärdsarbetet inom hela universitetet, exempelvis: • Flera åtgärder är formulerade på en så pass övergripande nivå att det svårt att få en uppfattning om vilka konkreta åtgärder som ska vidtas inom ett område, vad åtgärden innebär och vad som krävs för att området ska anses omhändertaget och därmed bedömas som klart. • Flera åtgärder är formulerade så att arbetet begränsas till IT-enheten snarare än att de tar höjd för hela universitetet och dess institutioner. • Ansvar och tidplan för respektive åtgärd är på en övergripande nivå.
Risk	Risk att risker/observationer inte åtgärdas på önskvärt sätt om handlingsplanen inte är utformad på ett ändamålsenligt sätt och involverar hela organisationen där detta bedöms vara nödvändigt. Brister i handlingsplanen kan även påverka åtgärdsarbetets effektivitet samt att brister och/eller förseningar i åtgärdsarbetet inte identifieras, rapporteras och hanteras på önskvärt sätt. Vidare finns risk att tid och resurser inte används på ett effektivt och ändamålsenligt sätt i åtgärdsarbetet
Rekommendation	Överse handlingsplanen, och utformningen av denna, så att den blir ett effektivt verktyg för god intern styrning och kontroll av åtgärdsarbetet. Det är viktigt att handlingsplanen bidrar till ökad tydlighet, samt ger det stöd och kraft som krävs för att tidigare identifierade brister ska omhändertas på ett effektivt sätt. Säkerställ att man i samband med översynen av handlingsplanen förtydligar och bryter ner både ansvar och tidsplanering för handlingsplanens alla åtgärder. Detta för att det enklare ska gå att följa arbetet och att framgångar och motgångar lättare ska kunna rapporteras in och hanteras på ett effektivt sätt. Säkerställ att projektet tar fram tydliga rapporteringspunkter som är förankrade med mottagaren för att säkerställa att rapporteringen ger det värde som är avsätt.

2.2 Bristfällig förankring av handlingsplan	
Observation	Genomförda intervjuer indikerar att handlingsplanen inte har förankrats på alla nivåer i verksamheten på önskvärt sätt. PwC noterar att detta till viss del kan bero på att handlingsplanen inte är fullständig och därmed inte tar höjd för hela informationssäkerhetsperspektivet och universitets samtliga verksamhetsdelar på önskvärt sätt. Vidare indikerar granskningen att den generella medvetenheten om institutionernas delegerade ansvar för att bedriva ett systematiskt informationssäkerhetsarbete inom den egna verksamheten kan stärkas. Genomförda intervjuer visar även att exempelvis chefsutbildningen, som är obligatorisk för alla nya prefekter, inte innehåller någon information om de krav som ställs avseende systematiskt informationssäkerhetsarbete PwC noterar att behovet av åtgärder i syfte att säkra kontinuerlig utbildning för universitets personal framgick av internrevisionsrapporten 2017 och att åtgärder skulle vidtas enligt rektors yttrande.
Risk	Risk att åtgärdsarbetet avseende informationssäkerhet, liksom det systematiska informationssäkerhetsarbetet över tid, ej bedrivs effektivt inom hela verksamheten pga bristfällig förankring av regelverk och handlingsplan.
Rekommendation	Etablera rutiner som säkerställer att relevanta styrdokument, och beslutad handlingsplan, avseende informationssäkerhetsarbetet, förankras på alla nivåer inom universitetet. Det är av stor vikt att alla som har ett informationssäkerhetsansvar på universitetet också har nödvändig kunskap och förståelse för vad detta ansvar innebär i relation till beslutad handlingsplan och systematiskt säkerhetsarbete.

Revisionsfråga 2 - Övergripande bedömning

Baserat på ovanstående observationer är vår sammanfattade bedömning att den interna styrningen och kontrollen av åtgärdsarbetet ej är uppbyggd på ett sätt som säkrar ett effektivt arbete och att detta bedrivs på alla relevanta nivåer in universitetet. Revisionsfråga 2 har riskklassificerats som: **Mycket hög**.

3.3 Revisionsfråga 3

Finns det processer som säkerställer att hinder och utmaningar i arbetet fångas upp och omhändertas?

3.1 Hinder och utmaningar identifieras ej på systematiskt sätt	
Observation	Nuvarande rutiner/arbetssätt säkerställer inte att potentiella eller konstaterade hinder och utmaningar för åtgärdsarbetet identifieras och hanteras på ett systematiskt och förebyggande sätt.
Risk	Avsaknad av rutiner/arbetssätt för att identifiera och hantera hinder och utmaningar i arbetet, ökar risken för att åtgärdsarbetet blir reaktivt snarare än proaktivt. Resultatet kan bli att potentiella risker inte hanteras på önskvärt sätt, att ineffektivitet i arbetet uppstår och/eller att förhöjda kostnader eller ökad resursåtgång uppstår på lång sikt.
Rekommendation	Överväg att genomföra regelbundna riskanalyser för att på så sätt identifiera hinder och utmaningar i åtgärdsarbetet avseende informationssäkerhet. Identifierade risker, och förslag till hantering, bör därefter regelbundet kommuniceras till relevanta beslutsfattare som genom beslut om hantering kan ge förutsättningar för ett fortsatt effektivt åtgärdsarbete.

Revisionsfråga 3 - Övergripande bedömning

Baserat på ovanstående observationer är vår sammanfattade bedömning att det saknas processer som säkerställer att hinder och utmaningar i arbetet fångas upp och omhändertas på önskvärt sätt. Revisionsfråga 3 har riskklassificerats som: **Hög**.

3.4 Revisionsfråga 4

Sker systematisk och kvalitetssäkrad återrapportering av arbetet med, och effekten av, handlingsplanen till universitetsstyrelsen och andra beslutsfattare/intressenter?

4.1 Bristande återrapportering av åtgärdsarbete utifrån handlingsplanen	
Observation	Utförd granskning visar att det saknas tydlighet på kraven för återrapportering av åtgärdsarbetet avseende vad som ska rapporteras, av vem, till vem och med vilken frekvens. Återrapportering har skett enligt uppgift, revisionen har dock inte kunnat ta del av tydliga uppgifter om vad som har rapporteras, till vem, med vilken frekvens och om rapporteringen har föranlett några korrigerande åtgärder. Revisionen har inte kunnat verifiera att det har skett någon systematisk och kvalitetssäkrad återrapportering av åtgärdsarbetet med, och effekten av, handlingsplanen till universitetsstyrelsen, projektstyrgrupp och andra beslutsfattare/intressenter på universitetsövergripande nivå.
Risk	Risk att brister/avvikelser åtgärdsarbetet inte identifieras och hanteras på ett systematiskt och effektivt sätt. Risk för att universitetsstyrelsen och andra beslutsfattare/intressenter inte kan agera och säkerställa att observationer/risker hanteras på önskvärt sätt pga bristfällig återrapportering.
Rekommendation	Identifiera relevanta intressenter/beslutsfattare från hela universitetet, fastställ vilken information de bör ta del av och utarbeta rutiner som säkerställer en behovsbaserat och systematisk återrapportering. Inriktning och omfattning av rapporteringen bör anpassas utifrån mottagarens ansvar och behov. Genomför en genomgång med identifierade beslutsfattare/intressenter och verifiera att planerad rapportering, är i linje med deras önskemål. Överväg att integrera statusrapporteringen avseende handlingsplanens åtgärder med redan befintliga rapporteringsstrukturer som exempelvis tertialrapportering och riskrapportering.

Utökad beskrivning av observation 4.1

PwC noterar det faktum att handlingsplanen i flera fall endast beskriver aktiviteter på en övergripande nivå (se Revisionsfråga 1) vilket i sin tur försvårar en adekvat uppföljning och statusrapportering som på ett tydligt sätt visar hur långt man har kommit och vad som återstår.

Vidare bedömer PwC att nuvarande organisation, där informationssäkerhetschefen är placerad hos sektionen för arkitektursektionen och rapporterar enligt linjen, ger upphov till långa och i viss utsträckning otydliga rapporteringsvägar. Sammantaget ökar detta risken för att rapporteringen blir tidskrävande, ineffektiv och splittrad.

Avslutningsvis noteras att det i genomförda intervjuer uppges att åtgärdsarbetet ska bedrivas annorlunda framgent och att tätare rapporteringar till projektets styrgrupp ska säkras i och med den nya organisationen som trädde i kraft 14 september 2020. Vid granskningstillfället är dock den nya rapporteringsrutinen ännu inte fastställd.

Som exempel på brist i statusrapporteringen i oktober 2020 kan nämnas att rapporten inte förklarar vad som ligger till grund för klarmarkering av åtgärder. Till exempel har aktivitet ”SU-IT-02” bedömts som klar i rapporten men granskningen visar att informationssäkerhetsorganisation anser att man endast är klar till 70%.

Revisionsfråga 4 - Övergripande bedömning

Baserat på ovanstående observationer är vår sammanfattade bedömning att det saknas systematisk och kvalitetssäkrad återrapportering av arbetet med, och effekten av, handlingsplanen till universitetsstyrelsen och andra beslutsfattare/intressenter. Revisionsfråga 4 har riskklassificerats som: **Mycket hög**.

3.5 Revisionsfråga 5

Finns det processer som anpassar handlingsplanen utifrån ändrade förutsättningar?

5.1	
Observation	PwC har ej kunnat spåra några processer med syfte att fånga upp ändrade förutsättningar och anpassa krav/åtgärder i handlingsplanen utifrån dessa. Med förändrade förutsättningar menas exempelvis förändrad lagstiftning, nya direktiv från regeringen, nya revisioner/utvärderingar etc Enligt uppgift ska förändrade förutsättningar inte fångas upp och inkluderas i handlingsplanen utan dessa ska fångas upp och hanteras av linjeorganisationen i det löpande arbetet. Linjeorganisationens arbete med detta har inte granskats inom ramen för denna revision.
Risk	E/T
Rekommendation	E/T

Revisionsfråga 5 - Övergripande bedömning

Då handlingsplanen enligt uppgift ej ska omfatta åtgärder med anledning av förändrade förutsättningar har PwC valt att inte göra någon övergripande bedömning för detta område. Dock vill PwC poängtera vikten av att åtgärder som vidtas i linjen stäms av mot befintliga åtgärder i handlingsplanen för att säkra ett effektivt arbete, och undvika risk för dubbelarbete.

4 Bilagor

4.1 Bilaga 1

Genomförda intervjuer

Intervjuer har genomförts med följande personer:

Titel	**Tillhörighet**
Informationssäkerhetschef	IT-avdelningen
IT-chef	IT-avdelningen
Säkerhetschef	Fastighetsavdelningen
Datasskyddsombud	Rättssekretariatet vid Rektors kansli
IT-säkerhetsspecialist	IT-avdelningen
Universitetsdirektör	Rektors kansli
Professor	Institutionen för data- och systemvetenskap
Projektledare (konsult)	IT-avdelningen
Chefsarkitekt	IT-avdelningen
Överbibliotekarie	Universitetsbibliotek
Administrativ chef	Institutionen för molekylär biovetenskap Wenner-Grens institut
Professor	Institutionen för molekylär biovetenskap Wenner-Grens institut
Datoransvarige	Historiska respektive Filosofiska institutionen
Universitetslektor	Filosofiska institutionen

4.2 Bilaga 2

Dokumentlista

Handlingsplan för ökad IT- och informationssäkerhet
SU yttrande informationssäkerhet styrelsen 2 juni 2017
Stockholms Universitet Infosäk Rapport 15 maj
Skrivelse från dep_Vikten av ett systematiskt säkerhetsarbete
Säkerhetspolicy vid Stockholms universitet RF 2017-01-26
Riktlinjer för informationssäkerhet RF 2017-01-26
PwCrapport_utvärdering infosäk_2018
Intranättext_Stockholms universitets ledningssystem för informationssäkerhet
Informationsklassning
GDPR-folder för prefekteradm chefer_2018-05-04
Besluts- och delegationsordning 2020-08-27
Arbetsordning vid Stockholms universitet (fr.om. 200922)
Uppföljning av HPITINFOSÄK-status maj 2020
Uppföljning Handlingsplan för bättre IT- och informationssäkerhet för Stockholms universitet

4.3 Bilaga 3

Klassificering

Bedömningsskala	***Bedömning av ett helt granskningsområde (rapport)***
Otillfredsställande	En eller flera mycket kritiska iakttagelser i den interna styrningen och kontrollen vilka innebär att organisationen exponeras för en oacceptabel risknivå.
Större förbättringsmöjligheter	En eller flera kritiska iakttagelser i den interna styrningen och kontrollen noterade vilka kan resultera i en oacceptabel risknivå.
Förbättringsmöjligheter	En eller flera iakttagelser i den interna styrningen och kontrollen noterade vilka kan resultera i en oacceptabel risknivå.
Tillfredsställande	Inga väsentliga brister i den interna styrningen och kontrollen har identifierats.
Ej tillämplig	Uppdraget genomfördes inte enligt en PwC metodik där en sammanfattande bedömning av granskat område ingår.

Varje enskild revisionsfråga har riskklassificerats enligt följande skala:

Mycket hög	**Hög**	**Medel**	**Låg**

Kriterierna för den riskbedömning som gjorts avseende granskningen har grundat sig på en sammanvägning av sannolikheten för händelsens inträffande samt den möjliga konsekvens som händelsens inträffande kan innebära för verksamheten.

Denna rapport har upprättats inom ramen för vårt uppdrag att utföra internrevisionstjänster. Rapporten är endast upprättad för vår uppdragsgivares räkning, Stockholms universitet, och får inte lämnas ut eller göras tillgänglig för andra fysiska eller juridiska personer utan Öhrlings PricewaterhouseCoopers AB:s/ PricewaterhouseCoopers AB:s skriftliga godkännande. I avsaknad av skriftligt godkännande, tar Öhrlings PricewaterhouseCoopers AB/ PricewaterhouseCoopers AB inte något som helst ansvar gentemot någon annan än uppdragsgivaren som väljer att förlita sig på eller att agera utifrån innehållet i denna rapport. Inte heller tas något ansvar för att rapporten används för andra syften än för dem som förelegat vid uppdragets utförande.

Stockholms universitet

2021-02-19 Dnr SU FV 1.1.6-0295-20

Rektor

Ulf Nyman
Utredare
Rektors kansli

Yttrande över PwC-rapport Granskning av informationssäkerhet

Bakgrund

Under 2017 och 2018 skedde ett antal granskningar av Stockholms universitets IT- och informationssäkerhet, och det arbete som görs inom ramen för dessa områden. Några av granskningarna gjordes med anledning av ett allmänt behov av översyn och utveckling, medan ett par hade en mer direkt koppling till en större IT-incident under september 2018. Granskningarna var:

- Övergripande granskning av informationssäkerhetsarbetet vid Stockholms universitet, genomförd i maj 2017 av PwC på uppdrag av universitetets internrevision.
- Mognadsanalys av universitetets IT-säkerhet, genomförd i april 2018 av SecureLink.
- IT-forensisk utredning, genomförd i september 2018 med anledning av IT-incidenten.
- *Internal Penetration Test* på ett urval system samt en sårbarhetsanalys, genomförda i november 2018 av SecureLink.
- Granskning av universitetets informationssäkerhet, genomförd i december 2018 av PwC.

Som ett resultat av dessa beslutades i januari 2019 om ett uppdrag till IT-avdelningen att genomföra en sammantagen analys av granskningarna, och att utifrån dem ta fram en handlingsplan med en prioritering av åtgärder på kort och lång sikt. Handlingsplanen färdigställdes i mars 2019.

PwC:s granskning och rapport

På uppdrag av internrevisionen gjorde PwC under 2020 en förnyad granskning av Stockholms universitets informationssäkerhetsarbete, och en granskningsrapport lades fram i november 2020. Granskningens övergripande syfte var att utvärdera universitetets interna styrning och kontroll av åtgärdsarbetet utifrån tidigare gjorda granskningar.

Rapportens sammantagna bedömning är att den interna styrningen och kontrollen av universitetets åtgärdsarbete är otillfredsställande. Detta menar PwC har sin grund i flera komponenter, och som kan sammanfattas i följande övergripande observationer:

- Handlingsplanen från 2019 är ofullständig och täcker inte in de observationer/risker som framkommit i tidigare granskningar.
- Handlingsplanen är inte ändamålsenlig, och bedöms inte ge tillräckliga förutsättningar för en effektiv styrning, kontroll och rapportering av åtgärdsarbetet.

Stockholms universitet

- Nuvarande rutiner/arbetssätt säkerställer inte en proaktiv identifiering och hantering av hinder och utmaningar.
- Återrapporteringen av åtgärdsarbetet behöver tydliggöras och stärkas.

Rektors bedömning och förslag på åtgärder

Information och tillhörande informationsteknik är en ytterst viktig strategisk resurs för verksamheten vid Stockholms universitet. Genom att ha en god informationssäkerhet tryggas den information som är viktig för universitetet. Bevarande av informations konfidentialitet, riktighet och tillgänglighet måste säkras.

Rektor instämmer i allt väsentligt i rapportens konstateranden och slutsatser, och bedömer PwC:s och Internrevisionens rekommendationer som rimliga.

För att på sikt kunna nå en tydlig nivåhöjning av det löpande arbetet är bedömningen att det i nuläget krävs en grundlig översyn av hur informationssäkerhetsarbetet bedrivs vid universitetet.

Översynsarbetet är påbörjat och ett särskilt projekt kommer att inrättas för att:

1. Identifiera särskilt skyddsvärd information vid universitetet och bedöma risken för eventuella informationsförluster kopplat till dessa. I den samlade bedömningen av risker ska universitetsledningen involveras. För att säkerställa en systematisk återrapportering av informationssäkerhetsarbetet ska det så långt möjligt integreras i universitetets ordinarie verksamhetsledningsprocess.
2. Etablera och resurssätta en organisation som möjliggör styrning och uppföljning av det löpande informationssäkerhetsarbetet vid hela universitetet. Att åstadkomma ett ändamålsenligt stöd till institutioner och enskilda forskare ska vara en utgångspunkt i det arbetet.
3. Säkerställa att de brister som i övrigt uppmärksammas i granskningsrapporten hanteras.
4. Säkerställa att samordning sker med andra arbetsområden där så är relevant.

Rektor uppdrar därför åt universitetsdirektören att i samråd med vicerektorer och berörda enhetschefer inom förvaltningen tillsätta en strategisk styrgrupp för projektets genomförande.

Projektresultatet ska återrapporteras till universitetsledningen i slutet av december 2021. Därefter vidtar verksamhetens fortsatta implementering av projektresultatet; detta arbete rapporteras löpande till universitetsledningen under 2022.