



Stockholms  
universitet

Universitetsstyrelsen

Protokoll fört vid sammanträde  
2025-04-28 (nr 2 2025)  
kl 09.00-12.00

- Närvarande: Justitierådet Helena Jäderblom (ordförande), rektor Hans Adolfsson, stadsdirektören Fredrik Jurdell, senior ekonom Robert Bergqvist, styresman Sanne Houby-Nielsen, civilingenjör Anna Rathsmann, universitetsrektor Tiit Land, Senior Advisor Tuula Teeri, verkställande direktör Erik Brandsma, professor Martin Jakobsson, professor Yvonne Svanström, professor Stefan Helgesson, kårordförande Hermela Embaye, vice kårordförande Victor Nygren och doktorand Karl Sigfrid
- Huvudföredragande: Universitetsdirektör Åsa Borin
- Föredragande: Planeringschef Karin Fürstenbach (pp. 4 och 8), utredare Anna Riddarström (p. 5), internrevisionschef Tobias Björn (pp. 6-7), universitetsdirektör Åsa Borin (pp. 6-7), IT-revisor Magnus Andersson (p. 7), controller Clara Ersson (p. 9), controller Marie Eriksson (p. 9) samt säkerhetschef Peter Klysing (p. 10)
- Övriga närvarande: Professor Jane Reichel (ersättare) (pp. 1-4, 7-11), professor Joakim Edsjö (ersättare), prorektor Clas Hättestrand, universitetsdirektör Åsa Borin, avdelningschef Lena Ousbäck, internrevisionschef Tobias Björn, planeringschef Karin Fürstenbach, chefsjurist Markos Stavroulakis, controller Clara Ersson (pp. 6, 7 och 9), IT-revisor Magnus Andersson (p. 7), IT-chef Petra Lagerkvist (p. 7), informationssäkerhetschef Fredrik Bolinder (p. 7), controller Marie Eriksson (p. 9), säkerhetschef Peter Klysing (p. 10), Camilla Gamrell (ST), Ingrid Lander (SACO) samt utredare Anna Riddarström
- Protokollförelse: Utredare Anna Riddarström

1. Utseende av justeringsperson Robert Bergqvist utses till justeringsperson.
2. Fastställande av dagordning Dagordningen fastställs.
3. Information från rektor Rektor informerar om diskussioner kring den akademiska friheten i USA, vårpropositionen och vårändringsbudgeten samt om antagningsstatistik för sommar- och höstterminen 2025. Vidare informerar rektor om kommande utredningar, om samordning av nationell e-infrastruktur och om olika aktioner på campus.
4. Anmälan av Riksrevisionens revisionsberättelse samt revisors rapport för 2024 (dnr SU FV-3877-24) Universitetsstyrelsen beslutar att lägga revisionsberättelsen och revisors rapport till handlingarna (bilaga 1).

- |     |  |  |
|-----|--|--|
| 5.  | Beslut om utseende av prorektor för perioden 2025-07-01 – 2031-06-30 (dnr SU FV-2996-24)   | Universitetsstyrelsen beslutar att utse professor Jane Reichel till prorektor för perioden 2025-07-01 – 2031-06-30.<br><br>Punkten förklaras omedelbart justerad.<br><br>Det antecknas att Jane Reichel inte närvarade vid beslutet.   |
| 6.  | Beslut med anledning av Internrevisionens institutionsgranskningar 2024 (dnr SU FV-0495-24 och SU FV-0973-25)                        | Universitetsstyrelsen beslutar att uppdra åt rektor att vidta erforderliga åtgärder i enlighet med yttrandet (bilaga 2) samt att lägga Internrevisionens rapport till handlingarna (bilaga 3).   |
| 7.  | Beslut med anledning av revisionsrapport från Internrevisionen avseende granskning av IT-säkerhet (dnr SU FV-0495-24 och FV-0975-25) | Universitetsstyrelsen beslutar att uppdra åt rektor att vidta erforderliga åtgärder i enlighet med reviderat yttrande (bilaga 4) samt att lägga Internrevisionens rapport till handlingarna (bilaga 5).  |
| 8.  | Komplettering av beslut om fördelning av anslagsmedel för budgetåret 2025 (dnr SU FV-2544-24)  | Universitetsstyrelsen beslutar att ge rektor delegation att besluta om fördelning av den generella förstärkningen av basanslaget för forskning och utbildning på forskarnivå om 10 888 000 kronor.<br><br>Vidare beslutar universitetsstyrelsen att de 8 000 000 kronor som enligt vårändringsbudgeten avser Nordita fördelas dit. |
| 9.  | Årsredovisning 2024 – jämförelse med andra statliga universitet (dnr SU FV-1188-25)  | Information  |
| 10. | Information om säkerhetsarbetet vid Stockholms universitet   | Information  |
| 11. | Övriga frågor  | Inga övriga frågor anmäldes.   |

## Revisionsberättelse

Beslutad: 2025-03-21

Diarienummer: 3.1.2-2024-167

---

Regeringen  
103 33 Stockholm

# Revisionsberättelse för Stockholms universitet 2024

Riksrevisionen har enligt 5 § lagen (2002:1022) om revision av statlig verksamhet m.m. utfört en revision av årsredovisningen för Stockholms universitet 2024, daterad 2025-02-19.

Revisionsberättelsen innehåller sammantaget fem uttalanden. Om inget av dessa uttalanden innehåller en reservation eller avvikande mening innebär det att Riksrevisionen bedömer att redovisningen och underliggande redovisning är tillförlitlig, räkenskaperna är rättvisande samt att ledningens förvaltning följer tillämpliga föreskrifter och särskilda beslut.

## Rapport om årsredovisningen

### Uttalanden

Enligt Riksrevisionen har myndigheten

- upprättat årsredovisningen enligt förordningen (2000:605) om årsredovisning och budgetunderlag, högskolelagen (1992:1434), högskoleförordningen (1993:100), regleringsbrev och särskilda regeringsbeslut för myndigheten

- i alla väsentliga avseenden gett en rättvisande bild av Stockholms universitets ekonomiska resultat, finansiering och finansiella ställning per den 31 december 2024
- lämnat en resultatredovisning och information i övrigt som är förenlig med och stödjer en rättvisande bild i årsredovisningen som helhet.

## Grund för uttalanden

Riksrevisionen har utfört revisionen enligt International Standards of Supreme Audit Institutions (ISSAI) för finansiell revision, samt Riksrevisionens interna föreskrifter

- Riksrevisionens granskning av resultatredovisning och övrig information i årsredovisningen, inklusive ledningens bedömning av intern styrning och kontroll (IFRF)
- Riksrevisionens granskning av ledningens förvaltning som del i årsredovisningsgranskningen (IFRLF)

Vårt ansvar enligt standarderna beskrivs närmare i avsnittet Revisorns ansvar. Vi är oberoende i förhållande till myndigheten i enlighet med ISSAI 130 Code of Ethics och har i övrigt fullgjort vårt ansvar i enlighet med dessa etiska regler. Vi anser att de revisionsbevis vi har erhållit är tillräckliga och ändamålsenliga som grund för Riksrevisionens uttalanden.

## Uttalande om ledningens efterlevnad av tillämpliga föreskrifter för användning av anslag och inkomster

Baserat på vår revision av årsredovisningen, bedömer Riksrevisionen att myndigheten i alla väsentliga avseenden använt anslag och inkomster i enlighet med av riksdagen beslutade ändamål och i överensstämmelse med tillämpliga föreskrifter.

## Grund för uttalande

Riksrevisionen har utfört revisionen enligt ISSAI för finansiell revision och IFRLF. Vårt ansvar enligt dessa standarder beskrivs närmare i avsnittet Revisorns ansvar. Vi anser att de revisionsbevis vi har erhållit är tillräckliga och ändamålsenliga som grund för Riksrevisionens uttalanden.

## Uttalande om ledningens bedömning av intern styrning och kontroll

Det har vid vår revision av årsredovisningen inte framkommit något som skulle tyda på att ledningen i sin bedömning av intern styrning och kontroll inte har följt förordningen (2007:603) om intern styrning och kontroll.

## Grund för uttalande

Riksrevisionen har utfört revisionen enligt ISSAI för finansiell revision samt IFRF och IFRLF. Vårt ansvar enligt dessa standarder beskrivs närmare i avsnittet Revisorns ansvar. Vi anser att de bevis vi har erhållit är tillräckliga och ändamålsenliga som grund för Riksrevisionens uttalanden.

## Myndighetsledningens ansvar

Myndighetsledningen ansvarar för myndighetens verksamhet och ska se till att den bedrivs effektivt och enligt gällande rätt och de förpliktelser som följer av Sveriges medlemskap i Europeiska unionen, att den redovisas på ett tillförlitligt och rättvisande sätt samt att myndigheten hushållar väl med statens medel. Detta framgår av 3 § myndighetsförordningen (2007:515).

Myndighetsledningen har även ansvaret för att upprätta en årsredovisning som ger en rättvisande bild enligt förordningen (2000:605) om årsredovisning och budgetunderlag samt i enlighet med högskolelagen (1992:1434), högskoleförordningen (1993:100), regleringsbrev och övriga regeringsbeslut för myndigheten. Myndighetsledningen är även ansvarig för att anslagsmedel och inkomster har använts enligt de bestämmelser och villkor som anges i föreskrifter, regleringsbrev och andra regeringsbeslut.

Myndighetsledningen ansvarar också för att det finns en intern styrning och kontroll som säkerställer att årsredovisningen kan upprättas utan väsentliga felaktigheter, vare sig dessa beror på oegentligheter eller misstag. I myndighetsledningens ansvar ingår att lämna en bedömning om den interna styrningen och kontrollen vid myndigheten. Det framgår av förordningen (2000:605) om årsredovisning och budgetunderlag. Myndighetsledningen ansvarar även för att det finns en process för intern styrning och kontroll vid myndigheten som fungerar på ett betryggande sätt. Detta framgår av förordningen (2007:603) om intern styrning och kontroll. Denna process ska säkerställa att myndigheten med rimlig säkerhet fullgör sina uppgifter, uppnår verksamhetens mål och uppfyller kraven i 3 § myndighetsförordningen (2007:515).

Vid upprättandet av årsredovisningen ska myndighetsledningen förutsätta att myndigheten ska fortsätta sin verksamhet. De upplyser, när så är tillämpligt, om avvikelser och skälen för dessa avvikelser.

## Revisorns ansvar

Vårt ansvar är att granska årsredovisningen. Våra mål är att uppnå en rimlig grad av säkerhet om att årsredovisningen som helhet inte innehåller några väsentliga felaktigheter, vare sig dessa beror på oegentligheter eller misstag, och att lämna en revisionsberättelse som innehåller Riksrevisionens uttalanden. Rimlig säkerhet är en hög grad av säkerhet, men är ingen garanti för att en revision som utförs enligt ISSAI, IFRF och IFRLF alltid kommer att upptäcka en väsentlig felaktighet om en

sådan finns. Felaktigheter kan uppstå på grund av oegentligheter eller misstag och anses vara väsentliga om de enskilt eller tillsammans rimligen kan förväntas påverka de ekonomiska beslut som användare fattar med grund i årsredovisningen.

Som en del av en revision enligt ISSAI använder vi professionellt omdöme och har en professionellt skeptisk inställning under hela revisionen. Dessutom

- identifierar och bedömer vi riskerna för väsentliga felaktigheter i årsredovisningen, vare sig dessa beror på oegentligheter eller misstag. Därefter utformar och utför vi granskningsåtgärder bland annat utifrån dessa risker, och inhämtar revisionsbevis som är tillräckliga och ändamålsenliga för att utgöra en grund för våra uttalanden. Risken för att inte upptäcka en väsentlig felaktighet till följd av oegentligheter är högre än för ett fel som beror på misstag eftersom oegentligheter kan innefatta agerande i maskopi, förfalskning, avsiktliga utelämnanden, felaktig information eller åsidosättande av intern styrning och kontroll
- skaffar vi oss en förståelse för den del av myndighetens interna styrning och kontroll som har betydelse för vår revision för att utforma revisionsåtgärder som är lämpliga med hänsyn till omständigheterna, men inte för att uttala oss om effektiviteten i myndighetens interna styrning och kontroll
- utvärderar vi lämpligheten i de redovisningsprinciper som används och rimligheten i ledningens uppskattningar i redovisningen och tillhörande upplysningar
- drar vi en slutsats om det riktiga i att myndighetsledningen använder antagandet om fortsatt drift vid upprättandet av årsredovisningen. Vi drar också en slutsats, med grund i de inhämtade revisionsbevisen, om huruvida det finns någon väsentlig osäkerhetsfaktor som avser sådana händelser eller förhållanden som kan leda till betydande tvivel om myndighetens förmåga att fortsätta verksamheten. Om vi drar slutsatsen att det finns en väsentlig osäkerhetsfaktor, ska vi i revisionsberättelsen fästa uppmärksamheten på upplysningarna i årsredovisningen om den väsentliga osäkerhetsfaktorn och den bedömning som lämnats eller, om sådana upplysningar är otillräckliga, modifiera våra uttalanden om årsredovisningen
- utvärderar vi den övergripande presentationen, strukturen och innehållet i årsredovisningen, däribland upplysningarna, och om årsredovisningen återger de underliggande transaktionerna och händelserna på ett sätt som ger en rättvisande bild.

Som en del av granskningen i enlighet med IFRF planerar och genomför vi revisionen för att

- för väsentlig information, av finansiell eller icke finansiell natur som lämnas i resultatredovisningen inhämta tillräckliga och ändamålsenliga revisionsbevis

för att sådan information har upprättats med syfte att tillsammans med årsredovisningens övriga delar ge en rättvisande bild av verksamheten utifrån regelverket

- för övrig information, förvissa oss om att denna är förenlig med de övriga delarna i årsredovisningen och fri från väsentliga fel, baserat på vår kunskap om myndigheten.

Vår kommunikation med myndighetsledningen innefattar bland annat revisionens planerade omfattning och inriktning och betydelsefulla iakttagelser under revisionen, däribland eventuella betydande brister i den interna styrningen och kontrollen som vi identifierar under revisionen.

Vårt ansvar är också att granska om ledningens förvaltning följer tillämpliga föreskrifter och särskilda beslut. Vi genomför granskningen enligt IFRLF. Utöver de regelverk och särskilda beslut som direkt påverkar redovisningen, innefattar detta de föreskrifter som är direkt hänförliga till användningen av medel som riksdag och regering beslutar om<sup>1</sup>. På basis av genomförd revision av årsredovisningen lämnar vi ett uttalande med rimlig säkerhet om myndighetens efterlevnad av dessa regelverk.

Vid planering och genomförande av revisionen enligt ISSAI och IFRF beaktar vi de delar av den interna styrningen och kontrollen som är relevanta för hur myndigheten upprättar årsredovisningen för att ge en rättvisande bild, inklusive ledningens bedömning om den interna styrningen och kontrollen. Det innebär att vi har granskat den bedömning som ledningen har gjort om intern styrning och kontroll i årsredovisningen. I vårt ansvar ingår däremot inte att göra ett uttalande om effektiviteten i myndighetens interna styrning och kontroll. Vi gör ett uttalande med begränsad säkerhet avseende ledningens bedömning av intern styrning och kontroll baserat på de åtgärder vi har vidtagit för att granska årsredovisningen. Ett uttalande med begränsad säkerhet har inte den säkerhet som ett uttalande grundad på en revision har.

Ansvarig revisor Henrik Laginder har beslutat i detta ärende. Uppdragsledare Erik Lejon har varit föredragande.

Henrik Laginder

---

<sup>1</sup> Anslagsförordningen (2011:223), avgiftsförordningen (1992:191), förordningen (2011:211) om utlåning och garantier, kapitalförsörjningsförordningen (2011:210), förordningen (1996:1190) om överlåtelse av statens fasta egendom och förordningen (1996:1191) om överlåtelse av statens lösa egendom.

**Kopia för kännedom**

Stockholms universitet

Utbildningsdepartementet

Finansdepartementet, budgetavdelningen

## Revisors rapport

Beslutad: 2025-03-21

Diarienummer: 3.1.2-2024-167

---

Regeringen  
103 33 Stockholm

# Revisors rapport i enlighet med 7§ transparenslagen, Stockholms universitet för 2024

Enligt lag (2005:590) om insyn i vissa finansiella förbindelser m.m. (i fortsättningen benämnd transparenslagen) ska myndighetens revisor för varje räkenskapsår granska om en öppen redovisning och en separat redovisning har fullgjorts i enlighet med bestämmelserna i transparenslagen. Det har Riksrevisionen, i egenskap av revisor för Stockholms universitet, gjort för räkenskapsåret 2024 genom en översiktlig granskning. Enligt transparenslagen får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om redovisning och revision. Eftersom sådana föreskrifter inte utfärdats har myndigheten gjort sin egen tolkning av transparenslagen och upprättat sin redovisning för räkenskapsåret 2024 i enlighet därmed.

Det är myndighetens ansvar att tillse att redovisningsskyldigheten fullgörs. Det är Riksrevisionens ansvar som revisor i myndigheten att uttala sig om huruvida denna skyldighet har fullgjorts.

Den översiktliga granskning som har utförts har bestått av att göra förfrågningar, i första hand till personer som inom myndigheten är ansvariga för finansiella frågor och redovisningsfrågor, att utföra analytisk granskning och att vidta andra översiktliga granskningsåtgärder. En översiktlig granskning har en annan inriktning och en betydligt mindre omfattning jämfört med den inriktning och omfattning som en revision enligt god revisionsse i övrigt har. De granskningsåtgärder som vidtas

vid en översiktlig granskning gör det inte möjligt för Riksrevisionen att skaffa sig en sådan säkerhet att Riksrevisionen blir medveten om alla viktiga omständigheter som skulle kunna ha blivit identifierade om en revision utförts. Den uttalade slutsatsen grundad på en översiktlig granskning har därför inte den säkerhet som en uttalad slutsats grundad på en revision har. På grund av avsaknad av föreskrifter kan Riksrevisionen inte entydigt uttala sig om huruvida myndigheten fullgjort sin skyldighet i enlighet med lagstiftningens intentioner. Sålunda kan det inte uteslutas att en annan tolkning än myndighetens kan gälla.

Baserat på den översiktliga granskningen av efterlevnaden av nämnda lag gör Riksrevisionen följande uttalande med begränsad säkerhet.

Det har inte kommit fram några omständigheter under den översiktliga granskningen som tyder på att myndigheten inte fullgjort sin skyldighet i enlighet med transparenslagen.

Ansvarig revisor Henrik Laginder har beslutat i detta ärende. Uppdragsledare Erik Lejon har varit föredragande.

Henrik Laginder

**Kopia för kännedom**

Stockholms universitet

Utbildningsdepartementet

Finansdepartementet, budgetavdelningen

Yttrande

2025-04-28

Dnr SU FV-0973-25

Handläggare:  
Clara Ersson  
Verksamhetscontroller  
Rektors kansli

Universitetsstyrelsen 2025-04-28

## Yttrande över internrevisionens institutionsgranskningar 2024

### Internrevisionens granskning

Internrevisionen har under 2024 granskat den interna styrningen och kontrollen vid två institutioner vid Stockholms universitet. Granskningen har fokuserat på ett antal administrativa rutiner som bedöms vara grundläggande för en god intern styrning och kontroll inom väsentliga riskområden.

### Rekommendationer och åtgärder på central nivå

Internrevisionens iakttagelser och rekommendationer från granskningarna sammanfattas i rapporten ”Internrevisionens institutionsgranskningar 2024 – styrelsesammanfattning” (dnr SU FV-0495-24, daterad 2025-02-19). Rapporten är ställd till universitetsstyrelsen och ger en övergripande bild av utfört granskningsarbete och resultat. I rapporten redovisas att ett antal brister återkommer hos institutionerna. Inom riskområdena lärarnas bisysslor och säkerhet bedömer internrevisionen att universitetsövergripande åtgärder bör övervägas för att komplettera lokala åtgärder som vidtas på institutionsnivå.

Internrevisionens rekommendationer till universitetsledningen:

1. Vidta åtgärder för att säkerställa kännedom och efterlevnad av gällande regler rörande bisysslor.
2. Vidta åtgärder för att säkerställa institutionernas kännedom och efterlevnad av krav avseende personuppgiftsbehandling samt genomför uppföljning av efterlevnad.
3. Tydliggör ansvar och nästa steg i arbetet med att utveckla det systematiska arbetet med informationssäkerhet.

### Rektors kansli

## Rekommendationer och åtgärder på institutionsnivå

Internrevisionens iakttagelser och rekommendationer efter de två institutionsgranskningarna redovisas i en revisionsrapport för respektive institution. Mot bakgrund av rekommendationerna avser rektor, efter samråd med dekan för berörd fakultet respektive med universitetsdirektören, att uppdra till institutionerna att senast den 1 november 2025 åiterrapportera vilka åtgärder som genomförs för att hantera internrevisionens rekommendationer. I och med att vissa av de rekommenderade åtgärderna i institutionsrapporterna är beroende av att universitetet centralt genomför åtgärder omfattar åiterrapporteringen endast de åtgärder som ligger inom institutionens ansvarsområde.

## Rektors yttrande

Rektors yttrande över rapporten, som avges i samråd med universitetsdirektören, följer nedan.

### ***1. Internrevisionen rekommenderar:***

Vidta åtgärder för att säkerställa kännedom och efterlevnad av gällande regler rörande bisysslor.

### ***Rektors yttrande:***

Flera åtgärder pågår inom universitetsförvaltningen för att det ska vara lätt för lärarna att göra rätt vid rapportering av bisysslor. Ett arbete har påbörjats med syfte att förenkla rapportering av bisysslor, vilket inkluderar hanteringen i Primula som är det system där lärare ska anmäla bisysslor alternativt fylla i att de inte har några bisysslor. Parallellt pågår en översyn av dokumentet *Föreskrifter om bisysslor för anställda vid Stockholms universitet*. Inom ramen för arbetet planeras även information förtydligas och förenklas så att institutionerna kan arbeta med information, rapportering och uppföljning på ett ändamålsenligt sätt. Arbetet förväntas vara klart vid årsskiftet 2025/2026.

**Åtgärder:** Rektor bedömer att rekommendationen hanteras inom ramen för det pågående och planerade arbetet. Arbetet ska åiterrapporteras till rektor senast 31 januari 2026.

### ***2. Internrevisionen rekommenderar:***

Vidta åtgärder för att säkerställa institutionernas kännedom och efterlevnad av krav avseende personuppgiftsbehandling samt genomför uppföljning av efterlevnad.

### ***Rektors yttrande:***

Den 19 december 2024 beslutade rektor om ett omfattande regelverk rörande genomförande av dataskydd vid universitetet och en handläggningsordning för omhändertagande av registrerades rättigheter. Informationsinsatser rörande de



beslutade styrdokumenterna har genomförts, via möte mellan universitetets dataskyddsombud och administrativa chefer, nyhetsutskick och e-post till prefekter, föreståndare och avdelningschefer. Universitetsförvaltningen har därutöver tagit fram utbildning och stöd gällande dataskydd som publicerats på medarbetarwebben, inklusive stödmaterial för upprättande av registerförteckning enligt artikel 30 GDPR.

Institutioner och avdelningar ska i enlighet med det beslutade regelverket utse verksamhetsnära dataskyddssamordnare som ska stötta den egna verksamheten i det lokala arbetet med dataskydd, inklusive upprättande av registerförteckningar. Verksamhetsnära dataskyddssamordnare skulle utses av institutioner och avdelningar under första kvartalet 2025 och ett första dialogmöte hölls den 1 april 2025. Rådgivning och stöd till de verksamhetsnära dataskyddssamordnarna sker främst via dataskyddsombudet genom möten och dialog. Därutöver erbjuder universitetsförvaltningen utbildning och löpande juridiskt stöd gällande dataskydd vid personuppgiftsbehandlingar där detta är relevant.

Nästa steg i arbetet är att säkerställa att samtliga institutioner och motsvarande har upprättat registerförteckningar enligt artikel 30 GDPR (artikel 30-register). Detta innebär att institutioner med hjälp av det framtagna stödmaterialet (mall och tillhörande instruktionsfilm) behöver upprätta eller aktualitetsgranska sina artikel 30-register.

Det finns här ett behov av att omgående stärka kapaciteten för det operativa stödet till institutionerna i detta arbete. På kort sikt ska detta lösas med intern omprioritering av resurser för att få så omgående effekt som möjligt i verksamheten.

**Åtgärder:** Rektor avser att i samråd med dekaner och vicerektorer fatta beslut om att samtliga institutioner och motsvarande ska ha upprättat en registerförteckning enligt artikel 30 GDPR senast den 30 september 2025. Rektor avser att uppdra till universitetsdirektören att följa upp att institutioner och motsvarande har ett aktuellt register på plats. Uppdraget ska återrapporteras till rektor den 1 november 2025. Verksamhetens arbete med dataskydd och regelefterlevnad följs dessutom årligen upp genom dataskyddsombudets årsrapport till styrelsen.

### ***3. Internrevisionen rekommenderar:***

Tydliggör ansvar och nästa steg i arbetet med att utveckla det systematiska arbetet med informationssäkerhet.

#### ***Rektors yttrande:***

Ett flertal vakanser inom IT- och informationssäkerhetsarbetet vid IT-avdelningen har orsakat fördröjningar av planerade åtgärder inom området. En

tillsvidareanställd informationssäkerhetschef är nyligen rekryterad och det är nu prioriterat att stärka kapaciteten för det operativa säkerhetsstödet inklusive stöd till institutionerna i deras arbete, vilket beskrivs närmare i rektors yttrande över internrevisionens granskning av IT-säkerhet, dnr SU FV-0975-25.

Risk för att informationssäkerhetsbrister leder till skada för universitetet är en av universitetets prioriterade risker att hantera perioden 2025–2026. Riskåtgärder under perioden för universitetsförvaltningen, inklusive tidsplan, framgår från universitetsförvaltningens åtgärdsplan som fastställdes av universitetsdirektören den 30 januari, dnr SU FV-0417-25. En av riskåtgärderna är att implementera ett systematiskt arbete med återkommande informationsinventering och informationsklassificering. Detta innebär att modellen och arbetssättet som utvecklades inom ramen för ESIR-projektet<sup>1</sup> ska anpassas och övergå i löpande arbete där institutioner och avdelningar återkommande genomgår informationsinventering och efterföljande informationsklassning.

Riskåtgärder inom perioden vid de två verksamhetsområdena inkluderar informationsinsatser avseende hur känslig information, såväl personuppgifter som andra former av säkerhetsinformation, ska behandlas, lagras och gallras samt att verka för att institutionerna fortsätter arbetet med informationsinventering och efterföljande informationsklassning.

Den 16 april 2025 beslutade rektor om ett kompletterande styrdokument till informationssäkerhetspolicyn i form av en *Handläggningsordning för ansvarsfördelning och vägledning avseende säkerhetsåtgärder i informationssystem vid Stockholms universitet*, dnr SU FV-1582-25. Syftet var bl.a. att förtydliga ansvarsfördelningen inom IT-säkerhet.

**Åtgärder:** Pågående arbete och nästa steg i arbetet med att utveckla det systematiska arbetet med informationssäkerhet sammanfattas kortfattat ovan. Arbetet med informationssäkerhet rapporteras löpande till styrelsen inom ramen för tertialrapporterna och förvaltningens riskåtgärder följs upp inom ramen för ordinarie processer i tertialerna.

---

<sup>1</sup> Etablering av systematiskt informationssäkerhetsarbete och resultatstyrning” (ESIR) pågick 2021–2024. Syftet med projektet var att stärka den interna styrningen och kontrollen av det systematiska informations- och IT-säkerhetsarbetet och efterlevnaden av dataskyddsförordningen inom hela universitetet.



Tobias Bjöörn  
Internrevisionschef

## Internrevisionens institutionsgranskningar 2024 – styrelse-sammanfattning

### 1. Inledning

Internrevisionen (IR) har i enlighet med internrevisionsplanen för 2024 granskat den interna styrningen och kontrollen vid universitetets institutioner. I årets granskning har följande institutioner ingått: Institutionen för arkeologi och antikens kultur (108) och Institutionen för astronomi (401).

Syftet med granskningarna har varit att besvara följande revisionsfråga:

*”Har institutionen ändamålsenliga och effektiva rutiner som säkerställer god intern styrning och kontroll inom väsentliga riskområden?”*

Denna styrelsesammanfattning syftar till att ge Universitetsstyrelsen en övergripande bild av IR:s genomförda granskningsarbete och granskningsresultatet för respektive riskområde. Granskningarna är dokumenterade i separata granskningsrapporter som bifogas till denna sammanfattning. I de bifogade rapporterna finns IR:s iakttagelser och rekommendationer som lämnas till respektive institution.

Granskningen visar att några av bristerna i den interna styrningen och kontrollen återkommer hos institutionerna. Mot bakgrund av detta bedömer IR att universitetsövergripande åtgärder behövs för att komplettera lokala åtgärder som vidtas på institutionsnivå. IR lämnar därför följande rekommendationer till universitetsledningen:

1. Vidta åtgärder för att säkerställa kännedom och efterlevnad av gällande regler rörande bisysslor.
2. Vidta åtgärder för att säkerställa institutionernas kännedom och efterlevnad av krav avseende personuppgiftsbehandling samt genomför uppföljning av efterlevnad.
3. Tydliggör ansvar och nästa steg i arbetet med att utveckla det systematiska arbetet med informationssäkerhet.

## 2. Årets institutionsgranskning i korthet

Granskade institutioner:

- Institutionen för arkeologi och antikens kultur (108)
- Institutionen för astronomi (401)

Granskade områden:

- Ekonomi (budgetering, resultat och resultatuppföljning samt redovisning)
- Anläggningstillgångar och stölbegärliga förbrukningsinventarier (SFI)
- Inköp och upphandling
- Lärarnas bisysslor
- Säkerhet (personuppgiftsbehandling, informations-/IT-säkerhet och fysisk säkerhet)
- Tentafusk

Dokumentstudier:

- Delegationsordning, institutionsstyrelseprotokoll, årsbudget, resultatrapporter, verifikationer, förteckning av attest- och utanordningar, inventeringsprotokoll, registerförteckning och lokala rutiner/checklistor m.m.

Stickprov:

- Kontering av kostnader och moms, underlag till bokförda kostnader, underlag för representation och resor, redovisning och registrering av anläggningar och stölbegärliga inventarier (SFI) i respektive register, inventering, avrop från ramavtal, och registrering av lärarnas bisysslor m.m.

Intervjuer:

- Prefekt, administrativ chef, ekonom, inköpskoordinator, studierektor, data- och systemansvarig m.fl.

Granskningsperiod:

- Primärt 2024

### Sammanställning resultat av institutionsgranskningar

Rekommendationer har lämnats till de granskade institutionerna inom de riskområden där IR har noterat brister i den interna styrningen och kontrollen. Brister, risker och rekommendationer beskrivs i respektive granskningsrapport, medan mindre iakttagelser har kommunicerats muntligt till respektive institution under granskningsarbetet.

I nedanstående tabell framgår antal rekommendationer och IR:s bedömning av den interna styrningen och kontrollen för respektive riskområde och institution. Bedömningen av den interna styrningen och kontrollen hos granskade institutioner utgår från IR:s analys av granskningsresultatet per riskområde. Vid bedömningstillfället har följande kategorier tillämpats: tillfredställande, förbättringsmöjligheter, bristfällig samt otillfredsställande.

Riskområden	Institutionen för arkeologi och antikens kultur (108)	Institutionen för astronomi (401)
<b>Budgetering</b>		
<b>Resultat och resultatuppföljning</b>	<b>1</b>	
<b>Redovisning</b>	<b>2</b>	<b>2</b>
<b>Anläggningstillgångar och SFI</b>	<b>2</b>	<b>1</b>
<b>Inköp och upphandling</b>	<b>1</b>	<b>1</b>
<b>Lärarnas bisysslor</b>	<b>1</b>	<b>2</b>
<b>Säkerhet</b>	<b>3</b>	<b>4</b>
<b>Tentafusk</b>	<b>1</b>	<b>1</b>

### 3. Universitetsgemensamma brister, risker och rekommendationer

Granskningen visar att ett antal av bristerna i den interna styrningen och kontrollen återkommer hos institutionerna. Mot bakgrund av detta bedömer IR att universitetsövergripande åtgärder bör övervägas för att komplettera lokala åtgärder som vidtas på institutionsnivå.

I tabellerna nedan redovisas de brister och risker som återkommer i årets institutionsgranskning, och i förekommande fall rekommendationer till universitetsledningen.

Riskområde redovisning	
<p><b>Återkommande brister:</b></p> <ul style="list-style-type: none"> <li>• Institutionerna redovisar emellanåt moms felaktigt vid utgifter för representation.</li> <li>• Institutionerna brister i kontrollerna vid konterings- och attesteringstillfället.</li> <li>• Institutionerna saknar alternativt behöver stärka rutinerna vid efterkontroll och rättning.</li> </ul>	<p><b>Risker:</b></p> <ul style="list-style-type: none"> <li>• Ingående moms som ej kostnadsförs vid representation innebär att universitetet äskar återbetalning av ingående moms som vi inte har rätt till.</li> <li>• Bristande kontroller medför att felbokningar inte upptäcks och rättas.</li> <li>• Kostnader på fel huvudboks konto påverkar redovisning och rapportering samt ger felaktigt underlag för analyser från institutionsnivån upp till SU-nivån.</li> </ul>
<p><b>Rekommendationer till universitetsledning:</b></p> <p>Ingen rekommendation.</p>	

Riskområde anläggningstillgångar och SFI	
<p><b>Återkommande brist:</b></p> <ul style="list-style-type: none"> <li>• Inga återkommande brister. Olika brister har identifierats och förmedlats till berörd institution.</li> </ul>	<p><b>Risk:</b></p> <ul style="list-style-type: none"> <li>• -</li> </ul>
<p><b>Rekommendationer till universitetsledning:</b></p> <p>Ingen rekommendation.</p>	

Riskområde inköp och upphandling	
<p><b>Återkommande brist:</b></p> <ul style="list-style-type: none"> <li>• Omkring hälften av de leverantörer som institutionerna genomför inköp hos saknar avtal.</li> </ul>	<p><b>Risk:</b></p> <ul style="list-style-type: none"> <li>• Risk för bristande följsamhet mot interna inköps- och upphandlingsregler.</li> </ul>
<p><b>Rekommendationer till universitetsledning:</b></p> <p>Fjolårets institutionsgranskning utmynnade i följande rekommendation till universitetsledningen: "Vidta åtgärder för att säkra att institutionernas inköp, där det är möjligt, genomförs via avrop från ramavtal, och stärk uppföljningen av ramavtalstrohet".</p> <p>Årets granskningar visar att utveckling inom området fortsatt är relevant men rekommendationen upprepas ej då IR har noterat att Inköps- och upphandlingssektionen vid Ekonomiavdelningen som åtgärd har tilldelats permanent förstärkning av anslagsmedel om 3500 tkr respektive 600 tkr i tillfälliga medel.</p>	

Riskområde lärarnas bisysslor	
<p><b>Återkommande brist:</b></p> <ul style="list-style-type: none"> <li>• Institutionerna brister i information och kontroll av lärarnas bisysslor.</li> </ul>	<p><b>Risk:</b></p> <ul style="list-style-type: none"> <li>• Risk att institutionerna inte lever upp till externa och interna krav.</li> </ul>
<p><b>Rekommendationer till universitetsledning:</b></p> <ol style="list-style-type: none"> <li>1. Vidta åtgärder för att säkerställa kännedom och efterlevnad av gällande regler rörande bisysslor.</li> </ol>	

Riskområde säkerhet	
<p><b>Återkommande brister:</b></p> <ul style="list-style-type: none"> <li>• Register över personuppgiftsbehandling saknas.</li> <li>• Otydlig systematik och ansvarsfördelning för att säkerställa ett systematiskt informationssäkerhetsarbete.</li> </ul>	<p><b>Risker:</b></p> <ul style="list-style-type: none"> <li>• Risk att SU ej lever upp till krav i om aktuell registerförteckning (artikel 30 i dataskyddsförordningen, GDPR).</li> <li>• Risk att det systematiska informationssäkerhetsarbetet inte kan ske effektivt och ändamålsenligt.</li> </ul>
<p><b>Rekommendationer till universitetsledning:</b></p> <ol style="list-style-type: none"> <li>1. Vidta åtgärder för att säkerställa institutionernas kännedom och efterlevnad av krav avseende personuppgiftsbehandling samt genomför uppföljning av efterlevnad.</li> <li>2. Tydliggör ansvar och nästa steg i arbetet med att utveckla det systematiska arbetet med informationssäkerhet.</li> </ol>	

Riskområde tentafusk	
<p><b>Återkommande brist:</b></p> <ul style="list-style-type: none"> <li>• Inga återkommande brister. Olika brister har identifierats och förmedlats till berörd institution.</li> </ul>	<p><b>Risk:</b></p> <ul style="list-style-type: none"> <li>• -</li> </ul>
<p><b>Rekommendationer till universitetsledning:</b></p> <p>Ingen rekommendation.</p>	



# Institutionen för arkeologi och antikens kultur (108)

## Revisionsrapport från Internrevisionen

## Innehåll

<b>SAMMANFATTNING OCH REKOMMENDATIONER .....</b>	<b>3</b>
<b>1. BAKGRUND OCH SYFTE .....</b>	<b>5</b>
1.1.1. <i>Omfattning och metod .....</i>	5
1.1.2. <i>Beskrivning av Institutionen för arkeologi och antikens kultur .....</i>	6
<b>2. GRANSKNINGSRESULTAT .....</b>	<b>7</b>
<b>2.1. RISKOMRÅDE – EKONOMI .....</b>	<b>7</b>
2.1.1. <i>Budgetering .....</i>	7
2.1.2. <i>Resultat och resultatuppföljning .....</i>	9
2.1.3. <i>Redovisning .....</i>	11
2.1.4. <i>Bedömningar och rekommendationer .....</i>	16
<b>2.2. RISKOMRÅDE - ANLÄGGNINGSTILLGÅNGAR OCH STÖLDBEGÄRLIGA FÖRBRUKNINGSSINVENTARIER .....</b>	<b>18</b>
2.2.1. <i>Anläggningstillgångar .....</i>	18
2.2.2. <i>Stöldbegärliga förbrukningsinventarier (SFI) .....</i>	18
2.2.3. <i>Inventering och utrangering .....</i>	19
2.2.4. <i>Bedömning och rekommendationer .....</i>	19
<b>2.3. RISKOMRÅDE – INKÖP OCH UPPHANDLING .....</b>	<b>20</b>
2.3.1. <i>Direktupphandling över 100 000 kronor .....</i>	21
2.3.2. <i>Bedömning och rekommendationer .....</i>	21
<b>2.4. RISKOMRÅDE – LÄRARNAS BISYSSLOR .....</b>	<b>22</b>
2.4.1. <i>Bedömning och rekommendationer .....</i>	23
<b>2.5. RISKOMRÅDE – SÄKERHET .....</b>	<b>24</b>
2.5.1. <i>Personuppgiftsbehandling .....</i>	24
2.5.2. <i>Informationssäkerhet .....</i>	25
2.5.3. <i>IT-säkerhet .....</i>	26
2.5.4. <i>Fysisk säkerhet .....</i>	27
2.5.5. <i>Bedömning och rekommendationer .....</i>	28
<b>2.6. RISKOMRÅDE - TENTAFUSK .....</b>	<b>29</b>
2.6.1. <i>Bedömning och rekommendationer .....</i>	30

## Sammanfattning och rekommendationer

Internrevisionen (IR) har under året 2024 granskat den interna styrningen och kontrollen vid Institutionen för arkeologi och antikens kultur. Granskningen har fokuserats på ett antal administrativa rutiner som bedöms vara grundläggande för en god intern styrning och kontroll inom väsentliga riskområden.

IR:s bedömning<sup>1</sup> är att institutionens interna styrning och kontroll var *tillfredsställande* inom området budgetering.

Vidare bedömer IR att det finns *förbättringsmöjligheter* inom områdena resultatuppföljning, anläggningstillgångar och stölbegärliga förbrukningsinventarier, inköp och upphandling, samt tentafusk.

IR har bedömt några områden som *bristfälliga*: redovisning och kontroller, lärarnas bisysslor, samt säkerhet.

Baserat på genomförd granskning lämnar IR lämnat följande rekommendationer:

1. Genomför extra kontroller av institutionens resultat mellan tertialen, så att prefekt och institutionsledning hinner vidta förbättringsåtgärder vid behov.
2. Förbättra kontroller vid kontering och attest av kostnader samt säkra att moms kostnadsförs vid representationskostnader.
3. Inför en rutin för efterkontroller.
4. Överväg att märka de anläggningstillgångar som har förutsättningar att märkas med ett anläggnings-id.
5. Inför en rutin som bekräftar att SU:s egendom återlämnas vid entledigande av personal.
6. Vidta åtgärder för att minska andelen inköp hos leverantörer som saknar ramavtal.
7. Säkerställ att lärarna löpande (t.ex. i årliga utvecklingssamtal) informeras om sina skyldigheter vid utövandet av bisysslor.

---

<sup>1</sup> IR använder följande fyra nivåer i sin bedömning av den interna styrningen och kontrollen: tillfredsställande, förbättringsmöjligheter, bristfällig samt otillfredsställande.



8. Säkerställ att institutionen tar fram en aktuell registerförteckning innehållande de processer som innebär behandling av personuppgifter.
9. Klargör, i samarbete med IT-avdelningen, nästa steg i arbetet med informationssäkerhet.
10. Säkerställ kompetensutveckling för de medarbetare som hanterar viktig/känslig information i sitt arbete i enlighet med MSB:s föreskrifter, samt generellt för säkerhetsfrågor.
11. Säkerställ att tentamensvakter upprättar en rapport vid misstanke om fusk i sals-examinationer.

Tobias Björn  
Internrevisionschef

Christoffer Skyberg  
Internrevisor

## 1. Bakgrund och syfte

Universitetets decentraliserade styrmodell innebär ett långtgående delegerat ansvar och beslutsmandat till verksamhetens områden, institutioner och förvaltningsavdelningar. Modellen ställer höga krav på ändamålsenliga och effektiva styrstrukturer för att önskad intern styrning och kontroll ska genomsyra alla nivåer i organisationen. Oavsett verksamhet gäller myndighetsförordningens krav på effektivitet, god hushållning av statens medel, regelefterlevnad och tillförlitlig samt rättvisande rapportering.

IR har mot bakgrund av ovanstående granskat intern styrning och kontroll vid två institutioner, varav en är Institutionen för arkeologi och antikens kultur (108).

Syftet med granskningen är att besvara följande revisionsfråga: *Har institutionen ändamålsenliga och effektiva rutiner som säkerställer en god intern styrning och kontroll inom väsentliga riskområden?*

### 1.1.1. Omfattning och metod

Granskningen fokuserat på följande riskområden:

- Ekonomi (budget, redovisning, uppföljning och rapportering, resor och representation)
- Anläggningstillgångar och stölbegärliga förbrukningsinventarier
- Inköp och upphandling
- Bisysslor
- Säkerhet (personuppgiftsbehandling, informations-/IT-säkerhet och fysisk säkerhet)
- Tentafusk

Internrevisionens granskning omfattar ej följande områden:

- Bedömning/utvärdering av systemstöd
- Bedömning/utvärdering av kvalitet i utbildning på grund- och avancerad nivå
- Bedömning/utvärdering av kvalitet i forskning och forskarutbildning

Genomförandet har i bestått av:

- Upptastmöte med prefekt och administrativ chef.
- Dokumentstudier.
- Genomgång av redovisning, befintliga processbeskrivningar, rutiner etc. för utvalda riskområden.
- Intervjuer med nyckelpersoner på institutionen.
- Test av identifierade nyckelkontroller.

- Analys samt eventuellt kompletterande intervjuer.
- Sammanställning av brister, risker och rekommendationer.

Baserat på identifierade brister och relaterade risker bedömer Internrevisionen den interna styrningen och kontrollen inom respektive riskområde.<sup>2</sup>

Institutionen har givits möjlighet att faktagranska ett utkast av rapporten innan färdigställandet.

### 1.1.2. Beskrivning av Institutionen för arkeologi och antikens kultur<sup>3</sup>

Institutionen för arkeologi och antikens kultur (108) ingår i Humanistiska fakulteten, som i sin tur är en del av det Humanvetenskapliga området. Institutionen har ett 80-tal anställda professorer, forskare, lektorer, forskarstuderande, forskningsingenjörer, laboratorieassistenter, postdoktorer och administratörer.

Institutionen består av följande enheter och centra:

- Antikens kultur och samhällsliv
- Arkeologi
- Arkeologiska forskningslaboratoriet
- Numismatiska forskningsgruppen
- Osteoarkeologiska forskningslaboratoriet
- Centrum för paleogenetik
- Evolutionär kulturforskning

Institutionen för arkeologi och antikens kultur skapades genom en sammanslagning 2005 av Arkeologiska institutionen och Institutionen för antikens kultur och samhällsliv. All verksamhet bedrivs i Wallenberglaboratoriet i området Lilla Frescati, förutom Centrum för paleogenetik som har sina lokaler i Arrheniushuset i Stora Frescati.

Ansvarig för verksamheten är institutionens prefekt. Institutionens ledningsgrupp består av prefekt, ställföreträdande prefekt, administrativ chef, avdelningsföreståndare (Antikens kultur och samhällsliv), avdelningsföreståndare (Arkeologi), avdelningsföreståndare, (Laborativ Arkeologi), avdelningsföreståndare (Numismatiska forskningsgruppen), avdelningsföreståndare (Osteoarkeologi), samt avdelningsföreståndare (Centrum för paleogenetik). Vid institutionen finns en institutionsstyrelse som är institutionens högsta beslutande organ. Institutionens prefekt är ordförande i institutionsstyrelsen.

<sup>2</sup> IR använder följande fyra nivåer i sin bedömning av den interna styrningen och kontrollen: tillfredställande, förbättringsmöjligheter, bristfällig samt otillfredsställande.

<sup>3</sup> Från institutionens hemsida, januari 2025

## 2. Granskningsresultat

I detta avsnitt återfinns en beskrivning av granskningsresultatet inom respektive riskområde. Noterade brister, risker och en sammanfattande bedömning av intern styrning och kontroll samt rekommendationer återfinns i slutet av respektive riskområde.

### 2.1. Riskområde – Ekonomi

Institutionens ekonomifunktion består av administrativ chef (AC), en ekonomihandläggare och en personalhandläggare. Ekonomifunktionen tillsammans med bland annat några administratörer och en IT- och fastighetstekniker bildar kostnadsstället *Stödverksamhet*, där AC är chef och har personalansvar för kostnadsstället.

AC och ekonomihandläggaren budgeterar för institutionen och de tillsammans följer upp institutionens resultat.

Institutionens omsättning 2023 uppgick till 85,1 mnkr, vilket omsättningsmässigt var en av de större på Humanistiska fakulteten, nr 5 av 14.

Institutionens verksamhet består av utbildning på grund- och avancerad nivå (UGA) samt forskarutbildning och forskning (FUF). 14% av institutionens kostnader år 2023 avsåg UGA och 86 % FUF.

Verksamhetens kostnader finansieras både av anslag och externa medel. Under 2023 finansierades kostnaderna av:

- Anslag 56 % externa medel 44% (varav bidrag 42% och uppdrag 2%).
- UGA finansierades så gott som helt av anslag 99,6% och endast 0,4% av bidrag.
- FUF finansierades 50% av anslag och 50 % av externa medel (48 % bidrag och 2% uppdrag).

Institutionen har 10 kostnadsställen, inklusive de obligatoriska: *Institutionens övergripande verksamhet* och *verksamhetsstöd*. Verksamhetsstödet kostnader fördelas till kärnverksamheten på basis av kärnverksamhetens löner och LKP med hjälp av fördelningsprocenten framräknade av institutionen.

#### 2.1.1. Budgetering

Budgetarbetet är en viktig del i institutionens styrning av verksamheten och dess ekonomi. En plan över intäkter och kostnader är även en förutsättning för en effektiv resultatuppföljning.

Vid framtagandet av institutionens budget är flera personer involverade. Administrativ chef (AC) organiserar institutionens budgetering tillsammans med prefekten och ledningsgruppen. Budgeten tas fram enligt följande:

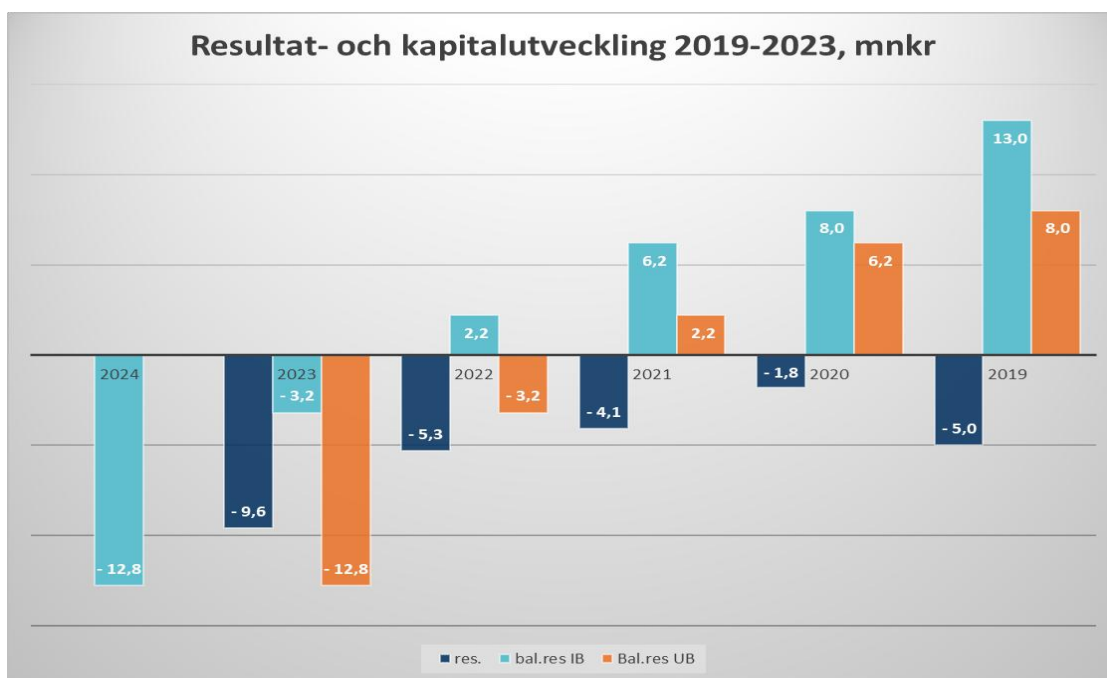
- AC lägger personalbudgeten för hela institutionen och anslagsbudgeten i dialog med avdelningsansvariga. Budgeterat anslagsintäkt fördelas till kostnadsställen med detaljerade parametrar.
- Ekonomihandläggaren budgeterar externa projekt efter dialog med projektansvariga forskare om projektens förväntade kostnader och bemanning.
- AC och ekonomihandläggaren går igenom budgeten tillsammans och räknar fram fördelningsprocenten för stödkostnader och lokalkostnader samt budgeterar samfinansiering till bidragsprojekt som inte har full kostnadstäckning.
- Alla kostnadsställeansvariga får budgetutkastet för avstämning och när alla parter är överens går budgeten till prefekt. Institutionsledningen är mån om att alla avdelningar har en egen ekonomi och medföljande ansvar.
- Prefekten gör sista kontrollen om budget och dess rimlighet.
- Institutionsstyrelsen fattar beslut om institutionens budget i årets första institutionsstyrelsemöte.

Institutionens totalbudget avvek under 2022 och 2023 mot budgeterat resultat med -4,2 mnkr respektive -8,0 mnkr. Budgetavvikelserna mot utfall har varit i intervallet 5,3 % respektive 9,4 % av årets omsättning. Budgetar är i allmänhet försiktiga och utfallet blir ofta bättre än det budgeterade. Resultaten 2022 och 2023 blev dock sämre än budgeterat. 2023 berodde avvikelsen enligt AC dels på att institutionen hade flera stora bidragsprojekt som inte hade full kostnadstäckning och som behövde samfinansieras med anslagsmedel, dels på ”dubbelbemanning” inför beräknade pensionsavgångar och ett par anställda valde att fortsätta arbeta men institutionen hade redan anställt ersättare.

Mnkr.	2022	2023	2024
Budget, resultat	-1,1	-1,6	-5,8
Utfall, resultat	-5,3	-9,6	
Avvikelse budget jmf. Utfall	-4,2	-8,0	
Årets omsättning	79,8	85,1	
Avvikelse i % av årets oms.	5,3	9,4	

### 2.1.2. Resultat och resultatuppföljning

Institutionens resultat har visat underskott de senaste fem åren (2019 – 2023) och underskotten har ökat de senaste åren. Institutionens balanserade kapital som vid utgången av 2019 uppgick till 8 mnkr har förbrukats och uppgår vid utgången av 2023 till -12,8 mnkr.



Resultatet 2023 visade ett underskott på 9,6 mnkr, bestående av UGA-resultat -1,5 mnkr och FUF-resultat -8,1 mnkr.

Därtill har institutionen *Ej förbrukade bidrag och ej förbrukade uppdrag*. Ej förbrukade bidrag har minskat från 7,8 mnkr (2019) till 4,0 mnkr (2023). Ej förbrukade uppdrag har ökat från 0,5 mnkr (2019) till 4,0 mnkr (2021) och sedan minskat till 1,8 mnkr (2023). För bidrag stipuleras det i bidragsavtal från en del finansiären att ej förbrukade bidrag som kvarstår efter att dispositionstiden gått ut ska återbetalas.

Resultatet till och med T2, augusti 2024 (-3,7 mnkr jmf. -5,5 mnkr augusti 2023) visar ett lägre underskott än samma period föregående år. Intäkterna har ökat med 7,4 mnkr och kostnaderna har ökat med 5,6 mnkr. När resultatets (-3,7 mnkr) olika beståndsdelar per augusti 2024 granskas, kan noteras att UGA resultat är positiv +1,9 mnkr, FUF resultat är -7,0 mnkr samt att finns en portion ej ännu fördelade stödkostnader +1,4 mnkr.

Orsakerna till underskottsresultaten enligt AC är flera, t.ex. en av främsta är stora bidragsprojekt från ej statliga finansiärer utan fullkostnadsstäckning, vilka behöver samfinansieras med

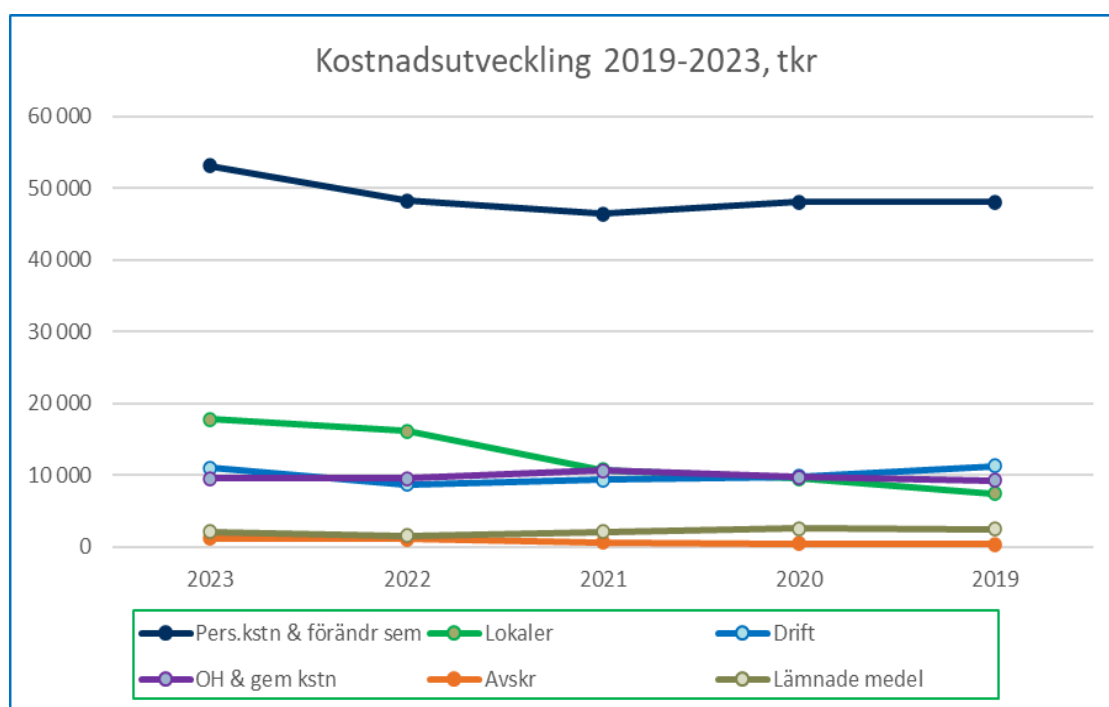
anslagsmedel. Inom utbildning underprestationer under pandemiåren, tillfällig dubbelbemanning. Ökade lokalkostnader pga. högre enhetshyra och att centrumbildningen inom institutionen har expanderat och behövt större lokaler. I centrumet deltar även andra institutioner inom SU och Nationalhistoriska museet, institutionen har ”koordinatörrollen”, dvs får alla fakturor men vidare fakturerar sedan de övriga deltagarna för deras del av kostnader. Institutionen har också renoverat/byggt om i institutionens lokaler, som institution nu har fått veta att de måste lämna och flytta till andra lokaler.

Prognos för 2024 årsresultat var enligt AC vid tidpunkten för granskningen cirka 700 tkr bättre än budgeten för 2024, vilket var -5,8 mnkr.

**Arbetet med rektorsbeslut ”Ekonomi i balans”<sup>4</sup>.** Projektet ”Ekonomi i balans” hade slutdatum den sista december 2023, men arbete att se över ekonomin fortsätter på universitetet. Vid tertialrapportering till Humanistiska fakultetens controller har institutionen exempelvis angett att följande sparåtgärder görs:

- Översyn av kostnader, bemanning och kursutbudet.
- Kostnadsmedvetenhet inför varje inköp och nya anställningar.
- Nya anställningar planeras inte att finansieras med anslag de närmaste åren.
- Arbetar aktivt med prestationsgraden på kurser med låg prestationsgrad.
- Nya kurser erbjuds som bidragit till överprestation de senaste åren, även kvällskurser.
- Forskare, postdoc och lärare ansöker nya bidrag årligen vilket har varit framgångsrikt.

Institutionen erbjuder också uppdragsanalyser, vilka ger extra intäkter. Diagrammet nedan visar kostnadsutveckling på de olika kostnadsslagen på institutionen under 2019 – 2023.





**Resultatuppföljningen** på institutionen genomförs tertialvis av AC och ekonomihandläggaren. Uppföljningen av totalresultat görs på institutionsnivå och på kostnadsställenivå för varje kostnadsställe. Utfallet i både institutionsrapporten och kostnadsställerapporterna är även brutna till verksamhetsnivå<sup>5</sup> samt visar institutionens respektive kostnadsställets årsbudget.

För resultatuppföljning används SU:s officiella EKUP-resultatrapportmodell.

Resultatuppföljningen rapporteras till institutionsstyrelsen och ledningen tertialvis. Ekonomi är en stående punkt vid varje IS möte, vilket är bra även om det enligt protokollen inte alltid funnits något att rapportera.

Ibland görs det en extra rapportering till ledningsgruppen exempelvis när det gäller samfinansiering av bidragsprojekt, generell kostnadsutveckling eller lokalkostnader. Resultat för externa projekt följs upp tertialvis av AC tillsammans med ekonomihandläggaren. Projektrapporter skickas till respektive projektledare.

AC gör dessutom en prognos för externa projekt vid projektstart och när det är ca 1,5 år kvar av projekttiden för att tillsammans med projektägaren se hur pengarna kommer att räcka.

### 2.1.3. Redovisning

Införandet av ny ekonomimodell, delvis ny kontoplan och nytt redovisningsprogram<sup>6</sup> fr.o.m. januari 2022 har haft påverkan på arbetet med budgetering, redovisning och uppföljning för alla på SU. I viss mån har det nya redovisningsprogrammet påverkat arbetet även 2023–2024 då modulerna för budgetering och prognos togs i bruk.

**Fakturahantering** i det nya systemet har tre behörigheter: beställare, lokalekonom och beslutsattestant. Alla dessa behörigheter har kontrollplikter om leveransen, fakturan, konteringen och underlagen.

*Beställare*, beställer varor/tjänster via Raindance e-portalen.

- På institutionen beställer IT-teknikern tekniska varor. Tre forskare och en lab.tekniker beställer kemikalier. Administrationen beställer, kontorsmateriel, kaffe, catering mm.
- Innan beställningen görs kräver inte institutionen något preliminärt godkännande av beställningen. Enligt AC litar institutionen att beställningar som görs är korrekta.
- Innan e-beställning går iväg till leverantören krävs att beslutsattestanten har attesterat beställningen.

---

<sup>5</sup> Utbildning på anslag, forskning på anslag, forskarutbildning på anslag, forskning på bidrag, forskarutbildning på bidrag, och stödverksamhet till utbildning och forskning.

<sup>6</sup> Helt ny och helt omarbetad version av Raindance.

- Kontroller som beslutsattestanten ska göra vid e-beställning: *att kostnaden får belasta den verksamhet som är angivet i konteringen av beställningen, att finansiering finns, att anskaffningen är förenlig med de regler som gäller universitetets verksamhet.*<sup>7</sup>
- Kontroller som ska göras vid inleveransen: *att varan/tjänsten är levererad/utförd, att leveransen stämmer med beställningen, att varan är felfri.*<sup>8</sup>

*Lokalekonom*, tar emot och konterar fakturor som inte kommer via e-beställning, kontering räknas inte som attest.

- Institutionen har två registrerade lokalekonomer/fakturamottagare: AC och ekonomi-handläggaren.
- Kontroller som ska göras vid kontering av faktura: *att fakturan är utställd på SU och rätt institution/avdelning, att den innehåller uppgift om leverantörens organisationsnummer och F-skatt, att leverantörens och SU:s VAT-nummer finns angivet på fakturor från leverantör inom EU, att fakturan specificerar vad som är inköpt och antal, att fakturabeloppet och momsbeloppet är korrekt, att fakturerings- eller andra avgifter ej debiteras, att inskannade uppgifter i ekonomisystemet stämmer med fakturan, att utbetalning sker till rätt mottagarkonto och vid rätt tidpunkt samt att fakturan är konterad enligt gällande kodplan.*<sup>9</sup>

*Beslutsattestant*, attesterar e-beställningar, bokföringsorder och fakturor på den verksamhet de är ansvariga för.

- Institutionen enligt Raintance- register har 6 beslutsattestanter. Prefekt är attestant för alla kostnadsställen, AC för stödkostnadsstället och respektive kostnadsställesansvarig för kostnadsställen 108001, 108002, 108003 och 108010. Limit för prefekt enligt SU:s regler 2 mnkr, för övriga beslutsattestanter 0,5 mnkr. Kostnader gällande AC ska attesteras av prefekten och prefektens kostnader av dekanen.
- Kontroller som ska göras vid attest: *Att kostnaden får belasta den verksamhet som är angivet i konteringen av fakturan, att finansiering finns, att kostnaden är inom universitetets verksamhet.*<sup>10</sup>

---

<sup>7</sup> Dnr SU FV-4558-22 Attestordning- regelverk om att förfoga över universitetets medel, Ekonomiavdelningen 2022-12-08. Gäller från 2022-12-08

<sup>8</sup> Ibid.

<sup>9</sup> Ibid.

<sup>10</sup> Dnr SU FV-4558-22 Attestordning- regelverk om att förfoga över universitetets medel, Ekonomiavdelningen 2022-12-08. Gäller från 2022-12-08.



**Utlägg.** I personalsystemet Primula varierar atteststrukturen beroende på typ av ärende. För att godkänna anställdas utlägg/resor krävs, utöver personen som registrerar utlägget, *en granskare* och *en attestant*.

Utlägg/reseräkningar registreras vanligtvis av den anställde själv och då väljs huvudboks konto och internkontering, med viss vägledning från systemet. Detta är också fallet på institutionen. Eftersom alla anställda inte har kunskaper i redovisning, förutsätter det att granskare och attestanter är särskilt uppmärksamma att underlag är bifogad och att allt, inklusive huvudboks konto, stämmer innan de godkänner ärenden.

Behörighet att **granska** ärenden i Primula på Institutionen för arkeologi och antikens kultur har AC och en relativt nyanställd personalhandläggare.

#### **Attestbehörigheten**

- Prefekt för hela institutionen, AC för stödkostnadsställe och fyra avdelningsföreståndare/kostnadsställeansvariga för sina avdelningar.
- Prefektens utlägg och resor överlätas till dekanen för attest.

#### **Kontering och kontroller**

För att säkerställa god kvalitet på redovisning, krävs det en fungerande rutin för förebyggande- och efterkontroller.

Inkommande fakturor hanteras elektroniskt i redovisningssystemet Raindance. Systemet har en inbyggd dualitetskontroll som kräver att fakturan först konteras av en person, och därefter attesteras av en annan person, för att en leverantörsfaktura ska släppas till betalning. Denna inbyggda kontroll finns också i Primula<sup>11</sup> gällande utlägg/reseräkningar. Dualitetsprincipen vid hantering av fakturor är en automatisk förebyggande kontroll mot oegentligheter. Dock behöver konteraren och attestanten fortfarande genomföra de manuella förebyggande kontrollerna enligt Attestordningen (se föregående sida) och alltid vara observanta på vad de godkänner.

**Kontering.** Kontering ska ske i enlighet med redovisningsregler, universitetets kontoplan samt med stöd av lathundar. Förutom att fakturans/utläggens belopp stämmer, att det är rätt konterat enligt gällande regler behöver man också se till att rätt underlag är bifogad.

Syftet med krav på underlag och förklarande texter är att styrka att kostnaden tillhör universitetets verksamhet och att kostnaden är konterad på rätt konto och med korrekt kodsträng. Korrekt kontering är också viktigt bland annat för att redovisningen ska ge en rättvisande bild av verksamheten, och även bidra till tillförlitliga underlag i samband med

---

<sup>11</sup> Primula är ett personal- och lönesystem.

uppföljning, analys och budgetarbete. Underlag och förklarande texter verkar även förebyggande mot oegentligheter.

Hos Institutionen för arkeologi och antikens kultur består *förebyggande kontroller* av att konteraren frågar beställaren om fakturan är korrekt och får då också projektnummer till vilket kostnaden ska bokföras. Vid kontering används kontoplanen, likaså Ekonomiavdelningens Lathund. Konteraren kontrollerar också att underlaget som krävs enligt Lathunden och anvisningar till kontoplan finns med. AC och ekonomihandläggaren har läst SU:s policy för representation. Radtexter på leverantörsfakturer finns i regel. En del är bra och informativa, en del kunde vara tydligare om vad har anskaffats. AC, som attesterar stödkostnadsställets fakturer, förutom sina egna och prefektens, uppger att förebyggandekontroll främst brukar ske av kontot och projektnumret. Vid granskning av utlägg kontrolleras att kvittona är bifogade, att syfte framgår och att deltagarförteckning finns vid representation.

*Efterkontroller*, månatligen/kvartalsvis/tertiärsvis, görs av bokförda kostnader/intäkter för att säkerställa att inget har hamnat på fel huvudboks konto, projekt och kostnadsställe. Enligt AC gör institutionen översiktliga kontroller i samband med tertialredovisning avseende personalkostnader, driftskostnader och lokalkostnader. Det görs inga efterkontroller av att kostnader har bokförts på rätt konto/kontoklass eller på transaktionsnivå.

IR har genomfört stickprovsgranskning av olika kostnadskonton och testat att ekonomiska händelser har attesterats och konterats i enlighet med attestordning, redovisningsregler samt universitetets kontoplan och kompletterande lathundar. Granskningen visade att personal- och driftskostnader i vissa fall har sammanblandats. När olika typer av varor köps in och faktureras på samma faktura så konteras allt på samma konto. Detta gäller exempelvis kaffe, te, mjölk (personalkostnader, konto 4942<sup>12</sup>), bullar, tårter (personalkostnader, konto 4981 krävs underlag)<sup>13</sup>, serviceavgift för kaffemaskin (driftkostnad, kontogrupp 52\*) rengöringsmedel (driftkostnad, 569\*) läkarundersökning för dykare underwater archeology har konterats till personalen fikakonto 4942. Vid en ”städdag” om en timme har lunch serverats, vilket borde medföra en kostförmån för alla deltagare. Städdag bedöms inte uppfylla kriterier för intern kurs/konferens, som även den kräver minst 6h dokumenterat sakinnehåll för att skattefri måltid kan serveras<sup>14</sup>. IR noterar också att så gott som alla externa konferens- och kurskostnader” (personalens utbildning, konto 4821) köps via utlägg och saknar program<sup>15</sup>. Anledningen anges vara att de flesta avser konferenser anordnade i utlandet, där betalning endast kan ske. I dessa fall finns krav att alltid bifoga konferensprogrammet samt att det också är bra att bifoga information om organisatören<sup>16</sup>.

<sup>12</sup> Se punkt 5.1 Lathund för redovisning av representation mm, Ekonomiavdelning

<sup>13</sup> Se punkt 5.2 Lathund för redovisning av representation mm, Ekonomiavdelning

<sup>14</sup> Se punkt 6.2 Lathund för redovisning av representation mm, Ekonomiavdelningen.

<sup>15</sup> Se punkt 6.1 Lathund för redovisning och representation mm, Ekonomiavdelningen.

<sup>16</sup> ”Lathund för redovisning av representation m.m. vid Stockholms universitet” Ekonomiavdelningen, punkt 6.1.



Måltider (frukost/lunch/middag) som bjuds vid externa kurser, oavsett om de specificeras i fakturan eller inte, eller faktureras separat, ska förmånsbeskattas som kostförmån och ska också avdras från eventuellt traktamente.

*Underlagen* var oftast bifogade, förutom kurs- och konferensprogrammen som saknades i allmänhet. Meddelande-rutan i Raindance och vid utlägg i Primula kan med fördel användas för att ge kompletterande information.

### ***Resor och representation***

Rese- och representationskostnader har en inneboende risk för sammanblandning med privata kostnader. För statliga myndigheter är det även viktigt att hushålla väl med statens medel. Representationskostnader omfattas av externa regler och krav, exempelvis att hela ingående moms ska kostnadsföras, att syfte för representation behöver anges och att deltagarlista måste bifogas.

För extern representation gäller också krav för omedelbart samband gällande tid, plats och personer som deltar i förhandlingen och den efterföljande representationsmåltiden. För intern representation, dvs personalrepresentation (personalfester), gäller dessutom att hela personalen är inbjuden och personalrepresentationer är max 2 ggr/år för att den ska vara skattefri.

Från stickprov framgick att institutionen inte har bokfört några kostnader för personalfester som internrepresentation (personalrepresentation, konto 4962) 2023 eller 2024 per augusti. Julbord för personalen 2023, som genomfördes efter institutionens årliga konferens, har istället redovisats som en intern konferenskostnad (Hotell-och restaurangtjänster, konto 5572) och moms var ej kostnadsförd. Enligt ESV ska en middag, som har karaktären av personalfest, efter avslutad internkonferens bokföras som personalfest och moms ska kostnadsföras (konto 4962). Institutionens ekonomifunktion kände inte till detta.

Per augusti 2024 har institutionen endast haft ett par transaktioner på externrepresentation, två kondoleansbuketter, där den ena saknade syfte och den andra överskred SU:s beloppsgräns utan rektors godkännande. I båda fall var moms inte kostnadsfört utan rättades efter Ekonomiavdelningens stickprov. Den tredje extern representation var utlägg vid ett besök från ett universitet från Boston. Den följde alla regler gällande kontering, kostnadsföring av moms och underlag: syfte, deltagarlista och kvitton.

Bland granskade stickprov på resekostnader var kontering korrekt på flygbiljetter inrikes/utrikes, och hotellövernattningar, vilket är viktigt eftersom SU följer upp resekostnader. Dock saknades syftet till resor, vilket skulle verifiera att dessa tillhör verksamheten, på samtliga stickprov. Inga kurs/konferensprogram var bifogade, om det hade varit syftet för resan eller övernattningen. Bland övriga resekostnader fanns en del diverse reserelaterade kostnader, bl.a. en faktura från en privatperson i England för flygbiljetter och bilhyra, men utan bilagor av

kvitton som skulle verifiera kostnaderna. Fakturan har sedan tagits som ett utlägg för en anställd på institutionen.

Exempel av stickproven har diskuterats med administrativ chef och ekonomihandläggaren.

#### 2.1.4. Bedömningar och rekommendationer

##### ***Budgetering***

IR bedömer att institutionens interna styrning och kontroll avseende budgetering är tillfredsställande. Institutionen har god ordning på budgeteringsprocessen. Ekonomifunktionen leder budgetarbetet. Alla verksamhetstyper budgeteras. Ledningsgruppen och avdelningsföreståndarna är involverade och lika så projektledarna. Budgeten stäms av med de involverade, slutligen av prefekten och beslutas av institutionsstyrelsen.

Institutionens totalbudgetens avvikelse till utfallet har ökat de senaste två åren, förlustresultaten har blivit sämre än budgeterat. Enligt AC är anledningen oväntade händelser som inte kunnat förutses.

##### ***Resultatuppföljning***

IR bedömer att institutionens interna styrning och kontroll avseende resultatuppföljning har förbättringsmöjligheter. Institutionen följer upp resultatet tertialvis och presenterar uppföljningen med SU:s officiella EKUP rapporter till institutionsstyrelsen, ledningsgruppen och avdelningsföreståndarna. Uppföljning görs för institutionens totalresultat<sup>17</sup> och enskilt för institutionens 10 kostnadsställen. Både institutionens totalresultat och varje kostnadsställets resultat är sedan även nedbruten till resultat per verksamhetslag. Projekt uppföljs också tertialvis och projektledarna får uppföljningen.

Dock bedömer IR med anledning av institutionens mycket ansträngda ekonomi att tertialvisa uppföljningar är för sällan för att hinna agera om utvecklingen går åt fel håll. Institutionens kapital har stadigt sjunkit från + 8 mnkr IB 2019 till -12,8 mnkr IB 2024. Rekommendationerna framgår nedan.

##### ***Redovisning***

IR bedömer att institutionens interna styrning och kontroll avseende redovisning är bristfällig. Det finns sammanblandning mellan personalkostnader och driftskostnader, exempelvis regelbundna serviceavgifter och rengöringsmedel för kaffemaskin är bokförda som personalkostnader istället för driftskostnader. Även gällande huvudboks-kontot har inte instruktioner i

---

<sup>17</sup> Totalresultat innehåller alla typer av verksamheter: anslag, bidrag och uppdrag och alla kostnadsställen som institutionen har.

kontoplan och Lathund följts gällande huvudbokskontot. Syfte till resan saknas så gott som i samtliga granskade fall. Syftet behöver ibland förtydligas vid representation/resor, institutionen kan använda meddelande-rutan till det, både i redovisningssystemet och i Primula. Program till konferens/kurs saknas i de flesta fall.

Förkontroller vid kontering och attest behöver förbättras. Vid kontering använd alltid gällande kontoplan och Ekonomiavdelningens Lathund samt SU:s regler för representation och gåvor mm. Ur lathund framgår även vilka underlag som krävs för de olika kostnaderna.

Institutionen har inte haft rutin för efterkontroller på kontonivå, vilka görs för att upptäcka och korrigera kostnader eller intäkter som hamnat på fel konto, fel moms eller komplettera saknade uppgifter. Institutionen behöver försöka skriva så tydliga och beskrivande radtexter som möjligt.

Brister	Risker	Sammanfattande bedömning ISK
<b>Budgetering</b>	Ej tillämbart.	Tillfredställande
<b>Resultatuppföljning</b> och information till institutionsledning	Med anledning av institutionens ansträngda ekonomi är tertialvisa resultatuppföljningar för sällan för att hinna vidta förbättringsåtgärder i tid.	Förbättringsmöjligheter
<b>Redovisning och kontroller</b> Momsfel vid representation förekom.  Bristande kontroller vid kontering och attest  Rutin för efterkontroll och rättning saknas.	Ingående moms ej kostnadsförs vid representation innebär att universitetet äskar återbetalning av ingående moms som vi inte har rätt till.  Bristande kontroller medför att felbokningar inte upptäcks och rättas.  Kostnader på fel huvudbokskonto påverkar redovisning och rapportering samt ger felaktigt underlag för analyser från institutionsnivån upp till SU-nivån.	Bristfälligt
<b>Rekommendationer</b> <ol style="list-style-type: none"> <li>Genomför extra kontroller av institutionens resultat mellan tertialen, så att prefekt och institutionsledning hinner vidta förbättringsåtgärder vid behov.</li> <li>Förbättra kontroller vid kontering och attest av kostnader samt säkra att moms kostnadsförs vid representationskostnader.</li> <li>Inför en rutin för efterkontroller.</li> </ol>		

## 2.2. Riskområde - Anläggningstillgångar och stöldbegärliga förbrukningsinventarier

### 2.2.1. Anläggningstillgångar

Anläggningstillgångar redovisas först som preliminära anläggningar i universitetets anläggningsregister och redovisning. Innan anläggningar kan aktiveras (definitivsättas) behöver institutionen välja anläggningstyp och komplettera med uppgifter som ansvarig, placering, serienummer och övrig information. När anläggningar aktiveras, vilket ska ske när de kan tas i bruk av institutionen, överförs anläggningar automatiskt till rätt tillgångskonto så avskrivningskostnaderna kan starta.

I intervjun framgick det att institutionen inte har några dokumenterade rutiner vid redovisning av anläggningstillgångar då institutionen använder universitetets gemensamma riktlinjer. Uppstår det ett behov av att anskaffa anläggningstillgångar beställer någon av institutionens inköpskoordinatorer anläggningen och när leverantörsfakturorna inkommer bokförs fakturorna som pågående anläggningar av institutionens ekonomihandläggare. Vidare behandlar ekonomihandläggaren anläggningstillgångar i Raindance genom att registrera uppgifter som ansvarig, placering, serienummer och övrig information samt väljer anläggningstyp. När anläggningen är färdigbehandlad och kan tas i bruk aktiverar (definitivsätter) ekonomihandläggaren anläggningen.

Enligt anläggningsregistret den 2024-11-04 har institutionen 93 st anläggningar varav över hälften av anläggningarna är helt avskrivna. Under perioden januari – oktober 2024 har institutionen bokfört 5 st fakturor som pågående nyanläggningar. IR:s översiktliga genomgång av krediterade belopp på konto 1271 visar att institutionen skyndsamt aktiverar tillgångar. Vid genomgång av institutionens anläggningsregister har IR noterat att institutionen registrerar uppgifter som underlättar identifieringen. I intervjun med institutionen framgick att sedan 2022 kompletteras även uppgifterna i registret med ett foto på anläggningen.

### 2.2.2. Stöldbegärliga förbrukningsinventarier (SFI)

Till skillnad från anläggningstillgångar fördelas inte kostnaderna för SFI under tillgångens nyttjandeperiod utan kostnadsförs i sin helhet vid anskaffningstillfället. Vid anskaffning av nedanstående kategorier via e-handel i Raindance kommer varan per automatik att läsas in i SFI-registret när köpet har beslutsattesterats och definitivsatts.

- dator/tablet/smatphone/storbildsskärm, 0 – 25 000 kr
- AV-utrustning mellan 5 000 – 25 000 kr
- smartphone

Övriga kategorier saknar koppling till registret. Det går också att registrera SFI i registret då inkommande leverantörsfakturor konteras. Anges en SFI-kod i S-kolumnen på konteringsraden



kommer SFI att registreras i registret när fakturan är beslutsattesterad och definitivsatt. Gemensamt för tillvägagångssätten är att kompletterande uppgifter som ansvarig, placering, serienummer och övrig information registreras i efterhand av institutionens ekonomi-handläggare.

Likt redovisning av anläggningstillgångar har institutionen inte några dokumenterade rutiner vid redovisning av SFI då institutionen använder universitetets gemensamma riktlinjer. Uppstår det ett behov av att anskaffa en SFI beställer institutionens IT- och fastighetstekniker varan i e-handelssystemet. Vid institutionen är det IT- och fastighetsteknikern som är SFI-ansvarig medan det är institutionens ekonomihandläggare som registrerar uppgifter som ansvarig, placering, serienummer och övrig information i SFI-registret.

Enligt SFI-registret den 2024-11-04 har institutionen 63 st SFI:er. Under perioden januari – oktober 2024 har institutionen bokfört 7 st. anskaffningar på konto 5610 – datorer och mobiltelefoner som har registrerats i SFI-registret. IR:s genomgång av registrerade uppgifter i SFI-registret visar att institutionen registrerar uppgifter som underlättar identifieringen.

Vid entledigande av personal används inte någon checklista eller liknande för att säkerställa att universitetets egendom återlämnas. Enligt uppgift informerar personalansvarig chef medarbetarna muntligt om vad som gäller vid avslut av tjänst, där bland annat återlämnandet av universitetets utrustning berörs.

### 2.2.3. Inventering och utrangering

Inventering är en viktig åtgärd för att säkra kontroll över universitetets tillgångar. I intervjun framgick det att institutionen årligen inventerar anläggningstillgångar (ej märkta med anläggnings-ID) och SFI samt att inventeringen genomförs fysiskt med undantag för tillgångar som finns i renrumsmiljö hos centrum för paleogenetik vid Arrheniuslaboratoriet. Vid genomförandet av 2024 års inventering utsågs institutionens IT- och fastighetstekniker till inventeringsförrättare. Vidare har institutionen upprättat och signerat ett inventeringsprotokoll som har inlämnats till Ekonomiavdelningen. I samband med intervjutillfället genomförde IR en stickprovsinventering där samtliga tillgångar kunde identifieras.

I intervjun framfördes att institutionen utranger anläggningar och SFI efter behov och vid inventeringstillfället. Vidare använder institutionen Ekonomiavdelningens blankett vid utrangering av anläggningstillgångar samt kontaktar Ekonomiavdelningen genom serviceportalen när SFI:er ska utrangeras.

### 2.2.4. Bedömning och rekommendationer

IR:s bedömning av den interna styrningen och kontrollen avseende anläggningstillgångar och SFI är att det finns förbättringsmöjligheter. Granskningen visar att institutionen inte märker anläggningstillgångar med anläggnings-id och saknar tydliga rutiner vid återlämnandet av SU:s egendom. IR bedömer att det är viktigt att institutionen inför rutiner som försäkrar att

medarbetarna återlämnar SU:s egendom, framför allt när det kommer till teknisk utrustning. Vidare anser IR att det är lämpligt att institutionen märker anläggningstillgångar i syfte att underlätta inventeringstillfället men även för att minska personberoendet.

Brister	Risker	Sammanfattande bedömning ISK
Anläggningstillgångar ej märkta med anläggnings-id.	Risk att inventeringstillfället blir ineffektiv och att identifieringen försvåras.	Förbättringsmöjligheter
Saknas tydlig rutin vid återlämning av SU:s egendom.	Risk att SU:s egendom inte återlämnas.	
<b>Rekommendationer</b> <ol style="list-style-type: none"> <li>4. Överväg att märka de anläggningstillgångar som har förutsättningar att märkas med ett anläggnings-id.</li> <li>5. Inför en rutin som bekräftar att SU:s egendom återlämnas vid entledigande av personal.</li> </ol>		

## 2.3. Riskområde – Inköp och upphandling

Vid institutionen finns det 17 medarbetare som har beställarbehörighet i Raindance/Marknadsplatsen, vilket innebär att medarbetarna kan registrera beställningar i universitetets e-handelssystem. För att registrerade beställningar ska skickas till leverantörer behöver beställningarna attesteras. På institutionen kan prefekt, administrativ chef och fyra avdelningsföreståndare attestera beställningar. Vidare har institutionen sex inköpskoordinatorer som har genomfört Inköps- och upphandlingssektionens utbildningar ”Certifierad inköpskoordinator – IK1” och ”Kommers eLite Direktupphandling – IK2”.

I intervjun med institutionen framgick det att institutionen inte har några dokumenterade riktlinjer för inköp och upphandling då institutionen använder universitetets gemensamma regler för inköp och upphandling. Uppstår det ett behov av att göra ett inköp i verksamheten genomförs detta normalt i universitetets e-handelssystem av institutionens beställare. Om det inte finns något avtal och inköpet understiger 100 000 kronor vänder sig medarbetarna till någon av institutionens inköpskoordinatorer för hjälp.

Eftersom universitetet anskaffar varor och tjänster genom beställning, avrop och upphandling har IR granskat hur stor andel av institutionens inköp som sker via avtal. Granskningen avser bokförda leverantörsfakturer i kontogrupp 52xx – 57xx för perioden januari – september 2024. Bokförda fakturer har med hjälp av leverantörernas ID-nummer matchats mot registrerade ID-nummer i leverantörsregistret. I leverantörsregistret finns det registrerade uppgifter om det existerar ett hyresavtal, ett eget ramavtal, ett statligt ramavtal eller om det saknas ett avtal med



leverantören. I de fall då det var noterat att det saknas ett avtal eller då det inte fanns några uppgifter registrerade har IR sökt efter leverantören i universitetets avtalskatalog och bland Kammarkollegiets leverantörer på avropa.se.

Granskningen visar att institutionen anskaffar varor och tjänster genom avrop eller beställningar från egna och statliga ramavtal. Av de granskade leverantörerna saknar dock merparten avtal med universitetet eller med Kammarkollegiet; andelen leverantörer utan avtal uppgår till 60 procent. De totala kostnaderna för anskaffningarna i urvalet uppgår till drygt 2,6 mkr.

### 2.3.1. Direktupphandling över 100 000 kronor

I intervjun framgick det att institutionen har anmält en direktupphandling över 100 000 kronor till Inköps- och upphandlingssektionen under perioden januari – november 2024 samt att direktupphandlingen genomfördes under ledning av en inköpskoordinator. Universitetets upphandlingschef har godkänt anskaffningen och institutionen har upprättat ett tilldelningsbeslut samt ingått ett avtal med anbudsgivaren som har undertecknats av prefekt. Vidare har institutionen skickat en upphandlingsrapport till Ekonomiavdelningen samt diariefört underlagen.

### 2.3.2. Bedömning och rekommendationer

IR:s bedömning av den interna styrningen och kontrollen avseende inköp och upphandling är att det finns förbättringsmöjligheter. Granskningen visar att merparten av de leverantörer som institutionen genomför inköp från saknar avtal med universitetet eller Kammarkollegiet. I ”Regler för inköp och upphandling”<sup>18</sup> anger universitetet följande: *även om det i ett enskilt fall finns förutsättningar för direktupphandling, så är det normalt bättre att planera och konkurrensutsätta anskaffning, eftersom det kan förväntas ge lägre pris och högre kvalitet.* Med anledning av vad som nämns i regelverket bedömer IR att det är viktigt att institutionen arbetar långsiktigt mot att minska andelen inköp utanför ramavtal.

Brister	Risker	Sammanfattande bedömning ISK
Merparten av de leverantörer som institutionen genomför inköp hos saknar avtal.	Risk för bristande följsamhet mot interna inköps- och upphandlingsregler.	Förbättringsmöjligheter
<b>Rekommendationer</b>		
6. Vidta åtgärder för att minska andelen inköp hos leverantörer som saknar ramavtal.		

<sup>18</sup> Dnr SU-2.2.1-1679-15 ”Regler för inköp och upphandling” Beslutad av Förvaltningschefen. Beslutsdatum 2017-12-21

## 2.4. Riskområde – Lärarnas bisysslor

Enligt 3 kap. 7§ högskolelagen (1992:1434) har lärare på universitet och högskolor rätt att inneha bisysslor som rör forskning eller utvecklingsarbete inom anställningens ämnesområde, men det finns begränsningar i lagstiftningen. En bisyssla får inte bidra till att lärosätets förtroende skadas och bisysslor ska hållas klart åtskilda från lärarnas arbete. Vidare ställer 4 kap. 15§ i högskoleförordningen (1993:100) krav på att lärarna ska informera lärosätet om bisysslor som har anknytning till anställningens ämnesområde.

För att universitetet ska leva upp till de externa kraven har universitetet tagit fram interna styr- och stöddokument. Regler om redovisningsplikt och var uppgifter om bisyssla ska redovisas återfinns i ”Föreskrifter om bisysslor för anställda vid Stockholms universitet”<sup>19</sup> och i kompendiet ”Information avseende bisysslor vid Stockholms universitet”<sup>20</sup>. I dokumenten framgår att redovisning av bisysslor sker i personalsystemet Primula och att lärare som inte har någon bisyssla årligen ska redovisa detta.

I intervjun med prefekt framgick att institutionen inte har några dokumenterade rutiner gällande lärarnas bisysslor och att institutionen inte har någon uttalad policy att informera nyrekryterade lärare om universitetets regler. Vidare är det oklart hur ofta institutionens närmaste chefer (vid institutionen finns det sex avdelningsföreståndare som leder varsin enhet) diskuterar bisysslor med lärarna och om cheferna berör bisysslor i de årliga utvecklingssamtalen.

Institutionens lärare har tillgång information om bisysslor på institutionens webbplats där det finns länkar till medarbetarwebben och Primula. På webbplatsen informeras medarbetarna om att bisysslor anmäls i Primula och att lärarna fortlöpande ska anmäla bisysslor. Från och med hösten 2024 tar prefekten fram uppgifter ur Primula på höstterminen för att kontrollera vilka lärare som har registrerat uppgifter om bisyssla eller inte. De lärare som inte har registrerat några uppgifter får ett påminnelse-mail av institutionens prefekt. I påminnelsen uppmanas lärarna att registrera uppgifterna i Primula.

I lärarkategorin<sup>21</sup> vid Stockholms universitet ingår följande befattningar/titlar:

- Professorer (alla typer, som biträdande, adjungerade, gäst, befordrade, kallade m.m.)
- Lektorer (alla typer, som universitetslektor, befordrad universitetslektor, biträdande universitetslektor m.m.)
- Adjunkter (alla typer som universitetsadjunkt, adjungerad m.m.)

<sup>19</sup> Dnr SU FV-1.1.2-0592-16 ”Föreskrifter om bisysslor för anställda vid Stockholms universitet”. Beslutad av Rektor. Beslutsdatum 2016-02-25.

<sup>20</sup> Medarbetarwebben -> Anställd -> Min anställning -> Bisysslor -> Läs mer information om bisysslor.

<sup>21</sup> Lärarpersonalens befattningar/titlar i personalsystemet Primula och enligt Dnr SU FV-1.1.2-0354-20 ”Anställningsordning för anställning som och befordrad till lärare vid Stockholms universitet (AOSU)”. Beslutad av universitetsstyrelsen. Beslutsdatum 2020-02-18.

- Lärare (alla typer som adjungerad, gäst, även timlärare, som dock inte kan anmäla sina bisysslor i Primula)

Enligt ett rapportutdrag från Primula den 2024-09-30 har drygt 20 procent av institutionens lärare registrerat uppgifter om bisyssla. Ett utdrag i Primula den 2024-11-15 visar att samtliga lärare har registrerat uppgifterna. Vid 2023 års utgång var motsvarande andel 25 procent.

#### 2.4.1. Bedömning och rekommendationer

IR:s bedömning är att den interna styrningen och kontrollen avseende lärarnas bisysslor är bristfällig. När granskningen påbörjades hade merparten av institutionens lärare inte registrerat några uppgifter om bisyssla i Primula. Efter den inledande granskningsperioden har dock åtgärder vidtagits och samtliga lärare har registrerat uppgifterna. Granskningen visar även att det saknas ruiner för att informera nyrekryterade lärare om universitetets regler. Vidare kan institutionens löpande information om bisysslor i de återkommande utvecklingssamtalen förtydligas.

Brister	Risker	Sammanfattande bedömning ISK
Institutionen genomför inga informationsinsatser åt nyrekryterade lärare gällande universitetets regler för bisysslor.	Risk att institutionen inte uppfyller externa och interna krav.	Bristfällig
Oklart om lärarna löpande (t.ex. vid årliga utvecklingssamtal) informeras om att registrera uppgifter i Primula.		
Före genomförandet av granskningen skedde inga uppföljningar/kontroller av registrerade uppgifter i Primula.		
Efter granskningens start har samtliga lärare registrerat uppgifter om bisyssla i Primula. Innan granskningen påbörjades hade dock merparten av lärarna inte registrerat några uppgifter.		
<b>Rekommendationer</b>		
7. Säkerställ att lärare som rekryteras till institutionen informeras om universitetets föreskrift och information avseende bisysslor samt att de har förstått reglerna.		
8. Säkerställ att lärarna löpande (t.ex. i årliga utvecklingssamtal) informeras om sina skyldigheter vid utövandet av bisysslor.		

## 2.5. Riskområde – Säkerhet

Inom område Säkerhet har Internrevisionen översiktligt granskat fyra delområden: personuppgiftsbehandling, informationssäkerhet, IT-säkerhet och fysisk säkerhet.

### 2.5.1. Personuppgiftsbehandling

När det gäller personuppgiftsbehandlingen saknar institutionen en upprättad registerförteckning. Av institutionens genomförda informationsklassning (se vidare nedan under avsnitt om informationssäkerhet) avseende administrativ data, fastställd 2024-04-29, framgår emellertid att registerförteckning GDPR ingår bland informationen som har klassats, tillsammans med utpekat informationsägarskap för registerförteckningen.

Institutionen uppger att de inte har något behov av registerförteckning. De har listor över studenter i Ladok, och vidare framhålls att de, som en konsekvens av GDPR, använder skriftliga tillstånd när de fotograferar vid utgrävningar, innan något publiceras, så att studenter ger medgivande till att fotografier används till exempel i marknadsföring. De upprättar även tillfälliga listor med kontaktuppgifter till anhöriga, i säkerhetssyfte om något skulle hända när de är i fält.

Institutionen har inte haft någon kontakt med universitetets dataskyddsombud i frågan om personuppgiftsbehandling.

Institutionen har inga rutiner som rör personuppgiftsbehandling eller incidentrapportering. Det har inte förekommit att det inkommit frågor om registerutdrag eller radering.

När det gäller utbildning inom området nämner institutionen Nimblr-utbildningen (Stockholm University Security Awareness Training) som erbjuds inom Stockholms universitet. De anställda förväntas genomföra utbildningsmodulerna. Det var vid granskningstillfället oklart hur många som genomgått de hittills erbjudna utbildningsmodulerna.<sup>22</sup> Information om dataskydd ingår inte introduktionen av nyanställda.

---

<sup>22</sup> Enligt uppgift erhållen från IT-avdelningen per 2024-12-05 kan de genom administrationsverktyget se statistik över hur många och vilka användare som har slutfört de moduler som skickats ut. En funktion har nyligen införts som gör det möjligt för varje institution att ha en egen administratör, som kan få tillgång till statistik specifikt för den egna institutionen. I dagsläget är dock användarna inte uppdelade per institution i databasen, vilket beror på att SUKAT inte är kopplat till Nimblrs databas, vilket innebär att användardata måste uppdateras manuellt, vilket uppges vara en tidskrävande process. IT-avdelningen arbetar med en lösning för att förenkla kopplingen vilket skulle göra det enklare att fördela användare per institution och därmed förbättra uppföljningen.

### 2.5.2. Informationssäkerhet

Regelverket ”MSB23 föreskrifter om statliga myndigheters informationssäkerhet” (MSBFS 2020:6) ställer krav på ett riskbaserat och systematiskt informationssäkerhetsarbete över tid. Enligt regelverken ska universitetets viktiga informationstillgångar, exempelvis forsknings- och utbildningsdata, hanteras på sådant sätt att det går att säkerställa att de skyddas mot obehörig åtkomst, felaktiga förändringar och att de finns tillgängliga då de behövs.

En förutsättning för att kunna bedriva ett ändamålsenligt och effektivt informationssäkerhetsarbete är att viktig information inom institutionen klassificeras av chef eller motsvarande (t.ex. objektsägare/informationsägare) utifrån aspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet. Utifrån denna klassificering ska sedan ändamålsenliga skyddsåtgärder utformas, exempelvis administrativa rutiner, utbildning av medarbetare, brandväggar, behörighetskontroller, skalskydd etc.

Institutionen har genom ESIR-projektet<sup>24</sup> genomfört en informationsklassning avseende forskningsdata, utbildningsdata samt administrativ data. Internrevisionen har tagit del av informationsklassningen, och det framgår att klassningen fastställdes 2024-04-29. När det gäller exempelvis administrativ data framgår att institutionens prefekt och administrativa chef huvudsakligen ansvarar för de olika informationstyperna som har klassats. Klassningen av information har tagits upp både i ledningsgruppen och i institutionsstyrelsen.

Merparten av informationen har klassats som nivå 2, dvs ”grundläggande skyddsnivå”. Ett flertal informationstyper har klassats som nivå 3, dvs ”utökad skyddsnivå”. Här återfinns exempelvis tentamensuppgifter och anställningsbeslut. Få delar har klassats med högsta känslighetsnivå, totalt tre informationstyper har klassats i nivå 4, dvs ”hög skyddsnivå”, utifrån konfidentialitet och spårbarhet. Det rör rehab-information, upphandlingar och lokalt arkiv. Klassificeringen har inte resulterat i några efterföljande åtgärder.

MBS:s föreskrifter ställer även krav på att utveckla och upprätthålla kompetens hos egen personal avseende informationssäkerhet genom utbildning, informationsinsatser och övning. Institutionens medarbetare förväntas ta del av de utbildningsmoduler (Stockholm University Security Awareness Training) som rör olika aspekter av informations- och IT-säkerhet som erbjuds. Utöver detta har ingen specifik utbildning skett för att säkra kompetens inom informationssäkerhet.

---

<sup>23</sup> Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

<sup>24</sup> ESIR - Etablering av Systematiskt Informationssäkerhetsarbete och Resultatstyrning

### 2.5.3. IT-säkerhet

Av institutionens cirka 80 anställda har ingen SUA-datorer. Samtliga anställda har SUKAT-konto och SU-mail.

Institutionen har valt att ha egna datorer och en egen lokal IT-tekniker, då detta dels framhålls vara en billigare lösning, dels innebär att institutionen har IT-personal på plats vilket behövs för stöd med utrustning och salar på institutionen. Institutionen använder inte Printomat, men en Printomat-skrivare finns för studenterna, och en finns även på Centrum för paleogenetik, CPG.

I december 2018 fattade rektor beslutet ”Anslutning till IT-tjänster för ökad säkerhet”<sup>25</sup>. Av beslutet framgår att anslutning till de fyra IT-tjänsterna för ökad säkerhet (inloggningstjänst, skydd mot virus och skadlig kod, inventeringsprogram och avvecklingstjänst) är obligatorisk för samtliga institutioner. Enligt genomförda intervjuer har institutionen anslutit sig till de fyra IT-tjänsterna men osäkerhet fanns huruvida det var helt klart. En kontroll med IT-avdelningen har givit vid handen att institutionen har och använder inloggningstjänsten, men IT-avdelningen har inte kontroll över eventuella lokala IT-system med inloggning som används inom institutionerna. Institutionen använder avvecklingstjänsten. Institutionen har huvudsakligen PC, och enligt lokalt IT-ansvarig använder de skydd mot virus. Institutionen har ca 130 datorer med inventeringsprogramvaran.

Administrativ chef beslutar om behörigheter. Alla har SUKAT-konto<sup>26</sup>. Behörigheterna uppges uppdateras årligen, och sägs upp när någon avslutar sin anställning.

Institutionen har egna program som är kopplade till laboratorerna. Samarbete sker med IT-avdelningen genom lagring, ej i övrigt. Institutionen lagrar sin data genom IT-avdelningens molnlösning. Backup tas automatiskt av IT-avdelningen genom denna lösning, och det uppges gälla samtliga anställda vid institutionen.

Enligt uppgift har inga dataintrång eller andra incidenter förekommit under de senaste 2-3 åren. Institutionen har ingen egen incidentrapporteringsrutin.

Grundläggande information om allmän säkerhet och laboratoriesäkerhet ges till nyanställda, men ingen särskild information om informationssäkerhet eller IT-säkerhet. Någon IT-utbildning har inte genomförts utöver den pågående universitetsgemensamma Stockholm University Security Awareness Training som erbjuds i flera korta moduler.

<sup>25</sup> Dnr: SU FV 2.8.3-0207-17 ”Anslutning till IT-tjänster för ökad säkerhet”. Beslutad av rektor. Beslutsdatum 2018-12-20.

<sup>26</sup> Databas som innehåller information om alla användare vid Stockholms universitet, både anställda och studenter. Alla användare får ett universitetskonto (kopplat till IT-access), och detta ger tillgång till en mängd olika tjänster, t ex e-post, trådlöst nätverk, lärplattformen Athena m.m.

#### 2.5.4. Fysisk säkerhet

Vid institutionen är prefekt övergripande ansvarig för säkerhet. Institutionen har en kris-  
hanteringsplan som är fastställd av institutionsstyrelsen 2024-09-30. I kris-  
hanteringsplanen är bland annat krisgruppens uppgift definierad, och roller beskrivna för prefekt, utrymningsledare  
för våning 1-4, arbetsmiljöombud m fl. Krishanteringsplanen innehåller plan för olika typer av  
krissituationer (brand, dödsfall, hot samt akut sjukdomsfall) och har enligt uppgift skickats via  
e-post till alla anställda samt finns tillgänglig på institutionens hemsida. Institutionen upprättar  
till åtgärdsplaner inför arkeologiska fältarbeten. Där finns information om larmnummer,  
telefonnummer till anhöriga, vägbeskrivningar och aktuella koordinater. Institutionen har en  
årlig halvdagsutbildning för arkeologistudenter inför fältarbetet, utbildningen ges av  
företagshälsovården, och även lärarna har möjlighet att delta. Utbildningen uppges innehålla  
första hjälpen/HLR/L-ABC. När det gäller kompetens inom brandskydd möts kraven genom  
föreståndarna för arkeologiska forskningslaboratoriet och osteoarkeologiska forsknings-  
laboratoriet, samt en labbkoordinator på Centrum för Palaeogenetik.

Avseende skalskydd är institutionens ytterdörr vanligtvis låst, men hålls olåst t ex vid kursstart.  
Ingång 1 och 2 vid institutionen har alltid låsta dörrar. Plan 3 och 4 är öppet under arbetstid men  
låst under natten. Studenter har kod till de låsta delarna mellan kl. 8-18, och tillträdet kan  
förlängas vid behov, exempelvis vid kvällskurser. Institutionen har även öppna forskar-  
seminarium och allmänna seminarium. Tillgång till lokalerna har personal och studenter, samt  
tillfälliga gäster, men då även med närvaro av institutionens personal.

Institutionen har inget eget serverrum. Vid institutionen finns laboratorier, och två laboratorie-  
säkerhetssamordnare finns utsedda. Arbetet sker med bl a årlig inventering av kemikalier och  
regelbunden kontakt finns med fastighetsavdelningens samordnare.

När det gäller inbrott och stölder har några incidenter förekommit. Datorer stals 2018, och för  
några år sedan skedde ett försök till inbrott, men vakter hann komma innan inbrottet genom-  
fördes. En bärbar dator som används till en projektor stals för cirka 3 år sedan, vilket skedde  
genom ett fönster. Efter detta har datorn till projektorn placerats så att den inte är synlig från  
fönstret. Institutionens lokaler ligger tämligen isolerade vid Wallenberglaboratoriet, i området  
Lilla Frescati. Institutionen kommer dock att lämna nuvarande lokaler för en flytt till Frescati.

Några fall av hot har skett vid institutionen, som exempel har nämnts hot i samband med  
utgrävning nära Jordbro centrum, och en professor vid institutionen som blev hotad i samband  
med tv-serien "Sveriges historia".

Kontaktuppgifter till företagshälsovård respektive studenthälsan finns på institutionens hemsida  
med hänvisning till SU:s hemsida.

### 2.5.5. Bedömning och rekommendationer

IR:s bedömning av området säkerhet är att den interna styrningen och kontrollen är bristfällig. Institutionen saknar registerförteckning för personuppgiftsbehandling, vilket är ett krav sedan många år enligt artikel 30 i GDPR. När det gäller informationssäkerhet är det positivt att institutionen har genomfört en klassning av forsknings-, utbildnings- och administrativ data. Några åtgärder är inte vidtagna efter klassningen. IR ser ett behov av systematik samt tydligare information och utbildning inom informationssäkerhet. Det är en brist att institutionen inte har en tydlig bild av nästa steg i arbetet med informationssäkerhet. Inom IT-säkerhet finns ett uppbyggt samarbete med IT-avdelningen och backup av data tas med automatik vilket möjliggör återställning. När det gäller den fysiska säkerheten kommer institutionen att flytta från nuvarande lokaler. Det är viktigt att rutiner och ansvar uppdateras i samband med flytten till nya lokalerna. Vi har noterat att institutionen har roller på plats för exempelvis laboratoriesäkerhet och brand. Ett generellt utvecklingsområde är att tydliggöra och säkerställa samtliga delar av institutionens ansvar före kris i enlighet med SU:s krisplan, såsom att säkerställa kunskaper och informera all personal om vad som gäller och förväntas.

Brister	Risker	Sammanfattande bedömning ISK
Register över personuppgiftsbehandling saknas.	Risk att institutionen ej lever upp till krav i om aktuell registerförteckning (artikel 30 i dataskyddsförordningen, GDPR).	Bristfällig
Systematik och ansvarsfördelning för att säkerställa ett systematiskt informationssäkerhetsarbete.	Risk att institutionens systematiska informationssäkerhetsarbete inte kan ske på ett effektivt och/eller ändamålsenligt.	
Medarbetares kompetensutveckling i säkerhetsfrågor behöver säkras.	Risk att samtliga delar av SU:s krisplan inte följs om all personal inte har kunskap om vad som gäller och förväntas.	
<b>Rekommendationer</b> <ol style="list-style-type: none"> <li>9. Säkerställ att institutionen tar fram en aktuell registerförteckning innehållande de processer som innebär behandling av personuppgifter.</li> <li>10. Klargör, i samarbete med IT-avdelningen, nästa steg i arbetet med informationssäkerhet.</li> <li>11. Säkerställ kompetensutveckling för de medarbetare som hanterar viktig/känslig information i sitt arbete i enlighet med MSB:s föreskrifter, samt generellt för säkerhetsfrågor.</li> </ol>		

## 2.6. Riskområde - Tentafusk

Disciplinära åtgärder regleras i 10 kap. högskoleförordningen (1993:100) och i 10 kap. 1§ framgår bland annat att ”disciplinära åtgärder får vidtas mot studenter som med otillåtna hjälpmedel eller på annat sätt försöker vilseleda vid prov eller när en studieprestation annars ska bedömas”.

Enligt ”Regler och handlägningsordning för disciplinärenden”<sup>27</sup> är det institutionen som utreder och bedömer om det föreligger misstanke om disciplinär förseelse och Rektors kansli (Rättssekretariatet) eller Disciplinnämnden som avgör i ärendet. För att minimera fusk vid examinationer är institutionens förebyggande arbete centralt. En viktig åtgärd är att tidigt informera studenter om vad som gäller på universitetet, vilket även lyfts fram i det universitetsgemensamma styrdokumentet.

På institutionen är det studierektor tillika utredningsansvarig som utreder misstänkta disciplinärenden och sammanställer underlagen som skickas till Rektors kansli för slutligt avgörande. Visar institutionens utredning att det inte föreligger någon grundad misstanke om försök till vilseledande vid examinationstillfället skickas inte ärendet till Rektors kansli.

I intervjun med utredningsansvarig framgick det att studenterna informeras av institutionen om vad som gäller vid fusk och plagiat. Studenterna har tillgång till institutionens policy avseende fusk och plagiat via universitetets läroplattform Athena samt på institutionens webbplats. I policyn som antogs av institutionsstyrelsen den 2024-10-28 framgår att institutionen har nolltolerans mot plagiat och att institutionen använder textmatchningsverktyg samt synen på generativ AI<sup>28</sup>. Via institutionens webbplats kan studenterna också ta del av universitetets gemensamma information om fusk och plagiat samt universitetets handlägningsordning för disciplinärenden. Vidare informerar ansvariga kursexaminatorer studenterna om hur examinationer ska genomföras och lämnar skriftliga beskrivningar av examinationsuppgifterna i Athena.

För att upptäcka plagiat använder institutionen textjämförelseverktyget Urkund i Athena. I institutionens etikpolicy framgår det att om en student fuskar eller plagierar skall detta anmälas till studierektorn som vidtar åtgärder. På institutionen är det upp till ansvarig lärare att avgöra om Urkund ska aktiveras eller inte och hur resultatet kan tolkas. Institutionen tillämpar ingen särskild nivå på utfall i Urkund som föranleder att misstänkta ärenden överlämnas till utredningsansvarig. Det förs emellertid kollegiala samtal om vad som är att betrakta som

---

<sup>27</sup> Dnr SU FV-4242-21 ”Regler och handlägningsordning för disciplinärenden”. Beslutad av rektor. Beslutsdatum 2022-02-10.

<sup>28</sup> Exempelvis OpenAI:s applikation ChatGPT.

objektiv grund vid misstanke om fusk och ämnet brukar bli föremål för diskussion på institutionens årliga lektorskongress för alla lärare som leds av studierektor/utredningsansvarig.

Vid salsexaminationer hos institutionen finns det tentamensvakter som övervakar examinationen. Institutionen använder egna lokaler och har egna tentamensvakter (alumner, doktorander eller studenter som har studerat en längre tid på institutionen). Om tentamensvakten misstänker att en student fuskar vid examinationen kontaktas ansvarig lärare för en muntlig redogörelse. Enligt uppgift är det ovanligt med misstänkta fuskärenden på institutionen. Institutionen har endast haft ett fuskärende (plagiat) de senaste två åren som har skickats till Rektors kansli för slutligt avgörande.

### 2.6.1. Bedömning och rekommendationer

IR:s bedömning av den interna styrningen och kontrollen avseende tentafusk är att det finns förbättringsmöjligheter. Granskningen visar att institutionens tentamensvakter inte skriver en rapport vid misstanke om fusk i salsexaminationer. Det bör dock nämnas att institutionen ännu inte har haft något misstänkt fuskärende vid examinationer i sal. Mot bakgrund av att universitetet anger i regelverket ”Regler för salstentamen”<sup>29</sup> att tentamensvärdar skriver en rapport som skickas till institutionernas prefekt eller studierektor för eventuell anmälan till rektor, bedömer IR att ett sådant tillvägagångssätt bör förekomma hos institutionen. IR bedömer vidare att det är positivt att institutionen har upprättat en policy avseende fusk och plagiat, där institutionen bland annat fastställer att omformulerade texter med stöd av AI, i brist på källhänvisningar betraktas som plagiat. IR ser även positivt på att institutionen haft kollegiala samtal om vad som är att betrakta som objektiv grund vid misstanke om fusk.

Brister	Risker	Sammanfattande bedömning ISK
Institutionens tentamensvakter skriver inga rapporter vid misstanke om fusk i salsexaminationer.	Risk för bristande efterlevnad mot universitetsgemensamma regler.	Förbättringsmöjlighet
<p><b>Rekommendationer</b></p> <p>12. Säkerställ att tentamensvakter upprättar en rapport vid misstanke om fusk i salsexaminationer.</p>		

<sup>29</sup> Dnr SU FV-1.1.2-2346-20 ”Regler för salstentamen”. Beslutad av rektor. Beslutsdatum 2020-08-27.

Internrevisionen

# Institutionen för astronomi (401)

## Revisionsrapport från Internrevisionen

## Innehåll

<b>SAMMANFATTNING OCH REKOMMENDATIONER .....</b>	<b>3</b>
<b>1. BAKGRUND OCH SYFTE .....</b>	<b>5</b>
1.1.1. <i>Omfattning och metod .....</i>	5
1.1.2. <i>Beskrivning av Institutionen för astronomi .....</i>	6
<b>2. GRANSKNINGSRESULTAT.....</b>	<b>7</b>
<b>2.1. RISKOMRÅDE – EKONOMI .....</b>	<b>7</b>
2.1.1. <i>Budgetering.....</i>	7
2.1.2. <i>Resultat och resultatuppföljning .....</i>	9
2.1.3. <i>Redovisning.....</i>	11
2.1.4. <i>Bedömningar och rekommendationer.....</i>	15
<b>2.2. RISKOMRÅDE - ANLÄGGNINGSTILLGÅNGAR OCH STÖLDBEGÄRLIGA FÖRBRUKNINGSSINVENTARIER .....</b>	<b>17</b>
2.2.1. <i>Anläggningstillgångar .....</i>	17
2.2.2. <i>Stöldbegärliga förbrukningsinventarier (SFI).....</i>	18
2.2.3. <i>Inventering och utrangering .....</i>	19
2.2.4. <i>Bedömning och rekommendationer .....</i>	19
<b>2.3. RISKOMRÅDE – INKÖP OCH UPPHANDLING .....</b>	<b>20</b>
2.3.1. <i>Direktupphandling över 100 000 kronor .....</i>	21
2.3.2. <i>Bedömning och rekommendationer .....</i>	21
<b>2.4. RISKOMRÅDE – LÄRARNAS BISYSSLOR.....</b>	<b>22</b>
2.4.1. <i>Bedömning och rekommendationer .....</i>	23
<b>2.5. RISKOMRÅDE – SÄKERHET .....</b>	<b>24</b>
2.5.1. <i>Personuppgiftsbehandling .....</i>	24
2.5.2. <i>Informationssäkerhet.....</i>	25
2.5.3. <i>IT-säkerhet .....</i>	26
2.5.4. <i>Fysisk säkerhet .....</i>	27
2.5.5. <i>Status efter granskning av fysisk säkerhet i IT-utrymmen .....</i>	28
2.5.6. <i>Bedömning och rekommendationer .....</i>	28
<b>2.6. RISKOMRÅDE - TENTAFUSK.....</b>	<b>30</b>
2.6.1. <i>Bedömning och rekommendationer .....</i>	31

## Sammanfattning och rekommendationer

Internrevisionen (IR) har under 2024 granskat den interna styrningen och kontrollen vid Institutionen för astronomi (401). Granskningen har fokuserats på ett antal administrativa rutiner som bedöms vara grundläggande för en god intern styrning och kontroll inom väsentliga riskområden.

IR:s bedömning<sup>1</sup> är att institutionens interna styrning och kontroll är *tillfredsställande* inom områdena budgetering och resultatuppföljning.

Vidare bedömer IR att det finns *förbättringsmöjligheter* inom områdena anläggningstillgångar och stöldbegärliga förbrukningsinventarier, inköp och upphandling, samt tentafusk.

IR har bedömt några områden som *bristfälliga*: redovisning och kontroller, lärarnas bisysslor samt säkerhet.

Baserat på genomförd granskning har IR lämnat följande rekommendationer:

1. Förbättra kontroller vid kontering och attest av kostnader samt säkra att moms kostnadsförs vid representationskostnader.
2. Inför en rutin för efterkontroller.
3. Överväg att märka de anläggningstillgångar som kan märkas med ett anläggnings-id.
4. Vidta åtgärder för att minska andelen inköp hos leverantörer som saknar ramavtal.
5. Säkerställ att lärare som rekryteras till institutionen informeras om universitetets föreskrift och information avseende bisysslor samt att de har förstått reglerna.
6. Säkerställ att lärarna löpande (t.ex. i årliga utvecklingssamtal) informeras om sina skyldigheter vid utövandet av bisysslor.

---

<sup>1</sup> IR använder följande fyra nivåer i sin bedömning av den interna styrningen och kontrollen: tillfredsställande, förbättringsmöjligheter, bristfällig samt otillfredsställande.

7. Säkerställ att institutionen tar fram en aktuell registerförteckning innehållande de processer som innebär behandling av personuppgifter.
8. Klargör, i samarbete med IT-avdelningen, nästa steg i arbetet med informationssäkerhet.
9. Säkerställ kompetensutveckling av de medarbetare som hanterar viktig/känslig information i sitt arbete i enlighet med MSB:s föreskrifter, samt generellt för säkerhetsfrågor.
10. Fortsätt arbetet med att åtgärda brister i den fysiska säkerheten i IT-utrymmen.
11. Överväg att föra återkommande kollegiala samtal om vad som är att betrakta som objektiv grund vid användning av textjämförelseverktyg.

Tobias Björn  
Internrevisionschef

Christoffer Skyberg  
Internrevisor

## 1. Bakgrund och syfte

Universitetets decentraliserade styrmodell innebär ett långtgående delegerat ansvar och beslutsmandat till verksamhetens områden, institutioner och förvaltningsavdelningar. Modellen ställer höga krav på ändamålsenliga och effektiva styrstrukturer för att önskad intern styrning och kontroll ska genomsyra alla nivåer i organisationen. Oavsett verksamhet gäller myndighetsförordningens krav på effektivitet, god hushållning av statens medel, regel efterlevnad och tillförlitlig samt rättvisande rapportering.

IR har mot bakgrund av ovanstående granskat intern styrning och kontroll vid två institutioner, varav en är Institutionen för astronomi (401).

Syftet med granskningen var att besvara följande revisionsfråga: *Har institutionen ändamålsenliga och effektiva rutiner som säkerställer en god intern styrning och kontroll inom väsentliga riskområden?*

### 1.1.1. Omfattning och metod

Granskningen fokuserat på följande riskområden:

- Ekonomi (budget, redovisning, uppföljning och rapportering, resor och representation)
- Anläggningstillgångar och stöldbegärliga förbrukningsinventarier
- Inköp och upphandling
- Bisysslor
- Säkerhet (personuppgiftsbehandling, informations-/IT-säkerhet och fysisk säkerhet)
- Tentafusk

Internrevisionens granskning omfattar ej följande områden:

- Bedömning/utvärdering av systemstöd
- Bedömning/utvärdering av kvalitet i utbildning på grund- och avancerad nivå
- Bedömning/utvärdering av kvalitet i forskning och forskarutbildning

Genomförandet har i bestått av:

- Uppstartsmöte med prefekt och administrativ chef.
- Dokumentstudier.
- Genomgång av redovisning, befintliga processbeskrivningar, rutiner etc. för utvalda riskområden.
- Intervjuer med nyckelpersoner på institutionen.
- Test av identifierade nyckelkontroller.
- Analys samt eventuellt kompletterande intervjuer.

- Sammanställning av brister, risker och rekommendationer.

Baserat på identifierade brister och relaterade risker gör Internrevisionen en bedömning av den interna styrningen och kontrollen inom respektive riskområde.<sup>2</sup>

Institutionen har givits möjlighet att faktagranska ett utkast av rapporten innan färdigställandet.

### 1.1.2. Beskrivning av Institutionen för astronomi<sup>3</sup>

Institutionen för astronomi, (401) ingår i den matematisk-fysiska sektionen på Naturvetenskapliga fakulteten. Institutionen har ett femtital anställda lärare/forskare/postdocs. Över 600 studenter studerar varje år vid institutionen. Vid institutionen bedriver cirka 25 studenter sin doktorandutbildning. Vid institutionen finns 7 anställda som T/A-personal.

Institutionen för astronomi vid Stockholms universitet, det moderna Stockholms observatorium, kan räkna sina anor från det första observatoriet i Stockholm som invigdes 1753. Sedan 1973 är institution en del av naturvetenskapliga fakulteten vid Stockholms universitet.

På institutionen bedrivs förutom undervisning både teoretisk och observationell forskning inom astronomi och astrofysik. Vid institutionen finns också Institutet för solfysik som bedriver forskning inom solfysikområdet och är ansvarigt för driften av det svenska solteleskopet på La Palma, SST. Idag finns institutioner lokaler i AlbaNova universitetscentrum, Stockholms centrum för fysik, astronomi och bioteknik, vid Roslagstull.

Ansvarig för verksamheten är institutionens prefekt. Vid institutionen finns en institutionsstyrelse som är institutionens högsta beslutande organ. Institutionens prefekt är ordförande i institutionsstyrelsen.

---

<sup>2</sup> IR använder följande fyra nivåer i sin bedömning av den interna styrningen och kontrollen: tillfredställande, förbättringsmöjligheter, bristfällig samt otillfredsställande.

<sup>3</sup> Från institutionens hemsida, 2025

## 2. Granskningsresultat

I detta avsnitt återfinns en beskrivning av granskningsresultatet inom respektive riskområde. Noterade brister, risker och en sammanfattande bedömning av intern styrning och kontroll samt rekommendationer hittas i slutet av respektive riskområde.

### 2.1. Riskområde – Ekonomi

Institutionens ekonomifunktion består av administrativ chef (AC), tre ekonomer, en personalhandläggare på 80%. AC, ekonomer och personalhandläggare budgeterar för institutionen och AC följer upp institutionens resultat.

Institutionens omsättning år 2023 var 94 mnkr, vilket ligger omsättningsmässigt i mitten bland institutioner inom Naturvetenskapliga fakulteten, nr 11 av 19.

Institutionens verksamhet består av utbildning på grund- och avancerad nivå (UGA) samt forskarutbildning och forskning (FUF).

- 7 % av institutionens kostnader år 2023 avsåg UGA och 93 % FUF.

Verksamhetens kostnader finansieras av både anslag och externa medel. År 2023 finansierade:

- anslag 42 % av kostnaderna och externa medel 58%.
- UGA finansierades helt av anslag. FUF finansierades 42% av anslag och 58% av externa medel (bidrag).

Institutionen har fem kostnadsställen, inklusive de två obligatoriska: *Institutionens övergripande verksamhet* och *verksamhetsstöd*, vars kostnader fördelas till kärnverksamheten på basis av kärn-verksamhetens löner och LKP med hjälp av fördelningsprocenten framräknade av institutionen.

#### 2.1.1. Budgetering

Budgetarbetet är en viktig del i institutionens styrning av verksamheten och dess ekonomi. En plan över intäkter och kostnader är även en förutsättning för en effektiv resultatuppföljning. Vid framtagandet av institutionens budget är flera personer involverade. Administrativ chef (AC) koordinerar budgetarbetet.

- Personalhandläggaren budgeterar alla löner, och gör en preliminär budgetfil för lönerna som sedan går igenom tillsammans med AC så att konteringar, nyanställningar, löneuppräknung och avslut mm stämmer. Strategiska frågor, som eventuella nyanställningar av doktorander på anslagsmedel tas vidare till prefekten för diskussion i ledningsgruppen.

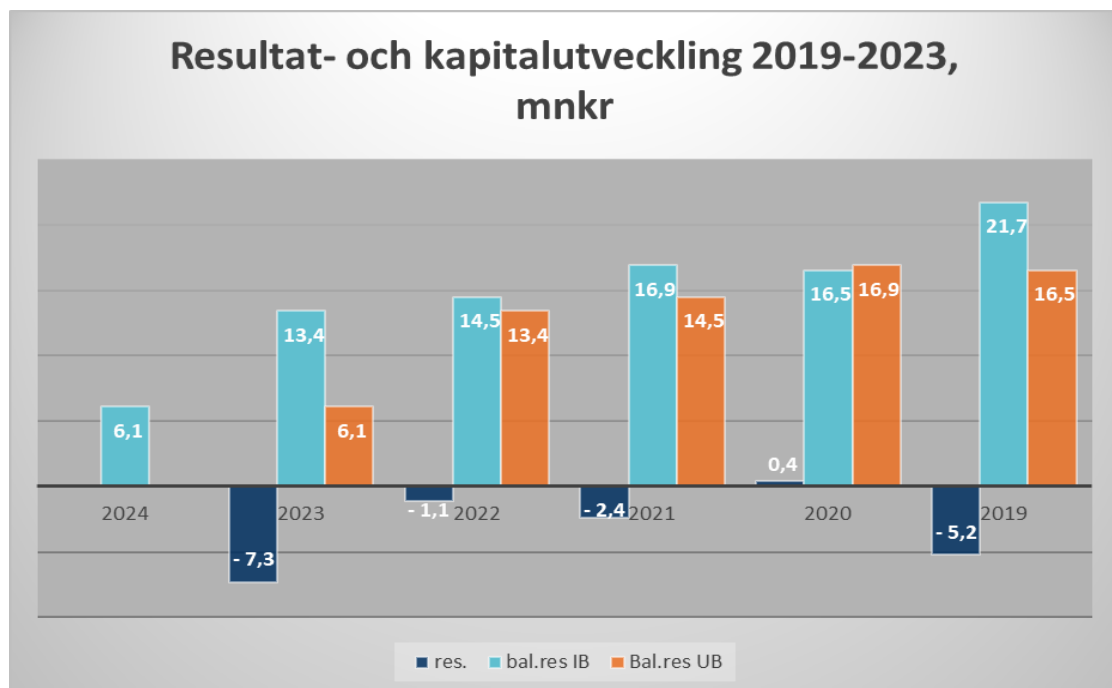
- Ekonomerna kontaktar sina respektive projektledare angående externa projektens budgetar, och därefter budgeterar ekonomerna externprojektens kostnader och intäkter.
- AC budgeterar institutionens anslagsintäkter och -kostnader inklusive stödkostnadsbäraren och räknar fram fördelningsprocenter för lokaler och stödkostnader.
- När alla parter är nöjda med den preliminära personalbudgeten registrerar personalhandläggaren in den i Rainedance.
- Prefekten granskar budgeten.
- AC presenterar budgeten till institutionsstyrelsen, som beslutar budgeten.
- Efter att budgeten beslutats av institutionsstyrelsen, definitivsätts den i Rainedance och skickas till fakultetscontroller.

Träffsäkerhet på institutionens totalbudget under de senaste åren har varit i intervallet mellan +3,4 mnkr till +2,6 mnkr (bättre än budget). Budgetavvikelse mot utfall räknat som procent av respektive årets omsättning har varit i intervallet 3,6 % till 2,8 %. Budgetar är i allmänhet försiktiga och utfallet blir ofta bättre än det budgeterade. Att år 2023 utfall blev bättre än budgeterat berodde på lägre kostnader än budgeterat, främst personal- och driftskostnader.

Mnkr.	2022	2023	2024
Budget, resultat	-4,5	-9,9	-6,0
Utfall, resultat	-1,1	-7,3	
Avvikelse budget jmf. Utfall	+3,4	+2,6	
Årets omsättning	95,4	94,0	
Avvikelse % av årets oms.	3,6	2,8	

### 2.1.2. Resultat och resultatuppföljning

Institutionens resultatutveckling under åren 2019 - 2023 har varierat med +0,4 mnkr år 2020 och därefter sjunkande igen med årliga underskottsresultat. Institutionen har positivt balanserat kapital, som har minskat med underskottsresultaten, men är fortfarande på plussidan vid årsskiftet 2023/2024 (balanserat resultat UB 2023/IB 2024, 6,1 mnkr) och motsvarar 6,5% år 2023 omsättning.



AC återger att 2019 fick institutionen höra att den har för mycket sparat kapital och en åtgärd som rekommenderades var att anställa doktorander med anslagsmedel, vilket institutionen också gjorde och kapitalet började minska. Under projektet "Ekonomi i balans" 2020–2023 var rekommendationen det motsatta, men för att behålla en bra verksamhet måste institutionen ha en viss miniminivå enligt AC. Dock kan inte institutionen helt förbruka sitt kapital och institutionen har diskuterat detta med dekanen.

År 2023 var enligt AC ett svårt år med hög inflation och bara liten ökning av anslagsintäkten. Institutionen kan inte minska för mycket på rekrytering av doktorander eller lärare, det är en lång process. AC:s prognos vid tidpunkten för granskningen var dock att resultatutvecklingen blir bättre och prognosen för 2024 års resultat är en förlust på ca -4 mnkr istället för det

budgeterade -6 mnkr. Målet är att nå plusresultat om ett par år, 2025–2026, behålla ca. 5% kapital och undvika stora vändningar i resultatet.

Resultatet till och med T2, augusti 2024 (-4,7 mnkr jmf. -5,4 mnkr augusti 2023) är något bättre än förra årets resultat samma period. Intäkterna har ökat med 2,1 mnkr, men kostnaderna har endast ökat med 1,4 mnkr. När resultatets (-4,7 mnkr) olika beståndsdelar per augusti 2024 granskas, kan noteras att UGA resultat är -0,5 mnkr, FUF resultat är -5,4 mnkr samt att det finns en portion ej ännu fördelade stödkostnader +1,2 mnkr.

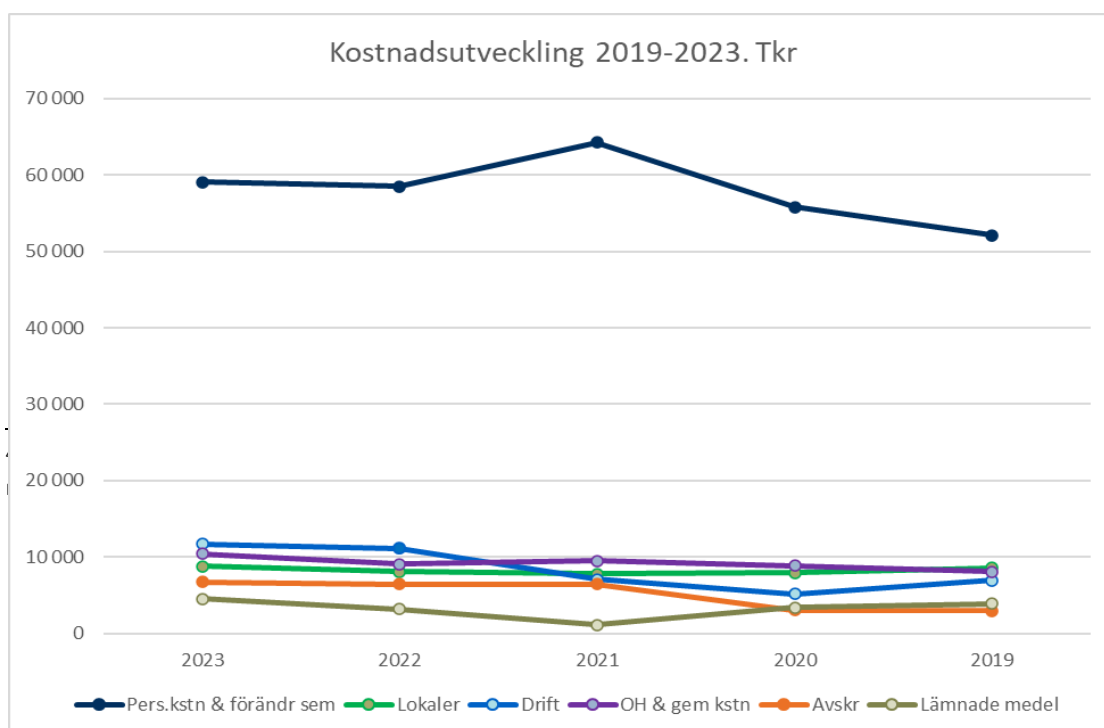
**Arbetet med rektorsbeslut ”Ekonomi i balans”<sup>4</sup>.** Projektet ”Ekonomi i balans” hade slutdatum den sista december 2023, men arbetet att se över sin ekonomi fortsätter. Exempel på åtgärder:

- Sagt upp lokalytan i hus 3.
- Antal nätter på kurs OBS II halverats år 2023.
- Löpande kostnader ses över.

Driftskostnader är det kostnadsslag som efter personalkostnader har ökat mest under de gångna 5 åren. Solfysik står för den största delen av drift. Utöver det är köpt teleskopstid en vanligt förekommande större driftskostnad, vilket kan vara dyrt, dock har institutionen fått mer pengar vilket ger möjligheten att köpa mer teleskopstid.

Även resekostnader är en del av driftskostnader och resandet har ökat till samma nivåer som före pandemiåren. Forskarna reser mycket för de har samarbeten i hela världen. Både teleskopstiden och resorna finansieras till den största delen av bidragsmedel, vilket gör att de fasta driftskostnaderna inte ökat mycket enligt AC.

Diagrammet nedan visar kostnadsutveckling på de olika kostnadsslagen på institutionen under 2019 – 2023.



**Resultatuppföljningen** på institutionen genomförs av AC i huvudsak tertialvis, men även månatligen. Institutionens ekonomi är en fast punkt i agendan vid varje institutionsstyrelsemöte där AC har olika teman på olika möten. Exempelvis efter tertialavslut är fokus på tertialresultatet, i decembermöte är fokus på budget och ramar, vid årets första möte tas årsbokslutet och budgetförslag upp, under löpande året om inget särskilt hänt kommenteras endast hur väl resultatet följer budgeten.

Resultat och budget som presenteras till institutionsstyrelsen är totalresultat på institutionsnivå och även resultat för UGA och FUF<sup>5</sup>. Vid årsbokslut innehåller den även en tabell om tidigare årens resultat (2019–2022). Rapportmall som används är SU:s officiella EKUP-modell.

Externa projekt på institutionens fem forskargrupp följs upp av varsin ekonom, som ansvarar för sammanställningar till projektledarna. Hur ofta uppföljningar sker beror på projektledarnas önskningar; vissa vill ha tätare uppföljningar och andra enligt bestämt plan.

Institutionen resultat kommunicerades tidigare till hela organisationen vid personalmöten, numera kan prefekten ta upp ekonomin på sitt nyhetsbrev till anställda.

### 2.1.3. Redovisning

**Fakturahantering** i systemet Raindance har tre behörigheter: beställare, lokalekonom och beslutsattestant. Alla dessa behörigheter har kontrollplikter om leveransen, fakturan, konteringen och underlagen.

*Beställare*, beställer varor/tjänster via Raindance e-portalen.

- Institutionens inköpskoordinator beställer kontorsmaterial, böcker åt lärare, kaffe mm till pentryt samt övriga förbrukningsvaror. Tre IT-tekniker beställer IT-utrustning och Solarfysik har två beställare som köper IT-utrustning för dem.
- Innan beställningen görs krävs inte förhandsgodkännande.
- Inleveransen av beställningar görs av beställaren.
- Kontroller som ska göras vid inleveransen: *att varan/tjänsten är levererad/utförd, att leveransen stämmer med beställningen, att varan är felfri.*

*Lokalekonom*, tar emot och konterar fakturor som inte kommer via e-beställning

- Institutionen har tre ekonomer som tar emot och konterar fakturor.
- Kontroller som ska göras vid kontering av faktura: *att fakturan är utställd på SU och rätt institution/ avdelning, att den innehåller uppgift om leverantörens organisationsnummer och F-skatt, att leverantörens och SU:s VAT-nummer finns angivet på fakturor från leverantör inom EU, att fakturan specificerar vad som köpts*

---

<sup>5</sup> UGA, utbildning på grund- och avancerad nivå. FUF, forskarutbildning och forskning.

*och hur många stycken, att fakturabeloppet och momsbeloppet är korrekt, och att fakturerings- eller andra avgifter ej debiteras samt att fakturan är konterad enligt gällande kodplan.<sup>6</sup>*

*Beslutsattestant, attesterar e-beställningar, bokföringsorder och fakturor på den verksamhet de är ansvariga för.*

- På institutionen är prefekt och AC attestanter för alla kostnadsställen. Limit för prefekt 2 mnkr, för AC 0,5 mnkr. AC är den främsta attestanten och attesterar alla institutionens fakturor under 0,5 mnkr. Kostnader gällande AC attesteras av prefekten och prefektens kostnader av dekanen.
- Kontroller som ska göras vid attest: *Att kostnaden får belasta den verksamhet som är angivet i konteringen, att finansiering finns, att anskaffningen är förenligt med de regler som gäller för universitetets verksamhet.<sup>7</sup>*

**Utlägg.** I personalsystemet Primula varierar atteststrukturen beroende på typ av ärende. För att godkänna anställdas utlägg/resor krävs utöver personen som registrerar utlägg, *en granskare och en attestant.*

Utlägg/reseräkningar registreras vanligtvis av den anställda själv och då väljs huvudboks konto och resten av kontering, med litet vägledning från systemet. Detta är också fallet på institutionen för astronomi. Institutionen har skrivit en manual på engelska om hur utlägg/traktamentet ska fyllas i. Men eftersom alla anställda inte har kunskaper i redovisning, förutsätter det att granskare och attestanter är särskilt uppmärksamma att underlag är bifogad och att allt, inklusive huvudboks konto, stämmer innan de godkänner ärenden.

Behörighet att **granska** ärenden om utlägg och traktamente i Primula har institutionens tre ekonomer.

#### **Attestbehörigheten**

- AC och prefekten har attestbehörigheten, men i praktiken attesterar AC ärendena förutom sina egna, som attesteras av prefekten.
- Prefektens utlägg och resor överlämnas till dekanen för attest.

---

<sup>6</sup> Dnr SU FV-0677-22 Attestordning – regelverk om att förfoga över universitetets medel, Ekonomiavdelningen 2021-11-18. Gäller från 2022-01-01.

<sup>7</sup> Ibid.

### ***Kontering och kontroller***

För att säkerställa god kvalitet på redovisning, krävs det en fungerande rutin för förebyggande kontroller och efterkontroller.

Inkommande fakturor hanteras elektroniskt i redovisningssystemet Raindance. Systemet har en inbyggd dualitetskontroll som kräver att fakturan först konteras av en person, och därefter attesteras av en annan person, för att en leverantörsfaktura ska släppas till betalning. Denna inbyggda kontroll finns också i Primula<sup>8</sup> gällande utlägg/reseräkningar. Dualitetsprincipen vid hantering av fakturor är en automatisk förebyggande kontroll mot risk för oegentligheter, genom att minska risken att endast en person både konterar och attesterar fakturan. Dock behöver konteraren och attestanten fortfarande genomföra de manuella förebyggande kontrollerna enligt Attestordningen (se föregående sida) och alltid vara observanta på vad de godkänner.

**Kontering.** Kontering ska ske i enlighet med redovisningsregler, universitetets kontoplan samt med stöd av lathundar. Förutom att fakturans /utläggens belopp stämmer, att det är rätt konterat enligt gällande regler behöver man också se till att rätt underlag är bifogat.

Syftet med krav på underlag och förklarande texter är att de ska visa att kostnaden tillhör universitetets verksamhet och att kostnaden är konterad på rätt konto samt med korrekt kodsträng, för intressenter såväl inom som utanför myndigheten. Korrekt kontering är också viktigt bland annat för att redovisningen ska ge en rättvisande bild av verksamheten, och även bidra till tillförlitliga underlag i samband med uppföljning, analys och budgetarbete. Underlag och förklarande texter verkar även förebyggande mot risk för oegentligheter.

Hos Institutionen för astronomi består *förebyggande kontroller* av att konteraren, ekonomen, vanligen frågar beställaren/ansvarig om fakturan kan godkännas och ibland också bekräftar projektnummer till vilket kostnaden ska bokföras. Den intervjuade ekonomen anger att kontering väljs huvudbokskontot lättast via sökfunktionen på rullningslisten i Raindance i stället för dokumentet *Kontoplan*. Ekonomen känner också till att det finns en Lathund, anvisningar i Kontoplanet för särskilda konteringar och en *Regeldokument för representationskostnader*, men tack vare sin erfarenhet behöves dem vanligen inte. Konteraren kontrollerar också att underlaget som krävs finns med.

AC, som attesterar alla fakturor och utlägg, förutom sina egna och prefektens, uppger att kontroll brukar ske av kontot och projektnumret och vid inköp av SFI<sup>9</sup> att rätt anläggningstyp är angivet. AC säger sig vara noga med kontrollerna och har inga problem att skicka fakturor tillbaka för komplettering.

---

<sup>8</sup> Primula är ett personal- och lönesystem.

<sup>9</sup> SFI, stöldbegärliga förbrukningsinventarier. Dessa ska registreras i eget register liknande anläggningsregister och inventeras årligen.

*Efterkontroller*, månatligen/kvartalsvis/tertiälvvis, sker av bokförda kostnader/intäkter för att säkerställa att inget har hamnat på fel huvudboks konto, projekt och kostnadsställe.

IR har genomfört stickprovgranskning av olika kostnadskonton och testat att ekonomiska händelser har attesterats och konterats i enlighet med attestordning, redovisningsregler samt universitetets kontoplan och kompletterande lathundar. Granskningen av några av årets kostnader visade, t ex att förklarande radtexter vanligen fanns, men skulle kunna förtydligas i vissa fall. Vid stickprov noterades att kostnader vanligen är konterade på rätt kontoklass, men en del på fel konto. Exempelvis förekommer det att institutionen konterar kostnader för bullar och tårter etc. i samband med disputationer m.m. på konto 4942 "Kostnader av enklare personalvårdande slag, utomstatlig", istället för att kontera kostnaderna på konto 4981 "Övriga personalkostnader, utomstatliga". Ett annat exempel är att institutionen har konterat ett skåp med tillhörande hyllsystem på konto 5610 "datorer och mobiltelefoner", istället för att kontera kostnaden på konto på konto 5616 "Möbler och inredning". IR noterade också att så gott som alla externa konferens- och kurskostnader köps via utlägg. Bra i dessa fall att också bifoga information om organisatören, som annars finns på fakturor och alltid bifoga konferensprogrammet, vilket också är ett krav<sup>10</sup>. Bra att tänka på är också måltider (frukost/lunch/middag) som bjuds på externa kurser, oavsett om dessa specificeras i fakturan eller inte, eller faktureras separat, ger alltid en kostförmån och ska också avdras från eventuellt traktamente.

*Underlagen* var i allmänhet bifogade, förutom konferensprogrammen. Meddelande-rutan i Raindance och vid utlägg i Primula kan med fördel användas för att ge kompletterande information.

### ***Resor och representation***

Rese- och representationskostnader anses ofta som mer känsliga kostnader, som har en större inneboende risk för sammanblandning av privata och verksamhetens kostnader. För statliga myndigheter är det även viktigt att hushålla väl med statens medel. Representationskostnader har dessutom flera externa regler och krav, exempelvis att hela ingående moms ska kostnadsföras, syfte för representation behöver anges och deltagarlista bifogas.

För extern representation gäller också krav för omedelbart samband gällande tid, plats och personer som deltar i förhandlingen och den efterföljande representationsmåltiden. För intern representation, dvs personalrepresentation (personalfester), gäller dessutom att hela personalen är inbjuden och personalrepresentationer är max 2 ggr/ år för att den ska vara skattefri.

Från stickprov av representation framgick bland annat att julbord inte var konterad som internrepresentation och moms var ej kostnadsfört. Detta enligt AC för att julbord var placerad till samma kväll som institutionens konferens. Dock enligt besked från ESV ska en middag som

---

<sup>10</sup> "Lathund för redovisning av representation m.m. vid Stockholms universitet" Ekonomiavdelningen, punkt 6.1.

har karaktären av en personalfest bokföras som personalfest.<sup>11</sup> Fakturan för mat till personalens sommarfest var korrekt bokfört och moms kostnadsfört samt underlag bifogad, men alkohol till sommarfesten köpt på utlägg var istället felbokfört som övrig personalkostnad (4981) och moms var inte kostnadsfört. Ej heller fanns det någon hänvisning att mat och dryck till samma fest kommer från olika håll. Därutöver har institutionen en tredje personalfest<sup>12</sup> för doktorander, som var korrekt bokfört. Stickprov på extern representation visade korrekt kontering och momshantering samt att underlag som krävs fanns bifogad. Men även ett fall där dricks var inkluderat i ett utlägg och beviljat<sup>13</sup> och något fall där syftet för representation inte var tydliga, ”EO dinner with F.J”.

Bland granskade resekostnader fanns utlägg för ”hyra för La Palma apartement”, konterad som övrig resekostnad istället för hotell och logi, underlag för överföring av pengar finns, men inget kvitto/bekräftelse vad överföring avser. En faktura för hotellövernattnig till en doktorand i New York, där syfte för resan saknas<sup>14</sup>. Faktura för hotellövernattnig för 2 veckor för en gäst i Stockholm, men syftet för övernattningskostnader är oklara. En faktura för en veckas hotellövernattningar i Heidelberg, men syftet för resan och övernattningar framgår inte.

Det finns även helt korrekta exempel som rese-och hotellkostnader vid konferens Cosmology in the Alps i, Schweiz, där syftet tydligt framgår från meddelanderutan och bifogat intyg från deltagande. Syftet för resekostnader framgår också tydligt från utlägget för att delta i konferensen för Extreme Solar Systems V i Nya Zeeland, dock program för konferensen var inte bifogad<sup>15</sup>.

Exempel av stickproven har diskuterats med administrativ chef och en av ekonomerna.

#### 2.1.4. Bedömningar och rekommendationer

##### ***Budgetering***

IR bedömer att institutionens interna styrning och kontroll avseende budgetering är tillfredsställande. Institutionen har bra ordning på budgeteringen. Budgetprocessen leds av AC och alla berörda parter är involverade i processen. Externa projekt budgeteras efter samråd med projektledarna. Institutionsstyrelsen beslutar om institutionens totalbudget.

---

<sup>11</sup> Ekonomistyrningsverket (ESV) besked vid tidigare förfrågan var att om en middag efter intern kurs/planeringdag har karaktären av en personalfest, ska det bokföras som en personalfest. Lathund för redovisning av representation m.m. vid Stockholms universitet, punkt 3.1.

<sup>12</sup> Ibid, punkt 3.1 max 2 personalfester per år.

<sup>13</sup> Ersättning för dricks i Sverige ges inte enligt SU:s ”Regler för representation och gåvor m.m. vid Stockholms universitet”, dnr SU FV 4642-22

<sup>14</sup> ”Lathund för redovisning av representation m.m. vid Stockholms universitet, punkt 6.1, krav på underlag

<sup>15</sup> Ibid, punkt 6.1, krav på underlag

Institutionens totalbudgetens avvikelse till utfallet har minskat något de senaste två åren, från + 3,4 mnkr till +2,6 mnkr (bättre utfall än budgeterat), vilket innebär bättre överensstämmelse mellan budget och utfallet.

### ***Resultatuppföljning***

IR bedömer att institutionens interna styrning och kontroll avseende resultatuppföljning är tillfredsställande. Ekonomi är en fast punkt i varje institutionsstyrelsemöte, där AC redogör den ekonomiska situationen grundligt tertialvis, förslag till nästa årsbudget är i fokus vid årets sista möte, årsresultat och uppföljning av resultatutveckling sedan år 2019 samt fastställande av nya budgeten i årets första möte. Vid övriga möten tas upp olika aktuella aspekter om ekonomin eller om inget särskilt hänt redogörs kort väl utfallet följer budgeten. Institutionens prognos för 2024 års resultat enligt AC är ett mindre underskott än budgeterat, -4 mnkr istället för -6 mnkr och målet är att uppnå ett plusresultat om ett par år.

Resultatuppföljningen görs tertialvis, på institutionens totalnivå och även för UGA och FUF resultat. Resultat presenteras i SU:s officiella EKUP-format.

### ***Redovisning***

IR bedömer att institutionens interna styrning och kontroll avseende redovisning är bristfällig. Kontogrupp vid redovisning stämmer vanligen, men inom kontogruppen bokförs kostnaden på fel konto, vilket kan indikera att varken kontoplanet eller Ekonomiavdelningens Lathund används vid kontering. Moms var inte alltid kostnadsfört på representation, speciellt vid personalfester, där julbord inte var bokfört som personalfest och därmed inte heller momsens kostnadsfört. Drycker från Systembolaget med utlägg till sommarpersonalfest var inte konterat som personalfest utan som övrig personalkostnad och moms var inte kostnadsfört. Syfte till resan saknas i flera fall. Syftet behöver ibland förtydligas vid representation och resor, institutionen kan använda meddelande-rutan till det för att få mera plats, både i redovisnings-systemet och i Primula. Program till konferens/kurs saknas i många fall.

Förkontroller vid kontering och attest behöver förbättras. Vid kontering använd alltid gällande kontoplan och Ekonomiavdelningens lathund samt SU:s regler för representation och gåvor mm. Ur lathund framgår även vilka underlag som krävs för de olika kostnaderna.

Institutionen har inte haft rutin för efterkontroller, vilka görs för att upptäcka och korrigera kostnader eller intäkter som hamnat på fel konto, fel moms eller komplettera saknade uppgifter. Institutionen behöver försöka skriva så tydliga och beskrivande radtexter som möjligt och därmed underlätta efterkontroller.

Brister	Risker	Sammanfattande bedömning ISK
<b>Budgetering</b>	Ej tillämbart.	Tillfredställande
<b>Resultatuppföljning</b> och information till institutionsledning	Ej tillämbart.	Tillfredställande
<b>Redovisning och kontroller</b> Momsfel vid representation fanns.  Bristande kontroller vid kontering och attest  Rutin för efterkontroll och rättning saknas.	Ingående moms ej kostnadsförs vid representation innebär att universitetet äskar återbetalning av ingående moms som vi inte har rätt till.  Bristande kontroller medför att felbokningar inte upptäcks och rättas.  Kostnader på fel huvudboks konto påverkar redovisning och rapportering samt ger felaktigt underlag för analyser från institutionsnivån upp till SU-nivån.	Bristfälligt
<b>Rekommendationer</b> <ol style="list-style-type: none"> <li>Förbättra kontroller vid kontering och attest av kostnader samt säkra att moms kostnadsförs vid representationskostnader.</li> <li>Inför en rutin för efterkontroller.</li> </ol>		

## 2.2. Riskområde - Anläggningstillgångar och stöldbegärliga förbrukningsinventarier

### 2.2.1. Anläggningstillgångar

Anläggningstillgångar redovisas först som preliminära anläggningar i universitetets anläggningsregister och redovisning. Innan anläggningar kan aktiveras (definitivsättas) behöver institutionen välja anläggningstyp och komplettera med uppgifter som ansvarig, placering, serienummer och övrig information. När anläggningar aktiveras, vilket ska ske när de kan tas i bruk av institutionen, överförs anläggningar automatiskt till rätt tillgångskonto så avskrivningskostnaderna kan starta.

I intervjun framgick det att institutionen inte har några dokumenterade rutiner vid redovisning av anläggningstillgångar då institutionen använder universitetets gemensamma riktlinjer. Uppstår det ett behov av att anskaffa anläggningstillgångar kontaktar medarbetarna

institutionens ekonom med ansvar för anläggningar. Beroende på om institutionen behöver genomföra en upphandling, direktupphandling alternativt ett avrop eller beställning är det administrativ chef, inköpskoordinator eller IT-ansvarig som sköter anskaffningen. När leverantörsfakturer inkommer är det institutionens ekonom med ansvar för anläggningar som bokför fakturorna som pågående anläggningar. Vidare behandlar institutionens ekonom med ansvar för anläggningstillgångar tillgångarna i Raindance genom att registrera uppgifter som ansvarig, placering, serienummer och övrig information samt väljer anläggningstyp. När anläggningen är färdigbehandlad och kan tas i bruk aktiverar (definitivsätter) ekonomen anläggningen. Avseende Institutet för solfysik hanteras anskaffningarna i första hand av Solfysiks personal och institutionens ekonom som sköter leverantörsfakturer tillhörande Solfysik.

Enligt anläggningsregistret den 2024-11-04 har institutionen 144 st anläggningar varav största delen av anläggningarna är helt avskrivna. Under perioden januari – oktober 2024 har institutionen bokfört 11 st fakturer som pågående nyanläggningar. IR:s översiktliga genomgång av krediterade belopp på konto 1271 visar att institutionen skyndsamt aktiverar tillgångar. Vid genomgång av institutionens anläggningsregister har IR noterat att institutionen registrerar uppgifter som underlättar identifieringen.

### 2.2.2. Stöldbärliga förbrukningsinventarier (SFI)

Till skillnad från anläggningstillgångar fördelas inte kostnaderna för SFI under tillgångens nyttjandeperiod utan kostnadsförs i sin helhet vid anskaffningstillfället. Vid anskaffning av nedanstående kategorier via e-handel i Raindance kommer varan per automatik att läsas in i SFI-registret när köpet har beslutsattesterats och definitivsatts.

- dator/tablet/smatphone/storbildsskärm, 0 – 25 000 kr
- AV-utrustning mellan 5 000 – 25 000 kr
- smartphone

Övriga kategorier saknar koppling till registret. Det går också att registrera SFI i registret då inkommande leverantörsfakturer konteras. Anges en SFI-kod i S-kolumnen på konteringsraden kommer SFI att registreras i registret när fakturan är beslutsattesterad och definitivsatt. Gemensamt för tillvägagångssätten är att kompletterande uppgifter som ansvarig, placering, serienummer och övrig information registreras i efterhand av institutionens ekonom med ansvar för anläggningar och SFI.

Likt redovisning av anläggningstillgångar har institutionen inte några dokumenterade rutiner vid redovisning av SFI då institutionen använder universitetets gemensamma riktlinjer. Uppstår det ett behov av att anskaffa en SFI kontaktar medarbetaren ansvarig projektledare för ett muntligt godkännande och därefter kontaktas institutionens inköpskoordinator eller IT-ansvarig som beställer varan i e-handelssystemet. Vid institutionen är det ekonom som hanterar

anläggningar samt SFI:er som är SFI-ansvarig och registrerar uppgifter som ansvarig, placering, serienummer och övrig information i SFI-registret.

Enligt SFI-registret den 2024-11-04 har institutionen 147 st SFI:er. Under perioden januari – oktober 2024 har institutionen bokfört 13 st. anskaffningar på konto 5610 – datorer och mobiltelefoner som har registrerats i SFI-registret. IR:s genomgång av registrerade uppgifter i SFI-registret visar att institutionen registrerar uppgifter som underlättar identifieringen.

Vid entledigande av personal använder institutionen en checklista som behöver signeras av medarbetarna, där medarbetarna bland annat intygar att de återlämnat universitetets utrustning till institutionens IT-ansvarig. Vidare använder institutionens arbetsgrupp för dataskydd programmet ”Asset management-databas” för att kontrollera så medarbetarna återlämnar institutionens tekniska utrustning.

### 2.2.3. Inventering och utrangering

Inventering är en viktig åtgärd för att säkra kontroll över universitetets tillgångar. I intervjun framgick det att institutionen årligen inventerar anläggningstillgångar (ej märkta med anläggnings-ID) och SFI fysiskt, i den mån det är praktiskt möjligt, med undantag för tillgångar som finns i rymden samt i La Palma (Kanarieöarna). Vid genomförandet av 2024 års inventering utsågs två av institutionens ekonomer till inventeringsförrättare. Vidare har institutionen upprättat och signerat ett inventeringsprotokoll som har inlämnats till Ekonomiavdelningen. I samband med intervjutillfället genomförde IR en stickprovsinventering där samtliga tillgångar kunde identifieras.

I intervjun framfördes att institutionen utrangerar anläggningar och SFI efter behov och vid inventeringstillfället. Vidare använder institutionen Ekonomiavdelningens blankett vid utrangering av anläggningstillgångar samt kontaktar Ekonomiavdelningen genom serviceportlen när SFI:er ska utrangeras.

### 2.2.4. Bedömning och rekommendationer

IR:s bedömning av den interna styrningen och kontrollen avseende anläggningstillgångar och SFI är att det finns förbättringsmöjligheter. Granskningen visar att institutionen inte märker anläggningstillgångar med anläggnings-id. IR bedömer att det är lämpligt att institutionen märker de anläggningstillgångar som kan märkas i syfte att underlätta inventeringstillfället men även för att minska personberoendet.

Brister	Risker	Sammanfattande bedömning ISK
Anläggningstillgångar ej märkta med anläggnings-id.	Risk att inventeringstillfället blir ineffektiv och att identifieringen försvåras.	Förbättringsmöjligheter
<b>Rekommendationer</b> 3. Överväg att märka de anläggningstillgångar som kan märkas med ett anläggnings-id.		

### 2.3.Riskområde – Inköp och upphandling

Vid institutionen finns det 35 medarbetare som har beställarbehörighet i Raindance/Marknadsplatsen, vilket innebär att medarbetarna kan registrera beställningar i universitetets e-handels-system. För att registrerade beställningar ska skickas till leverantörer behöver beställningarna attesteras. På institutionen kan prefekt och administrativ chef attestera beställningar. Vidare har institutionen en inköpskoordinator som har genomfört Inköps- och upphandlingssektionen utbildningar ”Certifierad inköpskoordinator – IK1” och ”Kommers eLite Direktupphandling – IK2”.

I intervjun med institutionen framgick det att institutionen inte har egna dokumenterade riktlinjer för inköp och upphandling utan institutionen använder universitetets gemensamma regler för inköp och upphandling. Uppstår det ett behov av att göra ett inköp i verksamheten genomförs detta normalt i universitetets e-handelssystem av inköpskoordinatorn eller IT-ansvarig. Om det inte finns något avtal och inköpet understiger 100 000 kronor vänder sig medarbetarna i första hand till institutionens inköpskoordinator och i andra hand till administrativ chef.

Eftersom universitetet anskaffar varor och tjänster genom beställning, avrop och upphandling har IR granskat hur stor andel av institutionens inköp som sker via avtal. Granskningen avser bokförda leverantörsfakturor i kontogrupp 52xx – 57xx för perioden januari – september 2024. Bokförda fakturor har med hjälp av leverantörernas ID-nummer matchats mot registrerade ID-nummer i leverantörsregistret. I leverantörsregistret finns det registrerade uppgifter om det existerar ett hyresavtal, ett eget ramavtal, ett statligt ramavtal eller om det saknas ett avtal med leverantören. I de fall då det var noterat att det saknas ett avtal eller då det inte fanns några uppgifter registrerade har IR sökt efter leverantören i universitetets avtalskatalog och bland Kammarkollegiets leverantörer på avropa.se.

Granskningen visar att institutionen anskaffar varor och tjänster genom avrop eller beställningar från egna- och statliga ramavtal. Av de granskade leverantörerna saknar dock flera avtal med

universitetet eller med Kammarkollegiet; andelen leverantörer utan avtal uppgår till 44 procent. De totala kostnaderna för anskaffningarna i urvalet uppgår till ca 3,5 mkr.

### 2.3.1. Direktupphandling över 100 000 kronor

I intervjun framgick det att institutionen har anmält en direktupphandling över 100 000 kronor till Inköps- och upphandlingssektionen under perioden januari – november 2024 samt att direktupphandlingen genomfördes under ledning av administrativ chef. Universitetets upphandlingschef har godkänt anskaffningen och institutionen har upprättat ett tilldelningsbeslut samt ingått ett avtal med anbudsgivaren som har undertecknats av prefekt. Vidare har institutionen skickat en upphandlingsrapport till Ekonomiavdelningen samt diariefört underlagen.

### 2.3.2. Bedömning och rekommendationer

IR:s bedömning av den interna styrningen och kontrollen avseende inköp och upphandling är att det finns förbättringsmöjligheter. Granskningen visar att närmare hälften av de leverantörer som institutionen genomför inköp hos saknar avtal med universitetet eller Kammarkollegiet. I ”Regler för inköp och upphandling”<sup>16</sup> anger universitetet följande: *även om det i ett enskilt fall finns förutsättningar för direktupphandling, så är det normalt bättre att planera och konkurrensutsätta anskaffning, eftersom det kan förväntas ge lägre pris och högre kvalitet.* Med anledning av vad som nämns i regelverket bedömer IR att det är viktigt att institutionen arbetar långsiktigt mot att minska andelen inköp utanför ramavtal.

Brister	Risker	Sammanfattande bedömning ISK
Nästan hälften av de leverantörer som institutionen genomför inköp hos saknar avtal.	Risk för bristande följsamhet mot interna inköps- och upphandlingsregler.	Förbättringsmöjligheter
<b>Rekommendationer</b> 4. Vidta åtgärder för att minska andelen inköp hos leverantörer som saknar ramavtal.		

<sup>16</sup> Dnr SU-2.2.1-1679-15 ”Regler för inköp och upphandling” Beslutad av Förvaltningschefen. Beslutsdatum 2017-12-21

## 2.4. Riskområde – Lärarnas bisysslor

Enligt 3 kap. 7§ högskolelagen (1992:1434) har lärare på universitet och högskolor rätt att inneha bisysslor som rör forskning eller utvecklingsarbete inom anställningens ämnesområde, men det finns begränsningar i lagstiftningen. En bisyssla får inte bidra till att lärosätets förtroende skadas och bisysslor ska hållas klart åtskilda från lärarnas arbete. Vidare ställer 4 kap. 15§ i högskoleförordningen (1993:100) krav på att lärarna ska informera lärosätet om bisysslor som har anknytning till anställningens ämnesområde.

För att universitetet ska leva upp till de externa kraven har universitetet tagit fram interna styr- och stöddokument. Regler om redovisningsplikt och var uppgifter om bisyssla ska redovisas återfinns i ”Föreskrifter om bisysslor för anställda vid Stockholms universitet”<sup>17</sup> och i kompendiet ”Information avseende bisysslor vid Stockholms universitet”<sup>18</sup>. I dokumenten framgår att redovisning av bisysslor sker i personalsystemet Primula och att lärare som inte har någon bisyssla årligen ska redovisa detta.

I intervjun med prefekt framgick att institutionen inte har några dokumenterade rutiner gällande lärarnas bisysslor. Vidare har lärarna inte tillgång till någon information om bisysslor på institutionens webbplats eller intranät (confluence). Institutionen har inte rekryterat några lärare de senaste 2–3 åren och har således inte informerat någon nyrekryterad lärare om universitetets regler under perioden. Det förs inga uttryckliga samtal om bisysslor i de årliga utvecklings-samtalen men lärarnas samverkan med omgivningen är föremål för diskussion och då kan bisysslor beröras.

Institutionens prefekt informerar samtliga lärare via mail i början av året att de behöver registrera uppgifter om bisyssla i Primula. Vid något av institutionens ”staff meetings” (institutionsmöte med undervisnings- och forskningspersonal, genomförs var 3:e vecka) på vårterminen påminner prefekten lärarna att registrera uppgifterna. Mot slutet av året tar prefekten fram uppgifter ur Primula för att kontrollera vilka lärare som har registrerat uppgifter om bisysslor eller inte. De lärare som inte har registrerat några uppgifter får ett påminnelse-mail av institutionens prefekt. I påminnelsen uppmanas lärarna att registrera uppgifterna i Primula.

I lärarkategorin<sup>19</sup> vid Stockholms universitet ingår följande befattningar/titlar:

- Professorer (alla typer, som biträdande, adjungerade, gäst, befordrade, kallade m.m.)

<sup>17</sup> Dnr SU FV-1.1.2-0592-16 ”Föreskrifter om bisysslor för anställda vid Stockholms universitet”. Beslutad av Rektor. Beslutsdatum 2016-02-25.

<sup>18</sup> Medarbetarwebben -> Anställd -> Min anställning -> Bisysslor -> Läs mer information om bisysslor.

<sup>19</sup> Lärarpersonalens befattningar/titlar i personalsystemet Primula och enligt Dnr SU FV-1.1.2-0354-20 ”Anställningsordning för anställning som och befordrad till lärare vid Stockholms universitet (AOSU)”. Beslutad av universitetsstyrelsen. Beslutsdatum 2020-02-18.

- Lektorer (alla typer, som universitetslektor, befördrad universitetslektor, biträdande universitetslektor m.m.)
- Adjunkter (alla typer som universitetsadjunkt, adjungerad m.m.)
- Lärare (alla typer som adjungerad, gäst, även timlärare, som dock inte kan anmäla sina bisysslor i Primula)

Enligt ett rapportutdrag från Primula den 2024-09-30 har 35 procent av institutionens lärare registrerat uppgifter om bisyssla. Ett utdrag i Primula den 2024-11-15 visar att drygt hälften av lärarna har registrerat uppgifterna. Vid 2023 års utgång var motsvarande andel 22 procent.

#### 2.4.1. Bedömning och rekommendationer

IR:s bedömning är att den interna styrningen och kontrollen avseende lärarnas bisysslor är bristfällig. När granskningen påbörjades hade merparten av institutionens lärare inte registrerat några uppgifter om bisyssla i Primula. Efter den inledande granskningsperioden ökade andelen lärare som har registrerat uppgifterna till drygt hälften. Trots genomförda informations- och uppföljningsinsatser av prefekt är det ett flertal lärare som inte har registrerat några uppgifter. Granskningen visar även att det saknas ruiner för att informera nyrekryterade lärare om universitetets regler. Vidare kan institutionens löpande information om bisysslor i de återkommande utvecklingssamtalen förtydligas.

Brister	Risker	Sammanfattande bedömning ISK
Institutionen genomför inga informationsinsatser åt nyrekryterade lärare gällande universitetets regler för bisysslor. Det bör nämnas att institutionen inte har rekryterat någon lärare de senaste 2-3 åren.	Risk att institutionen inte uppfyller externa och interna krav.	Bristfällig
Efter granskningens start har nästan hälften av lärarna ännu inte registrerat några uppgifter om bisyssla i Primula.		
<b>Rekommendationer</b> <ol style="list-style-type: none"> <li>5. Säkerställ att lärare som rekryteras till institutionen informeras om universitetets föreskrift och information avseende bisysslor samt att de har förstått reglerna.</li> <li>6. Säkerställ att lärarna löpande (t.ex. i årliga utvecklingssamtal) informeras om sina skyldigheter vid utövandet av bisysslor.</li> </ol>		

## 2.5. Riskområde – Säkerhet

Inom område Säkerhet har Internrevisionen översiktligt granskat fyra delområden: personuppgiftsbehandling, informationssäkerhet, IT-säkerhet och fysisk säkerhet.

### 2.5.1. Personuppgiftsbehandling

När det gäller personuppgiftsbehandlingen saknar institutionen en aktuell registerförteckning. Enligt uppgift upprättades en registerförteckning 2017 med stöd av konsult men den är inte aktuell och behöver göras om. Bland annat bedömer institutionen att de behöver stöd av jurist för att reda ut rättslig grund för personuppgiftsbehandling. Institutionen har inte haft någon kontakt med universitetets dataskyddsbud i frågan om personuppgiftsbehandling förutom att de har erhållit en mall som de efterfrågat och påbörjat använda. GDPR har inte dykt upp som något prefekten i sin roll erhållit information eller fått påstötning om.

Av institutionens genomförda informationsklassning (se vidare nedan under avsnitt om informationssäkerhet), fastställd 2024-05-24, framgår emellertid att registerförteckning GDPR ingår bland informationen som har klassats, tillsammans med utpekade informationsägarskap för registerförteckningen.

Institutionen har inga rutiner som rör personuppgiftsbehandling eller incidentrapportering. Det har inte förekommit att det inkommit frågor om registerutdrag eller radering. Institutionen är medvetna om att personuppgiftsincidenter behöver rapporteras. Det har inte förekommit att det inkommit frågor om registerutdrag eller radering.

När det gäller utbildning inom området nämner institutionen Nimblr-utbildningen (Stockholm University Security Awareness Training) som erbjuds inom Stockholms universitet men den täcker inte så mycket om just GDPR. De anställda förväntas genomföra utbildningsmodulerna men det är oklart hur många av institutionens anställda som tagit del av Nimblrs utbildningsmoduler.<sup>20</sup>

---

<sup>20</sup> Enligt uppgift från IT-avdelningen per 2024-12-05 kan de genom administrationsverktyget se statistik över hur många och vilka användare som har slutfört de moduler som skickats ut. En funktion har nyligen införts som gör det möjligt för varje institution att ha en egen administratör, som kan få tillgång till statistik specifikt för den egna institutionen. I dagsläget är dock användarna inte uppdelade per institution i databasen, vilket beror på att SUKAT inte är kopplat till Nimblrs databas, vilket innebär att användardata måste uppdateras manuellt, vilket uppges vara en tidskrävande process. IT-avdelningen arbetar med en lösning för att förenkla kopplingen vilket skulle göra det enklare att fördela användare per institution och därmed förbättra uppföljningen.

Information om dataskydd ingår inte introduktionen av nyanställda. Prefekten har dock ett veckobrev som skickas till de anställda och där har prefekten tagit upp bl a informationssäkerhet och information om Nimblr.

### 2.5.2. Informationssäkerhet

Regelverket ”MSB21 föreskrifter om statliga myndigheters informationssäkerhet” (MSBFS 2020:6) ställer krav på ett riskbaserat och systematiskt informationssäkerhetsarbete över tid. Enligt regelverken ska universitetets viktiga informationstillgångar, exempelvis forsknings- och utbildningsdata, hanteras på sådant sätt att det går att säkerställa att de skyddas mot obehörig åtkomst, felaktiga förändringar och att de finns tillgängliga då de behövs.

En förutsättning för att kunna bedriva ett ändamålsenligt och effektivt informationssäkerhetsarbete är att viktig information inom institutionen klassificeras av chef eller motsvarande (t.ex. objektsägare/informationsägare) utifrån aspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet. Utifrån denna klassificering ska sedan ändamålsenliga skyddsåtgärder utformas, exempelvis administrativa rutiner, utbildning av medarbetare, brandväggar, behörighetskontroller, skalskydd etc.

Institutionen har genom ESIR-projektet<sup>22</sup> genomfört en informationsklassning. Klassningen omfattar forskningsdata, utbildningsdata samt administrativ data. Internrevisionen har inom ramen för granskningen tagit del av informationsklassningen, och det framgår att klassningen fastställdes 2024-05-24. Av klassningen framgår att institutionens prefekt och administrativ chef är informationsägare för administrativ data; studierektor är informationsägare för utbildningsdata; prefekt är informationsägare för forskningsdata. Klassningen är genomförd tillsammans med institutionens administrativa chef och IT-ansvarig. När det gäller exempelvis administrativ data framgår att institutionens prefekt och administrativa chef huvudsakligen ansvarar för de olika informationstyperna som har klassats.

Merparten av informationen har klassats som nivå 2, dvs ”grundläggande skyddsnivå”. Ett flertal informationstyper har klassats som nivå 3, dvs ”utökad skyddsnivå”. Här återfinns exempelvis studenters tentaskrivningar, beslut om anpassningar för studenter med särskilda behov, klagomål om utpekande händelser och lärare, kris- och katastrofplaner, samt ekonomiska underlag som rör redovisning, budget och prognoser. Få delar har klassats med högsta känslighetsnivå, totalt två informationstyper har klassats i nivå 4, dvs ”hög skyddsnivå”, utifrån konfidentialitet och spårbarhet. Det rör läkarintyg för personal respektive läkarintyg för studenter.

Klassificeringen har inte resulterat i behov av åtgärdslista enligt institutionens bedömning. Läkarintyg erhålls emellanåt från studenter fastän institutionen inte önskar ta emot detta, och

---

<sup>21</sup> Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

<sup>22</sup> ESIR - Etablering av Systematiskt Informationssäkerhetsarbete och Resultatstyrning

enligt klassificeringen så kasseras läkarintyg direkt efter att beslut om åtgärd har tagits. Från institutionens sida upplevs ansvaret rörande informationssäkerhet i delar otydligt, och när det gäller informationsklassningen är det oklart vad som blir nästa steg: förväntas institutionen göra något mer på egen hand eller med hjälp av IT-avdelningen?

Institutionen har ett solteleskop på La Palma, Kanarieöarna. Internrevisionen har tagit del av ifylld checklista för PDA (produkter med dubbla användningsområden) som färdigställdes under 2024 för det solteleskopet. Checklistan är ett hjälpmedel för att avgöra om en produkt eller teknik behöver tillstånd innan export, och även ett sätt att dokumentera SU:s exporthantering. Hanteringen har skett i samverkan med Fastighetsavdelningens ansvarige för exportkontroll.

MBS:s föreskrifter ställer även krav på att utveckla och upprätthålla kompetens hos egen personal avseende informationssäkerhet genom utbildning, informationsinsatser och övning. Institutionen hänvisar till Nimblr, dvs de utbildningsmoduler (Stockholm University Security Awareness Training) som rör olika aspekter av informations- och IT-säkerhet som erbjuds. Utöver detta har ingen specifik utbildning skett för att säkra kompetens inom informations-säkerhet.

### 2.5.3. IT-säkerhet

Vid institutionen finns cirka 25 doktorander, ca 50 anställda lärare/forskare/postdocs, samt 7 T/A-anställda. All administrativ personal har SUA-datorer. Forskare har olika lösningar. De som vill ha Windows har SUA, övriga har andra lösningar som Mac och Linux.

I december 2018 fattade rektor beslutet ”Anslutning till IT-tjänster för ökad säkerhet”<sup>23</sup>. Av beslutet framgår att anslutning till de fyra IT-tjänsterna för ökad säkerhet (inloggningstjänst, skydd mot virus och skadlig kod, inventeringsprogram och avvecklingstjänst) är obligatorisk för samtliga institutioner. Enligt genomförda intervjuer använder institutionen de fyra IT-tjänsterna, dock inte till fullo i alla delar. Alla har inloggningstjänsten och avvecklingstjänsten. Vidare har alla med Windows och MacOS virussydd som administreras centralt via IT-avdelningen; de som har Linux har också installerat virussydd med det hanteras lokalt av institutionen. När det gäller inventeringsprogramvaran finns det på alla datorer med Windows och MacOS, men ej på Linux. Institutionen har efterfrågat detta från IT-avdelningen. Enligt inhämtad uppgift från IT-avdelningen har institutionen cirka 90 datorer med inventeringsprogramvaran.

Institutionen har inga upptäckta dataintrång att rapportera. I förebyggande syfte har antalet inloggningsförsök begränsats. En bärbar dator stals för något år sedan.

När det gäller backup och förmåga att återställa förlorad eller förstörd data har institutionen en egen lösning för lagring med infrastruktur för lokala konton. Säkerhetskopiering av personalens

<sup>23</sup> Dnr: SU FV 2.8.3-0207-17 ”Anslutning till IT-tjänster för ökad säkerhet”. Beslutad av rektor. Beslutsdatum 2018-12-20.

lagring sker varje natt. IT-ansvarige kontrollerar säkerhetskopieringen månatligen. Eget utrymme finns på servern, och kopiorna sparas i en annan brandcell. För att ytterligare öka IT-säkerheten och förmågan att skydda och återställa data överväger institutionen att ordna med en extra backup-server på Frescati. Enligt IT-ansvarige har återställning av data alltid fungerat hittills. Vidare ombeds forskarna separera sin data: det som har skapats och måste bevaras, samt sådant som är möjligt att ladda ned igen. Detta är en viktig fråga för fortsatt utbildning av personalen; det är en belastning att ta hand om eftersom mängden data hela tiden ökar.

Samverkan sker med IT-avdelningen kring flera frågor, ofta genom ärenden i Serviceportalen. Institutionen försöker använda centrala tjänster så mycket det går. Institutionen har tre lokalt anställda som arbetar med IT, vilket kommer av lokala behov utifrån institutionens forskning, utrustning och behov av IT-stöd. En av medarbetarna arbetar bland annat gentemot Solfysik och teleskopet på Kanarieöarna.

Någon IT-utbildning har inte genomförts utöver Nimblr, den pågående universitetsgemensamma Stockholm University Security Awareness Training som erbjuds i flera korta moduler.

#### 2.5.4. Fysisk säkerhet

När det gäller lokala ansvaret före kris har institutionen en upprättad krishanteringsplan som finns både på svenska och engelska. Planen är senast modifierad 2023-10-20, och utgör lokal version av universitetets centrala krisplan. Planen innehåller lokal krisledningsgrupp med personer, ansvar och telefonnummer. Prefekt är säkerhetsansvarig. Övriga roller i planen är kommunikationsansvarig, operativ ledning, protokollförare och skyddsombud. Gruppen har haft gemensam genomgång av krisplanen och även den centrala krisplanen för SU. Krisplanen behandlar olika typer av krissituationer, bland annat olyckor och akut sjukdom, dödsfall, hot och våld samt brand.

Kontaktuppgifter till företagshälsovård finns anslaget utanför prefekt och HR-ansvarigs kontor. Kontaktuppgifter till studenthälsan finns ej anslaget men ska åtgärdas. När det gäller utbildning i första hjälpen/HLR/L-ABC finns en äldre lista men institutionen uppger att detta är ett utvecklingsområde och att fler bör utbildas. Ett problem har varit att utbildning ej erbjuds på engelska.

Institutionen sitter samlokaliserad med KTH i AlbaNova. Institutionen har låsta dörrar till sin korridor men alla i huset har access till korridoren. När det gäller teleskop och datorhallar är åtkomsten begränsad. Tidigare hade institutionen serverutrustning i två rum, men vid tidpunkten för granskningen pågick en flytt för att samla serverutrustningen i ett rum. Förutom institutionen har även Fysikum och KTH access till serverrummet. Vid tidpunkten för granskningen pågick diskussioner vilka som ska ha access till det nya serverrummet.

Institutionen har inte haft något inbrott i nuvarande lokaler under de senaste åren. De intervjuade känner inte heller till att det har riktats några hot mot institutionen eller dess personal under

senare år. Däremot nämndes ett fall av sexuella trakasserier som skett under de senaste åren, vilket tagits upp inom ramen för RALV och personen i fråga har lämnat institutionen.

#### 2.5.5. Status efter granskning av fysisk säkerhet i IT-utrymmen

Under våren granskade internrevisionen den fysiska säkerheten i IT-utrymmen vid universitetet. Granskningen rapporterades till universitetsstyrelsen i 14 juni 2024. Syftet med granskningen var att utvärdera om tillräckliga åtgärder vidtagits för att säkerställa och skydda den fysiska IT-miljön samt att bedöma om detta har gjorts med en betryggande intern styrning och kontroll. Ett flertal IT-utrymmen granskades och Institutionen för astronomi var en av institutionerna som ingick urvalet. Uppdragen från rektor pågår och ska återrapporteras senast 30 juni 2025. Utifrån erhållen information vid granskningstillfället kan bland annat noteras om statusen inom området:

- Informationsklassning har skett.
- Golvbrunnar har täckts.
- Antistatiskt golv är på plats.
- Utrustningen flyttas från två rum till att samlas i ett rum.
- UPS (Uninterruptible Power Supply) är förstärkt.
- Nya kylaggregat och sensorer i rummet.
- Skyltning kvarstår.
- Inget nytt om brandsläckare.
- Ingen förändring kring larm, lås eller tillträde. Diskussion om vilka som ska ha tillträde till nya serverrummet är på gång.
- Ännu ingen panikregel i rummet.
- Ingen sektionering av rummet, men begränsat vilka från KTH som har tillträde. Strukturellt kvarstår dock problemet.

Sammanfattningsvis kan sägas att ett flertal åtgärder redan har vidtagits, samtidigt som det finns åtgärder som kvarstår att hantera.

#### 2.5.6. Bedömning och rekommendationer

IR:s bedömning av området säkerhet är att den interna styrningen och kontrollen har förbättringsmöjligheter. Institutionen saknar registerförteckning för personuppgiftsbehandling, vilket är ett krav sedan många år enligt artikel 30 i GDPR. IR har noterat oklarhet kring ansvar i frågan. När det gäller informationssäkerhet ser IR det som positivt att institutionen har genomfört en klassning av forskningsdata, utbildningsdata och administrativ data. Några åtgärder är inte vidtagna efter klassningen. IR noterar att det råder oklarhet om ansvar och fortsättning i arbetet med informationssäkerhet efter genomförd klassning. IR ser ett behov av systematik samt tydligare information och utbildning inom informationssäkerhet. Inom området IT-

säkerhet sker regelbunden backup av institutionens data. IR bedömer det som positivt att institutionen därigenom uppger att de har god förmåga till återställning.

När det gäller den fysiska säkerheten kan IR notera att krisplan och lokal organisation med ansvar finns på plats. IR bedömer att tydliggörande i genomgång och säkrande av det lokala ansvaret före kris kan ske enligt föreliggande krisplan. Säkerhetsaspekterna med KTH:s access till lokaler, som uppmärksammats i temagranskning av fysisk säkerhet i IT-utrymmen, kvarstår. IR noterat att arbete pågår med att åtgärda rekommendationerna från temagranskningen. Vid tidpunkten för granskningen hade redan ett flertal åtgärder vidtagits, samtidigt som det kvar åtgärder att hantera.

Brister	Risker	Sammanfattande bedömning ISK
Register över personuppgiftsbehandling saknas.	Risk att institutionen ej lever upp till krav i om aktuell registerförteckning (artikel 30 i dataskyddsförordningen, GDPR).	Bristfälligt
Systematik och ansvarsfördelning för att säkerställa ett systematiskt informations-säkerhetsarbete.	Risk att institutionens systematiska informationssäkerhetsarbete inte kan ske på ett effektivt och/eller ändamålsenligt.	
Medarbetares kompetensutveckling i säkerhetsfrågor behöver säkras.	Risk att samtliga delar av SU:s krisplan inte följs om all personal inte har kunskap om vad som gäller och förväntas.	
Brister kring fysisk säkerhet i IT-utrymmen har tidigare konstaterats. Åtgärdsarbete pågår och en del brister kvarstår.	Risk att skydd och drift av IT-utrymmen inte lever upp till krav/standards.	
<p><b>Rekommendationer</b></p> <ol style="list-style-type: none"> <li>7. Säkerställ att institutionen tar fram en aktuell registerförteckning innehållande de processer som innebär behandling av personuppgifter.</li> <li>8. Klargör, i samarbete med IT-avdelningen, nästa steg i arbetet med informationssäkerhet.</li> <li>9. Säkerställ kompetensutveckling av de medarbetare som hanterar viktig/känslig information i sitt arbete i enlighet med MSB:s föreskrifter, samt generellt för säkerhetsfrågor.</li> <li>10. Fortsätt arbetet med att åtgärda brister i den fysiska säkerheten i IT-utrymmen.</li> </ol>		

## 2.6. Riskområde - Tentafusk

Disciplinära åtgärder regleras i 10 kap. högskoleförordningen (1993:100) och i 10 kap. 1§ framgår bland annat att ”disciplinära åtgärder får vidtas mot studenter som med otillåtna hjälpmedel eller på annat sätt försöker vilseleda vid prov eller när en studieprestation annars ska bedömas”.

Enligt ”Regler och handlägningsordning för disciplinärenden”<sup>24</sup> är det institutionen som utreder och bedömer om det föreligger misstanke om disciplinär förseelse och Rektors kansli (Rättssekretariatet) eller Disciplinnämnden som avgör i ärendet. För att minimera fusk vid examinationer är institutionens förebyggande arbete centralt. En viktig åtgärd är att tidigt informera studenter om vad som gäller på universitetet, vilket även lyfts fram i det universitetsgemensamma styrdokumentet.

På institutionen är det studierektor tillika utredningsansvarig som utreder misstänkta disciplinärenden och sammanställer underlagen som skickas till Rektors kansli för slutligt avgörande. Visar institutionens utredning att det inte föreligger någon grundad misstanke om försök till vilseledande vid examinationstillfället skickas inte ärendet till Rektors kansli.

I intervjun med utredningsansvarig framgick det att studenterna informeras av institutionen om vad som gäller vid fusk och plagiat. Studenterna får muntlig och skriftlig information om institutionens etiska riktlinjer vid uppropstillfället för nya studenter. Vidare behöver studenterna skriftligt intyga att de har tagit del av information och har förstått innehållet i riktlinjerna. I de etiska riktlinjerna från 2024-06-05 framgår bland annat institutionens regler för salsexaminationer och riktlinjerna vid hemexaminationer samt riktlinjer vid användning av generativ AI<sup>25</sup>. Institutionen redogör även sin syn på fusk och plagiat samt informerar studenterna att alla misstankar om fusk ska rapportera till prefekt eller studierektor och att incidenter utreds och skickas till rektor om misstanken kvarstår.

Via institutionens webbplats kan studenterna också ta del av universitetets gemensamma information om fusk och plagiat samt universitetets handlägningsordning för disciplinärenden. Vidare informerar ansvariga kursexaminatorer studenterna om hur examinationer ska genomföras och lämnar skriftliga beskrivningar av examinationsuppgifterna i kurshandlingar/kursbeskrivningar som finns tillgängliga i läroplattformen Athena.

För att upptäcka plagiat använder institutionen textjämförelseverktyget Urkund i Athena. I institutionens etiska riktlinjer anges att ansvarig lärare bör ge tydliga instruktioner till studenterna avseende den förväntade graden på självständighet i arbetet. På institutionen är det upp till ansvarig lärare att avgöra om Urkund ska aktiveras eller inte och hur resultatet kan

---

<sup>24</sup> Dnr SU FV-4242-21 ”Regler och handlägningsordning för disciplinärenden”. Beslutad av rektor. Beslutsdatum 2022-02-10.

<sup>25</sup> Exempelvis OpenAI:s applikation ChatGPT.

tolkas. Institutionen tillämpar ingen särskild nivå på utfall i Urkund som föranleder att misstänkta ärenden överlämnas till utredningsansvarig. Det förs inga kollegiala samtal om vad som är att betrakta som objektiv grund vid misstanke om fusk på institutionen.

Vid salsexaminationer hos institutionen finns det tentamensvakter som övervakar examinationen. Institutionen använder egna lokaler och har egna tentamensvakter (civila personer utanför universitetet). Om tentamensvakten misstänker att en student fuskar vid examinationen upprättas en skriftlig rapport som överlämnas till ansvarig lärare. Enligt uppgift är det ovanligt med misstänkta fuskärenden på institutionen. Institutionen har endast haft ett fuskärende (plagiat) de senaste två åren som har skickats till Rektors kansli för slutligt avgörande.

### 2.6.1. Bedömning och rekommendationer

IR:s bedömning av den interna styrningen och kontrollen avseende tentafusk är att det finns förbättringsmöjligheter. Granskningen visar att institutionens inte för några samtal om vad som är att betrakta som objektiv grund vid misstanke om fusk. IR anser att det är värdefullt med hänsyn till likabehandling av studenter, framför allt vid misstanke om plagiat. Vidare anser IR att det är positivt att institutionen har upprättat etiska riktlinjer, där det framgår vad som är tillåtet eller inte vid användning av AI.

Brister	Risker	Sammanfattande bedömning ISK
Institutionen för inga formella diskussioner avseende objektiv grund vid användning av textjämförelseverktyg.	Risk för bristande likabehandling.	Förbättringsmöjlighet
<p><b>Rekommendationer</b></p> <p>11. Överväg att föra återkommande kollegiala samtal om vad som är att betrakta som objektiv grund vid användning av textjämförelseverktyg.</p>		



## Yttrande över internrevisionens granskning av IT-säkerhet

### Internrevisionens granskning

Internrevisionen har under 2024 granskat IT-säkerheten vid Stockholms universitet. Det övergripande syftet med granskningen har varit att utvärdera huruvida universitetets styrning och kontroll är tillräcklig gällande IT-säkerhet.

Bedömningen är att Stockholms universitets arbete med IT-säkerhet är *otillfredsställande* och innehåller allvarliga brister som behöver åtgärdas.

Internrevisionens iakttagelser och rekommendationer från granskningarna sammanfattas i rapporten "Granskning av IT-säkerhet" (dnr SU FV-0495-24, daterad februari 2025). Rapporten är ställd till universitetsstyrelsen och ger en övergripande bild av utfört granskningsarbete och resultat.

### Internrevisionens rekommendationer

Flera förbättringsområden i den interna styrningen och kontrollen har identifierats och åtgärder bör vidtas för att reducera risknivån rörande den fysiska säkerheten i IT-utrymmen. Med anledning av granskningsresultatet rekommenderar internrevisionen följande:

1. Åtgärda tekniska avvikelser.
2. Åtgärda bristfälliga mjukvaruuppdateringar.
3. Åtgärda bristfälliga säkerhetsinställningar och konfigureringar.
4. Specificera kravställning på IT-säkerhet och inför arbetssätt för att följa upp efterlevnad av kraven.
5. Stärk det operativa IT-säkerhetsarbetet.

### Rektors kansli

## Rektors yttrande

Rektors yttrande över rapporten, som avges i samråd med universitetsdirektören, följer nedan.

Internrevisionens iakttagelser och slutsatser bedöms i allt väsentligt vara befogade. Rektor konstaterar att det är av största vikt att universitetet har en god IT-säkerhet. Rektor ser därför mycket allvarligt på de påtalade bristerna och konstaterar att ambitionsnivån behöver höjas ytterligare samt att ett flertal åtgärder behöver vidtas.

Grundprincipen för arbetet är att de allvarligaste bristerna ska prioriteras och åtgärdas först, men i några fall kan det finnas anledning att göra åtgärder i en särskild ordning för att nyttja resurserna på bästa sätt. Kritiska sårbarheter som identifierats i granskningen ska dock åtgärdas omgående. Det antecknas att identifierade sårbarheter avser både universitetsgemensamma system och programvaror, och system och programvaror som hanteras av lokala IT-ansvariga vid institutioner. Samtliga kritiska sårbarheter rör dock lokal IT.

### ***1. Internrevisionen rekommenderar:***

Universitetet rekommenderas att åtgärda tekniska avvikelser.

### ***Rektors yttrande:***

Rektor noterar att det finns brister och sårbarheter i universitetets hantering av tekniska system som angripare skulle kunna dra nytta av för att skaffa sig obehörig åtkomst, stjäla och sprida information och data eller orsaka skada i universitetets IT-miljö. För att skapa ett robust system som förebygger att angripare får tillgång till universitetets uppgifter ska avvikelserna åtgärdas och de avvikelser som har högst risknivå ska prioriteras och hanteras skyndsamt. Avvikelser ska bedömas utifrån risknivå och i förhållande till den övergripande planen (se punkt 5 nedan) för att säkerställa att mer allvarliga brister hanteras först. Detta innebär att tekniska avvikelser med låg risknivå kan komma att prioriteras ned till förmån för mer allvarliga brister om sådana uppdagas.

**Åtgärder:** Rektor avser att i samråd med dekaner och vicerektorer besluta att de tekniska avvikelserna ska åtgärdas, och att avvikelser med hög risknivå ska hanteras skyndsamt. Rektor avser att uppdra till universitetsdirektören att åtgärda tekniska avvikelser relaterade till universitetsgemensamma system. Därutöver avser rektor att uppdra till universitetsdirektören att tillse att IT-ansvariga för lokal IT-system som berörs av avvikelser informeras om att dessa ska åtgärdas, samt att följa upp att det genomförs.

## **2. Internrevisionen rekommenderar:**

Universitetet rekommenderas åtgärda bristfälliga mjukvaruuppdateringar.

### **Rektors yttrande:**

Rektor noterar att flertalet föråldrade mjukvarufunktioner identifierades under de tekniska testerna. Universitetet ska inventera sina programvaror för infrastrukturer regelbundet, och se över möjligheten att göra det lätt att göra rätt genom att införa automatisk uppdatering där det är möjligt.

Målsättningen är att regelbundna sårbarhetsskanningar på sikt ska genomföras vid lärosätet. Förutsättningarna för det kommer ses över inom ramen för arbetet med att ta fram den övergripande planen (se punkt 5 nedan).

**Åtgärder:** Rektor avser att uppdra till universitetsdirektören att säkerställa att programvaror för universitetsgemensam infrastruktur är uppdaterade, och framöver uppdateras regelbundet. Där så är möjligt ska automatisk uppdatering införas. Därutöver avser rektor att uppdra till dekanerna att säkerställa att samtliga institutioner och centrumbildningar är medvetna om sitt ansvar att uppdatera programvaror för lokal infrastruktur utifrån ett informationssäkerhetsperspektiv.

Rektor avser att uppdra till universitetsdirektören att utreda förutsättningarna för att genomföra regelbundna sårbarhetsskanningar vid lärosätet.

## **3. Internrevisionen rekommenderar:**

Universitetet rekommenderas att åtgärda bristfälliga säkerhetsinställningar och konfigurationer.

### **Rektors yttrande:**

Rektor noterar att flertalet avvikelser är relaterade till bristfälliga konfigurationer och inställningar inom externt exponerad infrastruktur. Det finns ett behov av att ta fram universitetsövergripande regelverk avseende vilka principer och rutiner som gäller för konfiguration av all externt exponerad infrastruktur vid lärosätet. Förslag på process för att säkerställa att inställningar är korrekt konfigurerade planeras tas fram inom den övergripande planen (se punkt 5 nedan).

**Åtgärder:** Rektor avser att uppdra till universitetsdirektören att åtgärda de noterade bristfälliga säkerhetsinställningarna och konfigurationerna i universitetsgemensamt externt exponerad infrastruktur samt att ta fram förslag på process för att säkerställa att inställningar är korrekt konfigurerade.

#### **4. Internrevisionen rekommenderar:**

Universitetet rekommenderas att specificera kravställning på IT-säkerhet och införa arbetssätt för att följa upp efterlevnad av kraven.

#### **Rektors yttrande:**

För att säkerställa att lärosätet har en enhetlig och adekvat IT-säkerhet behövs kravställningar tas fram och ansvar för uppföljning konkretiseras. Ett kompletterande styrdokument till informationssäkerhetspolicyn i form av en handläggningsordning för IT-säkerhet har därför tagits fram. Det nya styrdokumentet, *Handläggningsordning för ansvarsfördelning och vägledning avseende säkerhetsåtgärder i informationssystem vid Stockholms universitet*, dnr SU FV-1582-25, fastställdes av rektor den 16 april 2025. Handläggningsordningen förtydligar den övergripande ansvarsfördelningen som framgår från informationssäkerhetspolicyn och reglerar formerna för arbetet avseende säkerhetsåtgärder i IT-system. Där framgår att IT-säkerhetsansvaret följer det delegerade verksamhetsansvaret, så att chefer för verksamhet också ansvarar för införande av de IT-säkerhetsåtgärder som krävs för att skydda information och informationssystem, vilket är konsekvent med det övergripande ansvaret för informationssäkerhet som framgår i informationssäkerhetspolicyn.

**Åtgärder:** Ett nytt styrdokument, *Handläggningsordning för ansvarsfördelning och vägledning avseende säkerhetsåtgärder i informationssystem vid Stockholms universitet*, har fastställts som förtydligar ansvaret för IT-säkerhet och uppföljning. Rektor bedömer därmed att rekommendationen har hanterats.

#### **5. Internrevisionen rekommenderar:**

Universitetet rekommenderas stärka det operativa IT-säkerhetsarbetet.

#### **Rektors yttrande:**

Med utgångspunkt i sitt uppdrag arbetar universitetet löpande med att förbättra IT-säkerhetsarbetet. Universitetets verksamhet bygger i hög grad på öppenhet och samverkan, och verksamhetens natur kan ställa särskilda krav på lärosätets IT, såsom exempelvis att det inom enskilda forskningsprojekt kan finnas behov av att köpa in och utveckla IT för ett särskilt ändamål, så kallad forsknings-IT. Det förändrade säkerhetsläget, både nationellt och internationellt, ställer vidare nya krav på universitetets arbete med säkerhetsfrågor.

De senaste åren har flera beslut fattats om både tillfälliga och permanenta förstärkningar till IT- och informationssäkerhet. Samtidigt har personalomsättning inom området orsakat fördröjningar av planerade åtgärder. En tillsvidareanställd informationssäkerhetschef är nyligen rekryterad och en stabil bemanning är nu på plats inom administrativ informationssäkerhet. Det är nu prioriterat att tillsätta



vakanser inom IT-säkerhetsområdet och stärka kapaciteten för det operativa säkerhetsstödet inklusive stöd till institutionerna i deras arbete. Mot bakgrund av att ambitionsnivån behöver höjas ytterligare avseende det operativa IT-säkerhetsarbetet samtidigt som hotbilden inte väntas minska i närtid kan det vara motiverat med ytterligare förstärkning till IT-avdelningen. Behov av och möjlighet till en permanent förstärkning ska därför ses över inför beslut om fördelning av anslagsmedel för 2026.

En plan ska tas fram i syfte att långsiktigt höja nivån på IT-säkerhetsarbetet och säkerställa en god IT-säkerhetsmiljö.

**Åtgärder:** Rektor avser att uppdra till universitetsdirektören att ta fram en plan i syfte att långsiktigt höja nivån på IT-säkerhetsarbetet och säkerställa en god IT-säkerhetsmiljö, vilket inkluderar att stärka det operativa IT-säkerhetsarbetet.

***Rektors yttrande, övrigt:***

Rektor konstaterar vidare att det i akuta situationer kan uppstå behov av omedelbara åtgärder från lärosätets sida, exempelvis vid en pågående IT-incident eller cyberattack. I sådana fall kan det vara avgörande att snabbt begränsa nätverksåtkomst för att förhindra spridning eller obehörig åtkomst till andra delar av verksamheten. För att kunna upprätthålla en hög nivå av informationssäkerhet i dessa situationer kan det därför vara nödvändigt att en person inom universitetsförvaltningen ges ett utökat mandat att agera, oberoende av om det rör universitetsgemensam IT, lokal IT eller forskningsrelaterad IT.

**Åtgärder:** Rektor avser att uppdra till universitetsdirektören att ta fram förslag på justering av delegationsordningen för att tillse att en lämplig person vid universitetsförvaltningen, exempelvis informationssäkerhetschefen, har mandat att besluta om akuta åtgärder för att upprätthålla informationssäkerheten vid lärosätet.

Samtliga uppdrag ska återrapporteras till universitetsstyrelsen i april 2026. Styrelsen ska löpande hållas uppdaterad kring arbetet.



## **Stockholms universitet**

Rapport: Granskning av IT-säkerhet  
Februari 2025

SU FV-0495-24

## Sammanfattning

EY har på uppdrag av internrevisionen vid Stockholms universitet granskat hur väl universitetets information hanteras i tekniska system. Granskningens syfte är att utvärdera huruvida Stockholms universitets styrning och kontroll är tillräcklig gällande IT-säkerhet. Granskningen omfattar teknisk säkerhetsnivå samt styrning, med huvudsaklig fokus på den tekniska aspekten.

Granskningen har utförts genom två tekniska tester, dels en sårbarhetsanalys av externt exponerad infrastruktur och dels ett tekniskt penetrationstest av behörighetsplattformen SUKAT som används av Stockholms universitet. Därutöver har intervjuer genomförts med nyckelpersoner inom verksamheten för att ge en bedömning på hur IT-säkerhetsarbetet bedrivs centralt.

Den samlade bedömningen är att Stockholms universitets arbete med IT-säkerhet är otillfredsställande och innehåller allvarliga brister som behöver åtgärdas. Bristande IT-säkerhet ökar risken att värdefull forskning eller andra informationstillgångar går förlorade.

De tekniska testerna har resulterat i allvarliga avvikelser som visar på kritiska sårbarheter i universitetets IT-miljö. Universitetets testresultat är svagt i jämförelse med vad EY vanligtvis observerar för svenska myndigheter. Därtill har avvikelser noterats i den övergripande IT-styrningen. Under granskningen har konstaterats att det inom organisationen finns en medvetenhet om att förbättring behövs inom området. Brister i både tekniska tester och övergripande IT-styrning har legat till grund för denna gransknings rekommendationer.

Granskningen har utmynnat i följande rekommendationer:

1. Åtgärda tekniska avvikelser.
2. Åtgärda bristfälliga mjukvaruuppdateringar.
3. Åtgärda bristfälliga säkerhetsinställningar och konfigureringar.
4. Specificera kravställning på IT-säkerhet och inför arbetssätt för att följa upp efterlevnad av kraven.
5. Stärk det operativa IT-säkerhetsarbetet.

EY har därtill lämnat detaljerade rekommendationer kopplat till åtgärder för samtliga identifierade avvikelser. Dessa återfinns i en teknisk underlagsrapport. Detaljerade resultat från granskningen och tillhörande tester redovisas inte i denna översiktliga och öppna revisionsrapport utan i en separat underlagsrapport som delats med IT-avdelningen och behandlas konfidentiellt.

## Innehållsförteckning

<b>Sammanfattning</b> .....	2
<b>1. Inledning</b> .....	4
1.1 Bakgrund .....	4
1.2 Syfte .....	4
1.3 Avgränsning .....	4
1.4 Metod och genomförande .....	4
1.5 Behörighetssystemet SUKAT .....	5
<b>2. Granskningsresultat</b> .....	6
2.1 Styrning IT-säkerhet .....	6
2.1.1 Iakttagelser .....	6
2.1.2 Bedömning .....	7
2.2 Tekniskt penetrationstest av behörighetsplattformen SUKAT .....	7
2.2.1 Iakttagelser .....	7
2.2.2 Bedömning .....	8
2.3 Sårbarhetsskanning av externt exponerad IT-infrastruktur .....	8
2.3.1 Iakttagelser .....	8
2.3.2 Bedömning .....	8
<b>3. Rekommendationer</b> .....	9
Akuta tekniska sårbarheter som bör hanteras omedelbart .....	9
3.1 Åtgärda tekniska avvikelser .....	9
3.2 Åtgärda bristfälliga mjukvaruuppdateringar .....	9
3.3 Åtgärda bristfälliga säkerhetsinställningar och konfigurationer .....	9
Rekommendationer avseende styrning och arbetssätt för att stärka IT-säkerhetsarbetet på sikt ....	9
3.4 Specificera kravställning på IT-säkerhet och införa arbetssätt för att följa upp efterlevnad av krav	9
3.5 Stärk det operativa IT-säkerhetsarbetet .....	10
<b>Bilaga 1: Intervjuade funktioner</b> .....	11
<b>Bilaga 2: Dokumentförteckning</b> .....	12
<b>Bilaga 3: Definitioner</b> .....	13

# 1. Inledning

## 1.1 Bakgrund

Den ständigt föränderliga hotbilden inom IT-området kräver ett proaktivt och dynamiskt säkerhetsarbete. För att möta dessa hot återfinns ett uppdrag i regeringens regleringsbrev för lärosäten 2024 att redogöra för hur framtidens behov och risker ska hanteras.

IT-säkerhet är av yttersta vikt för lärosäten på grund av den unika och känsliga information som hanteras inom dessa institutioner. Universitet har stora mängder data som genereras och lagras, inklusive forskningsresultat, samt personuppgifter om studenter och anställda. Denna information är inte bara värdefull för akademiska ändamål utan kan också vara måltavla för cyberattacker och dataintrång. Ett intrång kan leda till allvarliga konsekvenser, såsom förlust av intellektuell egendom och skada på universitetets rykte. Därför är robust IT-säkerhet avgörande för att skydda information och säkerställa oavbruten verksamhet samt förtroende från alla inblandade parter.

Universitetets IT-miljö skiljer sig från många andra verksamheter genom att den inkluderar både universitetsförvaltning och två vetenskapsområden innehållande ett flertal institutioner. Denna struktur medför att institutioner och forskare ofta själva ansvarar för inköp eller utveckling av IT-utrustning för sina specifika syften. Detta är en central del i universitetsverksamhet för att främja forskning och innovation, men kan medföra vissa utmaningar i att säkerställa god IT-säkerhet.

Tidigare granskningar vid Stockholms universitet har identifierat att säkerheten kan förbättras. Av nämnda anledningar har EY fått i uppdrag av internrevisionen på Stockholms universitet att utföra en IT-säkerhetsgranskning.

## 1.2 Syfte

Granskningens syfte är att utvärdera huruvida Stockholms universitets styrning och kontroll är tillräcklig gällande IT-säkerhet. Granskningen omfattar teknisk säkerhetsnivå samt styrning, med huvudsaklig fokus på den tekniska aspekten.

## 1.3 Avgränsning

Granskningen avgränsas till vissa IT-system och IT-miljöer, i syfte att ge en djupare förståelse av dessa. Denna granskning ger alltså inte en helhetsbild av universitetets totala arbete inom IT- och informationssäkerhet utan syftar till att ge en detaljerad bild över ett begränsat område. Intervjuer har utförts med deltagare från den centralt styrda IT-avdelningen, därmed har perspektivet från lokal- eller forsknings-IT ej inkluderats i rapporten.

Därtill har EYs IP-adress som använts för sårbarhetsskanningen vitlistats av universitetet. EY har således inte testat brandväggens tekniska skydd.

## 1.4 Metod och genomförande

Uppdraget omfattar internrevisionsgranskning enligt god internrevisionsstandard av Stockholms universitets IT-miljö utifrån ett IT-säkerhetsperspektiv och omfattar följande delar:

- ▶ Granskning av styrning inom IT-säkerhet
- ▶ Teknisk sårbarhetsanalys av externt exponerad infrastruktur
- ▶ Tekniskt penetrationstest av behörighetsplattformen SUKAT

Granskningen av styrning inom IT-säkerhet utfördes genom intervjuer med nyckelpersoner inom IT-avdelningen, samt granskning av styrdokument och övrigt relevant material inom ämnet.

För genomförandet av den tekniska sårbarhetsanalysen har EY mottagit IP-adresser som bedömts relevanta av universitetet. IP-adresser utöver dessa utvalda har inte ingått i analysen.

Tekniska penetrationstest kan genomföras med olika nivåer av ingångsinformation. Om en testare genomför ett penetrationstest med full förståelse för IT-miljön kallas detta för ett *white-box test*. Om ett penetrationstest i stället genomförs utan någon som helst kunskap eller förståelse för den specifika IT-miljön kallas detta för ett *black-box test*. Då denna granskning undersöker vad en angripare kan genomföra under ett intrångsförsök efter att ha kommit över vissa användaruppgifter från universitetets medarbetare genomfördes det tekniska penetrationstestet på behörighetsplattformen SUKAT med mottagna kontouppgifter för en student och en anställd. Penetrationstestet genomfördes därmed med viss kännedom och information om systemet och är därmed en kombination av ett white-box och ett black-box test, ett så kallat *gray-box penetrationstest*.

Resultatet av granskningen sammanställs i denna rapport i form av övergripande iakttagelser inom IT-säkerhetsområdet hos Stockholms universitet och rekommendationer på vad som bör förbättras. Samtliga avvikelser som iaktogs under de två tekniska testerna har bedömts utefter låg-, medium-, hög- eller kritisk risknivå. En teknisk underlagsrapport har delats med IT-avdelningen.

Tabell 1: Förklaring för de olika risknivåer för identifierade avvikelser

Riskenivå	Förklaring
Kritisk	Denna risknivå indikerar att säkerhetskontroller är så svaga att det finns en kritisk risk för universitetet som måste åtgärdas omedelbart.
Hög	Denna risknivå indikerar att det finns allvarliga svagheter i säkerhetskontrollerna och att det finns en allvarlig risk för universitetet som måste åtgärdas så snart som möjligt.
Medium	Denna risknivå indikerar att det finns svagheter i säkerhetskontrollerna som kan leda till en hög risk ifall de lämnas obevakade och bör åtgärdas utanför normala patch-cykler.
Låg	Denna risknivå indikerar att även om det finns svagheter i säkerhetskontrollerna är dessa av begränsad betydelse och kan åtgärdas under den normala livscykelhanteringen.

## 1.5 Behörighetssystemet SUKAT

SUKAT är Stockholms universitets centrala behörighetssystem. Det är en katalogtjänst som innehåller information om anställda och studenter. Tillgång till flertalet av universitetets tjänster sker via SUKAT där användare får tillgång till tjänsterna via Single-Sign-On (SSO). SUKAT i sig innehåller inte känslig information, men via autentisering får användare tillgång till tjänster som innehåller känslig information.

## 2. Granskningsresultat

### 2.1 Styrning IT-säkerhet

God styrning inom IT-säkerhet är avgörande för att säkerställa att säkerhetsåtgärder är välkoordinerade och effektivt implementerade. Genom att etablera tydliga riktlinjer och ansvarsområden kan Stockholms universitet skapa en god säkerhetskultur och rätt förutsättningar för att bedriva ett effektivt arbete inom IT-säkerhet.

#### 2.1.1 Iakttagelser

IT-avdelningen inom Stockholms universitet har ett övergripande ansvar för universitetets IT, vilket innefattar informations- och IT-säkerhet. IT-avdelningen är organiserade inom universitetsförvaltningen och ansvarar för att utveckla, förvalta, drifta och övervaka plattformar som stödjer forskare, lärare, studenter och verksamhetsstödet. Den leds av IT-chef som rapporterar direkt till universitetsdirektören.

Universitetet har en decentraliserad IT-organisation där IT-avdelningen ansvarar för det centrala IT-stödet, därtill så förekommer fristående IT i hos institutioner på universitetet. Enligt intervjuade nyckelpersoner på IT-avdelningen så finns det tre huvudsakliga kategorier av IT på universitetet:

1. IT-avdelningen. Den centralt styrda IT som ansvarar för informations- och IT-säkerhet, och service, support, utveckling och förvaltning för universitetsgemensam IT och infrastruktur.
2. Lokal IT. Institutioner som har egen IT-avdelning där institutionerna själva ansvarar för informations- och IT-säkerhet, support, drift och förvaltning.
3. Forsknings-IT. Detta innefattar IT som köpts in och utvecklats för enskilda forskningsprojekt.

Intervjuade nyckelpersoner på IT-avdelningen uppger att de har en varierad grad av insyn till den IT som faller utanför centralt styrd IT. I lokala IT har de begränsad insyn, och nästintill obefintlig insyn i forsknings-IT. Detta innebär att IT-avdelningen har begränsad insyn i huruvida det bedrivs ändamålsenligt IT-säkerhetsarbete för lokal- och forsknings-IT. *Informationssäkerhetspolicy*n vid Stockholms universitet omfattar all information som universitetet äger, hanterar eller bedriver forskning på. Det har under granskningen framkommit att det finns ett pågående arbete med att ta fram ytterligare riktlinjer gällande IT-säkerhet. Denna är vid tidpunkt för granskningen inte färdigställd och har därför inte ingått i granskning och bedömning.

I *Informationssäkerhetspolicy* beskrivs att det yttersta ansvaret för IT-säkerhet åligger rektorn och följer verksamhetsansvaret enligt universitetets besluts- och delegationsordning. Därtill nämns att informationssäkerhetschefen ansvarar för att driva, samordna och stödja universitetets arbete med informationssäkerhet. Inom IT-avdelningen är det AIITS (Arkitektur, Information- och IT-säkerhet) som arbetar övergripande med IT-säkerhet på universitetet. Enligt intervjuade nyckelpersoner har AIITS en roll som kravställare inom IT-säkerhet, samt rådgivare till institutionerna för deras arbete med IT-säkerhet. Arbetet inom informationssäkerhet är, enligt *Informationssäkerhetspolicy*n, baserat på lagar, förordningar och föreskrifter såsom MSB:s föreskrifter för informations- och IT-säkerhet (MSBFS 2020:6 och 2020:7).

Under intervjuer har det framkommit att det operativa arbetet med att säkerställa att kraven inom IT-säkerhet uppfylls saknas. Detta innebär bland annat att det inte utförs egna penetrationstester av

system, handlingsplaner och verkställande av de kravställningar som styr universitetets arbete med IT-säkerhet. I övrigt kan noteras att en av universitetets högst rankade risker enligt riskanalysen, *SU riskanalys 2023-2024*, handlar om informationssäkerhet (*risk att bristande informationssäkerhet leder till att viktig information går förlorad*), men åtgärder för att hantera risken har ej fullt ut vidtagits.

### 2.1.2 Bedömning

Vid intervjuer av nyckelpersoner inom IT-avdelningen så har den bristande insynen i lokal och enskild IT varit ett problem som nämnts frekvent. Den IT som hanteras av institutionerna och forskare omfattas av *Informationssäkerhetspolicyn*. Eftersom den bedrivs lokalt begränsas IT-avdelningens möjlighet och mandat i att säkerställa ett tillräckligt säkerhetsarbete samt efterlevnad av kravställningar, såsom *informationssäkerhetspolicy* och MSB:s föreskrifter om säkerhetsåtgärder i informationssystem. EY bedömer att detta försvårar IT-avdelningens arbete i att upprätthålla en enhetlig strategi för IT-säkerhet och därmed kan försvaga universitetets totala IT-säkerhet och öka risken för cyberattacker och dataintrång. Det är också viktigt att betona att forsknings-IT bör vara tekniskt isolerad från universitetets centrala nätverk. Det är nödvändigt att forskare ska kunna bedriva forskning med och på olika typer av teknik, men det måste separeras från universitetets övriga IT-miljö. Detta är nödvändigt för att skydda hela universitetets IT-infrastruktur från potentiella intrång och för att underlätta hanteringen och åtgärdandet av säkerhetsincidenter.

AIITS, som är en del av IT-avdelningen, har en roll som kravställare och rådgivare för den institutions- och forsknings-IT som bedrivs på universitetet. Intervjuade nyckelpersoner uppger att denna funktion som rådgivare inte alltid utnyttjas som den bör, och därmed har de inte möjlighet att säkerställa att den IT som bedrivs på universitetet upplever krav som är ställda på IT-säkerhet. Utan specialiserad personal riskerar universitetet att inte kunna identifiera och hantera säkerhetshot i tid, vilket kan leda till dataintrång, förlust av känslig information, och skada till universitetets rykte. För att säkerställa en robust IT-säkerhet är det avgörande att ha dedikerade resurser som kontinuerligt arbetar med att implementera och övervaka säkerhetsåtgärder.

## 2.2 Tekniskt penetrationstest av behörighetsplattformen SUKAT

Det tekniska penetrationstestet av behörighetsplattformen SUKAT syftade i huvudsak till att identifiera säkerhetsbrister i SUKAT webbapplikation för att avgöra om en angripare kan få obehörig åtkomst med hjälp av funktionaliteten och komma åt känslig information.

### 2.2.1 Iakttagelser

Totalt noterades 8 avvikelser, varav ingen bedöms som kritisk. Av de avvikelser som observerades bedöms 2 emellertid medföra en hög risk, 3 bedöms medföra en medelhög risk och 3 bedöms medföra en låg risk. De högre rankade riskerna omfattar främst säkerhetsinställningar som skapar sårbarheter i systemet, varav de medel- och lågrankade riskerna innefattar säkerhetsinställningar och andra inställningar som kan förbättras.

Detaljerade redogörelser för samtliga avvikelser har förmedlats till IT-avdelningen i en teknisk underlagsrapport.

### 2.2.2 Bedömning

Baserat på de avvikelser som har observerats bedömer EY att sårbarheter i SUKAT skulle kunna utnyttjas av en angripare som vill komma åt den funktionen eller data som åtkomst till SUKAT skulle ge tillgång till. Det tekniska penetrationstestet påvisar att det finns brister i autentiserings-metoder, föråldrade mjukvaruversioner, samt brister i vissa systeminställningar. Dessa sårbarheter skulle kunna utnyttjas av angripare som i värsta fall skulle kunna få obehörig åtkomst till systemet, stjäla data eller orsaka skada på IT-infrastruktur. Stockholms universitet bör gå igenom resultaten för att diskutera åtgärder för att minska de identifierade riskerna kopplat till identifierade avvikelser.

## 2.3 Sårbarhetsskanning av externt exponerad IT-infrastruktur

Sårbarhetsskanningen av Stockholms universitet externt exponerade IT-infrastruktur syftade i huvudsak till att identifiera säkerhetsbrister och sårbarheter som kan leda till säkerhetsincidenter.

### 2.3.1 Iakttagelser

Totalt observerades 22 avvikelser, varav 4 bedöms som kritiska. Av de övriga avvikelser som observerades bedöms 4 medföra en hög risk, 9 bedöms medföra en medelhög risk och 5 bedöms medföra en låg risk. De kritiska riskerna avser bristande inställningar för autentisering i delar av miljön samt föråldrade versioner av mjukvara i IT-miljön. Dessa avvikelser skulle kunna utnyttjas av angripare för att få tillgång till information som exempelvis kan spridas eller användas för vidare intrång.

Detaljerade redogörelser för samtliga avvikelser har förmedlats till IT-avdelningen i en teknisk underlagsrapport.

### 2.3.2 Bedömning

Baserat på de noterade avvikelserna bedömer EY att universitetets externt exponerade infrastruktur har flertalet mycket allvarliga brister som kan underlätta för en angripare att få tillgång till IT-miljön. EY bedömer att universitetets testresultat är svagt jämfört med vad som vanligtvis observeras för svenska myndigheter.

Noterade avvikelser kan tillåta anonyma användare att logga på servern och ladda upp filer, skriva in illvilliga filer till serverns diskar, och infektera servern med skadlig programvara. Detta kan i sin tur leda till att angripare får tillgång till känslig information vilket kan leda till förlust av data, rättsliga konsekvenser och skada till universitetets rykte.

Andra noterade avvikelser avser föråldrade versioner av mjukvara i IT-miljön. Det innebär att en angripare kan använda kända sårbarheter, vilket kan leda till att tillgängligheten, riktigheten och konfidentialiteten i information och data som förvaras på servrar äventyras. Därtill bör nämnas att den information som exponeras av servern gör det enklare för angripare att kartlägga den teknik som används i IT-miljön och angripa dess svagheter.

Dessa sårbarheter skulle kunna utnyttjas av angripare som i värsta fall skulle kunna få obehörig åtkomst till systemet, stjäla data eller orsaka skada på IT-infrastruktur. Då flera kritiska avvikelser identifierade, och flera avvikelser av hög- och medium risknivå, rekommenderar EY att Stockholms universitet bör gå igenom resultaten för att omgående vidta åtgärder.

### **3. Rekommendationer**

Nedan beskrivs övergripande rekommendationer, vilka har delats upp i två kategorier. EY rekommenderar även att de ansvariga för IT-driften som tar del av de detaljerade rekommendationerna som återfinns i den tekniska underlagsrapporten skyndsamt åtgärdar bristerna.

#### **Akuta tekniska sårbarheter som bör hanteras omedelbart**

##### **3.1 Åtgärda tekniska avvikelser**

De genomförda tekniska testerna resulterade i totalt sett 30 avvikelser vilket visar att det finns allvarliga brister i universitetets hantering av tekniska system. Avvikelser med högre risknivå visar att det finns brister och sårbarheter en angripare skulle kunna dra nytta av för att skaffa sig obehörig åtkomst, stjäla och sprida information och data eller orsaka skada i universitetets IT-miljö.

Därmed rekommenderar EY Stockholms universitet att säkerställa att samtliga avvikelser åtgärdas och att de avvikelser med högst risknivå prioriteras.

##### **3.2 Åtgärda bristfälliga mjukvaruuppdateringar**

Flertalet föråldrade mjukvaruversioner identifierades under de tekniska testerna. Enligt MSB 2020:7 föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (4kap. 12§) ska offentliga verksamheter upprätta interna regler för att upprätthålla säkerhet i mjukvara. EY rekommenderar därmed att universitetet genomför en inventering av de programvaror som används, samt deras versioner. Därtill rekommenderar EY att införa automatisk uppdatering där det är möjligt, samt införa rutiner för regelbundna oberoende sårbarhets skanningar för att minska risken för utnyttjanden av dessa brister i IT-miljön.

##### **3.3 Åtgärda bristfälliga säkerhetsinställningar och konfigurationer**

Flertalet avvikelser noterade i de tekniska testerna är relaterade till bristfälliga konfigurationer och inställningar. Enligt kontrollerna 8.9 och 8.27 i ISO 27002:2022 bör det upprättas principer för hur system bör konfigureras. Därmed rekommenderar EY att universitetet inför en process för att säkerställa att inställningar är konfigurerade korrekt, för att säkerställa att exponerad infrastruktur endast har funktionalitet aktiverad som krävs för kärnfunktionaliteten.

#### **Rekommendationer avseende styrning och arbetssätt för att stärka IT-säkerhetsarbetet på sikt**

##### **3.4 Specificera kravställning på IT-säkerhet och införa arbetssätt för att följa upp efterlevnad av krav**

EY rekommenderar att universitetet, specificerar och tydliggör kravställning på IT-säkerhet som omfattar all IT oavsett om den driftas centralt, lokalt eller enskilt. Detta innefattar den centrala universitets-IT som sköts av IT-avdelningen, fristående IT som driftas av institutioner, samt forsknings-IT som införskaffats för forskningsprojekt. Därutöver bör arbetssätt införas som innebär

att efterlevnad av krav följs upp. För den IT som inte lever upp till kraven bör luckorna åtgärdas inom en given tidsram, annars bör det ställas krav på att utrustningen kopplas bort från universitetets nät.

### **3.5 Stärk det operativa IT-säkerhetsarbetet**

EY rekommenderar att Stockholms universitet bedriver mer operativt arbete inom IT-säkerhet. Detta arbete bör innefatta säkerställande av efterlevnad av kravställningar, utförande av regelbundna penetrationstester, utveckling av handlingsplaner och införande av säkerhetsövervakning som bedrivs av IT-avdelningen för universitetets IT.

## **Bilaga 1: Intervjuade funktioner**

- ▶ IT-chef
- ▶ Chef IT-Produktion
- ▶ Systemtekniker
- ▶ Delportföljsamordnare för infrastruktur
- ▶ Sektionschef för IT-kompetens
- ▶ IT-säkerhetsspecialist

## Bilaga 2: Dokumentförteckning

- ▶ Ansvarsförbindelse systemadministratörer.pdf
  - ▶ Digitaliseringsplan 2024-2026 (RF 240208).pdf
  - ▶ Färdplan 2024 Infrastruktur & Dataplattform.pptx
  - ▶ Föreskrift för användning av information och informationshanterande resurser.pdf
  - ▶ Informations säkerhetspolicy.pdf
  - ▶ Om IT-avdelningen.pdf
  - ▶ Policy för grön IT.pdf
  - ▶ Policy för portföljstyrning.pdf
  - ▶ SU Organisation.png
  - ▶ Säkerhetspolicy vid Stockholms Universitet.pdf
  - ▶ SU riskanalys 2023-2024
- 
- ▶ MSBFS 2020:7 föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter
  - ▶ ISO/IEC 27002:2022

## Bilaga 3: Definitioner

**IT-infrastruktur:** IT-infrastruktur är de komponenter inom en organisation som tillsammans används för att producera, hantera, beräkna, hämta och lagra data. Exempel på detta kan vara en databas eller olika servrar.

**Sårbarhetsskanning:** En sårbarhetsskanning är en revision av en IT-miljö för att upptäcka sårbarheter som en angripare kan utnyttja.

**Tekniskt penetrationstest:** Ett tekniskt penetrationstest innebär att en aktör under kontrollerade former gör intrång i ett system. Detta kan genomföras på olika sätt och med olika nivåer av ingångslägen. Tekniska penetrationstest brukar delas upp i tre olika nivåer; White-box, Black-box och Gray-box testning.

**White-box testning:** En aktör genomför ett tekniskt penetrationstest med full initial förståelse för den IT-miljö som testas.

**Black-box testning:** En aktör genomför ett tekniskt penetrationstest utan någon initial information kring den IT-miljö som testas.

**Gray-box testning:** En aktör genomför ett tekniskt penetrationstest med viss information kring den IT-miljö som testas, exempelvis genom att ha tillgång till konton.

**Single-Sign-On (SSO):** är en autentiseringsteknik som gör det möjligt för en användare att logga in en gång och få tillgång till flera applikationer utan att behöva logga in igen för varje enskild applikation.