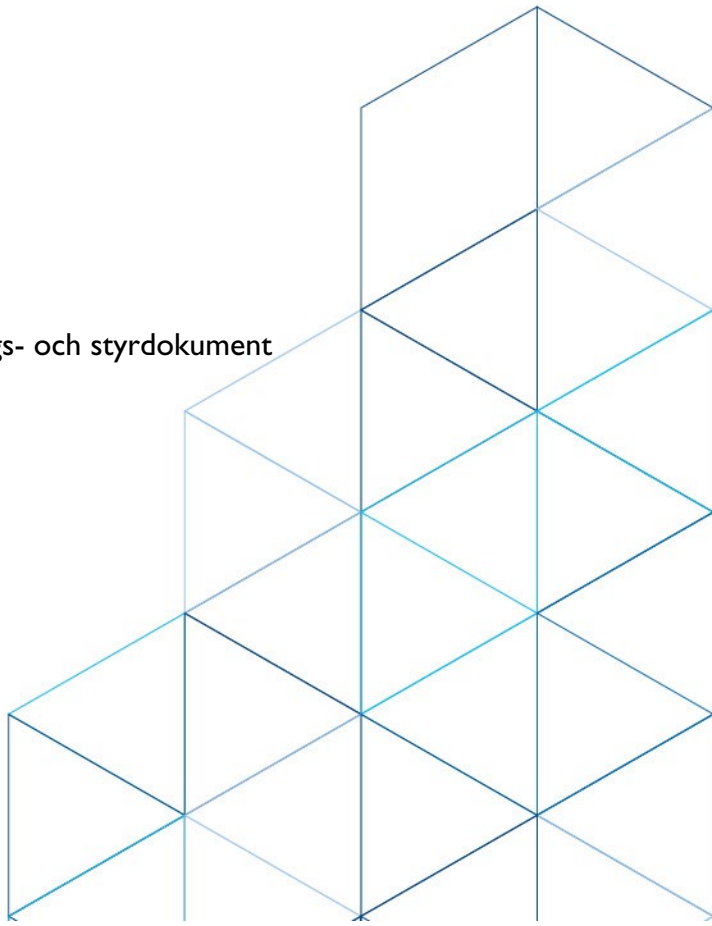
HÖGSKOLAN I HALMSTAD

System för samlad risk- och sårbarhetsbedömning

Dnr:	L 2025/156
Dokumenttyp:	Återkommande planerings- och styrdokument
Beslutsfattare:	Catarina Coquand
Beslutsdatum:	2025-12-15
Ansvarig avdelning:	Fastighetsavdelningen
Dokumentansvarig:	Rikard Ahlgren



Syfte

I en samlad risk- och sårberhetsbedömningen beskrivs de risker som rör omständigheter i form av förhållanden eller händelser som negativt kan påverka ledningens ansvar för verksamheten. Väsentliga risker är sådana som om de inträffar medför att myndigheten behöver informera regeringen om konsekvenserna, antingen i årsredovisningen eller genom annan återrapportering.

Syftet med detta dokument är att beskriva Högskolan systematik för att identifiera och värdera risker och sårbarheter.

Bakgrund

Det finns ett antal förordningar och föreskrifter som reglerar att riskbedömningar måste göras. Två av dem, Förordning (1995:1300) om myndigheters riskhantering och Förordning (2007:603) om intern styrning och kontroll, ser sig som överordnade de andra förordningarna i det avseende att de kräver en samlad riskanalys för hela myndigheten.

Det finns visst överlapp mellan A Säkerhetsrisker och B Risker inom intern styrning och kontroll, främst avseende korruption, otillbörlig påverkan, bedrägeri och andra oegentligheter samt inom ansvarsfull internationalisering.

Metod

För att hantera en samlad risk- och sårberhetsbedömning utifrån dessa perspektiv delas riskerna in i två riskområden:

A Säkerhetsrisker

- A1 IT- och informationssäkerhet
- A2 Fysisk säkerhet
- A3 Personalsäkerhet

B Risker inom intern styrning och kontroll

- B1 Risker för Högskolans förmåga att nå mål, fullgöra sina uppgifter och uppfylla verksamhetskraven.
- B2 Finansiella risker
- B3 Risker för korruption, otillbörlig påverkan, bedrägeri och andra oegentligheter

Risker och sårbarheter identifieras i Högskolans löpande riskhanteringsarbete och genom gruppdiskussioner med ledningsfunktioner, som leds av och sammanställs av säkerhetsansvarig, IT-chef, IT- och informationssäkerhetsstrateg, respektive planeringschef och ekonomichef enligt följande:

A Säkerhetsrisker

Högskolan identifierar i det systematiska säkerhetsarbetet säkerhetsrisker och sårbarheter, genom exempelvis arbetet med informationssäkerhetsklassning, säkerhetsskyddsanalys inkl exportkontroll, produkter med dubbla användningsområden och Kammarkollegiets verksamhetsanalys. Det övergripande systematiska säkerhetsarbetet hanteras av fastighets- respektive IT-avdelningen och sker

i samverkan med verksamhetsstödets avdelningar, Högskolans bolag och akademiledningarna för att få deras perspektiv på säkerhets och sårbarhetsrisker i sin verksamhet. Dessa möten genomför IT-chef, IT- och informationssäkerhetsstrateg, säkerhetsansvarig och säkerhetssamordnaren.

B Risker inom intern styrning och kontroll

I Högskolans verksamhetsplanering- och uppföljning samt kvalitetssäkringsarbete i Hypergene identifierar akademierna och verksamhetsstödets avdelningar risker och sårbarheter inom intern styrning och kontroll. Utifrån det som identifieras i Hypergene genomför planeringschef och ekonomichef en gemensam diskussion med akademicontrollers respektive en grupp ut verksamhetsstödets ledning för att få akademiernas respektive verksamhetsstödets perspektiv på risker inom interna styrning och kontroll.

Urval och värdering av väsentliga risker

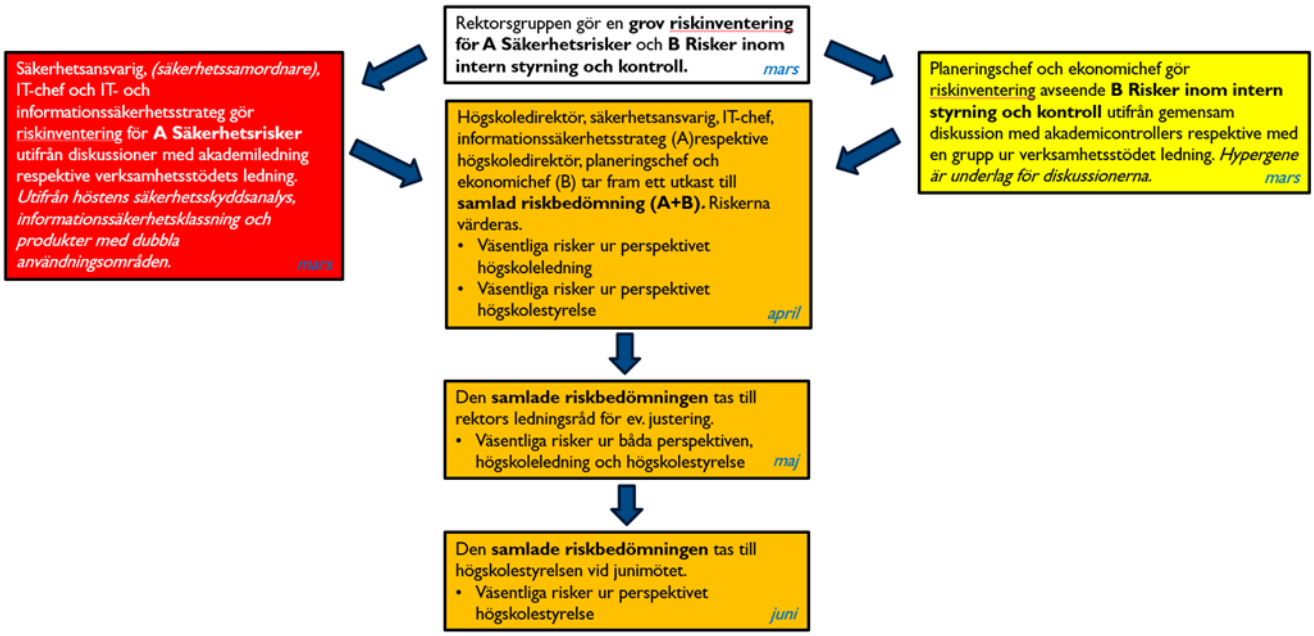
Med underlag från det löpande riskhanteringsarbetet tas en grov risk- och sårberhetsinvertering fram i rektorsgruppen. Utifrån det underlaget tas ett utkast till samlad riskbedömning fram och riskerna värderas. Utkastet till samlad riskbedömning tas upp i rektors ledningsråd för eventuell justering. Högskolestyrelsen fastställer årligen Högskolans samlade riskbedömning vid junimötet.

Utifrån sammanställningarna av diskussionerna i rektorsgruppen, gör högskoledirektör, säkerhetsansvarig, IT-chef, IT- och informationssäkerhetsstrateg, planeringschef och ekonomichef ett utkast till samlad riskbedömning med och värderar dem väsentliga riskerna. Ett första urval med väsentliga risker som högskoleledningen behöver informeras om tas till rektors ledningsråd. Utifrån ledningsrådets diskussion görs sedan ett urval av väsentliga risker som Högskolans styrelse behöver informeras om, genom Högskolans samlade riskbedömning. Riskbedömningen beskriver respektive risk och värdet för riskens sannolikhet och verksamhetskonsekvens.

Riskerna värderas i tre nivåer:

- Högt riskvärde – Röd – Risken ska hanteras så långt det är möjligt och följas upp
- Medelhögt riskvärde – Gul – Risken bör hanteras och följas upp
- Lågt riskvärde – Grön – Risken bevakas och kan eventuellt hanteras inom den ordinarie verksamheten

Processbild – samlad riskbedömning för hela Högskolan



Begrepp och förtydligande inom respektive riskområde

Säkerhetsrisker:

- **IT- och informationssäkerhet** handlar om att skydda information från olika typer av hot och risker för att säkerställa dess konfidentialitet, integritet och tillgänglighet.
- **Fysisk säkerhet** innebär åtgärder för att förebygga skadlig inverkan på och att obehöriga får tillträde till områden, byggnader eller specifika lokaler de kan få tillgång till säkerhetsskyddade uppgifter eller där säkerhetskänslig verksamhet i övrigt bedrivs.
- **Personalsäkerhet** innebär att förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i säkerhetskänslig verksamhet samt säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd.

Statlig intern styrning och kontroll:

- **Intern styrning och kontroll (inom statlig förvaltning)** innebär den process som med rimlig säkerhet säkerställer att en myndighet fullgör sina uppgifter och når verksamhetens mål.
- **Risk i verksamheten (inom statlig intern styrning och kontroll)** innebär en omständighet (förhållande eller händelse) som innebär att en myndighet (mer rimlig säkerhet) inte fullgör sina uppgifter eller når verksamhetens mål.
- **Riskanalys (inom statlig intern styrning och kontroll)** innebär samordnade aktiviteter för att identifiera händelser som utgör ett hot, värdera dessa och välja om och hur dessa ska hanteras.