Diarienummer SLU.ua.2013.1.1.1-4833

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Internrevisionen

Intern styrning och kontroll inom SLU – läge och rekommendationer

Rapport från internrevisionen

Fastställd av SLU:s styrelsen 18 december 2013

Innehåll

SLU
Box 7070, SE-750 07 Uppsala, Sweden
Org.nr 202100-2817

tel: +46 (0)76-7671625

Inga.astorsdotter@slu.se

Sammanfattning

Internrevisionen har granskat den interna styrningen och kontrollen inom SLU. Därvid har konstaterats att universitetets arbete med intern styrning och kontroll uppfyller de förordningsmässiga krav som finns. Se vidare avsnitt 4.

Utöver detta har granskningen innefattat frågan om arbetet kan förbättras och göras effektivare. Resultatet har blivit tio punkter/aspekter med utrymme för förbättringar.

1. Integrera rikskhanteringen i universitetets årscykel för planering och uppföljning.
2. Alla de tre organisatoriska nivåerna inom SLU bör delta i arbetet med den interna styrningen och kontrollen.
3. SLU bör försäkra sig om att kärnverksamheten i SLU, dvs. utbildningen, forskningen och miljöanalysen, är synlig i de riskanalyser som arbetas fram av universitetet.
4. SLU bör försäkra sig om att förtroenderiskerna i verksamheten blir ordentligt behandlade i riskanalysarbetet.
5. Arbetsmetoderna för att ta fram och åtgärda risker bör preciseras.
6. Utförligare analyser och beskrivningar av riskerna ger en bättre grund för den efterkommande riskvärdebedömningen och prioriteringen av risker.
7. Whistleblower-funktionen och behovet av att rapportera allvarliga störningar via de normala kontaktvägarna bör klargöras inom SLU.
8. Det bör göras åtskillnad mellan brister och risker i riskanalysarbetet.
9. För att säkra ett effektivt arbete för en god intern styrning och kontroll bör enhetliga begrepp och arbetssätt användas inom hela SLU.
10. Olika riskperspektiv med delvis olika former för riskhantering bör samordnas med arbetet med intern styrning och kontroll.

De olika förslagen förklaras närmare i avsnitt 5.

Utöver dessa förbättringsmöjligheter för den interna styrningen och kontrollen finns möjligheter att utvidga arbetet till företags- eller organisationsövergripande riskhantering. Det gäller särskilt den forskningsanknutna och konkurrensutsatta verksamheten inom SLU. Här framförs rekommendationer i tre punkter:

11. SLU bör pröva att utvidga riskanalysarbetet så att de framtagna riskbilderna även påverkar de mål som sätts för verksamheten.
12. Risker från olika riskperspektiv bör vägas samman i den företagsövergripande riskhanteringen.
13. SLU bör arbeta med frågor om tolererade risker (den s.k. riskaptiten) i den företagsövergripande riskhanteringen.

Dessa tre förslag förklaras i avsnitt 6.

Uppdraget

Internrevisionen har fått i uppdrag att granska den interna styrningen och kontrollen vid Sveriges Lantbruksuniversitet (SLU). Enheten har låtit mig, Torbjörn Wikland, som projektanställd genomföra granskningen. Beskrivningen av granskningsuppdraget framgår av revisionsplanen 2013:

> *”Sedan 2008 ska SLU enligt förordningen (2007:603) om intern styrning och kontroll (FISK) analysera, åtgärda, följa upp och dokumentera de risker som verksamheten är utsatt för på vägen mot att uppnå önskat resultat. Enligt myndighetsförordningen (2007:515) är det styrelsens ansvar att säkerställa att arbetet i enlighet med FISK fungerar på ett betryggande sätt. Styrelsen ska även i samband med fastställande av SLU:s årsredovisning lämna en bedömning av om den interna styrningen och kontrollen är betryggande.*
> *Efter första året avlämnade Riksrevisionen en rapport till ett antal lärosäten bland annat SLU, angående brister i följsamhet mot regelverket. Därefter har arbetet kontinuerligt förbättrats och Riksrevisionen har inte haft några invändningar inom detta område.*
> *Även om förbättringar skett bedömer internrevisionen att det finns potential för att förbättra och effektivisera arbetet med ISK, samt att bättre integrera processen i den ordinarie verksamhetsstyrningen.*
>
> *Internrevisionen avser att granska universitetets arbete med intern styrning och kontroll för att säkerställa att processen är ändamålenlig och effektiv och att den därmed ökar möjligheten för SLU att nå uppställda mål, bedriva effektiv verksamhet och följa gällande regelverk.”*

Granskningens omfattning och inriktning

Jag har i denna rapport beskrivit resultatet av min granskning först utifrån de myndighetskrav som ställs enligt gällande regelverk (främst FISK och myndighetsförordningen, se avsnitt 1 ovan), sedan utifrån de krav och önskemål på arbetet som kan ställas utifrån SLU: s eget styrningsperspektiv. Den senare aspekten kan också uttryckas som den egna nyttan för SLU med den interna styrningen och kontrollen. Det är samtidigt en fråga om universitetet därmed på ett bättre sätt kan nå uppställda mål och en i övrigt effektivare verksamhet.

Slutligen tillförs ytterligare en aspekt på frågan om SLU: s egen nytta med detta arbete. SLU kan etablera en fortsättning på arbetet med den interna styrningen och kontrollen. Det handlar om att göra en djupare och mer övergripande riskhantering som ett stöd i SLU: s strategiska arbete, särskilt i dess konkurrensutsatta verksamhet. Det handlar främst om vilka risker SLU *bör* ta för att nå strategiska mål och om riskerna ger uppslag till *en justering av målen* så att möjligheterna ökar att målen verkligen uppnås.

Denna granskningsrapport inleds med att lyfta fram några karaktäristiska drag i SLU: s verksamhet och organisationsform som är av betydelse för den interna styrningen och kontrollen. Därefter beskrivs gjorda iakttagelser med åtföljande rekommendationer.

Granskningen har genomförts genom dokumentstudier och intervjuer på olika nivåer i organisationen inkl. ledningen för SLU. Avsikten har varit att försöka belysa frågor och aspekter som rör granskningsområdet inom alla delar av SLU: s verksamhet.

Om karaktären på SLU: s verksamhet och organisation

Det finns tydliga och väl kända rekommendationer om vad intern styrning och kontroll är i generella termer. Det innefattar också hur den bör byggas upp och fungera både för organisationer i allmänhet och för svenska myndigheter.[1] Tillämpningen av dessa rekommendationer måste dock alltid anpassas till den specifika organisation som är berörd. Varje organisation har en egen styrprocess och verksamhet med egna särdrag. För att få rätt ansats i analysen av SLU: s arbete för en god intern styrning och kontroll försöker jag identifiera några drag som skiljer ut SLU från andra statliga myndigheter och andra organisationer. Dessa drag är dock här mycket översiktligt beskrivna.

SLU kan beskrivas på flera olika sätt:

- *Som en statlig myndighet.* Universitetet bedriver således anslagsfinansierad verksamhet med skattemedel hämtade ur statsbudgeten, utgör en del av staten som juridisk person och har en ledning som direkt ansvarar inför regeringen. Det är grunden för att universitetet måste följa regeringens förordning om intern styrning och kontroll.
- *Som lärosäte för universitetsutbildning.* SLU är en utbildningsorganisation med akademisk inriktning och tydlig tonvikt på lant- och skogsbrukets och djurskötselns behov av utbildningar. Även med dessa särdrag styrs och bedöms SLU som vilken annat universitet med akademisk utbildning som helst såväl inom som utom Sverige. Det innebär således att de specifika kraven på olika utbildningar kan vara en ren SLU-fråga men också delas med den övriga universitetsvärlden.
- *Som en forskningsorganisation.* Inom SLU bedrivs en omfattande forskning. Den finansieras genom anslag tilldelade av riksdag och regering men framför allt medel tillhandahållna av externa finansiärer. Även om forskningen bedrivs i en offentlig miljö och inom ramen av en myndighet, bedrivs den utifrån en vetenskaplig tradition med unika prestationer som resultat och som till stor del är bestämda inom berörda institutioner. Ett sätt att beskriva detta särdrag är att säga att SLU, liksom andra forskningsbedrivande institutioner, tillhandahåller en arena för forskare att åstadkomma individuella prestationer, dvs. unika prestationer med mycket höga kvalitetskrav. Själva arenan, universitetsmiljön med dess institutioner, forskningsledare, rekrytering av forskare m.m. blir avgörande om resultatet i form av god forskning kan realiseras. Detta är mycket långt från de standardiserade tjänster som stora delar av statsförvaltningen och många företag producerar.

[1] Den viktigaste allmänna rekommendationen utgår från COSO: s ramverk för intern styrning och kontroll. Det är utifrån den rekommendationen som krav på intern styrning och kontroll skapats inom t.ex. EU: s egna förvaltningar och svenska myndigheter i förordningen om intern styrning och kontroll. Se vidare bilaga 1.

- *Som en konkurrensutsatt organisation*. Sedan länge finns tydliga inslag av konkurrens om studenter och forskningsmedel med övriga högskole- och forskningsinstitutioner i Sverige. Det finns dessutom en allt starkare konkurrens med utländska universitet och kamp om forskningsmedel på den internationella arenan. Här finns tydliga skillnader jämfört med de allra flesta andra svenska myndigheter. Det finns skäl att anta att detta särdrag kommer att förstärkas framöver. Det innebär också att ett stort ansvar läggs på SLU: s ledning att klara av att styra verksamheten så att den blir framgångsrik i denna konkurrens.

Sammantaget kan konstateras att de mest utpräglade särdragen för SLU vid en genomgång av dess interna styrning och kontroll är dels dess roll som forskningsorganisation, dels dess drag av en konkurrensutsatt organisation. I denna granskning har dessa drag uppmärksammats särskilt.

Den interna styrningen och kontrollen utifrån de förordningsmässiga kraven

1.1 Förordningskraven

Det är tre förordningar som behandlar och berör frågor om intern styrning och kontroll i statliga myndigheter. Det är framför allt *förordningen för intern styrning och kontroll* (FISK). Dess krav har sin utgångspunkt i *myndighetsförordningen*. I *förordningen om årsredovisning* finns dessutom kravet formulerat om ett uttalande från myndighetsledningen om den interna styrningen och kontrollen. Kärnan i regeringens förordningskrav handlar om att myndighetsledningen ska redovisa de viktigaste riskerna för att mål och krav inte kan nås och redovisa de åtgärder man vidtagit eller tänker vidta för att hantera och reducera riskerna. Kraven handlar således egentligen inte om att uppvisa en felfri intern styrning och kontroll. Det ”normala” bland myndigheter är snarare att redovisa risker. Utifrån Riksrevisionens granskningar och påpekanden inom området kan man dra slutsatsen att den allvarligaste bristen för en myndighet i detta sammanhang kan vara att inte redovisa iakttagna risker[2]. I övrigt ska myndigheten kunna visa att man har en genomtänkt process för den interna styrningen och kontrollen i myndigheten. Det gäller således utöver kravet att dokumentera de viktigaste riskerna och redovisa att man hanterar redovisade risker.

1.2 Iakttagelser

Det finns en fastställd och tydlig process för SLU: s arbete i denna fråga från fakultetsnivån upp till styrelsen och som avslutas med ett uttalande av myndighetsledningen, dvs. styrelsen, i anslutning till årsredovisningen. Den beslutade processen har dessutom nyligen uppdaterats och förbättrats (”Riktlinjer för intern styrning och kontroll vid SLU 2012-10-01”). SLU följer även till mycket

[2] SIDA fick oren revisionsberättelse 2009 med hänvisning till att alla risker inte redovisats i samband med årsredovisningen.

stor del de råd ekonomistyrningsverket (ESV) utfärdat om arbetet genom dess utfärdade handledningar. Dess råd är dock inte är tvingande för arbetet med intern styrning och kontroll.

Det allvarligaste problemet inom SLU under senare år har handlat om stora brister i hanteringen av infrastrukturen (nybyggnader m.m.), som riskerar att underminera de ekonomiska ramarna för universitetetet. Det är risker som uppmärksammats av Riksrevisionen och av internrevisionen och som efterhand har åtgärdats eller börjat åtgärdas inom SLU. Alla åtgärder är inte slutförda men hade dessa problem inte börjat hanteras hade troligen konsekvenserna blivit mycket allvarliga. Det finns andra påpekanden om brister och risker från Riksrevisionen som universitetet har hanterat. SLU har under den tid problemen funnits dock redovisat riskerna i sin riskanalys och vidtagit därtill knutna åtgärder.

Mot denna bakgrund och utifrån den granskning som nu gjorts konstaterar jag att SLU uppfyller de förordningskrav som finns på universitetets arbete med intern styrning och kontroll.

Kan bättre resultat nås utifrån SLU: s eget perspektiv?

Även om SLU kan bedömas uppfylla förordningskraven återstår en viktig fråga: Har arbetet en sådan inriktning och form att den på bästa sätt bidrar till att SLU uppnår sina mål? Om således förordningskraven är basen så återstår frågan om arbetet kan göras bättre. Den frågan behandlas i detta avsnitt. Här följer iakttagelser om svagheter och förbättringsmöjligheter. Efter varje iakttagelse följer en rekommendation.

1.3 Arbetet med intern styrning och kontroll inkl. riskhantering hanteras inte fullt ut som en integrerad del av styrprocessen inom SLU

Jämfört med många andra statliga myndigheter har universiteten relativt sent uppfattats som sammanhållna styrande organisationer och därför något senare än andra myndigheter utvecklat väl fungerande gemensamma interna styrprocesser (långsiktsplaner, sammanhållna årsplaner för uppgivna mål och resultat knutna till årsbudgetar, uppföljningsprocesser m.m.). Det kanske kan förklaras av att universiteten har karaktär av arenor för god forskning utförda av forskarlag och forskare (se ovan) och därför inte helt passat in bland övriga statliga myndigheters standardiserade tjänster som grund för styrprocesser, där en tydlig målstyrning knutet till budgetprocessen dominerar. Numer finns emellertid en sammanhållen styrprocess med styrdokument inom alla universitet inkl. SLU.

Vad gäller SLU kan konstateras att processen för intern styrning och kontroll inkl. riskhantering brister i integrationen med universitetets styrprocess. I stället för att i första hand vara en integrerad del av den normala planeringsprocessen har den sitt fokus på ett uttalande om den interna styrningen och kontrollen i samband med årsredovisningen. Det kan försvåra möjligheterna att tillgodogöra sig värdet med

riskhanteringen. Riskanalysen och åtföljande riskåtgärder får sitt mest effektiva uttryck om den direkt knyts till planeringen av verksamheten. Riskåtgärderna utifrån riskanalysen ska sedan knytas till det normala uppföljningsarbetet. Det är i den senare delen av årscykeln som uttalandet om den interna styrningen och kontrollen bör komma in.

När det strategiskt viktiga förändringsarbetet (Framtidens SLU) för bl.a. en mer ändamålsenligt fakultets- och institutionsindelningen presenterades våren 2013 berördes inte betydelsen av en god intern styrning och kontroll. Tillsammans med andra gemensamma stödfunktioner (planering, uppföljning, fastighetsförvaltning m.m.) för hela SLU skulle detta arbete kunna lyftas fram som viktiga faktorer för att SLU ska vara rustad för ett framtida mer konkurrensutsatt läge. Det är ett annat exempel på att arbetet med intern styrning och kontroll inte är tillräckligt integrerat i styrprocessen.

Rekommendation: Integrera rikskhanteringen i universitetets årscykel för planering och styrning

Riskhanteringen knutet till den interna styrningen och kontrollen bör integreras ordentligt i universitetets årscykel för planering och uppföljning för att bli effektiv. Det innebär att den i första hand ska vara en del av planeringsarbetet med dess dokumentkrav och därefter en del av uppföljningsarbetet och dess dokumentkrav. Riskhanteringsarbetet i planeringsfasen bör ske i de tidiga delarna av planeringen så att det kan påverka den egentliga verksamhetsplaneringen. Den närmare utformningen i förhållande till den nuvarande årscykelns tidskrav och dokument är en fråga för SLU: s ledning att lösa.

1.4 Alla tre nivåerna inom universitetet är inte med i arbetet.

Det saknas en viktig komponent i SLU: s ovan nämnda riktlinjer för arbetet med intern styrning och kontroll. Institutionsnivån är inte med bland de ansvariga för det slutliga resultatet av riskarbetet. Det är ändå på den nivån som den egentliga kärnverksamheten bedrivs inom SLU. Erfarenheter från andra organisationer visar entydigt att nyttan av riskhantering och intern styrning och kontroll blir riktigt tydlig när dessa aktiviteter genomsyrar och pågår i hela organisationen, dvs. att arbetet med intern styrning och kontroll inkl. riskhantering inte bara har fokus på den högsta nivån i organisationen utan även blir viktiga aktiviteter från den lägsta till den högsta nivån. För SLU: s del innebär det institutioner, fakulteter, SLU:s verkställande ledning och styrelse. Resultatet av arbetet på såväl institutions- och fakultetsnivå bör leda till egna riskbilder och egna riskåtgärder utöver det man ”skickar vidare” till närmast högre nivå i organisationen. I dagsläget sker visst arbete inom fakulteterna i dessa frågor men på institutionsnivå saknas ett motsvarande arbete även om prefekter deltar i fakulteternas arbete.

Rekommendation: Alla de tre organisatoriska nivåerna inom SLU bör delta i arbetet med den interna styrningen och kontrollen

Institutionsnivån (eller motsvarande inom den lägsta organisatoriska nivån) bör genomföra ett eget arbete kring den interna styrningen och kontrollen. Det arbetet bör sedan integreras med det arbete som idag redan sker på fakultetsnivå och central nivå.

1.5 Kärnverksamheten i SLU, dvs. utbildningen och forskningen, är inte tydligt synlig i de riskanalyser som presenteras av universitet.

Trots att utbildning, forskning och miljöanalys är kärnverksamheten, dvs. det mest utmärkande för verksamheten inom SLU, syns inte detta tydligt i de riskanalyser som tagits fram under senare år. Det kan givetvis vara så att i den samlade riskbilden är sådana risker inte så framträdande. Eftersom riskerna i kärnverksamheten normalt bör vara mycket framträdande finns skäl att i en samlad riskanalys verifiera detta särskilt. Risker i kärnverksamheten kan förväntas vara särskilt framträdande på institutionsnivå och i viss mån på fakultetsnivå. Kan den riskhanteringsprocess, koncentrerad till fakulteter och den centrala administrationen, som finns idag vara en förklaring till att dessa risker inte är mer framträdande? Riskerna kan t.ex. gälla hur man kan eller inte kan bedriva framgångsrik forskning, vilket i sin tur spelar en avgörande roll för andra delar av verksamheten, bl.a. utbildningens attraktivitet. Eftersom forskningens produktion och resultat i så hög grad är koncentrerade till institutioner, enskilda forskarlag och forskare kanske dessa frågor inte kommer fram när det saknas en systematisk riskhanteringsprocess på denna nivå liksom en koppling upp till riskhanteringen för hela SLU.

Rekommendation: SLU bör försäkra sig om att kärnverksamheten i SLU, dvs. utbildningen, forskningen och miljöanalysen, är synlig i de riskanalyser som arbetas fram av universitetet.

Att kärnverksamheten speglas i riskanalyserna och följande åtgärdsförslag kan antagligen åstadkommas på flera sätt. Förutom att i högre grad engagera institutionsnivån i arbetet kan även fördjupade strategiska diskussioner om forskningen och utbildningen bidra till detta. Se därför även rekommendationer under avsnitt 6.

1.6 I de hittills framtagna riskbilderna för SLU är inte förtroenderiskerna framträdande.

För offentliga institutioner, som SLU är ett exempel på, spelar förtroenderisker ofta en mycket stor roll. Ytterst handlar det om att skattefinansierad verksamhet, liksom verksamhet reglerad via politiska styrelseorgan, följs uppmärksamt av allmänheten men även av andra intressenter till verksamheten. Det gäller särskilt när fel eller brister uppdagas. Detta intresse tas om hand av och blir synligt genom massmedias omfattande bevakning av den offentliga sektorn. Förtroenderisker i offentliga sektorn har dessutom blivit allt mer uppmärksammade under senare år. Förtroenderisker är samtidigt ett samlingsnamn på mycket olika risker. Det kan

t.ex. handla om mutor, förskingring, jäv, vetenskaplig oredighet, undanhållande av information, dålig ekonomisk hushållning och stora missbedömningar. Det kan också handla om till synes mycket små fel och brister, som kan uppfattas som tecken på större brister och problem. Det är inte ovanligt att flera av dessa risker uppfattas som relativt osannolika och att konsekvenserna vid ett eventuellt förverkligande underskattas. Det kan även gälla SLU. Det kan därför behövas mer omfattande diskussioner och analyser för att i hela organisationen skapa tydliga bilder av förtroenderiskerna. Som en del i det arbetet är det viktigt att även till synes små ”besvärliga” eller ”känsliga” frågor kommer till ledningens kännedom. Här spelar chefer och staber under den högsta ledningen en viktig roll (jämför även vad som sägs nedan om funktioner för whistleblowing).

Rekommendation: SLU bör försäkra sig om att förtroenderiskerna i verksamheten blir ordentligt behandlade i riskanalysarbetet.

Även det som här kallas förtroenderisker är inte framträdande i universitetets hittillsvarande riskanalyser. Det är ett samlingsnamn på många olika risker som kan leda till att förtroendet för SLU och dess verksamhet eroderar bland allmänheten och SLU: s intressenter. SLU bör därför särskilt uppmärksamma förtroenderisker i arbetet med riskanalysen.

1.7 Arbetsmetoderna för att ta fram och åtgärda risker har inte tydligt preciserats.

I SLU: s riktlinjer skrivs om arbetsmetoder, men det handlar då i huvudsak om hur processen för intern styrning och kontroll ska vara organiserad. Av mina intervjuer framgår t.ex. att den numer allt vanligare formen för att ta fram och diskutera risker och åtgärder, arbetsseminarier för självutvärdering, *workshopmetoden*, inte används genomgående i organisationen. Den grundläggande idén med en workshop är att samla en styr- eller ledningsgrupp (eller representanter för olika kunskapsområden inom ett område, ett projekt eller en enhet) för att tillsammans först diskutera fram de viktigaste riskerna inom området och sedan ta fram förslag till riskåtgärder. Arbetsformen innebär att de som kan verksamheten – med sina olika erfarenheter och kompetenser – själva tar fram och diskuterar riskerna gemensamt. Det skapar en bättre grund för både en gemensam riskbild och mer genomdiskuterade risker och riskåtgärder. Det som finns omnämnt i SLU: s riktlinjer, omvärldsanalyser, intervjuer med olika berörda etc., liksom även enkäter bland medarbetarna om brister och risker, bör ses som komplement till workshopmetoden.

Rekommendation: Arbetsmetoderna för att ta fram och åtgärda risker bör tydligare preciseras.

Den mest spridda arbetsmetoden för att ta fram risker och förslag till riskåtgärder, seminarier/arbetsgrupper för självutvärdering (den s.k. workshopmetoden) bör utgöra den viktigaste arbetsmetoden även i SLU (se även bilagan nedan om denna metod).

1.8 Utförligare analyser och beskrivningar av riskerna kan ge en bättre grund för den efterkommande riskvärdebedömningen och prioriteringen av risker.

Beskrivningarna av riskerna i SLU: s riskbilder är relativt kortfattade. SLU följer ESV: s rekommendation om en fyragradig skala för bedömning av sannolikheter och konsekvenser och beräkning av de sammanlagda riskerna. Själva uträkningen av riskvärdena har givits stort utrymme. Fram till den senaste riskvärderingen har även decimalvärden på riskvärdena räknats fram. En sådan inriktning på riskvärderingen kan, enligt min mening, t.o.m. försvåra en bra riskbedömning. Det kan kortfattat förklaras så här (mer underlag ges i en bilaga):

- *Den numeriska beräkningen bör endast ses som ett hjälpmedel för att ringa in de viktigaste riskerna för att sedan kunna gå vidare till lämpliga riskåtgärder.* Det år således bara ett mellansteg efter riskanalysen och före diskussionerna om riskåtgärder.
- *Sannolikhetsbedömningen bygger ofta på subjektiva sannolikheter,* dvs. uppskattningar som inte kan grundas på frekvensstudier och liknande beräkningsbart underlag.
- *Det kan finnas komplicerade bedömningar och avvägningar som döljs i framtagna numeriska värden.* För att bättre bedöma risken och sedan finna lämpliga riskåtgärder är det nödvändigt att *utförligt beskriva risken och olika omständigheter i ord* innan en numerisk beräkning görs.
- *Det går att prioritera risker utan att först ange dem i numeriska värden.* Även mätskalor som bygger på *enkel rangordning,* utan numerisk beräkning, kan användas. Då görs rangordningen direkt utifrån en bedömning av risken där både sannolikhet och konsekvens inkluderas. En rangordning kan vara tillräckligt för att få fram prioriterade risker direkt om det sker tillsammans med professionellt insatta och erfarna medarbetare inom de områden som berörs av riskanalysen. Ibland kan även den inbördes rangordningen vara en sekundär fråga om en tillräckligt tydligt bild skapats av de viktigaste riskerna.
- *Numerisk beräkning av risken kan vara särskilt tveksam vid ett par fall av extremvärden.* Bland riskanalytiker brukar man markera särdrag i bedömningen och hanteringen av risker som innehåller mycket små och mycket höga sannolikheter som inte klart framträder i användningen av numeriska värden. En precisering av sannoliksvärdet kan vara särskilt svårt vid *mycket små sannolikheter*. Det kan då vara bättre att först utförligt beskriva risken i konsekvenstermer och därefter lika utförligt diskutera när och hur sådana konsekvenser kan uppkomma ev. efter en känslighetsanalys utifrån olika sannolikhetsvärden. Det kan ge en bättre fingervisning för riskprioriteringen. Därmed kan också en god grund för en diskussion av riskåtgärder ha skapats. Det är ett förfarande som ofta används vid bedömning av samhällskriser och utformningen av krisberedskap. Om å andra sidan sannolikheten för en händelse *är mycket hög* och händelsen förväntas återkomma ofta är åtgärderna vanligtvis redan integrerade i den löpande verksamheten såsom en vanlig eller förutsedd variation i

verksamheten. Då behövs kanske inte risken närmare diskuteras inom ramen för prioriterade risker.

- *Riskprioriteringen kan ibland ske i kostnadstermer.* I affärsmässig verksamhet är det relativt vanligt att värdera riskerna utifrån en uppskattning av kostnader eller bortfall av intäkter om en händelse inträffar och sedan multiplicera med sannolikheten för att det inträffar. Detta förfaringssätt kanske kan vara användbart för intäktsfinansierad verksamhet såsom universitetsdjursjukhuset och inom SLU: s jordbruksdrift och fastighetsförvaltning. Då framträder riskvärdet såsom ett penningmässigt framräknat belopp. Även i detta fall måste diskussionen om risken och riskåtgärder få stor betydelse. Risken uppskattad i kostnadstermer måste dock ofta samsas med riskvärderingar inom andra områden som inte kan uppskattas i kostnader.

De här uppräknade aspekterna på riskprioriteringen behöver inte innebära att man avfärdar en numerisk riskvärdering utan snarare att den värderingen bör användas med försiktighet.

Rekommendation: Utförliga analyser och beskrivningar av riskerna ger en viktigare grund för den efterkommande riskvärdebedömningen och prioriteringen av risker.

Riskbedömningen med angivande av siffervärden bör användas med försiktighet i riskanalysarbetet och får inte skymma behovet av utförligare analyser och beskrivningar av riskerna.

1.9 Whistleblower-funktionen[3] och behovet av att rapportera allvarliga störningar via de normala kontaktvägarna är inte klargjorda inom SLU.

En god intern styrning och kontroll karaktäriseras av att även allvarliga brister och känsliga frågor kan rapporteras och tas om hand via de etablerade kontaktvägarna. Det är utöver detta som en funktion för whistleblowing bör komma in. För att rätt förstå dess funktion bör man först se till att den normala kontaktvägen och dialogen så långt möjligt verkligen fungerar inom organisationen och präglar relationerna mellan chefer och anställda. Om sådana etablerade relationer fungerar bra ska givetvis även allvarliga brister och känsliga frågor kunna föras fram och tas om hand den vägen. Förutsättningen är att det är högt i tak, dvs. ett öppet arbetsklimat på arbetsplatsen, som både är tillåtande och uppmuntrande för sådana känsliga frågor och som tar hand om frågorna på ett bra sätt. Att så inte alltid är fallet är uppenbart på många arbetsplatser i Sverige och kanske även inom SLU. Det är först och främst en ledningsfråga och bör vara en central fråga i strävan att åstadkomma en god intern styrning och kontroll. Det kan kräva både markeringar från ledningen och utbildning, särskilt bland chefer.

[3] Några försök till svensk översättning, ”visslare” eller ”visselblåsare”, har lanserats men har ännu inte slagit igenom. Jag använder därför det engelska uttrycket ”whistleblower”

Mot denna bakgrund bör en whistleblower-funktion betraktas som en nödutgång när andra kanaler inte fungerar. I det avseendet liknar den de nödutgångar som offentliga lokaler enligt lag ska ha, även om dessa nödutgångar bara utnyttjas just i nödsituationer. Dessutom kan anmälningar via whistleblower-funktionen tillsammans med incidentrapporter och signaler via andra kanaler skapa en översiktlig bild av svagheter i organisationens verksamhet och ge uppslag till närmare granskning av olika områden för att förbättra den interna styrningen och kontrollen.

Massmedia är redan idag en kanal för att ta hand om allvarliga och känsliga frågor. Som kanal handlar dock massmedias roll om att upptäcka oegentligheter, inte att förhindra dem. Det är uppenbart att många anställda och andra, kan känna sig tryggare med att gå till massmedia än till offentliga organisationer som SLU. Samtidigt kan man förmoda att om SLU blir skicklig i att hantera dessa frågor så kommer många som idag bara är redo att gå till massmedia i stället välja SLU: s kontaktkanaler. Därmed skulle SLU även slippa den bieffekt som ofta är förknippad med behandlingen i massmedia, att blotta misstanken om fel och brister beskrivs som förtroendekrisfrågor, innan frågorna utretts ordentligt och misstankarna kunnat verifieras eller avföras som falskt alarm.

Att det kan kännas tryggare att gå till massmedia kan kompenseras genom att ha två anmälningskanaler in till SLU – en intern kanal och en via en fristående juridisk instans, t.ex. en advokatbyrå, som har mycket lättare att hantera anmälningar, där uppgiftslämnare vill vara anonym. Det är ett sätt att arbeta som prövats av andra offentliga organisationer. Till viss del fungerar SLU: s juridiska funktion idag som en informell uppsamlingsplats för whistleblower-frågor. Den är dock inte jämförbar med en fullt utbyggd whistleblower-funktion. I denna fråga pågår arbete inom SLU som kan behöva stämmas av med det som nämnts ovan.

Rekommendation: Whistleblower-funktionen och behovet av att rapportera allvarliga störningar via de normala kontaktvägarna bör klargöras inom SLU.

En oberoende funktion för whistleblowing med möjligheter till anonymitetsskydd bör inrättas inom SLU. Samtidigt bör insatser göras för att se till att allvarliga störningar och brister även kan rapporteras in via de normala kontaktvägarna inom SLU (se även bilagan om whistleblowing).

1.10 Det görs inte alltid åtskillnad mellan brister och risker

Bland de rapporterade riskerna inom SLU finns även påpekanden om brister. Det är dock viktigt att skilja på brister och risker. En iakttagen brist finns som ett faktum eller en realitet men en risk handlar om något som kan hända. En brist kan direkt bli föremål för åtgärder, men en risk måste först värderas för att därefter leda till lämpliga åtgärder för att reducera risken. En brist kan emellertid vara en indikation om risker. Dessa risker måste då behandlas och bedömas särskilt för att leda till lämpliga åtgärder.

Rekommendation: Det bör göras en tydligare åtskillnad mellan brister och risker i riskanalysarbetet.

Iakttagna brister kan åtgärdas på olika sätt i det löpande arbetet. De risker som kan identifieras har en annan karaktär. I arbetet med riskanalysen ska risker och inte brister vara det centrala i arbetet att åstadkomma en god måluppfyllelse.

1.11 Enhetliga begrepp och arbetssätt för hela SLU saknas.

SLU är en stor organisation med olika verksamheter utspridda på flera orter. Precis som framförs i det stora förändringsarbete, Framtidens SLU, kräver detta gemensamma rutiner om organisationen ska fungera effektivt, inkl. gemensamma begrepp och arbetssätt i övrigt. Därför gäller kraven också arbetssättssätt och metoder för intern styrning och kontroll inkl. riskhantering. Så fungerar det inte idag. Inom några områden arbetar man utifrån den standard som kallas ISO 31 000 Riskhantering i stället för den standard som finns implicit i förordningen om intern styrning och kontroll, dvs. COSO: s ramverk för intern styrning och kontroll. Dessa två utgångspunkter inte är helt jämförbara och omfattar delvis olika frågor, men de går att förena i ett gemensamt arbetssätt[4]. Det gemensamma arbetssättet måste dock i så fall klargöras för hela SLU så att missförstånd och svårigheter att ställa samman resultat från olika områden undviks.

I detta sammanhang bör även påpekas att SWOT-analyser (som nämns i arbetet med Framtidens SLU) har vissa likheter med riskanalyser. Skillnaden handlar främst om att riskanalyser alltid relateras till uppsatta mål. SWOT-analyser handlar normalt om en bredare värdering av verksamheten som sådan[5]. SWOT-analyser och riskanalyser kan komplettera varandra.

Rekommendation: För att säkra ett effektivt arbete för en god intern styrning och kontroll bör SLU använda enhetliga begrepp och arbetssätt inom hela organisationen.

De olika standarder som används inom SLU idag för riskhantering bör ensas. Det innebär att enhetliga begrepp och arbetssätt införs inom hela organisationen.

1.12 Olika riskperspektiv med delvis olika former för riskhantering är inte knutna till arbetet med intern styrning och kontroll.

Förutom olika standards för generell riskhantering (se punkten ovan) finns flera väl utarbetade former för riskhantering inom mer specifika områden. Informationssäkerhet, fysisk säkerhet, samhällskriser, hållbarhetskrav, socialt ansvarstagande är några sådana viktiga områden. De har i flera avseenden utvecklat egna rutiner och system för riskhantering. Oavsett detta bör risker inom dessa

[4] Hur de kan sammanfogas antyds i en bilaga till denna rapport.
[5] Se även bilagan i denna fråga.

områden kunna finnas med i den samlade bedömningen av risker vad gäller den interna styrningen och kontrollen för hela SLU. Det är inte säkert att sådana risker kommer med i bedömningen i dag av SLU: s intern styrning och kontroll. Denna punkt berörs även i diskussionen under nästa avsnitt.

Rekommendation: SLU behöver säkerställa att risker framtagna inom särskilda riskområden samordnas med arbetet med det generella arbetet för intern styrning och kontroll.

De på andra sätt etablerade former för riskhantering inom speciella arbetsområden (t.ex. arbetsmiljö, personskydd, brandskydd) bör inte vara helt skilda från arbetet med intern styrning och kontroll (se även punkt 6.3 nedan) om man vill åstadkomma en effektiv riskhantering.

Möjlighet med en fördjupad riskhantering

Intern styrning och kontroll utgår normalt från att målen för verksamheten är givna och hanterar risker för att dessa mål inte uppnås genom olika åtgärder[6]. Det är en naturlig utgångspunkt i myndighetsreglerad verksamhet, eftersom regering och riskdag sätter målen för sådan verksamhet. Inom universitetsvärlden och särskilt inom SLU finns det emellertid utrymme att påverka målen och då kan det vara viktigt att låta ett riskperspektiv även beröra hur målen ska formuleras. Det finns några ytterligare riskaspekter som berör styrningen som SLU kan hantera. Tillsammans ingår de i det man kallar företags- eller organisationsövergripande riskhantering (ERM).

1.13 Att låta riskbilden påverka målen

Inom SLU finns områden där universitetet ges möjlighet att precisera målen för verksamheten. Det gäller särskilt den forskningsorienterade och konkurrensutsatta verksamheten. En central fråga för styrningen inom sådana områden är att målen påverkas av riskanalys. Målen kan vara alltför optimistiskt eller orealistiskt satta med hänsyn till de risker som finns. De kan å andra sidan vara alltför pessimistiskt och för lågt satta i förhållande till möjligheterna. Här finns också utrymme att formulera mål präglade av nytänkande och originalitet. Ett fiktivt exempel får illustrera detta. Om SLU hade formulerat ett mål så att alla ansökningar om forskningsmedel ska beviljas innehåller det ett kraftfullt åtagande men det kan vara orealistiskt. Om universitetet då hade satt in mycket stora resurser för att försöka nå det målet hade det troligen förblivit ouppnått. Det hade kanske dessutom tagit resurser som annars skulle använts för att nå andra mål inom universitetets verksamhetsområde, dvs. äventyra universitetets mål inom andra områden. Om SLU i stället hade bestämt att inga ansträngningar behöver göras för att underlätta arbetet med forskningsmedel kan det i stället vara ett uttryck för ett alltför pessimistiskt och för lågt satt mål. Då hade kanske resurserna inte använts på ett sätt som hade gynnat universitetets position i universitetsvärlden. Mål kopplade till

[6] COSO: s ramverk för intern styrning och kontroll har denna utgångspunkt, men det gäller normalt för allt arbete med intern styrning och kontroll.

hanteringen av forskningsmedel bör således förmodligen sättas så att de hanterar de ovan nämnda riskerna.

Att på detta sätt låta riskerna påverka målen hör till det som kallas för företags- eller organisationsövergripande riskhantering (ERM, Enterprise Risk Management). Det kan gälla alla slags mål men spelar störst roll inom det strategiska området. Förutom att det gäller konkurransutsatta forskningsanknutna verksamheten kan detta även gälla universitetsdjursjukhuset, jordbruksdriften och fastighetsförvaltningen.

Riskanalysen utvidgas således till att inte bara försöka undvika risker för oönskade händelser och lägen utan även inkludera frågan om att våga ta risker för att uppnå viktiga mål[7]. Med ett strategiskt synsätt kommer då två tillkommande aspekter att bli viktiga, att väga samman riskerna för hela organisationen och precisera den risknivå (riskaptiten) som organisationen är beredd att acceptera (det kan även innebära olika risknivåer för olika delar av verksamheten). Dessa två aspekter diskuteras nedan.

Rekommendation: SLU bör överväga att inom delar av verksamheten utvidga riskanalysarbetet så att de framtagna riskbilderna även påverkar målen för verksamheten.

Det finns utrymme inom universitetet för att införa företags- eller organisationsövergripande riskhantering (ERM). Det innebär framför allt att utöver arbetet med intern styrning och kontroll även ta med de strategiska målfrågorna och låta dessa mål påverkas av riskbilden (Hur de kan göras ges exempel på i bilagan nedan med en föreslagen riskhanteringsprocess).

1.14 Sammanvägningen av olika risker i organisationsövergripande riskhantering

I en stor organisation med verksamhet inom skilda områden och med olika gemensamma funktioner bör man vara beredd på att risker inom en del av verksamheten kan påverkas av risker inom en annan del av verksamheten. Om t.ex. en viss typ av forskning blir starkt ifrågasatt i den allmänna debatten och riskbilden växer kan detta även påverka riskbilden för den utbildning som är knuten till denna forskning.

Som framförts ovan (se punkt 5.10 i föregående avsnitt) finns dessutom krav på riskanalyser och åtgärder inom flera olika områden som SLU, liksom andra organisationer, berörs av. Det är i några fall lagkrav i andra fall rekommendationer och handlar om:

[7] Det kallas på engelska även upside risks och downside risks. I COSO: s ramverk kallas det för opportunities (möjligheter) till skillnad från det mer traditionella riskperspektivet. I Standarden för ISO 31 000 Risk Management har de två risktyper förts samman till ett riskbegrepp och definieras då som ”osäkerhetens inverkan på uppnåendet av mål”.

- riskanalyser som arbetsmiljölagen kräver, särskilt i samband med förändringar av organisationen och verksamheten för att vidmakthålla ett fullgott arbetarskydd,
- riskanalyser för att upprätthålla ett skalskydd och säkerhet (t.ex. brandskydd och personskydd) inom av SLU använda anläggningar,
- riskanalyser för att upprätthålla god informationssäkerhet. Det handlar till stor del om IT-säkerhet men även andra former av informationshantering,
- riskanalyser knutna till samhällskriser och kraven på krisberedskap hos många myndigheter,
- krav på hållbarhetsanalyser, socialt ansvarstagande m.m.

En del av dessa aspekter utgör traditionell riskhantering och är väl etablerade sedan länge (t.ex. arbetsmiljökrav). Andra aspekter har tillkommit under senare år (t.ex. socialt ansvartagande). SLU bör vara beredd på att nya eller skarpare krav kan dyka upp efter hand. Gemensamt för alla dessa krav är att det oftast bedrivs i skilda spår och inte är samordnade (organiserade som stuprör brukar det ofta kallas). Här är SLU inget undantag. Eftersom SLU, liksom andra organisationer, har begränsade resurser och övervakningsförmåga finns det starka skäl att försöka samordna analyserna av de olika riskområdena och prioritera resurserna på ett övergripande plan för universitetet. Det kan vara en viktig del av en effektiv företagsövergripande riskhantering.

Rekommendation: Risker från olika delar av verksamheten samt med olika riskperspektiv bör vägas samman i den företagsövergripande riskhanteringen.

Behovet att föra samman risker från olika delar av verksamheten och med olika riskperspektiv blir särskilt tydligt i den företagsövergripande riskhanteringen.

1.15 Att bestämma risktoleransen eller riskaptiten

Nästan all traditionell riskhantering handlar om att reducera risker (eller att dela dem med andra genom bl.a. försäkringar). Att helt eliminera en risk innebär nästan alltid att avstå från den verksamhet som genererar risken i fråga. Det går även att acceptera en risk. Att sätta in mer resurser för att reducera risken kan t.ex. överstiga nyttan av en riskreducering. Att acceptera en risk spelar en större roll i en mer företagsövergripande riskhantering. Det handlar då både om att reducera risker för oönskade händelser till lämplig nivå och att finna nivån på de risker man är beredd att ta för att nå vissa mål. Denna risknivå, som i affärsmässig verksamhet brukar kallas riskaptit, kan både vara svår att fastställa i numeriska värden och variera mellan olika verksamhetsdelar. I det första avseendet handlar det, som tidigare påpekats, till stor del om att analysera och beskriva riskerna tillräckligt utförligt för att kunna göra en risknivåbedömning även om den inte kan beräknas numeriskt. I det andra avseendet handlar det ofta om att strategiskt bedöma vilka verksamhetsdelar man vill satsa särskilt på och därför är beredd att ta högre risker inom dessa områden. I det sammanhanget bör man även uppmärksamma att risker inom en del av verksamheten kan vara beroende av andra delar av verksamheten, såsom kort beskrivits i förgående punkt. Ett exempel - Om ett visst

forskningsområde bedöms som särskilt känsligt för yttre störningar av olika slag (låg risktolerans) kan det kräva särskilt höga krav på informationssäkerhet och tillträdesskydd (även där låg risktolerans).

Rekommendation: SLU bör även arbeta med frågor om tolererade eller accepterade risker (riskaptit) i den organisationsövergripande riskhanteringen.

En effektiv övergripande riskhantering innefattar också att klargöra vilka risker som organisationen är beredd att ta. Det gäller både risker för oönskade händelser och risker för att nå önskade mål.

Inga Astorsdotter
Internrevisionschef

Torbjörn Wikland
Internrevisor

Bilaga A. En utbyggd riskhanteringsprocess – ett förslag för diskussion inom SLU

Några centrala steg i en riskhanteringsprocess för hela SLU
Här följer en beskrivning i punktform (succesiva steg) av hur en utvidgad riskhanteringsprocess kan utformas.

1. **Grundläggande förväntningar och värden** - Klargöra SLU: s värdegrund (inkl. syften och strategiska mål) utifrån
    a. egna ambitioner,
    b. universitetsvärldens ”standards”,
    c. lagstiftning m.m.
2. **Klargöra målen för verksamheten** (mål, inkl. ovan nämnda förväntningar och värden, som går att följa upp löpande)
    a. Formulerade utifrån befintliga lagar, förordningar etc.
    b. Preciserade mål utifrån styrelse och ledning (t.ex. kvalitetsmål och restriktioner)
    c. Utrymme för mål specifika för fakulteter och institutioner
    d. Målen bör följa mönstret för SMARTA mål (dvs. Specifika, Mätbara (eller observerbara), Accepterade (eg. relevanta), Realistiska (eg. nåbara =attainable), Tidsbestämda och Ansvarsfördelade – SMART är från början ett engelsk begrepp).

    Granska även om denna målstruktur tenderar att bli för komplicerad och omfattande – och om i så fall den kan göras enklare.
3. **Verksamhetsbilder av styrka och svagheter m.m.** – de bör vara en tidig del av verksamhetsplaneringen och kan baseras på t.ex.
    a. Årlig självdeklaration av hur man klarar de olika delarna i den interna styrningen och kontrollen (baserad på COSO: s indelning i fem komponenter)
    b. SWOT-analyser[8] (en genomgång av en verksamhets starka och svaga sidor samt hot mot och möjligheter för verksamheten – oavsett de mål som finns i utgångsläget)
    c. Incidentrapporter från olika delar av verksamheten
    d. Medarbetarenkäter m.m.
4. **Den grundläggande riskanalysen** - (utifrån gemensamma synsätt, begrepp och metodik och såsom en tidig del i den återkommande verksamhetsplaneringen och i första hand baserad på arbete i workshopform med ledningsgrupper på olika nivåer)

[8] SWOT= strengths, weaknesses, opportunities and threats

   a. Inventera risker för att mål inte uppnås (klarlägga oönskade lägen/händelser och sedan bedöma sannolikhet och konsekvens så långt det går)

   b. Prioritering av risker

5. **En kompletterande riskanalys** – Vilka risker bör SLU ta för att uppnå både strategiska och operativa mål? Risktagandet utgår från medvetna riskval och diskussioner om risknivåer (riskaptit).

6. **Riskåtgärder - reducera och acceptera risker**

   a. Befintliga riskåtgärder och kontroller (fungerande? tillräckliga?)

   b. Nya åtgärder och kontroller? (här bör fritt utrymme ges för innovativa idéer)

7. **Uppföljning/övervakning**

   a. Löpande åtgärdsuppföljning

   b. Stickprov

   c. Fördjupade kontrollanalyser

   d. Övervakning av nyckelkontroller[9]

[9] Nyckelkontroller är sådana som kan varna om brister och missförhållanden men som kräver ytterligare studier för att ta reda på vilka bakomliggande kontroller som inte fungerat eller varnat.

Bilaga B. Om ramverk och standards för riskhantering

Den första och mest spridda standarden för systematisk riskhantering genom intern styrning och kontroll utgår från den fristående amerikanska organisationen COSO, som lanserade ramverket för intern styrning och kontroll 1992. Det ramverket ligger till grund för EU: s direktiv inom området och den svenska förordningen om intern styrning och kontroll (FISK). COSO kompletterade det ramverket med en påbyggnad för företagsövergripande riskhantering 2004 (ERM, Enterprise Risk Management).

2008 tog organisationen ISO fram en övergripande standard för riskhantering (ISO 31 000) som tar upp samma riskperspektiv som COSO: s två ramverk, men i form av ett integrerat riskbegrepp. Den viktigaste skillnaden mellan dessa två standarder är att COSO: s ramverk[10] har som mål att kunna göra en samlad bedömning av först den interna styrningen och kontrollen och sedan den övergripande riskhanteringen. ISO-standarden har i stället fokus på hur olika risker bör hanteras utifrån en enhetlig modell för riskhanering. Det innebär också att det är fullt möjligt att både följa COSO: s ramverk och använda sig av ISO-standardens modell för den egentliga riskhanteringen. De begrepp som används i de två standarden måste dock ensas för att underlätta arbetet och skapa transparens i en organisation.

Det finns även standarder för mer specialiserad riskhantering såsom informationssäkerhet, kontinuitetsplanering, miljöledning, socialt ansvarstagande m.m. som kan beröra SLU.

[10] COSO publicerade i maj 2013 en uppdaterad version av sitt ramverk för intern styrning och kontroll. Den är i flera avseenden tydligare men i allt väsentligt densamma jämfört med den tidigare versionen från 1992.

Bilaga C. Seminarier för självutvärdering (workshop-metoden) för analys av risker och riskåtgärder

Det som kallas workshop-metoden eller metoden för självutvärdering har blivit en alltmer spridd metod för att arbeta med intern styrning och kontroll inkl. riskhantering. En beskrivning av metoden i engelsk litteratur:

"*Control self-assessment (CSA) is a way of helping organizations to improve their ability to meet business objectives. Most of the time, this is done through a series of workshops or meetings facilitated by the internal auditing department. These workshops can be applied to projects, processes, business units, functions, or basically any level whose objectives can be clearly defined. The workshops involve the personnel directly responsible for meeting an organizational objective, and are designed to examine, asses, and report the likelihood of the objective being achieved*." (Control Self-Assessment: A practical guide)

I denna beskrivning utgår man från att internrevisionen leder arbetet i en workshop. Den rollen kan givetvis andra fylla. Det viktiga i sammanhanget är att workshop-ledaren inte representerar ett av de olika intresseområden som finns i gruppen utan agerar som oberoende aktör för att få fram ett resultat som hela gruppen kan ställa sig bakom.

En mer formell definition av workshop-metoden lyder:

"*CSA is a process through which internal control effectiveness is examined and assessed. The objective is to provide reasonable assurance that all business objectives will be met.*" (samma källa som ovan)

De arbetssteg som bör finnas i en workshop är främst följande:

- Riskområdet, dess gränser - avstämning inom gruppen
- Mål och grundläggande värden inom riskområdet klargörs – ev. oklarheter noteras
- Oönskade händelser (inkl. lägen/hot) inventeras. Har vi fångat alla relevanta händelser/hot?
- Ta hänsyn till tidshorisonten för händelserna – notera stora skillnader i tidshorisont och avgränsa om nödvändigt till en bestämd tidshorisont.
- Händelsernas konsekvenser och sannolikheter bedöms för att få fram riskerna
- Gruppen prioriterar fram de viktigaste riskerna - genom omröstning eller samstämmighet efter diskussion
- Spegla riskerna mot befintlig åtgärder/intern styrning och kontroll – notera ”gapen”
- Ta fram åtgärdsförslag för att reducera riskerna – ge tid för diskussion och kreativitet. Åtgärdsförslag direkt eller efter fördjupad analys (vilka är avgörande riskdrivers)
- Sortera förslagen i a) egna åtgärder, b) åtgärder i samverkan med andra och c) andras åtgärder

- Överlämna förslagen till linjeorganisationen för ev. preciseringar, kostnadsbedömningar, beslut och genomförande.

Givetvis kan den mer detaljerade utformningen av en workshop variera på många sätt.

Bilaga D. Om whistleblower-funktionen

En effektiv intern styrning och kontroll förutsätter att iakttagelser om brister kan flöda uppåt i organisationen utan hinder så att de kan leda till åtgärder på olika nivåer. I praktiken har det visat sig svårt att förverkliga. Det kan finnas trögheter i organisationer (COSO hävdar att en organisation med mer än tre hierarkiska nivåer alltid leder till att information filtreras bort i rapporteringskanalerna uppåt i organisationen). Mellanchefer och högre chefer kan även välja bort ”besvärlig” information. Det ”besvärliga” kan kortsiktigt vara till nackdel för organisationen även om det långsiktigt kan vara till ovärderlig nytta för att säkra en framgångsrik verksamhet. I sådana lägen krävs det både kurage och kunskapsbaserad medvetenhet hos både medarbetare och chefer för att ta tag i ”besvärlig” inkommande information.

För att inte vara beroende av hur de nämnda kanalerna verkligen fungerar behövs sätt att säkra att sådan ”besvärlig” information verkligen rapporteras. För det krävs att någon form av Whistleblower-funktion inrättas. Det innebär att man försöker se till att det finns a) från organisationen helt oberoende rapporteringskanaler och b) ett ordentligt skydd för anonymitet. Att kanalen är helt oberoende innebär att den inte kan påverkas av mellanchefer eller högre chefer. Anonymitetsskyddet måste både finnas och vara väl känt bland personalen. För offentlig verksamhet kan det innebära att man inrättas en funktion helt utanför organisationen för att garantera anonymitet. Erfarenheten hittills visar att dessa krav är viktiga för att få till stånd en fungerande whistleblower-funktion. De kan också liknas vid nödutgångar vid allvarlig fara. I USA och några andra länder har särskild lagstiftning skapats för att säkerställa att funktioner för whistleblowing inrättas. I Sverige saknas ännu sådan lagstiftning. Det innebär bl.a. att anonymitetsskydd inte kan garanteras när whistleblowing kanaliseras inom en offentlig organisation. Oberoende whistleblowing-funktioner har ändå upprättats i flera större företag och i offentliga myndigheter såsom Göteborgs Stad och SIDA.

Bilaga E. Om numerisk beräkning av risker.

En numerisk beräkning av risker storlek är i grunden bara ett steg i arbetet mellan identifieringen av risker och framtagandet av åtgärder för att hantera identifierade risker. Detta steg kan motiveras med att resurserna för riskåtgärder är begränsade och att bara de risker som allvarligt kan påverka målen för verksamheten ska hanteras. Det är emellertid lätt både förstora och övertolka denna del av arbetet. Det är detta som berörs i avsnitt 5.6 ovan och som i några avseenden här behandlas mer utförligt.

a) Det kan finnas komplicerade bedömningar och avvägningar som döljs i framtagna numeriska värden på en risk. Sådana risker kan samtidigt vara mycket svåra att sätta numeriska värden på. En numerisk skala innebär även att man bestämmer hur mycket större en storhet är jämfört med en annan. Det går dock att prioritera risker utan att först ange dem i numeriska värden.

b) Även mätskalor som bygger på *enkel rangordning* av riskerna kan användas. Det kallas även en ordinal skala och innebär å ena sidan att i rangordningen är en storhet är större än en annan men man vet inte hur mycket större den ena storheten är i förhållande till den andra. En sådan rangordningen kan göras direkt utifrån en bedömning av risken där både sannolikhet och konsekvens inkluderas. En rangordning kan med fördel göras tillsammans med professionellt insatta och erfarna medarbetare inom de områden som berörs av riskanalysen. Ibland kan även den inbördes rangordningen vara en sekundär fråga om en tillräckligt tydligt bild skapats av de viktigaste riskerna.

c) Bland riskanalytiker brukar man markera särdrag i bedömningen och hanteringen av risker som innehåller mycket små och mycket höga sannolikheter som inte framträder i användningen av numeriska värden. Vid bedömningen av *mycket små sannolikheter* kan ett kvalitetsmässigt bra resultat vara att ha bestämt sannolikheten inom intervallet 1/100-del till 1/1000-del. Då varierar riskvärdet i storlek mellan 1 till 10 vid ett givet konsekvensvärde, vilket kan vara otillräckligt vid prioriteringen mellan olika risker. Det kan då vara bättre att först enbart beskriva risken i konsekvenstermer. Därefter görs en direkt bedömning av risken ev. efter en känslighetsanalys utifrån sannolikhetsvärdet. Det kan ge en bättre fingervisning om riskprioriteringen. Då kan sedan beskrivningen av omständigheterna när en händelse kan inträffa vara en god grund för en diskussion av riskåtgärder. Det är ett förfarande som ofta används vid bedömning av samhällskriser och utformningen av krisberedskap. Om å andra sidan sannolikheten för en händelse *är mycket hög* och händelsen förväntas återkomma ofta är åtgärderna vanligtvis redan integrerade i den löpande verksamheten såsom en vanlig eller nödvändig variation och kanske inte behöver diskuteras närmare inom ramen för prioriterade risker.

d) I affärsmässig verksamhet är det relativt vanligt att värdera riskerna utifrån en uppskattning av kostnader eller bortfall av intäkter om en händelse inträffar och sedan multiplicera med sannolikheten för att det inträffar. Det kan vara svårt att överföra till SLU som saknar en tydlig intäktsida i verksamheten som balanserar kostnadssidan. Detta förfaringssätt kan emellertid vara användbart för intäktsfinansierad verksamhet såsom universitetsdjursjukhuset och inom SLU: s jordbruksdrift och fastighetsförvaltning. Det ger också mer information än en ren siffermässig beräkning av riskvärdet. Det kan dock vara svårt att förena kostnadsmässigt beräknade riskvärden med icke kostnadsmässiga riskvärden.

De här uppräknade aspekterna på riskprioriteringen behöver inte innebära att man helt avfärdar en numerisk riskvärdering utan snarare att den värderingen bör användas med viss försiktighet.

DNR: SLU.ua.2013.1.1.1-4833

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Universitetsdirektören

ÅTGÄRDSPLAN
2013-12-09

Åtgärdsplan för internrevisionens rapport gällande intern styrning och kontroll inom SLU

Sammanfattning

Internrevisionen konstaterar att SLU:s arbete med intern styrning och kontroll uppfyller de förordningsmässiga krav som finns och lägger samtidigt fram 13 möjliga förbättringsförslag. I dessa förslag behöver investerad tid (som tas från bl a kärnverksamheten) vägas mot de effekter som förväntas uppnås.
Universitetsledningen anser att följande rutiner ska ses över:

- Tidsplanering/årscykel för arbetet med intern styrning och kontroll
- Användningen av olika metoder för framtagande av risker och riskåtgärder, t ex workshop och numerisk bedömning
- Införande av obligatoriskt deltagande av prefekter i fakulteternas riskarbete och ett eventuellt utnyttjande av universitetets olika råd i riskarbetet
- Översyn av riskanalysstrukturen inom universitetet och en eventuell harmonisering av densamma
- Whistleblower-funktionen inom SLU

Inledning

Internrevisionen har granskat den interna styrningen och kontrollen inom SLU. Därvid har konstaterats att universitetets arbete med intern styrning och kontroll uppfyller de förordningsmässiga krav som finns. Utöver detta har granskningen innefattat frågan om arbetet kan förbättras och göras effektivare. Resultatet har blivit tio punkter/aspekter med utrymme för förbättringar.

Utöver dessa förbättringsmöjligheter för den interna styrningen och kontrollen finns möjligheter att utvidga arbetet till företags- eller organisationsövergripande riskhantering. Det gäller särskilt den forskningsanknutna och konkurrensutsatta verksamheten inom SLU. Internrevisionen framför rekommendationer i tre punkter (punkt 11-13).

Nedan redovisas internrevisionens punkter tillsammans med universitetsledningens kommentarer, åtgärder, ansvariga och tidsplaner. Generellt gäller att de

förändringar som ska genomföras kodifieras i rektors beslut om processen för intern styrning och kontroll senast 2014-06-01.

Förslag och åtgärder

Generellt menar universitetsledningen att arbetet med intern styrning och kontroll och riskanalys är utmanande och kräver mycket av både dem som planerar arbetet och dem som gör bedömningarna i riskanalysen. De risker som identifieras och bedöms är de som påverkar möjligheten att uppnå verksamhetens uppsatta mål. Riskerna kan vara svåra att formulera på ett entydigt sätt och ur ett tydligt perspektiv. Olika verksamheter kan närma sig ett problem på olika sätt och därmed värdera risken helt olika. Enskilda personer kan också tänka på olika sätt över tid, vilket ger en variation i bedömningarna. Universitetsledningen konstaterar att förordningen för intern styrning och kontroll på senare tid har ifrågasatts av bl a Statens Innovationsråd, bl a av de ovan nämnda skälen. Därför är det välkommet att en granskning sker av universitetets riskarbete. Universitetsledningen konstaterar också att Internrevisionens rapport innehåller flera bra förslag, men att den eventuella ytterligare tid som investeras i riskarbetet hela tiden måste vägas mot effekten och vinsten av insatsen.

1. Integrera riskhanteringen i universitetets årscykel för planering och uppföljning.

Åtgärd: Styrelsen ska, i samband med att årsredovisningen beslutas i februari, intyga om universitetet har en betryggande intern styrning och kontroll. Därför har riskanalysen hittills tidsplanerats utifrån årsredovisningen. Det är dock mer naturligt att riskanalysen knyts hårdare mot verksamhetsplaneringsprocessen så att eventuella riskåtgärder kan planeras samtidigt som all annan verksamhet.

Universitetsledningen bedömer således att riskhanteringen ska integreras i universitetets årscykel för planering och uppföljning.

Ansvarig: Planeringschefen[1]

Tidsplan: Nytt rektorsbeslut om processen för intern styrning och kontroll senast 2014-06-01.

2. Alla de tre organisatoriska nivåerna inom SLU bör delta i arbetet med den interna styrningen och kontrollen.

Åtgärd: Riskarbetet är som ovan framhållits mycket komplext och kräver en stor insats för att ge insatt värde tillbaka. Om riskarbetet på hela SLU prioriteras upp i nämnd omfattning på institutionsnivå riskerar den tid som avsätts för kärnverksamhet att minska i samma omfattning. En förutsättning

[1] Planeringsavdelningen skapas 2014-01-01.

för ett konsekvent genomförande av riskanalysarbetet på alla nivåer är också att ett målarbete genomförs i organisationen eftersom inte alla institutioner har utvecklat egna tydliga och systematiskt uppsatta mål.

Universitetsledningen anser att den föreslagna insatsen skulle bli större än effekterna av detta förslag. Däremot bör prefektdeltagandet göras obligatoriskt i fakultetsarbetet, bl a för att bättre fånga upp risker i kärnverksamheten. Dessutom bör det övervägas om olika råd, såsom UN, FUR och FOMAR, ska involveras i riskarbetet.

Ansvarig: Planeringschefen

Tidsplan: Nytt rektorsbeslut om processen för intern styrning och kontroll senast 2014-06-01.

3. SLU bör försäkra sig om att kärnverksamheten i SLU, dvs. utbildningen, forskningen och miljöanalysen, är synlig i de riskanalyser som arbetas fram av universitetet.

Kommentar: Universitetsledningen anser att om prefekterna och råden deltar (i enlighet med punkt 2) bör det leda till större fokus på kärnverksamheten i riskarbetet.

4. SLU bör försäkra sig om att förtroenderiskerna i verksamheten blir ordentligt behandlade i riskanalysarbetet.

Kommentar: Universitetsledningen har ingen avvikande åsikt i detta fall. Förtroenderiskerna kommer även fortsättningsvis att beaktas i riskarbetet.

5. Arbetsmetoderna för att ta fram och åtgärda risker bör preciseras.
6. Utförligare analyser och beskrivningar av riskerna ger en bättre grund för den efterkommande riskvärdebedömningen och prioriteringen av risker.

Åtgärd: Internrevisionen rekommenderar SLU att använda den s k workshopmetoden. Redan i dag tas den universitetsgemensamma risklistan fram genom en workshop i universitetsledningen. Workshopmetoden bör även kunna användas mer systematiskt i dekaner och prefekters arbete. Enligt internrevisionens rapport ska siffervärden användas med försiktighet. Den numeriska metoden rekommenderades av ESV när förordningen om intern styrning och kontroll infördes. Det är universitetsledningens mening att en översyn av metoden ska göras, där mindre tyngd läggs på att räkna och poängsätta sannolikheter och konsekvenser och där riskbedömningarna sker utifrån kvalitativa resonemang.

Ansvarig: Planeringschefen

Tidsplan: Nytt rektorsbeslut om processen för intern styrning och kontroll senast 2014-06-01.

7. Whistleblower-funktionen och behovet av att rapportera allvarliga störningar via de normala kontaktvägarna bör klargöras inom SLU.

Kommentar: Universitetsledningen har för avsikt att se över frågan om whistleblowerfunktion under våren 2014.

Ansvarig: Ledningskansliet/chefsjuristen

Tidsplan: 2014-06-01.

8. Det bör göras åtskillnad mellan brister och risker i riskanalysarbetet.

Kommentar: Universitetsledningen anser att detta kommer att vara en naturlig del av det fortsatta riskanalysarbetet.

9. För att säkra ett effektivt arbete för en god intern styrning och kontroll bör enhetliga begrepp och arbetssätt användas inom hela SLU.
10. Olika riskperspektiv med delvis olika former för riskhantering bör samordnas med arbetet med intern styrning och kontroll.

Åtgärd: Universitetsledningen bedömning är att den interna riskanalysstrukturen ska ses över så att ställning kan tas till om och i vilken utsträckning en harmonisering av olika riskanalyser bör ske.

Ansvarig: Planeringschefen

Tidsplan: 2014-06-01

11. SLU bör pröva att utvidga riskanalysarbetet så att de framtagna riskbilderna även påverkar de mål som sätts för verksamheten.
12. Risker från olika riskperspektiv bör vägas samman i den företagsövergripande riskhanteringen.
13. SLU bör arbeta med frågor om tolererade risker (den s.k. riskaptiten) i den företagsövergripande riskhanteringen.

Kommentarer: Ovanstående punkter finns i internrevisionens rapport under rubrik 6 ”Möjlighet med en fördjupad riskhantering”. Universitetsledningen anser att det är viktigt att först skapa en bra och fungerande bas för hanteringen av risker innan eventuellt en fördjupad riskhantering enligt förslagen övervägs.