D11. RISKHANTERING

I detta moment är kravet olika utformat för organisationer i nivå 1 jämfört med nivå 2 och 3. Samtliga ska göra en riskanalys, för organisationer på nivå 2 och 3 ska en organisationsövergripande riskhanteringsplan upprättas med riskanalysen som grund.

Definition av risk

För att kunna arbeta med riskhantering, måste varje organisation definiera vad ”risk” är. Eftersom risk används i vardagsspråket med lite olika betydelser är det viktigt med en gemensam definition i detta sammanhang. Ett exempel är definitionen i ISO 31000, en internationell standard för riskhantering, som är ”osäkerhetens effekt på mål”. Där effekten, d v s påverkan, kan vara både positiv och negativ enligt just den definitionen.

Riskanalys

En riskanalys är en systematisk genomgång av framtida osäkra händelsers påverkan på organisationen. Ett vanligt angreppssätt är att kartlägga riskerna med hjälp av följande frågor.

- Vad skulle kunna hända? - identifiera
- Hur troligt är det att det skulle kunna hända? - sannolikhet
- Vad är effekten om det skulle hända? – konskvens

Det är lämpligt att använda någon form av bedömningsskala. En sätt att skapa överblick är att beskriva riskerna i en ”riskkarta” där sannolikhet och konsekvens sätts på x respektive y-axlen i ett diagram. Riskvärdet = Sannolikhet x Konsekvens. Detta ger ett underlag för prioritering och hantering av riskerna.

Riskanalysen ska enligt kravet i koden genomföras årligen för att undvika att den genomförda analysen inte blir inaktuell och för att säkerställa att den reflekterar faktiska risker. Naturligtvis kan organisationen göra en likartad bedömning av en risk från år till år. Det viktiga är att en noggrann genomgång görs.

Riskhanteringsplan (obligatoriskt för nivå 2 och 3)

En riskhanteringsplan bör omfatta de risker som vid riskanalysen fick det högsta värdet. Planen bör omfatta:

- Beskrivning av risken
- Strategi/metod för hantering av risken som kan innefatta
  - Hur kan sannolikheten att risken inträffar påverkas?
  - Hur kan konsekvensen påverkas?
  - Vilka varningssytem finns på plats?
  - Vem är ansvarig?

- Uppföljning av riskhanteringen

Fler användningsområden

Riskanalys och riskhanteringsplan bör integreras i allt beslutsfattande och vara en naturlig del av styrelsens och ledningens vardag. Det är också lämpligt som underlag för budget och verksamhetsplan samt som en del av introduktionsutbildning för styrelseledamöter och anställda.

Kvalitetskodens krav på dokumentation

Koden ställer krav på redovisande dokument i form av protokoll som visar att styrelsen gjort analysen, själva analysen är lämpligen en bilaga. För de större organisationerna gäller att själva riskhanteringsplanen ska finnas som bevis på att kravet är uppfyllt.