AEO-aktörens riskhanteringssystem

Med hjälp av sitt riskhanteringssystem bedömer ett företag risker samt övervakar och rapporterar de åtgärder som genomförs för hantering av risker och åtgärdernas inverkan. Företagets riskhanteringspolicy beskriver riskhanteringens syfte, mål och processer samt fastställer centrala begrepp och ansvar. Dessutom behöver företaget anvisningar och verktyg för identifiering och bedömning av risker.

Anvisningen beskriver, på en allmän nivå, anvisningar för hur man skapar och förvaltar ett riskhanteringssystem för företag samt de riskhanteringsarrangemang som förutsätts av en AEO-aktör. Kraven på en AEO-aktörs riskhantering grundar sig på de förpliktelser som beskrivs i AEO-riktlinjerna samt i ifyllningsanvisningarna för AEO-självutvärderingsformuläret.

AEO-aktörens riskhanteringssystem

En AEO-aktör ska i sina policyer/strategier ange som mål att följa tullreglerna och säkra sin del av leveranskedjan. AEO-riktlinjerna förutsätter att sökanden har antingen gjort eller låtit ett säkerhetsföretag göra en dokumenterad hot- och riskbedömning. Om sökanden inte kan uppvisa en sådan bedömning för tullmyndigheten, är det möjligt att det automatiskt rekommenderas att ansökan avslås.

AEO-aktörens riskhanteringssystem ska uppdateras regelbundet. Uppdateringsbehovet fastställs beroende på situationen: t.ex. med jämna mellanrum samt när det sker ändringar i företagets operationer och/eller personal. Aktören ska kunna bevisa att riskbedömningen och -hanteringen sker planmässigt och regelbundet.

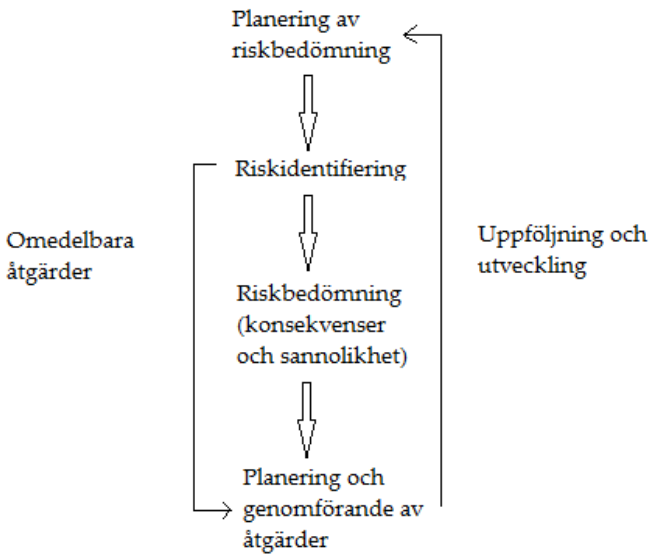

Bild: Riskhantering är en process i ständig utveckling.

Riskhanteringsansvar vid företaget

Riskhanteringsprocessen grundar sig på de mål som den högsta ledningen har satt för riskhanteringen, och därtill kan man beakta t.ex. lagkrav, standarder samt krav som ställts av utomstående. I riskbedömningsarbetet kan man i tillämpliga delar anlita utomstående experter, men att organisera riskhanteringen och att förankra sakerna i praktiken är företagets interna process.

AEO-aktören ska ha en namngiven person eller enhet (beroende på hur stor och komplex organisationen är), som svarar för bedömning av risker och hot samt för införande och bedömning av interna övervakningsåtgärder och andra åtgärder.

Identifiering av risker vid företaget

I början av riskbedömningsprocessen ska företaget på ett så omfattande sätt som möjligt försöka fastställa vilka saker som är viktiga för dess verksamhet (t.ex. människor, information, egendom, rykte). Utgående från de värden som ska skyddas kan företaget identifiera hot, dvs. risker, mot värdena. Företaget behöver anvisningar och verktyg för det praktiska riskbedömningsarbetet. Identifiering och hantering av risker är viktigt oberoende av företagets storlek, eftersom små företag i många hänseenden kan vara mer sårbara än stora.

Klassificering av risker underlättar både riskidentifiering och riskhantering. Riskerna kan indelas i riskslag utgående från deras natur och inverkan. Exempel på typiska riskslag: personrisker, avbrottsrisker, transportrisker, affärsrisker, egendomsrisker, brottsrisker, informationsrisker, ansvarsrisker gällande verksamheten, produktansvarsrisker och miljörisker.

Betydande risker för en AEO-aktör är t.ex. smuggling av olagliga varor, förorening av produkter, olovligt intrång i aktörens lokaler (anläggningar) eller i lokaler där exportvaror och information förknippad med dem förvaras eller hanteras. AEO-aktörens bedömning av säkerhets- och skyddsrelaterade risker och hot ska omfatta alla lokaler som har betydelse för den ekonomiska aktörens tulltransaktioner. Vid riskbedömningen ska följande delområden beaktas till den del de är förknippade med aktörens operationer:

Verifieringskedja för uppgifter samt tullrutiner och logistiksystem
- skattemässiga hot
- tillförlitlighet i information om tullverksamheter och logistiken för varorna
- en synlig verifieringskedja och förebyggande och upptäckt av bedrägerier och fel

Informationssäkerhet:
- dator- och IT-system
- redovisning och dokument

Fastighets- och lokalsäkerhet samt tillträdeskontroll
- säkerhetshot mot lokaler, byggnader och varor
- säkerhetsincidenter som skett nyligen (=säkerhetsavvikelser)

Lastenheter och logistik
- varor som sökanden hanterar, transporterar (transport, lastning, lossning, lastenheter) eller säljer

Personalsäkerhet
- personalen, personalens säkerhetsmedvetande
- anställning, användning av tillfälligt anställda, underleverantörsarbete, avslutande av anställning

Säkerhetskrav gällande affärspartner och externa tjänster
- avtalsarrangemang med affärspartner som deltar i leveranskedjan

Identifiering av risker förutsätter samarbete mellan olika delar av organisationen. Det kan löna sig att också andvända sig av befintliga färdiga riskanalysmetoder. Alla risker kan inte upptäckas genom en metod, utan avsikten är att utnyttja olika metoder i behövlig omfattning i riskidentifieringsarbetet. Föremålet för analysen ska vara tydligt begränsat och lagom stor, dvs. man ska bedöma t.ex. en funktion eller en avdelning åt gången. Nedan finns några exempel på möjliga riskanalysverktyg- och metoder:

- Workshop-metoden: man identifierar risker i team (per funktion, arbetsuppgift, projekt, avdelning osv.) Användning av färdiga checklistor (t.ex. SRHY:s sårbarhetsanalys): för varje risk fastställer man om den gäller den egna verksamheten.
- Analys av potentiella problem (POA-analys)
- Scenariemetod: man har som syfte att identifiera hotsituationer genom att gå igenom logiskt framskridande händelseförlopp i samarbete med målområdets experter
- Intervjuer, befintliga material (tidigare riskbedömningar, planritningar, brandsynsprotokoll, räddningsplaner, föremålets skadeuppgifter, tekniska uppgifter)
- Uppföljning av avvikelser: bakom upptäckta problem ligger ofta orsaker till risker

Vad gäller avtalspartner ska det beaktas att en AEO-aktör som utlokaliserar sina operationer ska känna till riskerna som gäller utlokaliseringsåtgärder samt vidta behövliga åtgärder för att motarbeta dessa risker. För Tullen ska aktören också lägga fram bevis gällande riskhantering av utlokaliserade operationer.

Riskidentifierings- och bedömningsprocessen ska införlivas i företagets dagliga verksamhet. Att teoretiskt gå igenom risklistorna med jämna mellanrum, t.ex. en gång om året räcker inte, utan att iaktta och bedöma risker gällande företagets olika operationer ska vara en ständig process. Med hjälp av tydliga riskhanteringsanvisningar kan företagets anställda i realtid beakta och bedöma risker förknippade med sina arbetsuppgifter samt rapportera om dem på behörigt sätt.

Företagets riskbedömning ska gälla alla lokaler och operationer som har betydelse för företagets tullverksamheter (information och varor gällande tullverksamheter och logistiken för varorna hanteras). Risker gällande företagets gemensamma operationer kan bedömas på ett centraliserat sätt (t.ex. risker gällande avtalspartner), men risker gällande lokalsäkerhet och andra risker gällande operationer som utförs lokalt ska bedömas för varje driftställe. Riskbedömningarna för varje driftställe ska också dokumenteras.

Systemet för rapportering av avvikelser är nära förknippat med riskhanteringssystemet. ”Nära ögat”-situationer är exempel på s.k. ”tyst kunskap”, och användning av den kan hjälpa att identifiera nya risker. För att kunna identifiera risker i praktiken ska AEO-aktören ha en skriftlig beskrivning/skriftliga anvisningar om organisationens rutiner för rapportering av avvikelser. Rapportering och hantering av säkerhetsavvikelser är en viktig del av riskidentifieringsprocessen, så rutinerna för rapportering av avvikande situationer borde kopplas till riskhanteringssystemet.

Bedömning av risker

Aktören ska på ett övergripande sätt försöka identifiera de risker som är förknippade med dess operationer och hantera de identifierade riskerna i sin hot- och riskbedömning. Vid riskbedömningen bedöms hur troligt det är att de identifierade riskerna förverkligas och vilka konsekvenser det skulle få.

De identifierade riskerna bedöms på lämplig nivå (t.ex. med en tre- eller femgradig skala). Genom att bedöma sannolikheten av att riskerna förverkligas och konsekvenserna kan man bedöma riskens storlek. Det är viktigt att bedöma riskerna noga, så att man kan planera riskhanteringsåtgärderna korrekt. Om t.ex. konsekvenserna bedöms på ett inkonsekvent sätt kan hela riskbedömningen bli förvrängd.

Bekämpning av identifierade risker

Utifrån riskbedömningen planerar man eventuella motåtgärder för riskhantering. Alla upptäckta risker går inte att eliminera, men man kan hantera dem t.ex. genom att minska, förflytta eller acceptera dem. Det väsentliga är att först när riskhanteringen genomförs i form av åtgärder är det möjligt att eliminera, minska eller förflytta risker.

Exempel på åtgärder för hantering av risker:

- Tekniska åtgärder: lösningar gällande apparater eller arbetsutrymmen, förbättrad skydd, larmsystem, utveckling av service och underhåll
- Utveckling av organisationens verksamhet: upprättande av anvisningar, förbättrad kommunikation, utveckling av uppföljning, mer specifik ansvarsfördelning
- Utveckling av de anställdas handlingsmöjligheter: utveckling av verktyg, inskolning, utbildning, anvisningar

För att bekämpa och minska risker ska de planerade åtgärderna i tillämpliga delar förankras hos både ledningens och personalens verksamhet. Företaget fastställer behovet av riskhanteringsåtgärder och fattar besluten själv, men vid planering och genomförande av åtgärderna kan det finnas ett behov av att anlita externa tjänsteleverantörer (t.ex. i fråga om olika tekniska åtgärder).

Det går inte att eliminera alla risker, så man ska också förbereda sig att en risk kan förverkligas. I fall där det inte är möjligt att påverka orsakerna till en risk kan det vara nödvändigt att koncentrera sig på att minska konsekvenserna av en risk t.ex. med hjälp av kontinuitets- och återställningsplanering. I riskhanteringssystemet ska alltså finnas anvisningar för skadesituationer samt en återställningsplan för avvikande situationer. På så sätt försöker man hålla konsekvenserna av en förverkligad risk så små som möjligt och säkerställer att verksamheten störs så lite som möjligt också i problemsituationen.

Vad gäller förverkligade risker ska man också se till att följa situationen och lära sig av händelserna. Med hjälp av inträffade skador och ”nära ögat”-situationer kan man avslöja brister i företagets verksamhet och säkerhetsarrangemang, och sedan beakta dem i riskbedömningsarbetet.

Källor som kan ge en AEO-aktör stöd i uppbyggandet av ett riskhanteringssystem:

- Kraven på en AEO-aktörs riskhanteringssystem finns i AEO-riktlinjerna, kapitel 3.III.6.1 Den ekonomiska aktörens riskhantering. Till stöd för bedömningen av kartlagda risker kan man använda sig av AEO COMPACT-modellen, som beskrivs i AEO-riktlinjerna (3.III.6.2. Tullens riskanalys och revision, Kartläggning av risker och AEO COMPACT-modellen).

- Utöver AEO-riktlinjerna lönar det sig att ta del av de förklarande anmärkningarna till AEO-självutvärderingsformuläret gällande självbedömning.

- Bilaga 2 ”Hot, risker och möjliga lösningar” till AEO-riktlinjerna ger exempel på hurdana risker en AEO-aktör borde beakta och hantera i sin verksamhet.

Mera information: aeo@tulli.fi