HEDEMORA KOMMUN	**STYRDOKUMENT**	Sida 1(11)
Skapad av: Ann-Christine Östlund Bäckehag	Datum 2020-11-23	Diarienummer: KS711-20 003
	Giltighet fr o m: 2021-02-16	Senast reviderad: -
Godkänd/antagen av: Kommunfullmäktige den 16 februari 2021 § 22.		
Dokumentansvarig: Kommunsekreterare		

Riktlinje för intern kontroll

Dok. Kategori:	Riktlinje
Stadie:	Beslutad
Gallring:	Bevaras
Kort beskrivning:	Riktlinje för internkontroll

Riktlinje för internkontroll

Denna riktlinje kompletterar det av kommunfullmäktige antagna reglementet för intern kontroll.

1. Inledning

En kommun är en offentlig verksamhet vilket innebär att kommunen har ett helhetsansvar gentemot invånare och medarbetare. Intern kontroll handlar om tydlighet, ordning och reda. Det handlar om att säkerställa att det som ska göras blir gjort på det sätt som det är tänkt. Denna riktlinje anger hur granskningen ska bedrivas.

Syftet med intern kontroll är att stödja och styra nämndens organisation i dess strävan att disponera tillgängliga resurser så effektivt som möjligt för att uppnå fastställda mål, upprätta en riktig och fullständig redovisning av ekonomiska transaktioner inom gällande regelverk samt säkerställa god ekonomisk hushållning.

Arbetet med intern kontroll är ett stöd för att säkerställa att kommunens verksamhet bedrivs ändamålsenligt, effektivt och rättssäkert och därför behöver arbetet vara integrerat i verksamhetens dagliga arbete. Det är ett led i kommunens arbete med ständiga förbättringar, vilket innebär att planera, genomföra, utvärdera och förbättra verksamhetens rutiner, processer och system. Det är viktigt att utvärdera verksamheten på ett strukturerat och kontinuerligt sätt.

Nämnden ska årligen upprätta en internkontrollplan och en åtgärdsplan. Som grund för internkontrollplanen ska risk- och väsentlighetsanalyser genomföras. Nämnden ska försäkra sig om att granskningen enligt internkontrollplanen genomförs och vid behov vidta åtgärder som säkerställer att den interna kontrollen är tillräcklig. Vid misstanke om brott ska nämnden utan dröjsmål vidta åtgärder.

Utifrån en risk- och väsentlighetsanalys ska nämnden välja ut ett antal rutiner/processer/system som särskilt ska granskas under nästkommande verksamhetsår för att verifiera att mål uppnås samt att styrdokument och fastlagda kontroller verkligen upprätthålls/genomförs.

2. Intern kontroll

En plan för intern kontroll ska upprättas årligen och minst innehålla:

- Vad ska kontrolleras? (rutin/process/system och kontrollmoment)
- Risknivå
- Vad ska åstadkommas med kontrollen? (kontrollmål)
- När ska kontrollen genomföras?
- Hur ska kontrollen genomföras? (metod och frekvens)
- Vem ska utföra kontrollen? (ansvarig)
- Hur, när och till vem ska resultatet av kontrollen rapporteras?

Blankett för intern kontroll, se nedan

2.1 Uppföljningsrapportens innehåll

- En sammanfattning av nämndens interna kontrollarbete
- Vilken rutin/process/system som avses
- Kontrollmoment
- Beskrivning av hur utförandet av respektive kontrollmoment har gått till
- Resultat av respektive kontrollmoment
- Åtgärder som nämnden avser att vidta och tidplan för åtgärd.
- Det ska framgå om respektive kontrollmoment ska med i nästa års interna kontrollplan. Om nämnden inte anser att ett bristfälligt moment behöver med i nästa års interna kontrollplan ska detta motiveras.

3. Risk- och väsentlighetsanalys

Det finns alltid en risk att oönskade situationer och oegentligheter kan förekomma i verksamheten. Sådana situationer påverkar möjligheten att nå de mål som satts upp. Alla risker kommer inte helt att kunna elimineras, men intern kontroll ska bidra till att minimera dem.

Det finns stora fördelar med att arbeta med risk- och väsentlighetsanalyser:

- Vi lär oss hantera risker.
- Vi får fram en realistisk bild av verkligheten.
- Vi blir medvetna om riskerna.
- Vi gör en realistisk och trovärdig värdering av riskerna

Följande frågor är stöd vid en risk- och väsentlighetsanalys:

- Vad är uppdraget, våra viktigaste rutiner/processer/system och mål?
- Vilka rutiner/processer/system behövs för fullständig kontroll? Vilka risker finns?
- Vad får absolut inte hända? Vilken beredskap finns?
- Vad blir konsekvensen om det händer?

Genom att utföra risk- och väsentlighetsanalyser så tydliggörs vad som kan komma att påverka verksamheten. Hur sannolikt är det att det händer och hur allvarligt (väsenlighet) är det i så fall. Höga värden i analysen ger anledning till fortsatt analys om bakomliggande orsaker och eventuella åtgärder för att förhindra att risken blir verklighet.

3.1 Åtgärdsplan

Vad gör vi åt riskerna? Hur kan vi behandla risker?

Vi kan:

- Undvika/eliminera
- Reducera/reducera sannolikheten/minska konsekvenserna
- Bibehålla/acceptera
- Överföra – skaffa sig en försäkring och överföra risken till annan

Man bör naturligtvis i första hand helt eliminera risk. Men då detta inte alltid är möjligt blir nästa steg att försöka skydda emot riskerna och reducera desamma. Om man tvingas bibehålla/acceptera riskerna, ska man hitta sätt hur man ska hantera kvarstående risker på bästa sätt för att skydda verksamheten.

3.2 Arbetssätt för hantering av risker

Intern kontroll görs på ordinarie rutiner, processer och system som förekommer i verksamheten. Att inom ramen för ett internkontrollarbete granska alla rutiner, processer och system inom en organisation skulle ge en mycket säker verksamhet, men kräva mycket tid och resurser. Mot bakgrund av detta måste vissa kontrollmoment väljas ut. För att kunna välja ut kontrollmomenten, och agera utifrån det viktigaste i planeringsarbetet, ska en risk- och väsentlighetsanalys årligen tas fram inom respektive verksamhetsområde och sedan sammanfattas i en nämndsövergripande risk- och väsentlighetsanalys.

Denna risk- och väsentlighetsmetod består av sex steg:

- **Steg 1 – Identifiering av risker**. Dokumentera rutiner, processer och system som anses som ett riskområde och definiera de väsentliga rutinerna, processerna och systemen. Beskriv händelser och situationer som kan få konsekvenser för verksamheten om risken realiseras, brainstorming.
- **Steg 2 – Sammanställning och gruppering av riskerna.**
- **Steg 3 – Bedöm riskerna**. Genomför risk- och väsentlighetsanalys på de olika riskområden som tagits fram. En bedömning görs av risken utifrån sannolikhet att den inträffar och konsekvensen om så sker. Detta genererar ett riskvärde (riskvärde = S x V - sannolikheten multiplicerat med konsekvensen/väsentlighet för att en risk inträffar), som man sedan kan sortera och prioritera alla risker utifrån. Ju högre riskvärde desto allvarligare är risken för verksamheten och ju högre bör den prioriteras/rangordnas i åtgärdsplanen. Av de risker som framkommit fattas beslut om vilka man ska arbeta vidare med. Parallellt dokumenteras även åtgärder som behövs för att förbättra och säkerställa kritiska rutiner, processer och system som inte hanteras i intern kontroll samt åtgärder om det upptäcks att kontrollmoment saknas.
- **Steg 4 – Dokumentera kontrollmoment** beträffande de risker man väljer att hantera. Kontrollmoment tas fram för att säkerställa att identifierade risker inte faller ut. Ett kontrollmoment avser en aktiv handling eller aktivitet som genomförs löpande inom en process för att hantera en specifik risk, vilket också skapar en spårbarhet som kan ligga till grund för en senare granskning. Notera att kontrollmoment alltså är en del av den dagliga och reguljära rutinen/processen/systemet och inte något som genomförs in den interna granskningen eller av revisionen. Kontrollmomentet är facit för hur verksamheten borde arbeta för att hantera en viss risk till vardags.
- **Steg 5 – Prioritera och välj ut några kontrollmoment som ska kontrolleras** under kommande år. Valda kontrollmoment redovisas för nämnden i enlighet med kommunens årligen fastställda tidplan för styrprocesser. Observera att kommunstyrelsen varje år antar kommunövergripande kontrollmoment.
- **Steg 6 – Intern kontrollplan och kontrollaktiviteter (åtgärdsplan)** redovisas till nämnden i början av varje år. Granskning ska ske för att säkerställa att kontrollmoment genomförs som förväntat i verksamheten, att rutiner, processer eller system är förstådda och följs i verksamheten eller något annat specifikt som efterfrågas av nämnden. Granskning är en revisionsliknande process för att granska att den ordinarie verksamheten fungerar som förväntat.
- **Steg 7 – Utför kontroll enligt plan**
- **Steg 8 – Redovisa genomförd kontroll och resultat med förslag till åtgärd till nämnden.** Redovisningsrapporten ska godkännas och beslutas i nämnden. Uppföljningsrapport angående den genomförda interna kontrollen samt nämndens

beslut ska skickas till kommunstyrelsen senat en månad innan årets sista kommunstyrelsemöte.

- **Steg 9 – Uppföljning och utvärdering.** Kontinuerlig uppföljning av bestämda åtgärder dokumenteras och redovisas till nämnden när de slutförts.

3.3 Kontrollaktiviteter

Ett sätt att motverka, minimera och eliminera risker är att göra kontroller, vilka kan vara förebyggande, upptäckande, manuella eller automatiska.

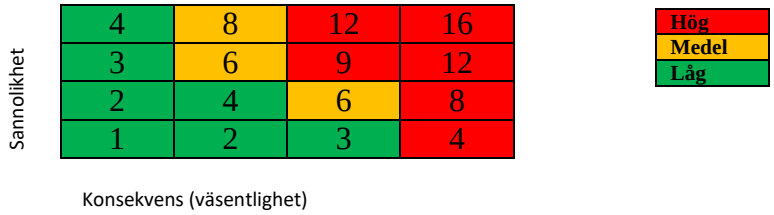
- Utförs arbetet enligt plan?
- Finns tydliga rutiner och ansvar?
- Följs fattade beslut?
- Är besluten aktuella?

3.4 Information och kommunikation

När medarbetare har rätt information vid rätt tillfälle så skapar det goda förutsättningar för korrekt agerande. Punkter att ta hänsyn till kan vara:

- Är styrdokument och informationsmaterial uppdaterade och lätta att förstå?
- Kommuniceras beslut på ett pedagogiskt sätt till exempel genom enkla rutiner/vägledningar?
- Finns en ändamålsenlig och effektiv struktur för rapportering och uppföljning?
- Hur tillvaratas erfarenheter och hur delas information?

3.5 Bedömning av risker



Om riskvärdet blir 9 poäng eller högre eller om konsekvenserna bedöms som 4:a ska risken med i internkontrollplan och kontrollmoment alltid anges.

Risk kan formuleras som sannolikheten för att fel, misskötsel, brister i måluppfyllelse i olika grad kan uppstå.

Väsentlighetsgrand kan uttryckas som ekonomiska, politiska, mänskliga och verksamhetsmässiga konsekvenser för nämnden eller för den enskilde som kan uppstå vid brister i hantering av ekonomi och/eller verksamhet eller vid bristande måluppfyllelse.

Vilka delar av verksamheten som är mer väsentlig än andra avgörs med avseende på ekonomisk omfattning, nytta för brukarna etc. Riskerna för fel och brister är ofta större vid förändringar i verksamhet, organisation, rutiner, processer och system med mera. Internkontrollen får inte bli orimligt dyr eller ett självständigt ändamål i förhållande till vad den ger i resultat, utan vägas mot de konsekvenser som blir om ett fel uppstår.

I följande tabell redovisas en bedömning av risker; konsekvenser/väsentlighetsgrad och dess sannolikhetsgrad (risk- och konsekvensbedömning).

Konsekvens-nivåer	Väsentlighetsgrad/Allvarlighetsgrad	Sannolik-hetsgrad	Risk- och konsekvensbedömning
1 - Ingen, mycket liten, försumbar eller liten risk	***Internkontroll*** Verksamheten påverkas inte alls eller så lite att den effektiva påverkan är försumbar. Nämnden/bolaget har inga svårigheter att utöva sin verksamhet. Ingen eller mindre skada och/eller påverkan. Inga svårigheter för verksamheten att nå målen. ***GDPR*** De registrerade påverkas inte alls eller så lite att den effektiva påverkan är försumbar. Den registrerade har inga svårigheter att utöva sina fri- och rättigheter. Ingen eller endast försumbar fysisk-, ekonomisk-, social- eller integritetsrelaterad påverkan/skada.	**1 – Obefintlig/ mycket liten/ osannolik/ försumbar risk**	Det är inte möjligt eller det finns en mycket liten risk, är osannolikt/inte troligt att risken förverkligas. Inträffar mycket sällan - mer sällan än vart femte år Det är inte möjligt för källan att förverkliga risken genom att utnyttja systemets egenskaper. Ex. stöld av pappersdokument från ett rum som skyddas av inpasseringssystem med två faktorer (chipkort och Pin-kod)
2 - Begränsad/ måttlig risk	***Internkontroll*** Verksamheten påverkas väsentligt, men man kan ta enkla steg för att eliminera påverkan. Nämndens/bolagets verksamhetskvalitet och förtroende kan inte garanteras. Verksamheten kan uppleva lindriga besvär, men endast måttlig ekonomisk eller verksamhetsmässig påverkan. Begränsad skada och/eller påverkan. Inga märkbara större svårigheter för verksamheten att nå målen. ***Infosäkerhet/GDPR*** Med måttlig negativ påverkan avses t ex förlust av konfidentialitet, riktighet eller tillgänglighet som för egen eller annan verksamhet kan a) orsaka en minskning i förmågan att lösa verksamhetsuppgifterna i en utsträckning och varaktighet innebärande att verksamhetens primära uppgifter kan fullföljas, men att effektiviteten är påvisbart reducerad; b) resultera i mindre skador på verksamhetens tillgångar; c) resultera i måttliga ekonomiska förluster; d) förorsaka begränsad negativ påverkan på enskild individs rättigheter eller hälsa. ***GDPR*** De registrerade påverkas väsentligt, men de kan ta enkla steg för att eliminera påverkan. Den registrerades fri- och rättigheter kan inte garanteras. Den registrerade kan uppleva lindriga besvär, men endast måttlig ekonomisk eller social påverkan.	**2 – Liten/ mindre sannolik/ begränsad risk**	Det är mindre sannolikt eller svårt att risken förverkligas. Liten risk - Inträffar sällan – oftare vart femte år men mer sällan än varje år. Skada/avvikelse närmsta året. Det är svårt för källan att förverkliga risken genom att utnyttja systemets egenskaper. Ex. stöld av pappersdokument från ett rum som skyddas av inpasseringssystem med en faktor (chipkort).

3 - Betydande/ kännbar/ signifikant risk	***Internkontroll*** Verksamheten påverkas väsentligt och den måste vidta omfattande och allvarliga åtgärder för att eliminera påverkan. Nämndens/bolagets kontroll över verksamheten hindras. Sannolik risk för negativ ekonomisk, förtroende, kvalitets- och verksamhetsmässig påverkan hos nämndens/bolagets verksamhet. Allvarlig skada och/eller påverkan. Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vida extraordinära åtgärder). ***Infosäkerhet/GDPR*** Med betydande negativ påverkan avses t ex förlust av konfidentialitet, riktighet eller tillgänglighet som för egen eller annan verksamhet kan a) orsaka en signifikant minskning i förmågan att lösa verksamhetsuppgifterna i en utsträckning och varaktighet innebärande att verksamhetens primära uppgifter kan fullföljas, men att effektiviteten är påtagligt reducerad; b) resultera i betydande skador på verksamhetens tillgångar, c) resultera i betydande ekonomiska förluster, eller d) förorsakar betydande negativ påverkan på enskild individs rättigheter och hälsa. ***GDPR*** De registrerade påverkas väsentligt och de måste vidta omfattande och allvarliga åtgärder för att eliminera påverkan. Den registrerade hindras utöva kontroll över sina personuppgifter. Trolig/sannolik risk för ekonomisk eller social påverkan hos den registrerade om åtgärder inte vidtas.	**3 - Stor/ möjlig/ signifikant risk**	Det är möjligt att risken förverkligas. Stor risk - Inträffar regelbundet – oftare än varje år men mer sällan än minst en gång per månad. Skada/avvikelse närmsta månaden. En allvarlig ekonomisk skada är en sådan som kan klaras av utan att hamna i obestånd, men kommer att leda till kraftfulla omprioriteringar. Risk för negativ publicitet eller negativ debatt kring organisationen som är en längre rapportering i lokalpress (även sociala medier) Det är möjligt för källan att förverkliga risken genom att utnyttja systemets egenskaper. Ex. stöld av pappersdokument från ett kontor utan inpasseringssystem men med registrering hos ex kundtjänst/reception för att få tillträde.
4 – Allvarlig/ maximal risk	***Internkontroll*** Nämndens/bolagets verksamhet påverkas väsentligt och den kan inte vidta åtgärder för att eliminera påverkan. Påtaglig risk för stora konsekvenser för verksamheten genom exempelvis stor ekonomisk förlust, stora kvalitetsbrister i verksamheten, förtroendet skadas väsentligt eller annan betydande ekonomisk och verksamhetsmässig nackdel. Kan även innebära fara för liv och hälsa. Mycket allvarlig skada och/eller påverkan. Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästa omöjligt att fullfölja uppdragen. Röjande av informationen medför skada för rikets säkerhet som inte endast är ringa.	**4 – Mycket stor/ sannolik/ maximal risk**	Det är sannolikt och/eller lätt att risken förverkligas. Mycket stor risk - Inträffar ofta – oftare än en gång per månad. Skada/avvikelse oftare än närmsta månad. Risk kan leda till att organisationen kan komma på ekonomiskt obestånd. Risk för negativ publicitet eller negativ debatt kring organisationen som är rikstäckande längre rapportering (så kallat drev) från ett rikstäckande mediaföretag. (även sociala medier)

	Infosäkerhet/GDPR Med allvarlig/katastrofal negativ påverkan avses t ex förlust av konfidentialitet, riktighet eller tillgänglighet som för egen eller annan verksamhet kan a) orsaka en allvarlig begränsning i förmågan att lösa verksamhetsuppgifterna i en utsträckning och varaktighet innebärande att verksamheterna inte kan fullgöra en eller flera av sina primära uppgifter; **b)** resultera i omfattande skador på verksamhetens tillgångar; **c)** resultera i stora ekonomiska förluster, eller **d)** förorsaka allvarligt negativ påverkan på enskild individs rättigheter till liv och hälsa. ***GDPR*** De registrerade påverkas väsentligt och de kan inte vidta åtgärder för att eliminera påverkan. Påtaglig risk för stora konsekvenser/stora besvär för den registrerades fri- och rättigheter genom exempelvis diskriminering, identitetsstöd eller identitetsbedrägeri, stor ekonomisk förlust, skadat anseende eller annan betydande ekonomiskt och social nackdel. Kan även innebära fara för liv och hälsa.		Det är lätt för källan att förverkliga risken genom att utnyttja systemets egenskaper. Ex stöld av pappersdokument från en hotellobby/skrivbord.

De riskområden som bör analyseras är:

- ***Omvärldsrisker*:** Omvärldsrisker kan utgöras av större händelser som kan påverka nämndens verksamhet och mål. Till exempel befolkningsförändringen i kommunen som kan påverka nämndens verksamhet och statliga ersättningar/bidrag som förändras/riskeras att förändras.
- ***Finansiella risker*:** Brister som kan medföra vikande/uteblivna intäkter respektive oönskade eller oförutsedda kostnader. Kan även utgöras av likviditetsrisk, valutarisk, ränterisk, kreditrisk och operativa risker vilka hanteras enligt kommunens finanspolicy.
- ***Rapporterings- och/eller redovisningsrisker*:** Risker för att räkenskaperna inte är rättvisande eller tillförlitliga i övrigt är en redovisningsrisk. Bortfall av relevant information kan innebära att underlag och antaganden är felaktiga och kan leda till att beslut fattas på felaktiga grunder.
- ***Legala risker*:** Brister som kan leda till brott mot gällande lagstiftning. Legala brister är också brister i förhållande till kommunens styrdokument och exempelvis ny lagstiftning som kan/kommer att påverka nämndens verksamhet
- ***Informations- och ITsäkerhet och GDPR*:** Av kommunens dataskyddsstrategi och informationssäkerhetspolicy framgår bl a att verksamheterna ska säkerställa att invånarnas och medarbetarnas integritet skyddas och att informationsteknik ska nyttjas som har invånarnas förtroende. Brister i verksamhetens informationssystem och hantering kan få oönskade effekter och det är viktigt att definiera de system som har avgörande betydelse för verksamheten.
- ***Verksamhetsrisker*:** Alla brister som hotar förutsättningarna att genomföra verksamheten och nå uppställda mål, inkluderar även kvalitetsfrågor och att verksamheten inte bedrivs på ett kostnadseffektivt sätt
- ***Förtroenderisker*:** Brister som kan leda till att förtroendet för nämnden, förvaltningen och/eller kommunen skadas. Förtroendeskador uppstår ofta som ett resultat av brister inom

ovan nämnda risker eller i form av till exempel vidlyftig representation, mutor och bestickning.

HEDEMORA KOMMUN

INTERN KONTROLLPLAN 2019

Nämnd:
Antagen datum:

Målperspektiv (*Medarbetare, ekonomi, Invånare, Juridik, HR, upphandling etc)*	Kontrollmål (Vad ska åstadkommas/mål med kontrollen)	Kontrollmoment (Vad ska kontrolleras?)	Kontrollmetod/frekvens (Hur ska kontrollen göras och hur ofta?)	Riskvärde (sannolikhet x konsekvens)	Ansvarig (Vem är ansvarig för att kontrollen genomförs?)	När och var genomförs kontrollen?	Rapport till vem och hur och hur ofta rapporteras kontrollen

HEDEMORA KOMMUN

RISK- OCH VÄSENTLIGHETSANALYS TILL INTERN KONTROLLPLAN

Nämnd:
År:

Mål	Riskidentifiering	Riskvärdering	Riskbehandling

Mål/uppdrag som risken kopplar till	Beskrivning av risk/oönskad händelse	Huvudsaklig typ av risk	Sannolikhet	Konsekvens	Riskvärde	Åtgärder för att ta bort/minska risk	Ansvarig för åtgärder	När ska åtgärden vara utförd?