God praksis for å hindre eksterne misligheter

November 2005

Et notat fra FEEs Public Sector Committee (FEEs komité for offentlig sektor)

Oversatt til norsk i regi av NKRF med bistand fra DnR, Januar 2007

Dette notatet (januar 2007) er en norsk oversettelse av FEE Position Paper "Good Practice in Tackling External Fraud". Oversettelsen og tilretteleggingen av den norske versjonen er finansiert av NKRF. DnR har bistått NKRF med kvalitetssikringen av oversettelsen.

Den europeiske revisororganisasjonen Fédération des Experts Comptables Européens (FEE) representerer revisjonsprofesjonen i Europa. 44 revisorforeninger fra 32 land er medlemmer i FEE. DnR er Norges medlem i FEE. FEEs medlemsforeninger representerer mer enn 500.000 revisorer i Europa.
Fédération des Experts-Comptables Européens, Avenue d'Auderghem, 22-28, B-1040 Brussels
Tlf. +32 2 285 40 85, secretariat@fee.be, www.fee.be

Norges Kommunerevisorforbund (NKRF) er en faglig interesseorganisasjon og et serviceorgan for alle som arbeider med revisjon av eller tilsyn med kommunal og fylkeskommunal virksomhet. NKRFs formål er å fremme en sunn utvikling av revisjon og tilsyn i kommunal sektor til beste for kommuner og fylkeskommuner. NKRF har tilnærmet full medlemsoppslutning fra virksomhetene som reviderer kommunene og fylkeskommunene og ca. 70 % av virksomhetene som ivaretar sekretærtjenester for kontrollutvalgene i kommuner og fylkeskommuner.
Norges Kommunerevisorforbund, Postboks 1417 Vika, 0115 Oslo, Tlf. 23 23 97 00, post@nkrf.no, www.nkrf.no

Den norske Revisorforening

Den norske Revisorforening (DnR) er en interesse- og kompetanseorganisasjon for statsautoriserte og registrerte revisorer. DnRs formål er å representere og ivareta medlemmenes generelle faglige, yrkesmessige og sosiale interesser ved å være en høyt anerkjent kompetanse- og interesseorganisasjon. DnR har i underkant av 4.000 medlemmer.
Den norske Revisorforening, Postboks 5864 Majorstuen, 0308 Oslo, Tlf. 23 36 52 00, firmapost@revisornett.no
www.revisornett.no

INNHOLD

INNLEDNING

1. Dette notatet[1] konsentrerer seg om eksterne misligheter hvor tredjeparter, for eksempel organiserte kriminelle grupper, uærlige selskaper eller personer, tar penger fra en offentlig etat eller en offentlig organisasjon, enten ved å motta pengebeløp de ikke er berettiget til, eller ved å la være å betale penger de skylder. Misligheter kan være opportunistiske forsøk fra enkeltkunder eller -selskaper på å oppnå en økonomisk fordel. Beløpene i hvert enkelt tilfelle kan være små, men samlet kan de utgjøre betydelige tap av offentlige midler dersom det dreier seg om mange tilfeller. I den andre enden av skalaen kan offentlige etater og organisasjoner rammes av mer systematiske og planlagte angrep fra organiserte kriminelle grupper. Disse kan være færre i antall, men tapet i hvert enkelt tilfelle kan være betydelig. I enkelte tilfeller kan bedragere samarbeide med virksomhetens egne medarbeidere. I tillegg til å underslå penger som kunne blitt brukt til offentlige tjenester, kan misligheter undergrave anseelsen til ærlige personer og selskaper og støtte aktivitetene til personer som er involvert i annen alvorlig kriminalitet. Alle offentlige etater og organisasjoner har et ansvar for å utarbeide retningslinjer for å forebygge misligheter for å vise de som vil bedra offentlig sektor, at slike handlinger er uakseptable og ikke vil bli tolerert.

2. Offentlige etater og organisasjoner er utsatt for et bredt spekter av risikoer for eksterne misligheter, som vist i figur 1. Revisorer i offentlig sektor må være oppmerksomme på disse risikoene. Det er også mange andre typer misligheter som begås av tredjeparter, blant annet av leverandører. I enkelte organisasjoner er eksterne misligheter et betydelig og vedvarende problem, mens det i andre kan forekomme fra tid til annen.

Figur 1: Eksempler på mangfoldet av misligheter mot offentlig sektor

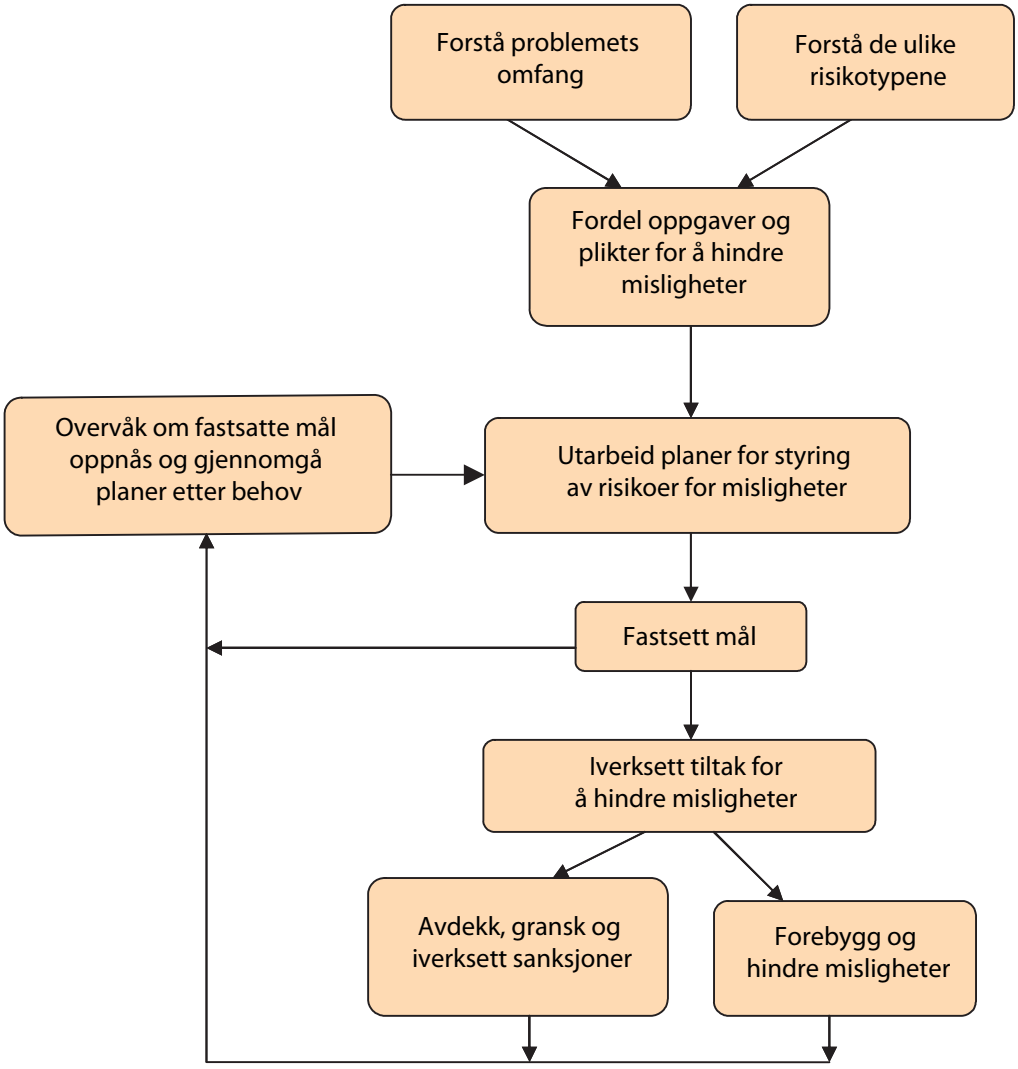
- Personer eller selskaper som krever støtte de ikke har krav på.
- Personer som arbeider svart og ikke betaler skatt av inntektene sine. De kan også motta behovsprøvd støtte som de ikke har krav på.
- Selskaper som driver svart virksomhet og ikke leverer pliktige opplysninger om sin virksomhet eller betaler skatt eller merverdiavgift.
- Medarbeidere som samarbeider med kriminelle for å bedra et offentlig organ.
- Alvorlig kriminelle som skaffer seg store beløp, for eksempel ved å ikke betale avgifter på tobakk, alkohol, bensin og diesel. De kan etablere tilsynelatende lovlige selskaper, men med den hensikt å bedra skattemyndighetene, for eksempel ved å unndra merverdiavgift. De kan også begå organisert bedrageri mot trygdesystemet ved hjelp av stjålne eller forfalskede betalingsmidler og ved å motta stønad på falskt grunnlag.
- Systematisk utnyttelse av svakheter i offentlige sosiale og andre ordninger for å motta fordeler på falskt grunnlag eller for å unngå innbetalinger, blant annet:

1) Dette notatet er basert på en veiledning utgitt av riksrevisjonen i Storbritannia og det britiske finansdepartementet under tittelen "Good Practice in Tackling External Fraud".

- Stønadsmottakere som ikke oppgir all inntekt eller formue, eller som skjuler familiære omstendigheter for å få stønad som de ikke har krav på.
- Personer som får dekket utgifter til medisiner på falskt grunnlag.
- Personer som unnlater å betale årsavgift på bil.

3. Offentlige organisasjoner bør vurdere å utarbeide en tiltakspakke som er skreddersydd for hver enkelt type mislighet. Det finnes ingen angrepsmåte som passer for alle problemstillinger. Det kan imidlertid være nyttig å spre kunnskap om hvordan andre håndterer misligheter og hvilke tiltak som fungerer andre steder. Mindre organisasjoner bør vurdere om de kan tilpasse og anvende tiltak som brukes av større organisasjoner for å hindre eksterne misligheter. Notatet beskriver en integrert strategisk angrepsmåte som oppsummeres i figur 2.

Figur 2 viser hovedelementene i en integrert strategisk angrepsmåte for å hindre misligheter



4. Dette notatet er bygd opp på følgende måte:

   • Hvordan forstå og styre risikoene for eksterne misligheter (del 1)
   • Hvordan forebygge og hindre eksterne misligheter (del 2)
   • Hvordan avdekke og granske misligheter og iverksette sanksjoner (del 3)

   Punktene i begynnelsen av hver del er ment som en hjelp til å evaluere organisasjonens praksis. Dersom det ikke er iverksatt noen særskilte tiltak, må det vurderes hvorvidt dette er hensiktsmessig ut fra omstendighetene[2].

5. Vi håper at notatet vil være en nyttig referansekilde for ledere i offentlig sektor for å videreformidle andres erfaringer og gode praksis. Det er ikke ment å gi deg "alt du trenger å vite" for å hindre eksterne misligheter. Det ville kreve flere bind. Eksemplene i dette notatet brukes kun i illustrasjonsøyemed. Det kan være mange andre eksempler i bruk i andre offentlige organisasjoner.

2) Når misligheter drøftes, er hvitvasking av penger stadig oftere tema. Hvitvasking kan defineres som omdanning av utbytte som stammer fra straffbare handlinger for å skjule deres ulovlige opprinnelse. Dette notatet konsentrerer seg om forebygging og avdekking av misligheter og ikke om utbyttet av disse.

DEL 1: HVORDAN FORSTÅ OG STYRE RISIKOENE FOR MISLIGHETER

Det må vurderes hvorvidt organisasjonen:

- Har en strategisk angrepsmåte for å håndtere risikoer for misligheter.
- Anslår tapsomfanget knyttet til eksterne misligheter og, der det er relevant, utfører en egen risikovurdering.
- Identifiserer de områdene som er mest sårbare for risiko for misligheter.
- Kjenner til hvor høy risikoen for misligheter er, hvilke typer misligheter som er begått, hvem som begår dem, hvor ofte de begås og hvor store beløp det dreier seg om.
- Har en tiltakspakke for å håndtere tap som skyldes misligheter der disse er betydelige.
- Har satt seg mål med hensyn til å stabilisere (unngå videre økning av misligheter) eller redusere forekomsten av misligheter.
- Har tildelt oppgaver og plikter for håndteringen av risikoer for misligheter for å sikre at risikoene styres, tiltaksplaner iverksettes og tiltakenes effektivitet kontrolleres.

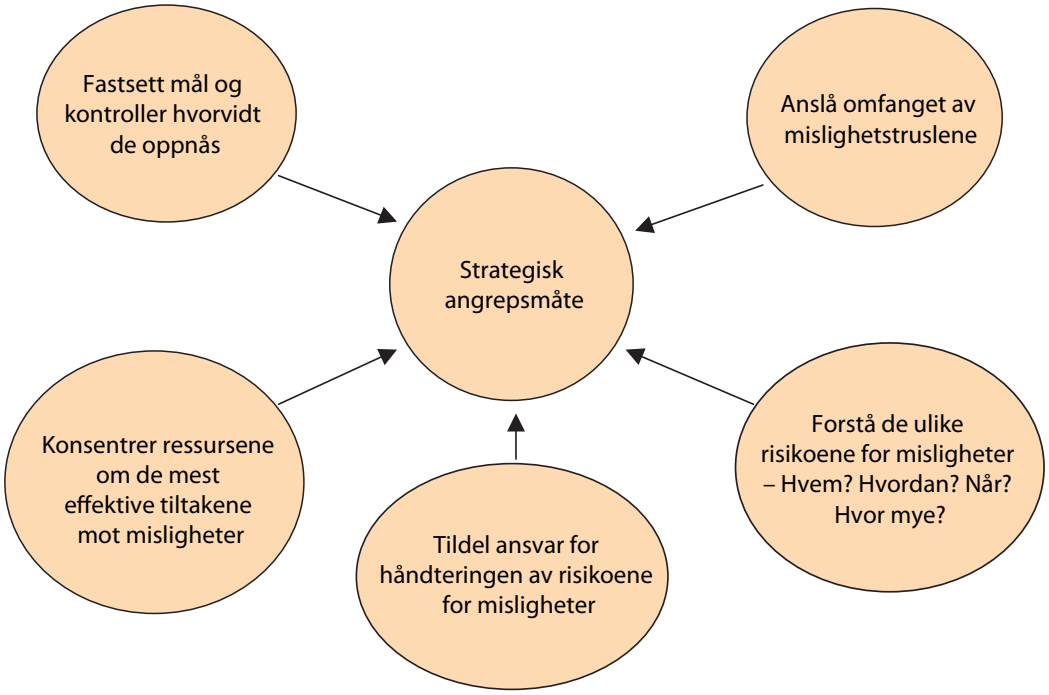
Denne delen av notatet omhandler hvordan disse problemstillingene kan håndteres og gir eksempler på hvordan andre har tatt tak i disse problemstillingene. Leseren må vurdere hvor hensiktsmessige tiltakene er ut fra egne forhold.

En strategisk angrepsmåte for å hindre eksterne misligheter

1.1 Noen offentlige organisasjoner har valgt en strategisk angrepsmåte for å forstå og styre risikoene for misligheter fordi dette:

- Hører med til god eierstyring. En viktig del av god eierstyring er en nøye vurdering av forretningsrisikoene. Risikoene for misligheter bør styres på samme måte som andre forretningsrisikoer og bør derfor gripes an på en systematisk måte både på organisasjons- og driftsnivå.
- Bidrar til å utvikle en rekke tiltak som utøver forholdsmessig og målrettet press på alle nivåer.
- Kan bidra til en kostnadseffektiv angrepsmåte for å hindre misligheter ved å fokusere på de områdene der risikoen er høyest og der tiltakene gir best uttelling. En strategisk angrepsmåte kan, om nødvendig, være et rasjonelt og solid grunnlag for å anmode om ytterligere ressurser til å bekjempe misligheter.
- Kan være en praktisk måte å videreformidle til medarbeiderne hva organisasjonen prøver å gjøre og hva som ventes av dem. Noen organisasjoner offentliggjør sine strategier for å informere allmennheten om at de har en nøye gjennomtenkt angrepsmåte for å hindre eksterne misligheter. Dette kan sende signaler til potensielle bedragere om at det er lite sannsynlig at de vil lykkes med å bedra organisasjonen. *Figur 3 viser hovedelementene i en strategisk angrepsmåte for å hindre misligheter.*

Figur 3 viser hovedelementene i en strategisk angrepsmåte for å hindre misligheter



1.2 Noen organisasjoner anvender en generell angrepsmåte for å hindre eksterne misligheter og noen tar for seg individuelle mislighetsrisikoer og utarbeider en strategi for hver enkelt. Andre håndterer misligheter innenfor en totalstrategi som tar sikte på å hindre tap fra alle typer regelbrudd. Den overordnede angrepsmåten tar hensyn til at det foreligger et "tapsspekter" som strekker seg fra utilsiktede kundefeil i den ene enden til bedrageri i den andre enden, med gråsoner imellom. Alle disse angrepsmåtene kan være hensiktsmessige avhengig av forholdene i den enkelte organisasjon og hvor langt den har utviklet sin angrepsmåte. Et fellestrekk er imidlertid at organisasjonene utvikler risikovurderingsverktøy for å avdekke risikoene for misligheter, sannsynligheten for at de skal forekomme, hvilke følger de har og hvordan risikoene kan styres. Disse verktøyene må evalueres for å fastslå hvorvidt de fortsatt er hensiktsmessige eller må oppdateres for å håndtere nye risikoer for misligheter.

Hvordan anslå omfanget av mislighetstruslene

1.3 Å utarbeide et anslag over omfanget av tap som skyldes misligheter, er et viktig første skritt i utviklingen av en strategi for å hindre eksterne misligheter. Anslått tapsomfang gir en pekepinn på innsparingspotensialet som kan bidra til å bestemme hvordan håndteringen av risikoer for misligheter skal prioriteres i forhold til annen ressursbruk. Estimatene gir et utgangspunkt for måling av tiltakenes effektivitet. Regelmessige beregninger kan hjelpe en organisasjon med å måle resultatene og hvorvidt trusselbildet endres. Det kan være forhold som medfører at en organisasjon ikke finner det hensiktsmessig å utarbeide totalestimater.

De vil allikevel kunne anvende en rekke teknikker, for eksempel utføre en dyptgående undersøkelse av et område der det foreligger mistanke om misligheter, for å få en bedre forståelse av trusselens omfang og art.

1.4 Noen vil hevde at:

- Det er for vanskelig å estimere tap knyttet til misligheter og at det er bortkastet å forsøke å gjøre det.
- Ressursene som brukes til å anslå tapsomfanget, heller bør brukes til å hindre misligheter, for eksempel ved å utføre flere granskninger.

Disse problemstillingene omhandles nærmere nedenfor.

Utarbeidelse av pålitelige estimater

1.5 Omfang av tap som skyldes misligheter og feil, kan estimeres ved hjelp av operasjonsanalyser og statistiske metoder. De to mest brukte metodene er ***statistisk modellering*** og ***stikkprøver***.

Statistisk modellering

1.6 Statistisk modellering er blitt brukt til å foreta generelle beregninger av omfanget av tap knyttet til misligheter, først og fremst tap av inntekter. Dette omfatter sammenligning av faktiske innbetalinger eller utbetalinger med de samlede innbetalinger eller utbetalinger som kan forventes ut fra andre kilder til data om aktivitetsnivået som evalueres.

1.7 Punkter som må tas i betraktning ved bruk av statistisk modellering er:

- De nødvendige dataene kan være ufullstendige. Modellen kan derfor benytte antakelser i et omfang som medfører en viss feilmargin i resultatene. Det er viktig å ta dette i betraktning når det skal treffes beslutninger om tiltak for å redusere tap.
- Ytterligere arbeid kan være påkrevd for å få et innblikk i hvem som begår mislighetene og hvilke tiltak som kan avskrekke dem. Dette kan omfatte mer dyptgående modelleringsarbeid.
- Det kan være behov for videre undersøkelser av årsakene til økninger eller nedganger i tapsomfanget og i hvilken grad dette skyldes iverksatte tiltak.

Stikkprøver

1.8 Tapsestimater kan utarbeides ved å kontrollere et representativt utvalg av tilfeller for å se hvorvidt misligheter forekommer og deretter ekstrapolere resultatene til hele populasjonen for å beregne det samlede omfanget av tap som skyldes misligheter på det aktuelle utgifts- eller inntektsområdet. Når konkrete tilfeller blir kontrollert, kan det være vanskelig å avgjøre om et avvik skyldes misligheter eller feil (uaktsomhet, skjødesløshet eller uvitenhet) som følge av de skjønnsmessige vurderingene som må foretas.

1.9 En nøkkelfaktor ved utarbeidelse av et estimat av tap som skyldes misligheter på et utgifts- eller inntektsområde, er graden av nøyaktighet som kreves. En høyere grad av presisjon gir mer pålitelige estimater (avgjørende for beregning av faktiske endringer i tapsomfanget over tid), men innebærer høyere kostnader siden antallet nødvendige stikkprøver vil være høyere. For noen organisasjoner kan det være tilstrekkelig å utarbeide et nasjonalt estimat. For andre kan det være nødvendig å også utarbeide estimater brutt ned på regioner.

Dette vil ha viktige konsekvenser for gjennomføringen av stikkprøvene og kostnadene, ettersom separate stikkprøver i hver region vil øke det samlede antallet stikkprøver som må kontrolleres.

Kostnader ved estimering av tapsomfanget

1.10 Som nevnt ovenfor, vil kostnadene ved estimeringen variere avhengig av:

- Hvor ofte beregningene foretas.
- Hvor mange stikkprøver som tas.
- Hvor mye arbeid det innebærer å kontrollere hver enkelt stikkprøve.
- Hvor mye arbeid det krever å validere resultatene.

1.11 For mindre organisasjoner kan et enkeltestimat eller en beregning som foretas med visse mellomrom, være tilstrekkelig. Det kan være en løsning å akseptere lavere presisjon med færre stikkprøver. Selv om resultatene da er mindre pålitelige, vil de gi en pekepinn på om fortsatt arbeid er ønskelig. Andre kan kreve kontinuerlige målinger for løpende å kunne beregne omfanget av tap som skyldes misligheter. Selv om dette innebærer høyere kostnader, gir det organisasjonen mulighet til å følge endringene i beregnet tapsomfang og i hvilke typer misligheter som begås, over tid.

1.12 Kostnadene kan fordeles over flere år ved å gjennomføre et rullerende estimeringsprogram. Et annet alternativ er å foreta én enkelt beregning (som eventuelt gjentas flere år senere) for å bekrefte hvorvidt omfanget av misligheter er betydelig. Dette kan være en nyttig metode dersom omfanget av misligheter antas å være av mindre betydning.

Forståelse av de ulike risikoene for misligheter

1.13 En offentlig organisasjon vil ikke være i stand til å utarbeide egnede tiltak mot misligheter kun basert på estimerte misligheter. De bør også helst vite:

- Hvilke typer misligheter som begås mot dem, hvor lenge de har pågått og hvilket økonomisk tap de har medført.
- Hvem det er som begår mislighetene, deres kjennetegn og atferd, hvor ofte de begår mislighetene, hvilke typer misligheter de begår, hvordan de gjør det og hvorvidt de er opportunistiske eller organiserte.

1.14 Undersøkelser av de mislighetstilfeller som er avdekket enten i forbindelse med gransking eller som resultat av stikkprøver som er foretatt for å beregne omfanget av tap, kan gi nærmere innsikt i disse spørsmålene. Større organisasjoner som står overfor alvorlige trusler, har også egne granskere og/eller gir noen i oppdrag å granske disse truslene nærmere. I den andre enden av spekteret er det noen organisasjoner som har få eller ingen nylige tilfeller av eksterne misligheter. Kontroll av et utvalg av saker eller en undersøkelse av mulige trusler kan bidra til å bekrefte om risikoen for misligheter er lav.

Konsentrasjon av ressursene om de mest effektive tiltakene mot misligheter

1.15 Det finnes ingen universell tiltakspakke som kan brukes av alle organisasjoner for å hindre misligheter. Tiltakene må tilpasses typen og omfanget av den trusselen som organisasjonen står overfor. For å avgjøre hvilke tiltak som skal iverksettes og i hvilket omfang, har noen organisasjoner vurdert hvilke besparelser de

kunne oppnå ved å målrette ressursene på en bedre måte. Besparelser kan oppnås på tre måter:

- Den direkte virkningen av å få tilbake midler som noen har tilegnet seg gjennom misligheter. Når tiltakene omfatter omfordeling av ressurser til eksisterende aktiviteter, kan organisasjonen se på de nåværende kostnadene/besparelsene som et grunnlag for å beregne utbyttet av å øke innsatsen mot misligheter. Når nye tiltak foreslås, er det god praksis å teste disse på forhånd for å finne ut hvordan de fungerer, eventuelt kan forbedres, samt vurdere tiltakenes sannsynlige effektivitet og typen besparelser som kan oppnås.
- Den forebyggende virkningen. Sannsynligheten for at de som tidligere er blitt avslørt skal begå ytterligere misligheter, blir mindre.
- Den avskrekkende virkningen på andre. Sannsynligheten for at andre vil begå misligheter blir mindre når de blir kjent med den økte innsatsen for å slå ned på misligheter. I praksis kan det være veldig vanskelig å anslå den avskrekkende virkningen med noen grad av nøyaktighet.

Fastsetting av mål og overvåking av hvorvidt de oppnås

1.16 Noen organisasjoner setter seg et antall mål for å stabilisere (unngå ytterligere økning av omfanget av misligheter) eller redusere omfanget av misligheter over en periode. Å konsentrere oppmerksomheten om totalnivået for misligheter eller tap, er en god måte å anslå måloppnåelsen på, og generelt en bedre målestokk enn antall avdekkede tilfeller av misligheter. Sistnevnte er vanskelig å tolke når man ikke kjenner det fulle omfanget av mislighetene. Andre målinger er nyttige kompletteringer til estimater på samlet tap som skyldes misligheter, for eksempel endringer i tapsomfanget regionalt, kostnadene ved tiltak mot misligheter sammenlignet med resultatet av tiltakene og prosentvis tilbakebetaling av tapte beløp.

1.17 Måloppnåelsesdata er ofte ikke tilgjengelige før lenge etter måleperioden på grunn av det omfattende arbeidet med å ta stikkprøver, kontrollere, beregne og validere resultatene. For å overvåke måloppnåelsen gjennom året, kan ledere bygge på resultatdata som et uttrykk for hvorvidt det er sannsynlig at man vil nå målene. Ledere kan for eksempel overvåke:

- Resultatene av driftskontroller av transaksjoner.
- Arbeidet med å granske misligheter og resultatet av dette.
- Antall og type sanksjoner som er iverksatt.
- Prosentvis tilbakebetaling av midler som noen har tilegnet seg gjennom misligheter.

Tildeling av ansvar for håndteringen av risikoene for misligheter

1.18 Ansvaret for å hindre misligheter og håndteringen av risikoer for misligheter begynner hos den øverste ledelsen. På dette nivået tildeles overordnet ansvar for å håndtere risikoene for misligheter og ansvar for styring av individuelle risikoer for misligheter. Selv om alle medarbeidere har en rolle å spille med hensyn til å hindre misligheter, har noen organisasjoner også opprettet sentrale enheter med ansvar for å håndtere risikoene for eksterne misligheter. Disse samordner arbeidet med å utvikle organisasjonens strategier, sikre iverksetting av disse, kontrollere resultatene og gi råd og veiledning. Målene kan være bevegelige ettersom omfanget og arten av risikoene endres. Det kan derfor være nødvendig med regelmessig overvåking av situasjonen for å identifisere og reagere på nye risikoer. Når forekomsten av misligheter og tapsomfanget er betydelig, har organisasjoner også team av profesjonelle granskere som tar seg av de nærmere undersøkelsene av mislighetene.

1.19 Uansett organisering må offentlige organisasjoner sørge for at noen er ansvarlige for at planene for å håndtere risikoene for misligheter på den tiltenkte måten, blir satt i verk og for at det finnes tilstrekkelige ressurser. Noen må også være ansvarlige for måling av hvorvidt målene oppnås. En nøye gjennomtenkt strategi har ingen hensikt, dersom den ikke iverksettes.

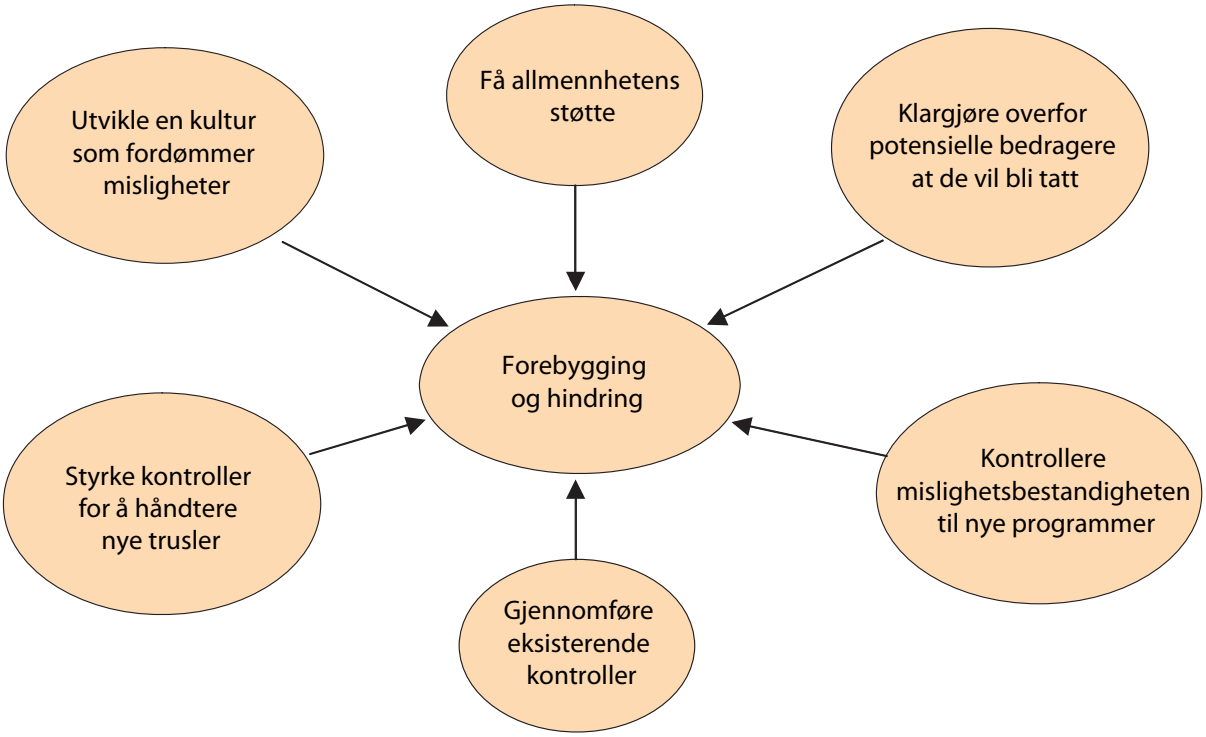
Del 2: Hvordan forebygge og hindre eksterne misligheter

2.1 **Forebygging** innebærer å overbevise potensielle bedragere om at misligheter mot en offentlig etat eller en offentlig virksomhet ikke lønner seg. Hindring innebærer tiltak for å forhindre at misligheter får innpass i organisasjonens systemer. Effektive tiltak for å forebygge og hindre misligheter er viktige elementer i bekjempelsen av misligheter. Realistisk sett vil det imidlertid alltid være noen bedragere som ikke lar seg avskrekke, og det er heller ikke mulig å hindre alle misligheter. I disse tilfellene er rask oppdagelse og profesjonell gransking nødvendig (del 3). Tiltak for å forebygge og hindre misligheter kan være dyre og organisasjonen må sikre at de utformes for å gi best mulig effekt. *Figur 4 viser hovedelementene ved forebygging og hindring av misligheter.*

Det må vurderes hvorvidt organisasjonen:

- Prøver å påvirke kundenes og allmennhetens holdning til misligheter.
- Sender et klart budskap til potensielle bedragere om at det er stor sannsynlighet for at de vil bli tatt og at sanksjoner vil bli iverksatt. Utgis det for eksempel pressemeldinger om personer/selskaper som granskes og gjennomføres det regionale eller nasjonale kampanjer?
- Vurderer hvorvidt nye programmer vil motstå misligheter.
- Sikrer at mislighetskontroller gjennomføres regelmessig og at de overvåkes. Hvilken rolle spiller internrevisjonen her?
- Vurderer å styrke kontrollen dersom nye risikoer for misligheter oppstår eller dersom omfanget av misligheter øker.
- Har en kultur som fordømmer misligheter og der medarbeiderne forstår hvilke holdninger som kreves og sitt personlige ansvar for å hindre misligheter, gjennomføre kontroller og melde fra ved mistanke om misligheter.

Figur 4: Hovedelementene ved forebygging og hindring av misligheter



Endring av allmennhetens holdning til misligheter

2.2 Offentlige organisasjoner kan prøve å påvirke kunders og allmennhetens holdninger til misligheter ved å avskrekke dem som vurderer å begå misligheter, og ved å gjøre misligheter sosialt uakseptable. Målet må være å få allmennhetens støtte i arbeidet med å bekjempe misligheter. Følgende er eksempler på forhold som vil virke avskrekkende:

- Sterke kontroller vil hindre dem i å lykkes, fulgt av
- Høy sannsynlighet for at de vil bli tatt
- Bevis på mislighetene vil deretter bli oppdaget
- De vil dermed bli straffet, og
- Midler som noen har tilegnet seg gjennom misligheter, må betales tilbake

2.3 Offentlige organisasjoner kan benytte mange forskjellige metoder for å offentliggjøre de gode resultatene av arbeidet sitt, for eksempel pressemeldinger og informasjon på nettsteder om avdekkede tilfeller. Dette er kostnadseffektive tiltak som også kan benyttes av mindre organisasjoner.

2.4 For å maksimere den avskrekkende virkningen kan organisasjoner:

- Undersøke bedragereres atferd og risikovillighet for å fastslå hvilke tiltak som er mest effektive for å endre atferden deres.
- Sende ut pressemeldinger for å oppnå maksimal effekt.
- Bruke egnede medier for å sikre at disse meldingene når potensielle bedragere.
- Gjenta budskapene regelmessig for å opprettholde den avskrekkende virkningen.
- Utarbeide indikatorer for virkningene for å evaluere hvor effektive tiltakene er. Det kan imidlertid

være vanskelig å fastslå en direkte sammenheng mellom en kampanje og en nedgang i omfanget av misligheter, ettersom det også er iverksatt andre tiltak mot misligheter.

- Følge opp evalueringen i nye kampanjer for å avskrekke bedragere.

Endring av medarbeidernes holdning for å fremme en kultur som fordømmer misligheter

2.5 For å forebygge eksterne misligheter er det avgjørende å utvikle en kultur som fordømmer misligheter, der alle medarbeiderne er bevisst på sitt personlige ansvar for å hindre misligheter og på viktigheten av kontroller. En tydelig intern formidling av organisasjonens strategiske angrepsmåte og formålet med den kan være en god måte å fremme denne kulturen på.

2.6 Opplæring kan bidra til å øke medarbeidernes bevissthet om risikoene for eksterne misligheter og viktigheten av å overholde de interne kontrollrutinene for å hindre misligheter. Nøye overvåking av hvorvidt medarbeiderne overholder kontrollrutinene, bidrar til å sikre at rutinene gjennomføres konsekvent. Opplæringen kan skje i mange forskjellige former, blant annet:

- Seminarer for å bevisstgjøre flere ulike grupper av medarbeidere om misligheter.
- Personlig veiledning av medarbeidere som arbeider på områder som er spesielt utsatt for misligheter.
- Tett ledelseskontroll med tilbakemelding til medarbeiderne om hvordan de overholder sikkerhetsrutinene.

2.7 En medarbeiderundersøkelse eller fokusgruppe kan brukes for å teste medarbeidernes holdning til sikkerhet og hvordan de overholder kontroller for å hindre misligheter. Resultatene av undersøkelsene kan bidra til å identifisere muligheter til å forbedre de forebyggende tiltak og styrke interne kontroller, identifisere budskap som må formidles klarere, avdekke områder der overholdelsen av kontrolltiltak er utilstrekkelig og innhente ytterligere informasjon om misligheter som er påvist av medarbeiderne.

Kontroller for å forebygge misligheter

2.8 Det finnes en rekke kontroller (for eksempel fysiske kontroller, avstemminger, ledelseskontroller og klar rolle- og ansvarsfordeling) rettet mot risikoer, herunder risiko for misligheter. Offentlige organisasjoner må vurdere hvilke kontrolltiltak som er best egnet for deres forhold. Konsistent anvendelse av interne kontroller kan være svært effektivt for å forebygge tap som skyldes misligheter. Internrevisjonen bør forsikre seg om at disse kontrollene gjennomføres og at de er effektive. Interne kontroller kan medføre både interne og eksterne kostnader. Det må utformes kontroller som står i forhold til risikoen og som samtidig gjør organisasjonen i stand til å levere de tjenestene som kundene etterspør.

2.9 To sentrale aspekter ved forebygging er:

- Gjøre nye programmer og systemer motstandsdyktige mot misligheter.
- Konsistent anvendelse av eksisterende kontroller og styrking av disse ved behov.

Gjøre nye programmer og systemer motstandsdyktige mot misligheter

2.10 Når offentlige organisasjoner utformer og iverksetter nye strategier, programmer og systemer, må de ivareta sitt ansvar for å bygge inn gode kontroller for å hindre misligheter der det foreligger risiko for det, eller for å utforme dem slik at de i utgangspunktet er mer motstandsdyktige mot misligheter. Kompliserte regler kan øke risikoen for misligheter. Bedragere kan utnytte situasjonen på to måter. Reglene kan være vanskelige å praktisere effektivt og medføre at medarbeidere stadig må slå opp i tykke veiledninger i det daglige arbeidet. Når kunder ofte er usikre på sine forpliktelser, er det enklere for bedragere å gi feil opplysninger og hevde at det var i god tro dersom de blir oppdaget.

2.11 Det bør legges tilstrekkelig vekt på ekspertråd om risikoene for misligheter i nye programmer og effektive mottiltak bør inngå i utformingen. Når nyutviklede systemer foreslås innført, er det god praksis å teste disse for å avdekke eventuelle nye risikoer for eksterne misligheter. Ved å rådføre seg med internrevisjonen og spesialister innen bekjempelse av misligheter på et tidlig tidspunkt, kan man få identifisert risikoene og få råd om hvordan disse kan minimeres i viktige faser under utviklingen og implementeringen av nye programmer. En evalueringsprosess er nyttig for å fastslå hvorvidt tidlige risikovurderinger har vært effektive med hensyn til å motvirke risikoer for misligheter under utviklingen, testingen og implementeringen.

Styrking av interne kontroller

2.12 Det er viktig at kontrollenes effektivitet evalueres regelmessig. Det kan være at kontroller som tradisjonelt har fungert godt, ikke lenger er effektive fordi bedragerne er blitt mer sofistikerte. De tilfeller av misligheter som avdekkes, kan vise at bedragere bruker nye metoder for å omgå kontroller, som derfor må styrkes. Internrevisjonens arbeid kan også identifisere systemsvakheter som kan føre til misligheter.

2.13 En styrking av intern kontrollen kan også bidra til å hindre eller redusere forekomsten av kriminelle handlinger. Ny lovgivning kan være påkrevd for å forbedre kontrollen eller avskrekke bedragere. Teknologiske fremskritt kan gi nye muligheter til å styrke kontrollen på en kostnadseffektiv måte for å redusere omfanget av eksterne misligheter.

Del 3: Hvordan avdekke og granske eksterne misligheter og iverksette sanksjoner

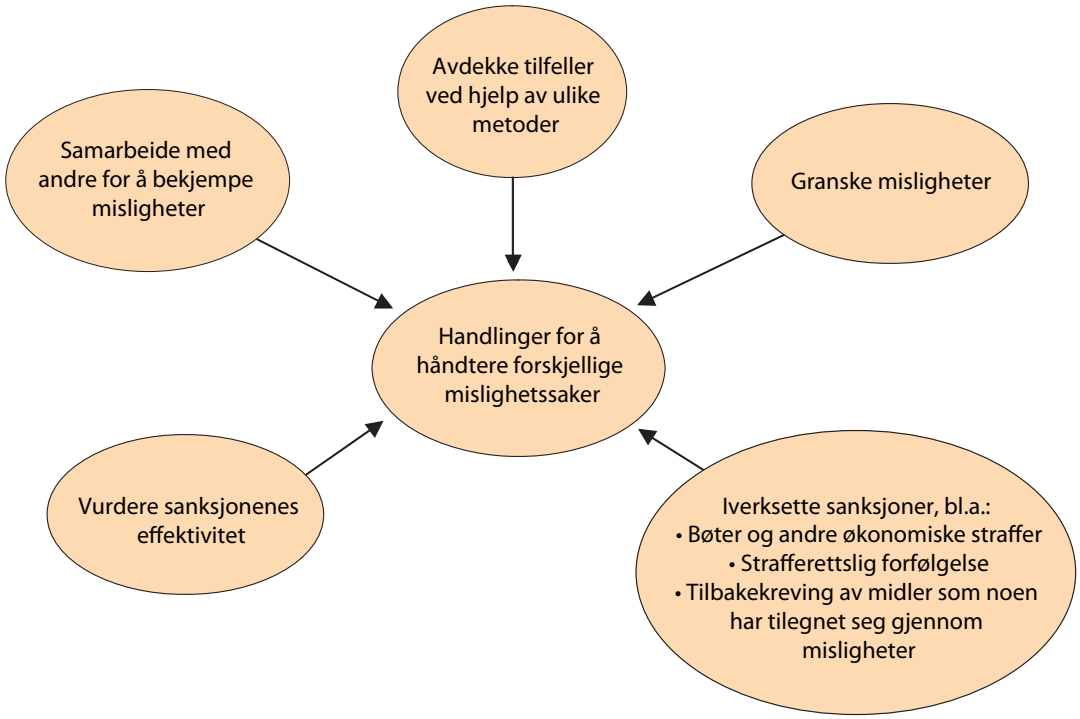
Det må vurderes hvorvidt organisasjonen:

- Har en allment kjent tipstelefon, e-postadresse eller lignende som allmennheten kan bruke til å melde fra om mulige misligheter.
- Proaktivt bruker teknikker for å avdekke tilfeller hvor det er mistanke om misligheter, for eksempel dyptgående gransking av "problemområder", datamatching, "data mining" og "nevrale nettverk" [3], der det passer.
- Vurderer hvorvidt mistanke om misligheter bør undersøkes nærmere, for eksempel gjennom bruk av poengsystemer.
- Vurderer hvorvidt antall tilfeller som etterforskes, står i forhold til det potensielle tapet som følger av misligheter.
- Følger fremgangen i granskingsarbeidet.
- Har et tilstrekkelig antall granskere med nødvendig teknisk kunnskap og erfaring.
- Foretar separate evalueringer av måten granskinger er blitt utført på.
- Iverksetter egnede sanksjoner mot bedragere, for eksempel bøter eller andre økonomiske straffer, eller strafferettslig forfølgelse når det er aktuelt.
- Prøver å få tilbake midler som noen har tilegnet seg gjennom misligheter.
- Evaluerer sanksjonenes effektivitet.
- Samarbeider med andre for å bekjempe misligheter.

3.1 For å vise at eksterne misligheter tas alvorlig, må offentlige organisasjoner avdekke misligheter som begås mot dem, granske dem der det er hensiktsmessig og iverksette sanksjoner som står i forhold til misligheten som er begått. Dette vil bidra til å avskrekke potensielle bedragere i fremtiden ved å vise at kriminalitet ikke lønner seg, særlig hvis resultatene av de tilfeller som forekommer, blir offentliggjort. Organisasjonene må også vurdere hvorvidt de avdekkede mislighetene tyder på at det foreligger nye trusler eller antyder at misligheter forekommer i et større omfang enn antatt. På grunnlag av dette arbeidet må organisasjonene vurdere hvorvidt den strategiske angrepsmåten må oppdateres. De må også vurdere hvorvidt misligheter tyder på systemsvakheter som må utbedres (figur 5).

3 "Nevrale nettverk" er datanettverk bygget opp etter mønster som kan minne om hjernens strukturer. Se punkt 3.12.

Figur 5: Håndtering av misligheter



Avdekking av misligheter

3.2 Misligheter kan oppdages på flere forskjellige måter. Tips kan komme fra medarbeidere som har kontrollert transaksjoner og fått mistanke om misligheter. Vanlige borgere kan informere den offentlige organisasjonen om sine mistanker. Offentlige organisasjoner bruker også en rekke metoder og teknikker for å identifisere mistenkelige tilfeller for nærmere undersøkelser. De kan også gjennomføre særskilte proaktive tiltak for å avdekke misligheter på spesielt utsatte områder. De som gransker misligheter, kan utvide granskingen ved å følge spor i de tilfeller der det kan være sammenheng med andre misligheter. Dette avsnittet tar for seg bruk av tipstelefoner og programvareteknikker.

Tipstelefoner

3.3 Tipstelefoner kan være en kostnadseffektiv metode å få opplysninger på fra medarbeidere og allmennheten om mulige tilfeller av eksterne misligheter som kan undersøkes nærmere. Gode tips:

- Opprette et gratis telefonnummer samt alternative muligheter til å kontakte organisasjonen, blant annet en e-postadresse eller lignende.
- Informere om telefonnummeret og andre kontaktmuligheter på den offentlige organisasjonens nettsted, ved hjelp av flygeblader og plakater og gjennom annonser i forbindelse med kampanjer mot misligheter.
- Garantere anonymitet og angi hvilke opplysninger som er viktige ved henvendelser, herunder hvilke typer misligheter den offentlige organisasjonen er særlig interessert i, og hvordan organisasjonen vil anvende opplysningene som gis.

3.4 Det er også god praksis å registrere opplysninger i et standardskjema. Dette kan hjelpe personen som gir tipset, med å gi så mye relevant informasjon som mulig. En elektronisk versjon av skjemaet kan legges ut på nettstedet for utfylling og innsending anonymt over internett. Personen kan ønske å vite hvilke

tiltak som vil bli iverksatt og en tilbakemelding om hva som har skjedd. Det er fullt mulig å gi generell informasjon om hvordan mottatte tips behandles, men det vil ikke alltid være mulig å gi nærmere opplysninger om individuelle tips siden det kan innebære brudd på taushetsplikt.

3.5 Tipstelefoner bør evalueres med jevne mellomrom, for eksempel ved å analysere antall og type tips som er mottatt, hva som har skjedd i hvert enkelt tilfelle og det samlede resultat.

Bruk av datateknikker for å avdekke misligheter

3.6 Det finnes en rekke forskjellige programvarer og datateknikker som kan brukes til å avdekke misligheter. Disse omfatter datamatching, data mining og nevrale nettverk. Mindre organisasjoner vil kunne anvende erfaringer fra andre ved bruk av disse teknikkene.

3.7 Datamatching innebærer skanning av data som er lagret i forskjellige datafiler, enten innen en og samme organisasjon eller i forskjellige organisasjoner. Denne teknikken kan brukes av ledelsen til en rekke formål, blant annet til å avdekke mulige misligheter. Med økende datakraft er det mulig å foreta datamatching av en meget stor mengde filer.

3.8 For å konsentrere ressursene om matcher som antyder mulige misligheter kan datamatchingprogrammer:

- Merke matcher med høy prioritet.
- Filtrere ut kun de matchene som oppfyller granskerens kriterier.
- Forklare viktigheten av hver matchtype og protokoller for deling av informasjon mellom de matchede enhetene.

3.9 Datamatching mellom forskjellige enheter forenkles i stor grad gjennom felles "data descriptors"[4], men er kun mulig dersom det er tillatt å overføre eller dele de relevante dataene mellom disse organisasjonene. Denne tillatelsen kan foreligge i form av en lovfestet rett til innsyn i eller til å gi opplysning om dataene. Usikkerhet i forbindelse med tillatelse til å dele data kan i enkelte tilfeller hindre bruk av datamatching. Datamatching innebærer også problemstillinger med hensyn til krenking av privatlivets fred.

3.10 Bruk av datamatching må skje i samsvar med bestemmelsene i datavernlover[5]. Prinsipper for datavern fastsetter at dataene:

- skal behandles på rimelig og lovlig vis.
- kun skal innsamles til bestemte, uttrykkelig angitte og berettigede formål.
- skal være adekvate, relevante og ikke for omfattende i forhold til de formålene de er innsamlet for.
- skal være nøyaktige.
- ikke skal oppbevares lenger enn nødvendig.
- skal behandles under hensyn til lovfestede personlige rettigheter.
- skal oppbevares på et sikkert sted.
- ikke må overføres til land uten tilstrekkelige datavern.

---

4) Dataprogrammering står fil deskriptor for en tilfeldig nøkkel til tilgang til en datafil. Andre systemer benytter begrepet filbehandling "file handle", skjønt dette rent teknisk er et annet objekt.

5) I Norge vil personopplysningsloven regulere muligheter for bruk av datamatching.

3.11 "Data mining" betyr å velge ut, undersøke og modellere store mengder data for å avdekke tidligere ukjente mønstre, atferder, trender eller sammenhenger som kan bidra til å identifisere misligheter. På grunn av de store datamengdene som må analyseres, brukes spesialprogramvare som vanligvis inneholder flere data mining-verktøy. Flere programvareleverandører har utviklet slike produkter. Data mining kan være en effektiv måte å undersøke data på for å avdekke avvik som ikke ville blitt oppdaget ved bruk av andre teknikker. For at denne teknikken skal fungere effektivt, må imidlertid medarbeiderne lære å bruke programvaren og få erfaring med å velge ut de verktøyene som er best egnet for å undersøke dataene og med å følge opp avvik for å oppdage misligheter.

3.12 "Nevrale nettverk" er databaserte flerbehandlingssystemer som er utformet for å koble sammen data fra flere kilder for å identifisere strukturer og mønstre, samt avvik fra en identifisert struktur eller et identifisert mønster. Disse "nettverkenes" evne til å identifisere aktivitetsmønstre og avvik fra et mønster som kan knyttes til misligheter, gir offentlige organisasjoner muligheten til å konsentrere sine ressurser om disse avvikene.

3.13 Et av problemene med å bruke disse teknikkene i stort omfang i offentlig sektor er at dataene ofte ikke er lagret på en måte som tillater en slik analyse. Det stadig økende tilbudet av nettjenester kan endre dette og gjøre analyser av transaksjoner i sanntid mulig gjennom den offentlige organisasjonens nettsted ved hjelp av noen av disse teknikkene.

Gransking av misligheter

3.14 Når misligheter er avdekket, må den offentlige organisasjonen vurdere:

- Hvordan mislighetene snarest mulig kan stanses, og se på hvorvidt de er gjennomført ved å utnytte svakheter i kontrollene, og om kontrollene derfor må styrkes.
- Hvorvidt saken skal forfølges strafferettslig eller om det skal iverksettes et straffetiltak.
- Hvordan tapte beløp og eventuelle økonomiske straffer kan inndrives for å sikre at den kriminelle handlingen ikke er lønnsom og for å avskrekke andre.

3.15 Noen offentlige organisasjoner har kriterier eller poengsystemer for å fastslå hvilke tilfeller som skal granskes og eventuelt forfølges rettslig, og i hvilke tilfeller det skal iverksettes andre sanksjoner. Organisasjonen må også vurdere hvorvidt antall tilfeller som etterforskes, står i forhold til det potensielle tapet som følge av av misligheter. Gransking kan være svært ressurskrevende. En vurdering av det økonomiske resultatet av den samlede arbeidsinnsatsen opp mot ulike typer misligheter, gir en pekepinn på den antatte nytten av å foreta flere undersøkelser eller av å fordele innsatsen mellom de ulike typene på en annen måte.

3.16 Når ledere følger fremdriften i granskingsarbeidet, vil de kunne vurdere den samlede arbeidsmengden (for eksempel hvorvidt undersøkelsene konsentreres om hovedtypene av misligheter som er fastsatt i organisasjonens strategi), identifisere problemområder der fremgangen er dårligere enn forventet, gjøre seg kjent med de kostnadene undersøkelsene medfører, og følgene for planleggingen av fremtidig ressursbruk eller følgene av å øke eller redusere ressursinnsatsen. Når offentlige organisasjoner gransker misligheter, må de vurdere hvorvidt de har et tilstrekkelig antall medarbeidere med den påkrevde tekniske og granskningsmessige kunnskap og erfaring og hvorvidt det er behov for et opplæringstilbud til dem som skal granske misligheter.

3.17 Gransking av misligheter bør være i samsvar med rettssystemets målsettinger om å redusere kriminalitet og frykt for kriminalitet samt å sørge for rettferdighet på en rimelig og effektiv måte som fremmer tilliten til rettssystemet. Gransking av misligheter må være av høy kvalitet. En uavhengig evaluering av hvordan granskingen er utført kan bidra til å sikre at gjeldende retningslinjer og lovkrav blir fulgt. Resultatene kan peke ut områder som må forbedres. Evalueringene kan foretas av:

- Uavhengige interne team spesialisert på gransking av misligheter.
- En utpekt ekstern evaluerer.

Iverksetting av sanksjoner

3.18 Når granskingen frembringer bevis på misligheter, vil den offentlige organisasjonen vanligvis iverksette sanksjoner i en eller annen form. Formålet er å avskrekke andre fra å begå liknende misligheter mot organisasjonen, få tilbake det som er tapt og straffe bedrageren ved å ilegge en straff, for eksempel en bot eller inndragning av eiendeler, eller ved å innlede strafferettslig forfølgelse. Noen organisasjoner offentliggjør tiltakene de iverksetter, for å avskrekke potensielle bedragere og sikre en konsistent håndtering.

Bøter og andre økonomiske straffer

3.19 Bøter og andre økonomiske straffer som ilegges de som begår misligheter, må innkreves for å sikre at de virker avskrekkende. Det er viktig å kontrollere innbetalingen av bøter og andre økonomiske straffer, herunder innkreving av økonomiske straffer som er ilagt av domstoler. Organisasjonene må her ta hensyn til eventuelle menneskerettslover.

Strafferettslig forfølgelse

3.20 Det å samle tilstrekkelige bevis for en strafferettslig forfølgelse kan ta lang tid og kreve betydelige ressurser. En beslutning om å innlede strafferettslig forfølgelse kan avhenge av om:

- Det foreligger tilstrekkelige bevis til å oppnå en domfellelse.
- Saken omfatter et systematisk angrep på organisasjonens systemer og har ført til tap av betydelige beløp.
- Det foreligger tidligere tilfeller av misligheter.
- Fagfolk, for eksempel advokater og revisorer, er innblandet i saken.
- En strafferettslig forfølgelse vil øke den avskrekkende virkningen.

3.21 Disse faktorene må veies opp mot tidsforbruket og kostnadene ved å bringe en sak inn for retten og andre tilgjengelige og mer hensiktsmessige former for sanksjoner. Noen offentlige organisasjoner har fastsatt under hvilke omstendigheter de vil forfølge en sak rettslig, for å sikre konsistent håndtering. Organisasjonen må vurdere hvorvidt antallet saker som bringes for retten, står i forhold til de potensielle verdier som kan tapes og den avskrekkende virkningen.

Tilbakekreving av tapte beløp

3.22 Tapte beløp kan kreves tilbake gjennom strafferettslig forfølgelse eller gjennom sivile søksmål. Under noen omstendigheter kan det være hensiktsmessig for en offentlig organisasjon å gå til sivilt søksmål mens en strafferettslig forfølgelse er under forberedelse. Som en del av granskingen kan organisasjonen undersøke den økonomiske situasjonen til den mistenkte bedrageren for å finne rettskraftige bevis for omfanget av fordelene som den saksøkte har oppnådd, og for at inndragning skal kunne bli besluttet. Før de(n) mistenkte personen(e) får kjennskap til at det foregår en granskning, kan det være nødvendig å iverksette tiltak for å sikre midlene som er unndratt, ved å begjære midlertidig sikring eller et disposisjonsforbud.

3.23 Når en offentlig organisasjon forsøker å få tilbake stjålne beløp gjennom et sivilt søksmål, kan det måtte bevise at det har rimelig grunn til å kreve at saken blir prøvet av domstolen. Videre kan saksøkeren måtte legge frem bevis for det beløpet som er tatt. Dersom saken fører frem, kan domstolen pålegge saksøkte å erstatte saksøkeren det stjålne beløpet samt i de fleste tilfeller saksomkostninger, som kan være høye. Organisasjonen må vurdere:

- Hvor store beløp som er stjålet og som er mulige å få tilbake.
- Sannsynligheten for å vinne saken.
- Verdien av eiendelene som den mistenkte bedrageren besitter.
- De antatte saksomkostningene.
- Om det vil være mulig å føre en sivil rettssak mens en strafferettslig forfølgelse er under forberedelse.

3.24 En organisasjon kan få tilbake stjålne beløp som en del av en straffesak. Dette skjer vanligvis i form av inndragning eller erstatning.

Evaluering av sanksjonenes effektivitet

3.25 En vurdering av sanksjonenes effektivitet er komplisert, først og fremst på grunn av at det er vanskelig å måle den avskrekkende virkningen. Generelt sett vil den avskrekkende virkningen av sanksjoner gjenspeiles i hvorvidt omfanget av misligheter er gått ned, men det er vanskelig å skille virkningen av sanksjoner fra andre tiltak mot misligheter og mer generelle økonomiske virkninger. Utviklingen i indikatorene kan bidra til å fastslå om tiltakene har den ønskede virkningen.

Samarbeid med andre for å hindre misligheter

3.26 Enkeltpersoner og selskaper kan begå misligheter mot mer enn én etat eller én organisasjon. Samarbeid gjør det mulig å identifisere felles trusler og å samle kunnskap og ekspertise for å granske misligheter. Andre fordeler ved å samarbeide for å bekjempe misligheter, er:

- God praksis i en organisasjon kan videreformidles til andre organisasjoner.
- Informasjon kan utveksles på en mer effektiv måte.
- Kunnskap, uformelle systemer og kultur utvikles på tvers av organisasjonene.
- Det kan utvikles en felles, mer konsistent angrepsmåte.
- Det kan etterprøves om opplysningene kunder gir til forskjellige organisasjoner, samsvarer.
- Det kan bygges opp tillit og forståelse mellom organisasjonene.

3.27 Samarbeid kan opprettes ved å inngå en samarbeidsavtale med andre organisasjoner for å muliggjøre deling av data og utføre datamatching og dataprofilering. Dette kan gjøres ved hjelp av datavarehus som er tilgjengelig for de deltakende organisasjonene. Datavarehuset kan omfatte data fra hver organisasjon og fra eksterne kilder, som for eksempel folkeregisteret, som inneholder opplysninger om personnummer, førerkortnummer, passnummer og stemmerett.[6] Samarbeidet kan også omfatte samarbeid om gransking av misligheter. Dette gjør det mulig for organisasjonene å granske tilfeller av felles interesse, slik at dobbeltarbeid unngås.

6) I Norge vil bruken av slike opplysninger være begrenset av bestemmelsene i personopplysningsloven.