# SVENSK STANDARD
# SS-ISO 37001:2017

Fastställd/Approved: 2017-05-09
Publicerad/Published: 2017-05-16
Utgåva/Edition: 1
Språk/Language: svenska/Swedish, engelska/English
ICS: 03.100.01; 03.100.70; 04.130

## Ledningssystem mot mutor – Krav och vägledning (ISO 37001:2016, IDT)

## Anti-bribery management systems – Requirements with guidance for use (ISO 37001:2016, IDT)

# Standarder får världen att fungera

*SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.*

**Delta och påverka**
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

**Ta del av det färdiga arbetet**
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standard-paket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

**Utveckla din kompetens och lyckas bättre i ditt arbete**
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

**Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.**

# Standards make the world go round

*SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.*

**Take part and have influence**
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

**Get to know the finished work**
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

**Increase understanding and improve perception**
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

**If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00**

Den internationella standarden ISO 37001:2016 gäller som svensk standard. Detta dokument innehåller den svenska språkversionen av ISO 37001:2016 följd av den officiella engelska språkversionen.

The International Standard ISO 37001:2016 has the status of a Swedish Standard. This document contains the Swedish language version of ISO 37001:2016 followed by the official English language version.



*Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS Förlag AB som även lämnar allmänna upplysningar om svensk och utländsk standard.*

*Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.*

Standarden är framtagen av kommittén för Socialt ansvarstagande, SIS/TK 478.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

## Innehåll

**1 Omfattning ..... 7**

**2 Normativa hänvisningar ..... 8**

**3 Termer och definitioner ..... 8**

**4 Organisationens förutsättningar ..... 14**
4.1 Att förstå organisationen och dess förutsättningar ..... 14
4.2 Att förstå intressenters behov och förväntningar ..... 14
4.3 Att bestämma omfattningen av ledningssystemet mot mutor ..... 14
4.4 Ledningssystem mot mutor ..... 15
4.5 Riskbedömning för mutor ..... 15

**5 Ledarskap ..... 16**
5.1 Ledarskap och åtagande ..... 16
5.2 Policy mot mutor ..... 17
5.3 Roller, ansvar och befogenheter inom organisationen ..... 18

**6 Planering ..... 19**
6.1 Åtgärder för att hantera risker och möjligheter ..... 19
6.2 Mål för förebyggande av mutor och planering för att uppnå dem ..... 19

**7 Stöd ..... 20**
7.1 Resurser ..... 20
7.2 Kompetens ..... 20
7.3 Medvetenhet och utbildning ..... 21
7.4 Kommunikation ..... 22
7.5 Dokumenterad information ..... 23

**8 Verksamhet ..... 24**
8.1 Planering och styrning av verksamheten ..... 24
8.2 Due diligence ..... 25
8.3 Finansiella kontroller ..... 25
8.4 Icke-finansiella kontroller ..... 25
8.5 Införande av kontroller mot mutor för kontrollerade organisationer och affärspartner ..... 25
8.6 Åtaganden mot mutor ..... 26
8.7 Gåvor, representation, donationer och liknande förmåner ..... 27
8.8 Hantering av otillräckliga kontroller mot mutor ..... 27
8.9 Rapportera problem ..... 27
8.10 Utreda och hantera mutor ..... 28

**9 Utvärdering av prestanda ..... 28**
9.1 Övervakning, mätning, analys och utvärdering ..... 28
9.2 Intern revision ..... 29
9.3 Ledningens genomgång ..... 30
9.4 Genomgång som görs av funktionen för efterlevnad avseende mutor ..... 31

**10 Förbättringar ..... 32**
10.1 Avvikelse och korrigerande åtgärd ..... 32
10.2 Ständig förbättring ..... 32

**Bilaga A** (informativ) **Vägledning för användning av detta dokument ..... 33**

**Litteraturförteckning..... 61**

# Förord

ISO (Internationella standardiseringsorganisationen) är en världsomspännande sammanslutning av nationella standardiseringsorgan (ISO-medlemmar). Utarbetande av internationella standarder sker normalt i ISO:s tekniska kommittéer. Varje medlemsorganisation som är intresserad av arbetet i en teknisk kommitté har rätt att bli medlem i den. Internationella organisationer, statliga såväl som icke-statliga, som samarbetar med ISO deltar också i arbetet. ISO har nära samarbete med International Electrotechnical Commission (IEC) i alla frågor rörande elektroteknisk standardisering.

De metoder som har använts för att utveckla detta dokument och för att utveckla det ytterligare beskrivs i ISO/IEC-direktiven, Del 1. Framförallt bör de olika godkännandekriterierna för olika typer av ISO-dokument noteras. Det här dokumentet har upprättats i enlighet med de redaktionella reglerna i ISO/IEC-direktiven, Del 2 (se www.iso.org/directives).

Observera att vissa beståndsdelar i denna internationella standard kan vara föremål för patenträtter. ISO ska inte hållas ansvarig för att identifiera någon eller alla sådana patenträtter. Information om eventuella patenträttigheter som identifierats under framtagandet av dokumentet finns i introduktionen och/eller på ISO-listan över mottagna patentförklaringar (se www.iso.org/patents).

Eventuella handelsnamn som används i dokumentet är information avsedd för användarnas bekvämlighet och utgör inget godkännande.

En förklaring av betydelsen hos ISO-specifika termer och uttryck som är kopplade till bedömningar om överensstämmelse samt information om ISO:s uppfyllande av WTO:s (World Trade Organization) principer i avtalet om tekniska handelshinder (TBT) finns på följande URL: www.iso.org/foreword-supplementary-information.html.

Detta dokument har utarbetats av projektkommittén ISO/PC 278, *Anti-bribery management systems*.

# Orientering

Mutor är ett utbrett fenomen. De ger upphov till allvarliga sociala, moraliska, ekonomiska och politiska problem, undergräver goda styrelseformer, hindrar utvecklingen och snedvrider konkurrensen. Mutor urholkar rättvisan, undergräver de mänskliga rättigheterna och hindrar fattigdomsbekämpning. Mutor ökar även kostnaderna för att bedriva affärsverksamhet, gör affärstransaktioner osäkra, ökar kostnaden för varor och tjänster och minskar kvaliteten på produkter och tjänster, vilket kan leda till förlust av människoliv och egendom, förstöra förtroendet för institutioner och störa en rättvis och väl fungerande marknad.

Regeringarna har gjort framsteg med att hantera mutor genom internationella avtal såsom OECD:s (Organisationen för ekonomiskt samarbete och utveckling) konvention om bekämpande av bestickning av utländska offentliga tjänstepersoner i internationella affärsförbindelser [15] och Förenta nationernas (FN) konvention mot korruption [14] samt genom nationella lagar. I de flesta jurisdiktioner är det ett brott för enskilda personer att vara inblandade i mutor, och det finns en ökande tendens att ställa såväl organisationer som enskilda personer till svars för mutor.

Enbart lagstiftning är dock inte tillräckligt för att lösa detta problem.

Organisationer har därför ett ansvar för att proaktivt bidra till att bekämpa mutor. Detta kan uppnås genom ett ledningssystem mot mutor, vilket detta dokument syftar till att tillhandahålla, och genom ledningars åtagande att skapa en kultur av integritet, insyn, öppenhet och efterlevnad. Karaktären hos en organisations kultur avgör om ett ledningssystem mot mutor blir ett misslyckande eller en framgång.

En välskött organisation förväntas ha en efterlevnadspolicy som stöds av lämpliga ledningssystem för att hjälpa den att uppfylla sina rättsliga skyldigheter och integritetsåtaganden. En policy mot mutor ingår i en allmän efterlevnadspolicy. Ett ledningssystem mot mutor och stödjande ledningssystem hjälper organisationen att undvika eller begränsa kostnader, risker och skador till följd av inblandning i mutor, främja tillit och förtroende i affärsrelationerna och stärka sitt anseende.

Detta dokument motsvarar internationell god praxis och kan användas i alla jurisdiktioner. Det är tillämpligt på små, medelstora och stora organisationer inom alla sektorer, inbegripet offentlig och privat sektor samt den ideella sektorn. Riskerna för mutor för en organisation varierar beroende på olika faktorer, t.ex. organisationens storlek, de platser och branscher där organisationen bedriver verksamhet samt typen, omfattningen och komplexiteten hos organisationens verksamheter. I detta dokument anges därför hur organisationer kan genomföra policyer, rutiner och kontroller som är rimliga och proportionella i förhållande till de risker för mutor som organisationen är exponerad för. Bilaga A ger vägledning om införandet av kraven i detta dokument.

Överensstämmelse med detta dokument kan inte garantera att inga mutor har förekommit eller inte kommer att förekomma inom organisationen, eftersom det inte är möjligt att helt undanröja risken för mutor. Detta dokument kan dock hjälpa organisationen att vidta rimliga och proportionella åtgärder som är utformade för att förebygga, upptäcka och hantera med mutor.

I dokumentet används följande verbformer:

— ”ska” anger ett krav;

— ”bör” anger en rekommendation;

— ”får” anger en tillåtelse;

— ”kan” anger en möjlighet eller en kapacitet.

Information markerad som ”ANM.” förtydligar det aktuella kravet.

Detta dokument överensstämmer med ISO:s krav för standarder för ledningssystem. Dessa krav inbegriper en högnivåstruktur, identisk grundtext och gemensamma termer med centrala definitioner, som är utformade för att hjälpa användare som genomför flera olika ISO-standarder för ledningssystem. Detta dokument kan användas tillsammans med andra ledningssystemsstandarder (t.ex. ISO 9001, ISO 14001, ISO/IEC 27001 och ISO 19600) och ledningsstandarder (t.ex. ISO 26000 och ISO 31000).

# Ledningssystem mot mutor – Krav och vägledning

## 1 Omfattning

Detta dokument anger krav och ger vägledning för att införa, genomföra, underhålla, granska och förbättra ett ledningssystem mot mutor. Systemet kan vara fristående eller integreras i ett övergripande ledningssystem. Detta dokument behandlar följande när det gäller organisationens verksamheter:

— mutor inom den offentliga, privata och ideella sektorn;

— mutor som ges av organisationen;

— mutor som ges av organisationens personal som agerar för organisationens räkning eller till förmån för organisationen;

— mutor som ges av organisationens affärspartner som agerar för organisationens räkning eller till förmån för organisationen;

— mutor som tas emot av organisationen;

— mutor som tas emot av organisationens personal i samband med organisationens verksamheter;

— mutor som tas emot av organisationens affärspartner i samband med organisationens verksamheter;

— direkta och indirekta mutor (t.ex. en muta som erbjuds eller tas emot via en tredje part).

Detta dokument är endast tillämpligt på mutor. Det anger krav och ger vägledning för ett ledningssystem som är utformat för att hjälpa organisationen att förebygga, upptäcka och hantera mutor samt uppfylla lagar mot mutor samt frivilliga åtaganden som är tillämpliga på organisationens verksamheter.

Detta dokument behandlar inte uttryckligen bedrägeri, karteller och andra brott mot konkurrenslagstiftning, penningtvätt eller andra verksamheter som är relaterade till korrupt beteende (även om en organisation kan välja att utvidga ledningssystemets omfattning till att inbegripa sådana verksamheter).

Kraven i detta dokument är allmänna och är avsedda att vara tillämpliga på alla organisationer (eller delar av en organisation) oavsett typ, storlek och verksamhetsinriktning, och oavsett om organisationen är verksam inom den offentliga, privata eller ideella sektorn. Omfattningen av tillämpningen av dessa krav beror på de faktorer som anges i 4.1, 4.2 och 4.5.

ANM. 1 Se avsnitt A.2 för vägledning.

ANM. 2 Nödvändiga åtgärder för att förebygga, upptäcka och begränsa risken för mutor av organisationen kan skilja sig från de åtgärder som används för att förebygga, upptäcka och hantera mutor

som ges av organisationen (eller dess personal eller affärspartner som agerar för organisationens räkning). Se A.8.4 för vägledning.

## 2 Normativa hänvisningar

Det finns inga normativa hänvisningar i detta dokument.

## 3 Termer och definitioner

För tillämpning av detta dokument gäller följande termer och definitioner.

ISO och IEC driver terminologiska databaser för användning i standardisering på följande adresser:

— ISO Online browsing platform: finns på http://www.iso.org/obp

— IEC Electropedia: finns på http://www.electropedia.org/

**3.1**
**mutor**
direkt eller indirekt erbjudande, utlovande, givande, tagande eller krävande av en otillbörlig förmån av något värde (som skulle kunna vara ekonomiskt eller icke-ekonomiskt), oavsett var detta sker och som är i strid mot tillämplig lag, som en uppmuntran eller belöning till en person som agerar eller låter bli att agera i relation till *prestandan* (3.16) av sina förpliktelser

ANM. 1 till termpost: Ovanstående är en allmän definition. Innebörden av termen ”mutor” definieras av den lag om bekämpande av mutor som är tillämplig på *organisationen* (3.2) och av det *ledningssystem* (3.5) mot mutor som har utformats av organisationen.

**3.2**
**organisation**
person eller grupp av personer, som har egna funktioner med ansvar, befogenheter och samband för att uppnå sina *mål* (3.11)

ANM. 1 till termpost: Begreppet organisation innefattar, men är inte begränsat till, egenföretagare, bolag, koncern, firma, företag, myndighet, affärspartner, välgörenhetsorganisation eller institution, eller delar, alternativt kombinationer av dem, oavsett ägarstruktur eller om de är offentliga eller privata.

ANM. 2 till termpost: För organisationer med fler än en enhet kan en eller flera av enheterna definieras som en organisation.

**3.3**
**berörd part** (föredragen term)
**intressent** (tillåten term)
person eller *organisation* (3.2) som kan påverka, påverkas av eller anser sig vara påverkad av ett beslut eller en åtgärd

ANM. 1 till termpost: En intressent kan vara intern eller extern i förhållande till organisationen.

**3.4**
**krav**
behov som är angivet och obligatoriskt

ANM. 1 till termpost: Den gemensamma definitionen av "krav" i ISO:s ledningssystemstandarder är "behov eller förväntning som är angivet, underförstått eller obligatoriskt". "Underförstådda krav" är inte tillämpliga i sammanhanget ledningssystem mot mutor.

ANM. 2 till termpost: Ett specificerat krav är ett som är angivet, t.ex. i dokumenterad information.

Svensk ANM. till termpost: I den engelska utgåvan av detta dokument finns felaktigt en ANM. 2 till termpost angående ordet "underförstått", som inte är tillämplig i detta dokument enligt förklaringen i ANM 1 till termpost. Denna felaktiga ANM. har tagits bort i den svenska översättningen och den engelska utgåvans ANM. 3 har numrerats till ANM. 2 i den svenska översättningen.

**3.5**
**ledningssystem**
grupp av samverkande eller varandra påverkande delar av en *organisation* (3.2) för att upprätta *policy* (3.10) och *mål* (3.11) samt *processer* (3.15) för att uppnå dessa

ANM. 1 till termpost: Ett ledningssystem kan gälla ett enda ämnesområde eller flera ämnesområden.

ANM. 2 till termpost: Ledningssystemets delar innefattar organisationens struktur, roller och ansvar, planering och verksamhet.

ANM. 3 till termpost: Ett ledningssystem kan omfatta hela organisationen, specifika och identifierade funktioner inom organisationen, specifika och identifierade delar av organisationen, eller en eller flera funktioner inom en grupp av organisationer.

**3.6**
**högsta ledningen**
person eller grupp av personer som leder och styr en *organisation* (3.2) på högsta nivå

ANM. 1 till termpost: Högsta ledningen har rätten att delegera befogenheter och tillhandahålla resurser inom organisationen.

ANM. 2 till termpost: Om *ledningssystemet* (3.5) omfattar endast en del av organisationen avses med högsta ledningen de som leder och styr denna del av organisationen.

ANM. 3 till termpost: Organisationer kan organiseras beroende på vilken ramlagstiftning de är skyldiga att verka inom och även enligt storlek, bransch etc. En del organisationer har både ett *styrande organ* (3.7) och en högsta ledning, medan andra organisationer inte har sina ansvarsfunktioner uppdelade i flera organ. Dessa variationer, både när det gäller organisation och ansvar, kan övervägas vid tillämpningen av kraven i avsnitt 5.

**3.7**
**styrande organ**
grupp eller organ som har det slutliga ansvaret och befogenheten för en *organisations* (3.2) verksamheter, styrning och policyer, och till vilken *högsta ledningen* (3.6) rapporterar och är ansvarig inför

ANM. 1 till termpost: Inte alla organisationer, särskilt små sådana, har ett styrande organ separat från högsta ledningen (se 3.6 ANM. 3 till termpost).

ANM. 2 till termpost: Ett styrande organ kan omfatta, men är inte begränsat till, en styrelse, styrelsekommittéer, tillsynsnämnd, förvaltare eller övervakare.

**3.8**
**funktion för efterlevnad avseende mutor**
person(er) med ansvar och befogenhet för att driva *ledningssystemet* (3.5) mot mutor

Svensk ANM. till termpost: Det börjar bli allt vanligare att den engelska termen "compliance" används i det svenska språkbruket men i detta dokument används "efterlevnad" som svensk motsvarighet till "compliance".

**3.9**
**verkan**
omfattning i vilken planerade aktiviteter har genomförts och planerade resultat har uppnåtts

**3.10**
**policy**
*organisations* (3.2) avsikter och inriktning, formellt uttalade av dess *högsta ledning* (3.6) eller *styrande organ* (3.7)

**3.11**
**mål**
resultat som ska uppnås

ANM. 1 till termpost: Ett mål kan vara strategiskt, taktiskt eller ha verksamhetsinriktning.

ANM. 2 till termpost: Mål kan röra olika ämnesområden (t.ex. mål för ekonomi, försäljning och marknadsföring, upphandling, arbetsmiljö och yttre miljö) och kan vara tillämpliga på olika nivåer (t.ex. strategisk nivå, organisationsövergripande nivå, samt på nivåerna projekt, produkt och *process* (3.15).

ANM. 3 till termpost: Ett mål kan uttryckas på andra sätt, t.ex. som ett avsett resultat, ett ändamål, ett verksamhetskriterium, som ett mål för förebyggande av mutor, eller genom användning av andra ord med liknande innebörd (t.ex. syfte, målsättning eller riktmärke).

ANM. 4 till termpost: Inom ramen för ett *ledningssystem* (3.5) mot mutor sätts mål för förebyggande av mutor av *organisationen* (3.2) i överensstämmelse med policyn (3.10) mot mutor för att uppnå specifika resultat.

**3.12**
**risk**
osäkerhetens effekt på *målen* (3.11)

ANM. 1 till termpost: En effekt är en avvikelse från det förväntade – positiv eller negativ.

ANM. 2 till termpost: Osäkerhet är det tillstånd, också partiellt, av bristande information som har att göra medförståelse för eller kunskap om en händelse, dess konsekvenser eller sannolikhet.

ANM. 3 till termpost: Risk karaktäriseras ofta utifrån potentiella händelser (enligt definition i ISO Guide 73:2009, 3.5.1.3) och konsekvenser (enligt definition i ISO Guide 73:2009, 3.6.1.3) eller en kombination av dessa.

ANM. 4 till termpost: Risk uttrycks ofta som en kombination av en händelses konsekvenser (inklusive förändrade omständigheter) och tillhörande sannolikhet (enligt definition i ISO Guide 73:2009, 3.6.1.1) för förekomsten.

**3.13**
**kompetens**
förmåga att tillämpa kunskap och färdigheter för att uppnå avsedda resultat

**3.14**
**dokumenterad information**
information som ska styras och underhållas av en *organisation* (3.2) samt det medium på vilket informationen finns

ANM. 1 till termpost: Dokumenterad information kan ha vilket format som helst, finnas på vilket medium som helst och ha vilken källa som helst.

ANM. 2 till termpost: Dokumenterad information kan avse:

— *ledningssystemet* (3.5), inklusive tillhörande *processer* (3.15);

— information som skapats så att organisationens verksamhet kan fungera (styrande dokument);

— belägg över uppnådda resultat (redovisande dokument).

**3.15**
**process**
grupp av aktiviteter som samverkar eller påverkar varandra, och som omformar insatser till utfall

**3.16**
**prestanda**
mätbart resultat

ANM. 1 till termpost: Prestanda kan avse kvantitativa eller kvalitativa iakttagelser.

ANM. 2 till termpost: Prestanda kan avse ledning av aktiviteter, *processer* (3.15), *produkter* (inklusive tjänster), system eller *organisationer* (3.2).

**3.17**
**utkontraktera (outsourcing)**
anlita en extern *organisation* (3.2) för att genomföra en del av en organisations funktion eller *process* (3.14)

ANM. 1 till termpost: En extern organisation omfattas inte av *ledningssystemet* (3.5), men den outsourcade funktionen eller processen omfattas.

ANM. 2 till termpost: Grundtexten i ISO:s ledningssystemsstandarder innehåller en definition och ett krav när det gäller outsourcing, som inte används i detta dokument eftersom kontraktstagande leverantörer inbegrips i definitionen av *affärspartner* (3.26).

**3.18**
**övervakning**
bestämning av status hos ett system, en *process* (3.15) eller en aktivitet

ANM. 1 till termpost: För att bestämma status kan det vara nödvändigt att kontrollera, ha uppsikt över eller kritiskt observera.

**3.19**
**mätning**
*process* (3.15) för att bestämma ett värde

**3.20**
**revision**
systematisk, oberoende och dokumenterad *process* (3.15) som syftar till att skaffa revisionsbelägg och utvärdera dessa objektivt för att avgöra i vilken utsträckning revisionskriterierna har uppfyllts

ANM. 1 till termpost: En revision kan vara intern (förstapartsrevision) eller extern (andra- eller tredjepartsrevision), och den kan också vara en kombinerad revision (då två eller fler ämnesområden kombineras).

ANM. 2 till termpost: En intern revision utförs av *organisationen* (3.2) själv eller för dess räkning av en extern part.

ANM. 3 till termpost: ”Revisionsbelägg” och ”revisionskriterier” definieras i EN ISO 19011.

**3.21**
**överensstämmelse**
uppfyllande av ett *krav* (3.4)

**3.22**
**avvikelse**
icke-uppfyllande av ett *krav* (3.4)

**3.23**
**korrigerande åtgärd**
åtgärd för att eliminera orsaken till en konstaterad *avvikelse* (3.22) och för att förebygga upprepning av denna

**3.24**
**ständig förbättring**
återkommande aktivitet för att förbättra *prestanda* (3.16)

**3.25**
**personal**
*organisations* (3.2) direktörer, chefer, anställda, tillfällig personal eller tillfälliga arbetstagare och volontärer

ANM. 1 till termpost: Olika typer av personal har olika typer och grader av *risk* (3.12) för mutor och kan behandlas olika i organisationens riskbedömning för mutor och riskförfaranden för mutor.

ANM. 2 till termpost: Se A.8.5 för vägledning om tillfällig personal eller tillfälliga arbetstagare.

**3.26**
**affärspartner**
extern part med vilken *organisationen* (3.2) har etablerat, eller planerar att etablera, någon form av affärsrelation

ANM. 1 till termpost: Affärspartner omfattar, men är inte begränsat till, klienter, kunder, gemensamma företag, gemensamma företagspartner, konsortiepartner, outsourcingleverantörer, entreprenörer, konsulter, underentreprenörer, leverantörer, säljare, rådgivare, ombud, distributörer, representanter, mellanhänder och investerare. Denna definition är avsiktligt bred och bör tolkas enligt organisationens riskprofil (3.12) för mutor för att tillämpas för affärspartner som rimligen kan utsätta organisationen för risker för mutor.

ANM. 2 till termpost: Olika typer av affärspartner utgör olika typer och grader av riskprofil (3.12) för mutor, och en *organisation* (3.2) har olika grader av förmåga att påverka olika typer av affärspartner. Olika typer av affärspartner kan behandlas olika i organisationens riskbedömning för mutor och förfaranden för hantering av risker för mutor.

ANM. 3 till termpost: Hänvisningen till ”affärer” i detta dokument kan tolkas brett för att avse sådana verksamheter som är relevanta för syftena med organisationens existens.

**3.27**
**offentlig tjänsteperson**
person som innehar ett lagstiftande-, administrativt- eller domarämbete, oavsett om de utnämnts, valts eller efterträder, eller en person som innehar en formell funktion, inklusive för en offentlig myndighet eller ett offentligt företag, eller tjänsteperson eller ombud för en offentlig nationell eller internationell organisation eller en kandidat till ett offentligt ämbete

ANM. 1 till termpost: För exempel på enskilda personer som kan anses vara offentliga tjänstepersoner, se avsnitt A.21.

**3.28**
**tredje part**
person eller organ som är oberoende gentemot *organisationen* (3.2)

ANM. 1 till termpost: Alla *affärspartner* (3.26) är tredje parter, men inte alla tredje parter är affärspartner.

**3.29**
**intressekonflikt**
situation där affärsintressen, familjeintressen eller ekonomiska, politiska eller personliga intressen skulle kunna blanda sig i personers omdömesförmåga när de fullgör sina förpliktelser mot *organisationen* (3.2)

**3.30**
**due diligence**
*process* (3.15) för att ytterligare bedöma typen och omfattningen av *risken* (3.12) för mutor och hjälpa *organisationer* (3.2) att ta beslut gällande specifika transaktioner, projekt, aktiviteter, *affärspartner* (3.26) och personal

Svensk ANM. till termpost: I kontexten ledningssystem mot mutor är det vanligt att använda "due diligence" även i det svenska språkbruket och därför används den termen i detta dokument (ibland förtydligat till "due diligence-process"). I Sverige används dock också bland annat termen "tillbörlig aktsamhet" för "due diligence".

# 4 Organisationens förutsättningar

## 4.1 Att förstå organisationen och dess förutsättningar

Organisationen ska avgöra vilka externa och interna frågor som är relevanta för dess syfte och som påverkar dess förmåga att nå de avsedda målen med sitt ledningssystem mot mutor. Dessa frågor omfattar, utan begränsningar, följande faktorer:

a) organisationens storlek, struktur och delegerade beslutsbefogenheter;

b) platserna och branscherna inom vilka organisationen verkar eller förväntar sig att verka;

c) typen, omfattningen och komplexiteten i organisationens aktiviteter och verksamheter;

d) organisationens affärsmodell;

e) enheterna som organisationen har kontroll över och enheter som utövar kontroll över organisationen;

f) organisationens affärspartner;

g) typen och omfattningen av kontakter med offentliga tjänstepersoner;

h) tillämpliga stadge-, regel-, avtals- och yrkesmässiga skyldigheter och förpliktelser.

ANM. En organisation har kontroll över en annan organisation om den direkt eller indirekt kontrollerar organisationens ledning (se A.13.1.3).

## 4.2 Att förstå intressenters behov och förväntningar

Organisationen ska bestämma:

a) vilka intressenter som är relevanta för ledningssystemet mot mutor;

b) dessa intressenters relevanta krav.

ANM. Vid identifiering av intressenters krav kan organisationen göra åtskillnad mellan intressenters obligatoriska krav, icke-obligatoriska förväntningar och frivilliga åtaganden gentemot intressenter.

## 4.3 Att bestämma omfattningen av ledningssystemet mot mutor

Organisationen ska bestämma avgränsningar och tillämplighet av ledningssystemet mot mutor för att fastställa dess omfattning.

När organisationen bestämmer denna omfattning ska den beakta:

a) de externa och interna frågor som det hänvisas till i 4.1;

b) kraven som det hänvisas till i 4.2;

c) resultaten av den riskbedömningen för mutor som det hänvisas till i 4.5.

Omfattningen ska finnas tillgänglig som dokumenterad information.

ANM. Se avsnitt A.2 för vägledning.

## 4.4 Ledningssystem mot mutor

Organisationen ska upprätta, dokumentera, införa, underhålla och ständigt ser över och, vid behov, förbättra ett ledningssystem mot mutor, inklusive nödvändiga processer och deras samverkan, enligt kraven i detta dokument.

Ledningssystemet mot mutor ska omfatta åtgärder som är utformade för att identifiera och utvärdera risken för, samt förebygga, upptäcka och hantera mutor.

ANM. 1 Det är inte möjligt att helt undanröja risken för mutor, och inget ledningssystem mot mutor kan förebygga och upptäcka alla mutor.

Ledningssystemet mot mutor ska vara rimligt och proportionellt, med beaktande av de faktorer som anges i 4.3.

ANM. 2 Se avsnitt A.3 för vägledning.

## 4.5 Riskbedömning för mutor

**4.5.1** Organisationen ska regelbundet utföra riskbedömning(ar) för mutor, som ska:

a) identifiera riskerna för mutor som organisationen rimligtvis kan förutse, med beaktande av de faktorer som anges i 4.1;

b) analysera, bedöma och prioritera de identifierade riskerna för mutor;

c) utvärdera om organisationens befintliga kontroller för att begränsa de bedömda riskerna för mutor är lämpliga och ändamålsenliga.

**4.5.2** Organisationen ska fastställa kriterier för att utvärdera sin nivå av risk för mutor, som ska beakta organisationens policyer och mål.

**4.5.3** Bedömningen av risker för mutor ska granskas:

a) regelbundet så att förändringar och ny information kan utvärderas på lämpligt sätt baserat på de tidpunkter och intervall som fastställs av organisationen;

b) i händelse av en betydande förändring av organisationens struktur eller verksamheter.

**4.5.4** Organisationen ska bevara dokumenterad information som visar att riskbedömningen för mutor har utförts och använts för att utforma eller förbättra ledningssystemet mot mutor.

ANM. Se avsnitt A.4 för vägledning.

# 5 Ledarskap

## 5.1 Ledarskap och åtagande

### 5.1.1 Styrande organ

När organisationen har ett styrande organ ska det tydligt visa ledarskap och åtagande i fråga om ledningssystemet mot mutor genom att:

a) godkänna organisationens policy mot mutor;

b) säkerställa att organisationens strategi och policy mot mutor överensstämmer med varandra;

c) vid planerade intervaller ta emot och granska information om innehållet i och användningen av organisationens ledningssystem mot mutor;

d) kräva att lämpliga och tillräckliga resurser, som behövs för ett välfungerande ledningssystem mot mutor, anslås och tillhandahålls;

e) utöva rimlig tillsyn av högsta ledningens införande av organisationens ledningssystem mot mutor samt systemets ändamålsenlighet.

Om organisationen inte har ett styrande organ ska dessa åtgärder utföras av högsta ledningen.

### 5.1.2 Högsta ledningen

Högsta ledningen ska tydligt utöva ledarskap och åtagande i fråga om ledningssystemet mot mutor genom att:

a) säkerställa att ledningssystemet mot mutor, inbegripet dess policy och mål, upprättas, införs, underhålls och granskas så att organisationens risker för mutor hanteras på lämpligt sätt;

b) säkerställa att kraven i ledningssystemet mot mutor integreras i organisationens processer;

c) tillhandahålla tillräckliga och lämpliga resurser för att ledningssystemet mot mutor ska fungera ändamålsenligt;

d) kommunicera policyn mot mutor internt och externt;

e) internt kommunicera betydelsen av ett effektivt ledningssystem mot mutor och av att uppfylla kraven i det;

f) säkerställa att ledningssystemet mot mutor är lämpligt utformat för att uppnå sina mål;

g) leda och stödja personalen så att den bidrar till ett väl fungerande ledningssystem mot mutor;

h) främja en lämplig kultur mot mutor inom organisationen;

i) främja ständig förbättring;