SVENSK STANDARD
SS-EN ISO 19011:2018

Fastställd/Approved: 2018-12-18
Publicerad/Published: 2018-12-20
Utgåva/Edition: 3
Språk/Language: svenska/Swedish, engelska/English
ICS: 03.100.70; 03.120.10; 03.120.20; 04.080; 04.100; 13.020.10

Vägledning för revision av ledningssystem (ISO 19011:2018)

Guidelines for auditing management systems (ISO 19011:2018)

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

Europastandarden EN ISO 19011:2018 gäller som svensk standard. Detta dokument innehåller den svenska språkversionen av EN ISO 19011:2018 följd av den officiella engelska språkversionen.

Denna standard ersätter SS-EN ISO 19011:2011 utgåva 2.

The European Standard EN ISO 19011:2018 has the status of a Swedish Standard. This document contains the Swedish language version of EN ISO 19011:2018 followed by the official English version.

This standard supersedes the Swedish Standard SS-EN ISO 19011:2011, edition 2.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS 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, who can also provide general information about Swedish and foreign standards.

Denna standard är framtagen av kommittén för Bedömning av överensstämmelse, SIS/TK 316.

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.

EUROPASTANDARD
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO 19011

Juli 2018

ICS 03.100.70; 03.120.20

Ersätter EN ISO 19011:2011

Svensk version

Vägledning för revision av ledningssystem (ISO 19011:2018)

Lignes directrices pour l'audit des systèmes de management (ISO 19011:2018)

Guidelines for auditing management systems (ISO 19011:2018)

Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018)

Denna standard är den officiella svenska versionen av EN ISO 19011:2018. För översättningen svarar SIS.

Denna Europastandard antogs av CEN den 18 juni 2018.

CEN-medlemmarna är förpliktade att följa fordringarna i CEN/CENELECs interna bestämmelser som anger på vilka villkor denna Europastandard i oförändrat skick skall ges status som nationell standard. Aktuella förteckningar och bibliografiska referenser rörande sådana nationella standarder kan på begäran erhållas från CENs centralsekretariat eller från någon av CENs medlemmar.

Denna Europastandard finns i tre officiella versioner (engelsk, fransk och tysk). En version på något annat språk, översatt under ansvar av en CEN-medlem till sitt eget språk och anmäld till CENs centralsekretariat, har samma status som de officiella versionerna.

CENs medlemmar är de nationella standardiseringsorganen i Belgien, Bulgarien, Cypern, Danmark, Estland, Finland, Frankrike, Grekland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Makedonien, Malta, Nederländerna, Norge, Polen, Portugal, Rumänien, Schweiz, Serbien, Slovakien, Slovenien, Spanien, Storbritannien, Sverige, Tjeckien, Turkiet, Tyskland, Ungern och Österrike.

CEN

European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. Nr. EN ISO 19011:2018 Sv

Innehåll

Sida

Förord

Texten till den internationella standarden från ISO/TC EN ISO 19011:2018 har överförts till Europastandard av CEN/TC CEN/SS F20. Sekretariatet hålls av ANSI (USA).

Denna Europastandard ska ges status av nationell standard, antingen genom publicering av en identisk text eller genom ikraftsättning senast januari 2019, och motstridande nationella standarder ska upphävas senast januari 2019.

Denna Europastandard har utarbetats under mandat som CEN fått av Europeiska Kommissionen och EFTA. Den stöder grundläggande krav i EUs direktiv.

Sambandet med EU-direktiv beskrivs i bilaga ZA, som ingår som en informativ del i denna standard.

Enligt CEN/CENELECs interna bestämmelser ska följande länder fastställa denna Europastandard: Belgien, Bulgarien, Cypern, Danmark, Estland, Finland, Frankrike, Grekland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Makedonien, Malta, Nederländerna, Norge, Polen, Portugal, Rumänien, Schweiz, Serbien, Slovakien, Slovenien, Spanien, Storbritannien, Sverige, Tjeckien, Turkiet, Tyskland, Ungern och Österrike.

Det bör uppmärksammas att vissa beståndsdelar i denna Europastandard möjligen kan vara föremål för patenträtter. CEN ska inte hållas ansvarig för att identifiera någon eller alla sådana patenträtter.

Ikraftsättningsnotering

Texten i den internationella standarden ISO 19011:2018 har godkänts av CEN som Europastandard utan någon ändring.

Orientering

Sedan den andra utgåvan av detta dokument publicerades år 2011 har ett antal nya ledningssystemstandarder publicerats, varav flera har en gemensam struktur, identiska grundkrav och gemensamma termer och definitioner. Som en följd av detta är det nu nödvändigt att betrakta revision av ledningssystem i ett vidare perspektiv och att ge vägledning som är mer allmän. Revisionsresultat kan ge information till analysdelen i affärsplaneringen och göra det möjligt att identifiera förbättringsbehov och förbättringsåtgärder.

En revision kan genomföras utifrån en rad revisionskriterier, separat eller i kombination, inklusive men inte begränsat till:

- krav som anges i en eller flera ledningssystemstandarder,
- policyer och krav som fastställts av relevanta intressenter,
- lagkrav och regelkrav,
- en eller flera processer inom ledningssystemet som definierats av organisationen eller andra parter,
- ledningssystemplan(er) för att uppnå specifika resultat med ett ledningssystem (t.ex. kvalitetsplan och projektplan).

Detta dokument ger vägledning för alla organisationer, oavsett storlek och typ, samt för revisioner med olika omfattning, inklusive revisioner som utförs av stora revisionsgrupper, vilket är vanligt för större organisationer, och revisioner som genomförs av enskilda revisorer, oavsett om organisationen är liten eller stor. Denna vägledning bör anpassas efter revisionsprogrammets innehåll, komplexitet och storlek.

Detta dokument inriktas på interna revisioner (förstapartsrevisioner) och organisationers revisioner av externa leverantörer och andra externa intressenter (andrapartsrevisioner). Dokumentet kan också vara användbart vid externa revisioner som genomförs för andra ändamål än certifiering av ledningssystem från tredje part. ISO/IEC 17021-1 innehåller krav för revision av ledningssystem för tredjepartscertifiering och detta dokument kan ge ytterligare användbar vägledning (se tabell 1).

Tabell 1 — Olika typer av revisioner

Förstapartsrevision	Andrapartsrevision	Tredjepartsrevision
Intern revision	Revision av extern leverantör	Revision för certifiering och/eller ackreditering
	Revision av annan extern intressent	Revision som föreskrivs enligt lag, av myndighet eller liknande

För att göra detta dokument enklare att läsa föredras singularformen av ”ledningssystem”, men läsaren kan anpassa tillämpningen av vägledningen till den egna situationen. Detta gäller även användningen av formerna ”person” och ”personer” liksom ”revisor” och ”revisorer”.

Detta dokument är avsett att kunna tillämpas av en rad olika potentiella användare, däribland revisorer, organisationer som tillämpar ledningssystem och organisationer som behöver genomföra revisioner av ledningssystem till följd av avtal eller föreskrifter. De som utarbetar egna krav med anknytning till revision kan ta hjälp av denna vägledning.

Vägledningen i detta dokument kan också användas för egenbedömning och kan vara användbar för organisationer som deltar i utbildning av revisorer eller personcertifiering.

Vägledningen i detta dokument är avsedd att vara flexibel. Såsom anges på olika ställen i texten, kan vägledningens användning variera beroende på storleken och mognadsgraden hos organisationens ledningssystem. Hänsyn bör också tas till karaktären och komplexiteten i den organisation som ska revideras, liksom till målet för och omfattningen på de revisioner som ska genomföras.

I detta dokument används begreppet kombinerad revision, vilket innebär att två eller flera ledningssystem inom olika ämnesområden revideras tillsammans. Om systemen är integrerade i ett enda ledningssystem är principerna och processerna för revision desamma som för en kombinerad revision (som ibland kallas en integrerad revision).

Detta dokument ger vägledning för att hantera ett revisionsprogram, för att planera och genomföra revision av ett ledningssystem samt vad gäller kompetens hos och utvärdering av en revisor och en revisionsgrupp.

1 Omfattning

Detta dokument ger vägledning för revision av ledningssystem, inklusive principer för revision, hantering av revisionsprogram, genomförande av revisioner av ledningssystem samt vägledning för utvärdering av kompetens hos den eller de personer som deltar i revisionsprocessen. Dessa aktiviteter omfattar den eller de personer som hanterar revisionsprogrammet, revisorer och revisionsgrupper.

Det kan tillämpas på alla organisationer som har behov av att planera och genomföra interna eller externa revisioner av ledningssystem eller hantera revisionsprogram.

Det är möjligt att tillämpa dokumentet på andra typer av revisioner, förutsatt att särskild uppmärksamhet ägnas åt den specifika kompetens som behövs.

2 Normativa hänvisningar

Detta dokument innehåller inga normativa hänvisningar.

3 Termer och definitioner

För tillämpning av detta dokument gäller de termer och definitioner som följer nedan.

3.1
revision
systematisk, oberoende och dokumenterad process för att inhämta *objektiva belägg* (3.8) och objektivt utvärdera dessa i syfte att avgöra i vilken utsträckning *revisionskriterierna* (3.7) har uppfyllts

Anm. 1 till termpost: Interna revisioner, ibland även kallade förstapartsrevisioner, genomförs av eller på uppdrag av organisationen.

Anm. 2 till termpost: Externa revisioner omfattar de revisioner som vanligen kallas andraparts- och tredjepartsrevisioner. Andrapartsrevisioner genomförs av organisationens intressenter, till exempel kunder, eller av andra personer för deras räkning. Tredjepartsrevisioner genomförs av oberoende revisionsorganisationer, till exempel organisationer som erbjuder certifiering/registrering av överensstämmelse eller myndigheter.

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.1 — Definitionen har ändrats. Anm. 2 och 3 till termposten har ändrats och Anm. 1, 4 och 5 till termpost har tagits bort.]

3.2
kombinerad revision
samtidig *revision* (3.1) av två eller flera *ledningssystem* (3.18) hos en *organisation eller verksamhet som revideras* (3.13)

Anm. 1 till termpost: När två eller flera ämnesområdesspecifika ledningssystem integreras till ett enda ledningssystem kallas detta ett integrerat ledningssystem.

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.2, ändrad]

3.3
gemensam revision
samtidig*revision* (3.1) av en *organisation eller verksamhet som revideras* (3.13), utförd av två eller fler reviderande *organisationer* (3.2.1)

[KÄLLA: ISO 9000:2015, 3.13.3, ändrad – Definitionen har ändrats.]

3.4
revisionsprogram
en eller flera *revisioner* (3.1) planerade att utföras under en viss tidsperiod och för ett visst ändamål

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.4, ändrad — formulering har lagts till i definitionen]

3.5
revisionsomfattning
omfattning och avgränsningar för en *revision* (3.1)

Anm. 1 till termpost: Revisionsomfattningen innefattar i allmänhet en beskrivning av fysiska och virtuella platser, funktioner, organisationsenheter, aktiviteter och processer liksom den tidsperiod som avses.

Anm. 2 till termpost: En virtuell plats är en plats där en organisation utför arbete eller tillhandahåller en tjänst via en webbaserad miljö, vilket gör det möjligt för personer att utföra arbetsuppgifter oavsett var de befinner sig.

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.5, ändrad — Anm. 1 till termpost har ändrats och Anm. 2 till termpost har lagts till]

3.6
revisionsplan
beskrivning av aktiviteter och arrangemang för en *revision* (3.1)

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.6, ändrad – Definitionen har ändrats]

3.7
revisionskriterier
krav (3.23) som används som referens och mot vilka *objektiva belägg* (3.8) jämförs

Anm. 1 till termpost: Om revisionskriterierna utgör rättsliga krav (inklusive lagkrav och regelkrav) används ofta termerna ”efterlevnad” och ”bristande efterlevnad” i *revisionsiakttagelser* (3.10).

Anm. 2 till termpost: Krav kan inbegripa policyer, förfaranden, arbetsinstruktioner, rättsliga krav, avtalsmässiga krav etc.

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.7, ändrad — definitionen har ändrats och Anm. 1 och 2 till termpost har lagts till]

3.8
objektiva belägg
uppgifter som stödjer förekomsten av eller sanningshalten hos någonting

Anm. 1 till termpost: Objektiva belägg kan erhållas genom observation, mätning, prövning eller på annat sätt.

Anm. 2 till termpost: Objektiva belägg för *revisionens* (3.1) ändamål utgörs i allmänhet av redovisande dokument, faktauppgifter och annan information som är relevant med hänsyn till *revisionskriterierna* (3.7) och som kan verifieras.

[KÄLLA: Anpassad efter ISO 9000:2015, 3.8.3 – definitionen och anmärkningarna har ändrats]

3.9
revisionsbelägg
redovisande dokument, faktauppgifter och annan information som är relevant med hänsyn till *revisionskriterierna* (3.7) och som är verifierbara

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.8— definitionen har ändrats]

3.10
revisionsiakttagelser
resultat av utvärderingen av insamlade *revisionsbelägg* (3.9) mot *revisionskriterierna* (3.7)

Anm. 1 till termpost: Revisionsiakttagelser kan visa på antingen *överensstämmelse* (3.20) eller *avvikelse* (3.21).

Anm. 2 till termpost: Revisionsiakttagelser kan medföra att risker och förbättringsområden identifieras eller att god praxis kartläggs.

Anm. 3 till termpost: Om revisionskriterierna utgörs av lagkrav eller myndighetskrav används termerna ”efterlevnad” och ”bristande efterlevnad” för revisionsiakttagelser.

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.9 — termen, definitionen och anmärkningarna till termposten har ändrats.]

3.11
revisionsslutsats
resultat av en *revision* (3.1), efter beaktande av revisionsmålen och samtliga *revisionsiakttagelser* (3.10)

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.10 – definitionen har ändrats]

3.12
revisionens uppdragsgivare
organisation eller person som begär en *revision* (3.1)

Anm. 1 till termpost: Vid en intern revision kan uppdragsgivaren också vara den *organisation eller verksamhet som revideras* (3.13) eller den person(er) som hanterar revisionsprogrammet. Begäran om extern revision kan lämnas av t.ex. tillsynsmyndigheter, avtalsparter samt potentiella eller befintliga kunder.

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.11 — Anm. 1 till termpost har lagts till.]

3.13
organisation eller verksamhet som revideras
hela eller delar av en organisation som ska revideras

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.12]

3.14
revisionsgrupp
en eller flera personer som genomför en *revision* (3.1), med stöd, om så är nödvändigt, av *tekniska experter* (3.16)

Anm. 1 till termpost: En *revisor* (3.15) i *revisionsgruppen* utses till ledare för revisionsgruppen.

Anm. 2 till termpost: Revisorer under upplärning kan ingå i revisionsgruppen.

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.14 — definitionen och anmärkningarna till termposten har ändrats.]

3.15
revisor
person som genomför en *revision* (3.1)

[KÄLLA: ISO 9000:2015, 3.13.15]

3.16
teknisk expert
<revisions>person som tillför särskild sakkunskap eller expertis till *revisionsgruppen* (3.14)

Anm. 1 till termpost: Särskild sakkunskap eller expertis är sådan som hänför sig till den organisation, aktivitet, process, produkt, tjänst eller det ämnesområde som revideras eller till språk eller kulturella förhållanden.

Anm. 2 till termpost: En teknisk expert för *revisionsgruppen* (3.14) agerar inte som *revisor* (3.15).

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.16 — Anm. 1 och 2 till termposten har ändrats.]

3.17
observatör
person som medföljer *revisionsgruppen* (3.14) men som inte agerar som *revisor* (3.15)

[KÄLLA: Anpassad efter ISO 9000:2015, 3.13.17 – definitionen har ändrats och Anm. 1 till termposten har tagits bort.]

3.18
ledningssystem
samverkande eller av varandra påverkande delar av en organisation för att upprätta policyer och mål samt *processer* (3.24) för att uppnå dessa mål

Anm. 1 till termpost: Ett ledningssystem kan omfatta ett enstaka ämnesområde eller flera ämnesområden, t.ex. kvalitetsledning, ekonomistyrning eller miljöledning.

Anm. 2 till termpost: Ledningssystemet beskriver organisationens struktur, roller och ansvar, planering, verksamhet, policyer, praxis, regler, värderingar, mål och processer för att uppnå dessa mål.

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 organisationer.

[KÄLLA: Anpassad efter ISO 9000:2015, 3.5.3 — Anm. 1 och Anm. 4 till termposten har tagits bort

3.19
risk
osäkerhetens effekt

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

Anm. 2 till termpost: Osäkerhet är det tillstånd, också partiellt, av bristande information som har att göra med förståelse för eller kunskap om en händelse, dess konsekvenser och 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 för förekomsten (enligt definition i ISO Guide 73:2009, 3.6.1.1).

[KÄLLA: Anpassad efter ISO 9000:2015, 3.7.9 — Anm. 3 till termpost har ändrats och anmärkning 5 och 6 har tagits bort.]

3.20
överensstämmelse
uppfyllande av ett *krav* (3.23)

[KÄLLA: Anpassad efter ISO 9000:2015, 3.6.11 — Anm. 1 till termpost har tagits bort.]

3.21
avvikelse
icke-uppfyllande av ett *krav* (3.23)

[KÄLLA: Anpassad efter ISO 9000:2015, 3.6.2 — Anm. 1 till termpost har tagits bort.]

3.22
kompetens
förmåga att tillämpa kunskaper och färdigheter för att uppnå avsett resultat

[KÄLLA: Anpassad efter ISO 9000:2015, 3.10.4 — definitionen har ändrats och anmärkningarna till termposten har tagits bort.]

3.23
krav
behov eller förväntningar som är angivna, underförstådda eller obligatoriska

Anm. 1 till termpost: ”Underförstådd” innebär att det är vanligt eller allmänt vedertaget att det berörda behovet eller förväntningen underförstås inom organisationen och av intressenter.

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

[KÄLLA: Anpassad efter ISO 9000:2015, 3.6.4 — Anm. 3, 4, 5 och 6 till termpost har tagits bort.]

3.24
process
aktiviteter som samverkar eller påverkar varandra, och som använder underlag för att åstadkomma ett avsett resultat

[KÄLLA: Anpassad efter ISO 9000:2015, 3.4.1 — definitionen har ändrats och anmärkningarna till termposten har tagits bort.]

3.25
prestanda
mätbart resultat

Anm. 1 till termpost: Prestanda kan relatera till kvantitativa eller kvalitativa iakttagelser.

Anm. 2 till termpost: Prestanda kan relatera till ledning av aktiviteter, *processer* (3.24), produkter, tjänster, system eller organisationer.

[KÄLLA: Anpassad efter ISO 9000:2015, 3.7.8 — Anm. 3 till termpost har tagits bort.]

3.26
verkan
omfattning i vilken planerade aktiviteter har genomförts och planerade resultat har uppnåtts

[KÄLLA: Anpassad efter ISO 9000:2015, 3.7.11 — Anm. 1 till termpost har tagits bort.]

4 Revisionsprinciper

Revision grundar sig på ett antal principer. Dessa bör bidra till att göra revisionen till ett effektivt och tillförlitligt verktyg till stöd för ledningens policy och styrning, bl.a. genom att ge information som en organisation kan agera utifrån för att förbättra sin verksamhet. Tillämpning av dessa principer är en förutsättning för att kunna presentera relevanta och godtagbara revisionsslutsatser och för att göra det möjligt för revisorer som arbetar oberoende av varandra att dra likartade slutsatser under likartade förhållanden.

Den vägledning som ges i avsnitt 5 till 7 grundas på följande sju principer.

a) Integritet: grund för yrkesmässighet

Revisorer och den eller de personer som hanterar ett revisionsprogram bör

- utföra sitt arbete på ett etiskt, ärligt och ansvarsfullt sätt
- endast åta sig sådana revisionsuppgifter som de har kompetens att utföra
- utföra sitt arbete på ett opartiskt sätt, dvs. förbli rättvisa och opartiska i sitt arbete
- vara uppmärksamma på påverkan som skulle kunna inverka på deras bedömning vid en revision.

b) Rättvisande rapportering: skyldighet att rapportera sanningsenligt och korrekt

Revisionsiakttagelser, revisionsslutsatser och revisionsrapporter bör avspegla revisionsarbetet på ett sanningsenligt och korrekt sätt. Större hinder som uppkommer under revisionen samt skilda uppfattningar mellan revisionsgruppen och den reviderade organisationen som inte har retts ut bör rapporteras. Kommunikationen bör vara sanningsenlig, korrekt, objektiv, tydlig och komplett och ske vid lämplig tidpunkt.

c) Tillbörlig yrkesmässig noggrannhet: tillämpning av noggrannhet och omdöme vid revision

Revisorer bör visa prov på tillbörlig aktsamhet med hänsyn till vikten av den uppgift de utför och det förtroende som de har fått av uppdragsgivaren och andra intressenter. En viktig faktor för att kunna utföra arbetet med tillbörlig yrkesmässig noggrannhet är att revisorn har förmåga att göra välgrundade bedömningar i alla revisionssituationer.

d) Sekretess: säkerhet vid hantering av information

Revisorer bör iaktta försiktighet när det gäller användning och skydd av sådan information som de får tillgång till under sitt arbete. Information som rör revision bör inte användas på ett otillbörligt sätt för egen vinning av revisorn eller av uppdragsgivaren, eller på något sätt som kan skada den reviderade organisationens eller verksamhetens berättigade intressen. Detta begrepp omfattar korrekt hantering av känslig och konfidentiell information.

e) Oberoende: grund för en opartisk revision och objektiva revisionsslutsatser

Där det är praktiskt möjligt bör revisorer ha en oberoende ställning i förhållande till den verksamhet som revideras och bör alltid agera på sådant sätt att de är fria från förutfattade meningar och intressekonflikter. Vid interna revisioner bör revisorerna, där så är praktiskt möjligt, ha en oberoende ställning i förhållande till de funktioner som revideras. Revisorer bör förhålla sig objektiva under hela revisionsförfarandet för att säkerställa att revisionsiakttagelser och revisionsslutsatserna endast grundas på revisionsbeläggen.

I mindre organisationer är det inte alltid möjligt för en intern revisor att ha en helt oberoende ställning i förhållande till den verksamhet som revideras, men allt som är möjligt bör göras för att motverka förutfattade meningar och uppmuntra objektivitet.

f) Evidensbaserad metod: rationell metod för att komma fram till tillförlitliga och reproducerbara revisionsslutsatser i ett systematiskt revisionsförfarande

Revisionsbelägg bör vara verifierbara. De bygger vanligen på ett urval av tillgänglig information, eftersom en revision genomförs under en begränsad tidsrymd och med begränsade resurser. Lämpliga urvalsmetoder bör användas eftersom det finns ett nära samband mellan urval och revisionsslutsatsernas trovärdighet.

g) Riskbaserad metod: revisionsmetod där risker och möjligheter beaktas

Den riskbaserade metoden bör spela en viktig roll i planeringen, genomförandet och rapporteringen av revisioner i syfte att säkerställa att fokus vid revisioner ligger på de frågor som är viktiga för uppdragsgivaren och för att uppnå revisionsprogrammets mål.

5 Hantera revisionsprogram

5.1 Allmänt

Revisionsprogram bör upprättas som kan omfatta revisioner som tar hänsyn till en eller flera ledningssystemstandarder eller andra krav. Revisionerna kan genomföras antingen separat eller i kombination (kombinerad revision).

Revisionsprogrammets omfattning bör baseras på den reviderade organisationens eller verksamhetens storlek och karaktär liksom på det eller de reviderade ledningssystemens typ, funktion, komplexitet, risker och möjligheter samt mognadsgrad.

Ledningssystemets funktion kan vara ännu mer komplex om merparten av de viktiga funktionerna utkontrakteras och hanteras under ledning av andra organisationer. Särskild hänsyn bör tas till var de viktigaste besluten fattas och vilka som utgör högsta ledningen för ledningssystemet.

I fall med flera platser/anläggningar (t.ex. i olika länder), eller där viktiga funktioner utkontrakteras och hanteras under ledning av en annan organisation, bör särskild hänsyn tas till utformningen, planeringen och valideringen av revisionsprogrammet.

I små eller mindre komplexa organisationer kan revisionsprogrammets omfattning anpassas därefter.

För att förstå den reviderade organisationens eller verksamhetens förutsättningar bör revisionsprogrammet ta hänsyn till dess:

- organisationsmål
- relevanta externa och interna frågor
- relevanta intressenters behov och förväntningar
- informationssäkerhet och sekretesskrav.

Planeringen av interna revisionsprogram och, i vissa fall program för revision av externa leverantörer, kan genomföras i syfte att bidra till att andra mål inom organisationen uppfylls.

Den eller de personer som hanterar revisionsprogrammet bör säkerställa att revisionens integritet upprätthålls och att inte revisionen påverkas på ett otillbörligt sätt.

Vid fördelningen av resurser och införandet av metoder bör revision av områden av betydelse för ledningssystemet med högre risk och lägre prestandanivå prioriteras.

Kompetenta personer bör utses att hantera revisionsprogrammet.

Revisionsprogrammet bör innefatta information och identifiera resurser som gör det möjligt att genomföra revisionerna på ett effektivt och verkningsfullt sätt inom angiven tidsram. Informationen bör innefatta:

a) revisionsprogrammets mål

b) risker och möjligheter förenade med revisionsprogrammet (se 5.3) och åtgärder för att hantera dem

c) omfattning (utsträckning, avgränsning, platser) för respektive revision inom revisionsprogrammet

d) schemaläggning (antal/varaktighet/frekvens) av revisionerna

e) revisionstyper, t.ex. intern eller extern

f) revisionskriterier

g) revisionsmetoder som ska användas

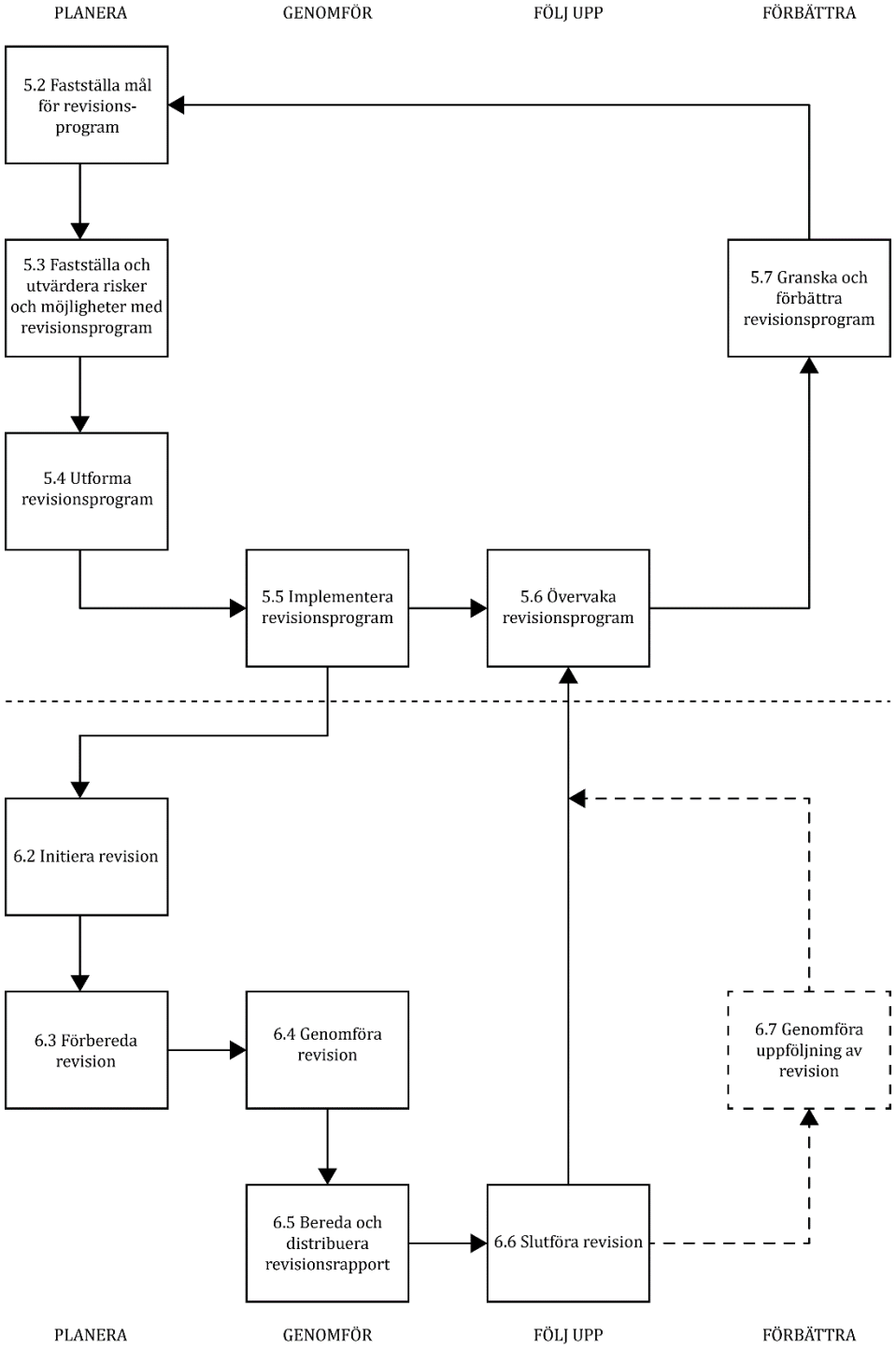
h) urvalskriterier för revisionsgruppmedlemmar

i) relevant dokumenterad information.

Delar av denna information är kanske inte tillgänglig förrän en mer detaljerad revisionsplanering är slutförd.

Genomförandet av revisionsprogrammet bör löpandeövervakas och mätas (se 5.6) för att säkerställa att målen uppfylls. Revisionsprogrammet bör granskas i syfte att identifiera behov av ändringar och eventuella förbättringsmöjligheter (se 5.7).

Figur 1 visar processflödet för hantering av revisionsprogram.



ANM. 1 Figuren illustrerar tillämpningen av PDCA-modellen (planera, genomför, följ upp, förbättra) i detta dokument.

ANM. 2 Numreringen av avsnitt/underavsnitt avser motsvarande avsnitt/underavsnitt i detta dokument.

Figur 1 — Processflöde för hantering av ett revisionsprogram

5.2 Fastställa mål för revisionsprogram

Revisionens uppdragsgivare bör säkerställa att revisionsprogrammets mål upprättas för att styra planering och genomförande av revisioner samt säkerställa att revisionsprogrammet genomförs på ett verkningsfullt sätt. Revisionsprogrammets mål bör överensstämma med uppdragsgivarens strategiska inriktning och ge stöd till ledningssystemets policy och mål.

När målen sätts kan följande beaktas:

a) behov och förväntningar hos relevanta intressenter, både externa och interna

b) egenskaper hos och krav på processer, produkter, tjänster och projekt, och ändringar därav

c) krav från ledningssystemet

d) behov av utvärdering av externa leverantörer

e) den reviderade organisationens eller verksamhetens prestanda och ledningssystemets mognadsgrad, enligt vad som framgår av prestandaindikatorer (t.ex. relevanta nyckeltal), förekomsten av bristande efterlevnad eller incidenter eller klagomål från intressenter

f) identifierade risker och möjligheter för den reviderade organisationen eller verksamheten

g) resultat vid tidigare revisioner.

Exempel på mål för revisionsprogram kan inkludera att

- identifiera möjligheter till förbättring av ett ledningssystem och dess prestanda
- utvärdera den reviderade organisationens eller verksamhetens förmåga att fastställa sina förutsättningar
- utvärdera den reviderade organisationens eller verksamhetens förmåga att fastställa risker och möjligheter samt att identifiera och implementera effektiva åtgärder för att hantera dem
- uppfylla alla relevanta krav, t.ex. lagkrav och regelkrav, åtaganden i fråga om efterlevnad, krav för certifiering mot en ledningssystemstandard
- upprätta och bibehålla förtroende för en extern leverantörs förmåga
- bestämma fortsatt lämplighet, tillräcklighet och verkan vad gäller den reviderade organisationens eller verksamhetens ledningssystem
- utvärdera förenligheten och överensstämmelsen mellan ledningssystemets mål och organisationens strategiska inriktning.

5.3 Fastställa och utvärdera risker och möjligheter med revisionsprogram

Det finns risker och möjligheter förenade med den reviderade organisationens eller verksamhetens förutsättningar som kan kopplas till ett revisionsprogram och påverka dess måluppfyllelse. Den eller de personer som hanterar revisionsprogrammet bör identifiera och för uppdragsgivaren presentera vilka risker och möjligheter samt resurskrav som beaktas när revisionsprogrammet upprättas, så att dessa kan hanteras på lämpligt sätt.

Det kan finnas risker som är förenade med följande:

a) planering, t.ex. att inte lyckas sätta relevanta revisionsmål eller fastställa revisionernas omfattning, antal, varaktighet, plats och schemaläggning

b) resurser, t.ex. att inte anslå tillräckligt med tid, utrustning och/eller utbildning för att utforma revisionsprogrammet eller genomföra en revision

c) val av revisionsgrupp, t.ex. otillräcklig samlad kompetens för att genomföra revisioner på ett effektivt sätt

d) kommunikation, t.ex. ineffektiva externa/interna kommunikationsprocesser/ kommunikationskanaler

e) genomförande, t.ex. ineffektiv samordning av revisioner inom revisionsprogrammet eller att hänsyn inte tas till informationssäkerhet och sekretess