Attestasjons-tjenester

Hvordan forstå og etablere
Attestasjonstjenester i din organisasjon.

Velg den riktige samarbeidspartner – den med bransjeforståelse, kunnskap og innsikt i de mest kritiske fohold.

2016

kpmg.com

Med økende global konkurranse og økte kostander har outsourcing av forretningskritiske funksjoner og prosesser blitt stadig mer vanlig. Hva kan gjøres for å få opprettholde tilliten til egne forretningsprosesser?

KPMG har en løsning for å bistå selskapene slik at alle krav til kvalitet opprettholdes.

Innhold

Tjenesteleverandørers økende behov for attestering 4

Løsninger tilpasset dine behov for attesteringstjenester 5

Bruksområder for SOC-rapporter 7

Oversikt over SOC-rapportering 8

Rapporteringstyper og -struktur 12

SOC-rapportstruktur 13

Forberedelse og utstedelse av en SOC-rapport 14

KPMGs attesteringstjenester er skreddersydd for din virksomhet 15

Tjenesteleverandørers økende behov for attestering

Bedrifter setter ut stadig flere funksjoner som ikke er knyttet til kjernevirksomheten. Likevel er de til syvende og sist selv ansvarlig for sitt eget kontrollmiljø. Dette har ført til større etterspørsel etter attestering av kontroller for aktiviteter som utføres av tredjeparter. KPMG forstår risikoene og utfordringene knyttet til outsourcing og kan hjelpe tjenesteleverandører med å møte den voksende etterspørselen etter dokumentasjon.

Økt global konkurranse
Global konkurranse og globalt kostnadspress har ført til at bedrifter setter ut stadig flere funksjoner til spesialiserte tjenesteleverandører. Outsourcing er ikke lenger begrenset til rutinemessig kontorstøtte. Det omfatter nå ofte igangsetting, registrering, behandling og rapportering av transaksjoner, noe som kan påvirke organisasjonens regnskaper og sentrale forretningsprosesser direkte.

Nye trusler
Outsourcing av mer informasjon fører til høyere risiko og nye sikkerhetstrusler. Bedrifter kan risikere at driften, renommeet og økonomien deres blir rammet, hvis manglende sikkerhet hos eksterne tjenesteleverandører fører til reelle eller antatte brudd på kundenes informasjonssikkerhet.

Forbrukere er også mer opptatt av hva som gjøres for å beskytte deres personlige opplysninger og helseinformasjon.

Bedriftenes risiko øker når eksterne tjenesteleverandører behandler og lagrer kundenes private og/eller konfidensielle informasjon, utfører transaksjonsbehandling for flere kunder og blir gjenstand for kunders eller myndigheters revisjon. En uavhengig gjennomgang av outsourcede kritiske IT-funksjoner og forretningsmessige funksjoner kan hjelpe bedriftene med å identifisere og kontrollere disse risikoene.

Myndighetskrav
Stadig strengere myndighetskrav (f.eks. amerikanske Sarbanes-Oxley-Act) tvinger organisasjoner til å fremskaffe dokumentasjon på at kontrollene deres er effektive. I likhet med håndtering av økt global konkurranse, forutsetter også overholdelse av myndighetspålagte standarder dokumentasjon på at outsourcede IT-systemer og -prosesser har de rette kontrollene.

Konkrete fordeler
Både tjenesteleverandører og brukerorganisasjoner kan oppnå betydelige fordeler med SOC-rapportering (Service Organization Control). Brukerorganisasjoner får trygghet for de outsourcede sidene av virksomheten sin, mens tjenesteleverandørene oppnår umiddelbare gevinster:

- Det blir færre avbrudd i forretningsdriften, ettersom det ikke lenger er nødvendig at en rekke brukerorganisasjoner utfører revisjoner
- Det interne kontrollmiljøet styrkes og blir mer finmasket som et resultat av uavhengige undersøkelser i forbindelse med attestering
- Revisjons- og kontrollaktiviteter blir mer effektive ved å kombinere leverandører av attesterings- og revisjonstjenester
- Et transparent kontrollmiljø skaper tillitt i markedet
- Løsninger tilpasset dine behov for attesteringstjenester

Løsninger tilpasset dine behov for attesteringstjenester

KPMG leverer en rekke attesteringstjenester som hjelper organisasjoner med å overholde tredjeparters krav om uavhengige undersøkelser av prosessene, IT-miljøene og systemene deres.

De vanligste attesteringstjenestene omfatter SOC (Service Organization Control) 1- og 2-rapporter, som utarbeides i samsvar med henholdsvis ISAE 3402- og ISAE 3000-standarden. En SOC-undersøkelse er en bredt anerkjent dokumentasjon på at en tjenesteleverandør har vært gjennom en uavhengig og grundig granskning av sine interne kontroller.

SOC-rapporter

Oversikt

I 2009 lanserte den internasjonale revisjonskomiteen IAASB standarden ISAE 3402, som har blitt en internasjonalt anerkjent standard for attesteringsoppdrag hos tjenesteleverandører. Denne rapporten er også kjent som en SOC1-rapport, og utarbeides i USA i samsvar med SSAE 18-standarden fra USAs revisorforening AICPA.

En ISAE 3402-rapport skal være til hjelp for tjeneste-leverandørenes kunder og deres revisorer ved regnskapsrevisjon, og dekker tjenester som sannsynligvis er relevante for brukerorganisasjonenes interne kontroll over regnskapsrapportering (ICOFR). Siden ISAE 3402-rapporter ikke er ment å omfatte kontroller som ikke er knyttet til regnskapsrapportering, ble ISAE 3000-rapportering (eller SOC2) utviklet som et alternativ for å hjelpe tjenesteleverandører med å dekke et bredere spekter av spesifikke behov blant brukerne – som å håndtere bekymringer i forbindelse med personvern, konfidensialitet og tilgjengelighet.

ISAE 3402

ISAE 3402-rapporten gir veiledning som gjør det mulig for en uavhengig revisor (tjenesterevisor) å uttale seg om en tjenesteleverandørs beskrivelse av systemet sitt og egnetheten til utformingen av og den driftsmessige effektiviteten til de tilhørende kontrollene, i en revisorrapport for tjenester. Bedrifter er pålagt å definere kontrollmål og -aktiviteter som dekker kundenes behov. Rapporten dekker typisk generelle IT-kontroller (f.eks. sikkerhetsadministrasjon, fysisk og logisk sikkerhet, endringsstyring, nettverks- og systemovervåking samt systemutvikling), transaksjonsbehandling, transaksjonssøknader og andre tjenestespesifikke kontroller.

ISAE 3000

SOC2-rapporter utarbeidet i samsvar med ISAE 3000-standarden bygger på en samling spesifikke krav (Trust Services Principles and Criteria) fra AICPA og den kanadiske revisorforeningen CICA. Kravene omfatter spesifikt definerte prinsipper og kriterier for sikkerhet, tilgjengelighet, konfidensialitet, prosessintegritet og personvern. Dette er gjort på en modulbasert måte, slik at en SOC2-rapport (heretter omtalt som en ISAE 3000-rapport) kan dekke ett eller flere av prinsippene, avhengig av behovene til tjenesteleverandøren og dens brukere.

ISAE 3402-rapporter forutsetter imidlertid at tjeneste-leverandøren definerer kontrollmål som sannsynligvis er relevante for kundenes (brukerorganisasjonenes) interne kontroll over regnskapsrapportering (ICOFR).

ISAE 3000-rapporter omfatter typisk flere områder som gir kundene større verdi enn bare ICOFR. Bransjeundersøkelser rangerer for eksempel stadig sikkerhet og tilgjengelighet som viktigste hensyn ved overgang til nettskyen. ISAE 3000 utgjør en effektiv mekanisme for å fremskaffe attestering fra tredjepart på disse områdene.

SOC3

SOC3-rapporten brukes når de generelle resultatene av et ISAE 3000-oppdrag skal kommuniseres til mange brukere uten å måtte avsløre detaljerte kontroller og testresultater. En SOC3-rapport kan publiseres på tjenesteleverandørens nettsted med SOC-autentisitetsmerket.

ISAE 3402-kontroller for regnskapsrapportering

- økonomitjenester – forvaltningstjenester
- behandling av krav til helsevesenet
- behandling av lønnsutgifter
- behandling av betalinger

- nettskybasert ERP-tjeneste
- datasentertjenester
- IT-systemadministrasjon

ISAE 3000-kontroller for drift

- nettskybasert bedrifts-e-post
- nettskybasert samarbeid
- software-som-en-tjeneste-(SaaS)-basert HR-tjenester
- SaaS-baserte personaltjenester
- enhver tjeneste der hensynet til sikkerhet, tilgjengelighet og personvern er viktig

Bruksområder for SOC-rapporter

Egnethet for ulike typer outsourcede tjenester
Tabellen på side 6 gjør det enklere å avgjøre hvilken SOC-rapport som er best egnet for bestemte kontroller og tjenester. Øverst i tabellen er tjenester tydelig innrettet mot regnskapsrapportering, og der ISAE 3402-rapporter sannsynligvis vil bli etterspurt og levert. Dette omfatter økonomitjenester samt behandling av lønnsutgifter, krav til helsemyndigheter, betalinger og økonomiske transaksjoner.

I tillegg kan det være tilfeller der brukere trenger mer detaljerte opplysninger om sikkerhet eller tilgjengelighet. I slike tilfeller kan tjenesteleverandøren levere en ISAE 3402-rapport for ICOFR-formål og en ISAE 3000-rapport for å dekke behovet for dokumentasjon av sikkerhet eller tilgjengelighet, forutsatt at etterspørselen etter slike rapporter, eller byrden ved å legge til rette for kunders sikkerhetsrevisjoner, er stor nok.

Tjenester som ikke passer naturlig inn i verken den ene eller den andre kategorien, er plassert midt i tabellen. Her kan ISAE 3402 og/eller ISAE 3000 være best egnet, avhengig av tjenestenes karakter og brukerens behov. Eksempel:

- For administrasjon av IT-systemer, som kan omfatte både generelle IT-tjenester til en portefølje av brukere og tilpassede tjenester til spesifikke brukere, kan rapportering i henhold til ISAE 3402 eller ISAE 3000 være egnet, avhengig av om brukernes attesterings-behov er tettest knyttet til ICOFR eller sikkerhet/ tilgjengelighet.
- En nettskybasert ERP-tjeneste gir brukerne en tjeneste for rapportering av kjerneregnskap. Derfor vil den sannsynligvis også gi en ISAE 3402-rapport. Imidlertid kan den i tillegg måtte levere en ISAE 3000-rapport om sikkerhet og tilgjengelighet for å håndtere brukernes attesteringsbehov spesifikt knyttet til nettskytjenester.
- Mange leverandører av datasentertjenester har tidligere utført ISAE 3402-undersøkelser begrenset til fysiske og miljømessige sikkerhetskontroller. De fleste datasenterleverandører huser imidlertid mer enn bare kundenes økonomisystemer. Derfor går ledende leverandører over til ISAE 3000-sikkerhetsrapportering. Noen tjenesteleverandører inkorporerer støttende miljø-sikkerhetskontroller i sin ISAE 3000-sikkerhetsrapport, mens andre også dekker tilgjengelighetskriteriene, avhengig av tjenestenes karakter.

I den andre enden av spekteret har vi driftsmessige og teknologifokuserte tjenester med svært liten – om noen – direkte tilknytning til brukernes ICOFR.

Disse typene outsourcede tjenester vil for eksempel neppe bli inkludert i regnskapsrapporteringen fra et offentlig aksjeselskap. Brukere av slike tjenester er vanligvis mest opptatt av sikkerheten til dataene sine og systemenes tilgjengelighet. Dette vil typisk bli håndtert gjennom en ISAE 3000-rapport som dekker sikkerhet og tilgjengelighet. Der det er aktuelt, kan ISAE 3000-rapporter også dekke konfidensialitet, prosessintegritet og/eller personvern. ISAE 3000 kan også være egnet for organisasjoner som lagrer og behandler sensitive tredjepartsdata. Der det er nødvendig å vise tredjeparter at det foreligger effektive sikkerhets- og konfidensialitetskontroller for å beskytte informasjon, utgjør ISAE 3000-rapporter en mekanisme for å fremskaffe slik dokumentasjon.

Oversikt over SOC-rapportering

SOC (Service Organization Control) viser til SOC-rapporter generelt, men spesifikke rapporter inkluderer ISAE 3402/SOC1 og ISAE 3000/SOC2. Denne tabellen sammenligner omfanget og kontrollområdene som dekkes av de to rapportene.

* Noen ganger også omtalt som SAS70-, SSAE16- eller AT101-rapporter.

** Basert på revisjonsstandarden ISAE 3402 kan disse rapportene, etter revisorens evaluering av kriterienes egnethet, være nyttige ved regnskapsrevisjon hos brukerorganisasjonen.

*** I visse tilfeller kan en rapport dekke bare støttende IT-kontroller, avhengig av karakteren til tjenesten som leveres.

**** Denne listen inneholder eksempler på aktuelle prosesser og omfatter ikke alle tjenesteleverandører.

	ISAE 3402/SOC1*	ISAE 3000/SOC2
Tilsiktet brukerbase	• intern kontroll over regnskapsrapportering (ICOFR) • detaljert rapport til brukerorganisasjoner og deres revisorer	• driftsmessige kontroller • detaljert rapport til brukerorganisasjoner, deres revisorer** og spesifiserte parter
Hensikt	• fokusert på risiko ved regnskapsrapportering og kontroller spesifisert av tjenesteleverandøren, mest egnet når tjenesteleverandøren utfører behandling av økonomiske transaksjoner eller støtter transaksjonsbehandlingssystemer	Fokusert på: • sikkerhet • tilgjengelighet • konfidensialitet • prosessintegritet og/eller • personvern Egnet for et bredt spekter av systemer
Systemets definerte omfang	• transaksjonsklasser • prosedyrer for behandling og rapportering av transaksjoner • systemets regnskapsbilag • håndtering av andre betydelige hendelser og tilstander enn transaksjoner • utarbeidelse av rapporter til brukere • andre aspekter som er relevante for behandling og rapportering av brukertransaksjoner	• infrastruktur • programvare • prosedyrer • medarbeidere • data
Kontrollområder som dekkes	• kontroller for transaksjonsbehandling*** • støttende generelle IT-kontroller	• sikkerhet • tilgjengelighet • konfidensialitet • prosessintegritet og/eller • personvern
Standardiseringsnivå	• Kontrollmålene er definert av tjeneste-leverandøren og kan variere avhengig av typen tjeneste som leveres	• Prinsippene velges av tjenesteleverandøren • Det brukes spesifikke forhåndsdefinerte kriterier i stedet for kontrollmål
Egnethet**	• revisjon og skattetjenester, forvaltningstjenester, inkasso, ERP-hovedbokprogramvare levert under en driftet/ASP-modell, helseplaner, utlånsbehandling, låseboksbehandling, lønnsbehandlere, behandling av eiendoms- og skadeforsikringskrav, pensjonsplaner og investeringsvirksomheter	• outsourcing av forretningsprosesser, nettsky-baserte løsninger, kredittkortbehandlere, dataanalyser, fasiliteter for datasenterkolokasjon, tilbydere av katastrofegjenopprettingssystemer, tilbydere av elektroniske pasientjournaler, selskaper innenfor e-markedsføring, telefoni, tilbydere av administrerte sikkerhetstjenester, PaaS- og SaaS-leverandører uten innvirkning på regnskapsrapportering, dokumentstyrings-selskaper, teknologistøtte, webhoteller, osv.
Fordeler	• kan håndtere kunders krav til testing av den driftsmessige effektiviteten av tjenesteleverandørens kontroller • gir detaljer og trygghet i forbindelse med effektiviteten til tjenesteorganisasjonens kontroller	• Revisjonen gjennomføres mot et standardsett med spesifikke kontroller (Trust Services Principles and Criteria) • Nyttig for tjenesteleverandørers kunder, myndigheter, forretningspartnere og due diligence hos selskaper som kjøper opp andre selskaper • Rapporten kan spille en viktig rolle i oversikten over tredjeparts-tjenesteleverandøren, leverandørstyringsprogrammene, den interne selskapsstyringen og risikostyringsprosessen

ISAE 2000/SOC2 Trust Services Principles
ISAE 3000-rapporter bygger på en samling spesifikke krav (Trust Services Principles and Criteria) utviklet av den amerikanske og den kanadiske revisorforeningen (henholdsvis AICPA og CICA) for å fremskaffe dokumentasjon utover interne kontroller over økonomiske prosesser. Kravene omfatter spesifikt definerte prinsipper og kriterier for sikkerhet, tilgjengelighet, konfidensialitet, prosessintegritet og personvern.

I motsetning til ISAE 3000 forutsetter ISAE 3402-rapporter at tjenesteleverandøren beskriver systemet sitt og definerer kontrollmål og mål som er relevante for kundenes interne kontroll over regnskapsrapportering. Generelt skal en ISAE 3402-rapport ikke dekke tjenester eller kontrollområder som ikke er relevante for brukere fra et regnskapsrevisjonsperspektiv (ICOFR), og den kan spesifikt ikke dekke områder som katastrofegjenoppretting og personvern.

	Prinsipp	Egnethet
Sikkerhet	• Systemet er beskyttet mot uautorisert tilgang (både fysisk og logisk)	• Mest etterspurte dekningsområde • Sikkerhetskriterier er også innlemmet i de andre prinsippene, ettersom sikkerhetskontroller utgjør et grunnlag for de andre områdene • Egnet for alle outsourcede miljøer, særlig der bedriftsbrukere trenger dokumentasjon i forbindelse med tjenesteleverandørens sikkerhetskontroller for et hvilket som helst system, ikke-økonomisk eller økonomisk
Tilgjengelighet	• Systemet er tilgjengelig for drift og bruk som lovt eller avtalt	• Nest mest etterspurte dekningsområde, særlig der katastrofegjenoppretting leveres som en del av standard-tjenestetilbudet • Mest egnet der bedriftsbrukere trenger dokumentasjon i forbindelse med prosesser for å oppnå SLA-er for systemtilgjengelighet, samt katastrofegjenoppretting som ikke kan dekkes som en del av ISAE 3502/SOC1-rapporter*
Konfidensialitet	• Informasjon betegnet som konfidensiell, er beskyttet som lovt eller avtalt	• Mest egnet der brukeren krever ytterligere dokumentasjon i forbindelse med tjeneste-leverandørens metoder for beskyttelse av sensitiv forretningsinformasjon
Prosessintegritet	• Systembehandling er komplett, nøyaktig, rettidig og godkjent	• Kan være egnet for et bredt spekter av ikke-økonomiske og økonomiske scenarier der det er nødvendig med dokumentasjon på systembehandlingens fullstendighet, nøyaktighet, rettidighet og godkjenning
Personvern	• Personopplysninger blir samlet inn, brukt, lagret, fremlagt og destruert i samsvar med forpliktelsene i enhetens personvernerklæring og kriteriene for globalt anerkjent personvern	• Mest egnet der tjenesteleverandøren samhandler direkte med sluttbrukere og samler inn deres personopplysninger • Utgjør en effektiv mekanisme for demonstrasjon

* Avhengig av nasjonale forskrifter om regnskapsrevisjon kan kontroller for sikkerhetskopiering og gjenoppretting være innenfor omfanget av en ISAE 3402/SOC1-rapport.

Rapporteringstyper og -struktur

SOC-rapporttyper
SOC-rapporter dekker vanligvis kontrollenes utforming og effektivitet i en tolv-månedersperiode med aktivitet, med kontinuerlig dekning fra år til år for å møte brukerens behov i forbindelse med regnskapsrapportering og selskapsstyring. I enkelte tilfeller kan en SOC-rapport dekke en kortere periode, for eksempel seks måneder, hvis systemet eller tjenesten ikke har vært i drift i et helt år, eller hvis årlig rapportering er utilstrekkelig for å dekke brukerens behov. En SOC-rapport kan også være begrenset til utformingen av kontroller for en ny tjeneste eller et nytt system på et bestemt tidspunkt, eller for første undersøkelse (revisjon) av et system eller en tjeneste.

Rapporter som dekker utforming og driftsmessig effektivitet i en periode, omtales vanligvis som Type 2-rapporter, mens rapporter som dekker utforming på et bestemt tidspunkt, vanligvis omtales som Type 1-rapporter. Eksempel: Hvis en brukerorganisasjon trenger en rapport som dekker sikkerhet og tilgjengelighet for et bestemt system i en periode, vil den be tjenesteleverandøren om en ISAE 3000 Type 2 sikkerhets- og tilgjengelighetsrapport. Hvis en brukerorganisasjon trenger en rapport som dekker kontroller knyttet til regnskapsrapportering (ICOFR) for et bestemt system i en periode, vil den be tjeneste-leverandøren om en ISAE 3402 Type 2-rapport for dette systemet.

SOC-rapportstruktur

Tabellen nedenfor viser rapporteringsområdene og hvem som er ansvarlig for dem. Rapporten kan dekke et tidspunkt (utforming – Type 1) eller en periode (utforming og driftsmessig effektivitet – Type 2).

ISAE 3402	Ansvarlig
Revisors oppfatning	Tjenesterevisor
Ledelsens påstander	Tjenesteleverandør
Systembeskrivelse (inkludert kontroller)	Tjenesteleverandør
Kontrollmål	Tjenesterevisor og tjenesteleverandør
Kontrollaktiviteter	Tjenesterevisor og tjenesteleverandør
Tester av driftsmessig effektivitet*	Tjenesterevisor
Resultater av tester*	Tjenesterevisor
Annen informasjon (hvis relevant) (dvs. ledelsens respons på mangler identifisert i tester)	Tjenesteleverandør

* Gjelder for Type-2 rapporter

Forberedelse og utstedelse av en SOC-rapport

For tjenesteleverandører som ikke tidligere har fått utført et attesteringsoppdrag, er forberedelse til, og gjennomføring av, SOC-undersøkelsen vanligvis en prosess i to faser.

Følgende punkter oppsummerer vår trinnvise strategi for første gangs attestering. Vi begynner med en forberedende fase, der vi samarbeider med tjeneste-leverandøren og gir veiledning for å legge til rette for et vellykket oppdrag. Gjennomføringsfasen bygger på den forståelsen av tjenesteleverandørens arkitektur og kontroller som vi skaffet oss i løpet av den forberedende fasen.

Forberedelser for attestering

- definere revisjonsomfang og prosjektets overordnede tidslinje
- identifisere eksisterende eller nødvendige kontroller gjennom samtaler med ledelsen og gjennomgang av tilgjengelig dokumentasjon
- utføre modenhetsgjennomganger for å identifisere mangler som krever ledelsens oppmerksomhet
- kommunisere prioriterte anbefalinger for å håndtere eventuelle identifiserte mangler
- avvikle arbeidsøkter for å drøfte alternativer og utbedringsplaner
- verifisere at mangler er utbedret før den formelle gjennomføringsfasen starter
- fastslå den mest effektive revisjons- og rapporterings-strategien for å håndtere tjenesteleverandørens eksterne krav

Gjennomføring

- levere en samlet prosjektplan
- fullføre forhåndsinnsamling av data før arbeidet på stedet innledes, for å akselerere revisjonsprosessen
- avvikle møter og utføre tester på stedet
- utarbeide ekstern analyse av innsamlet informasjon
- rapportere prosjektstaus og eventuelle identifiserte problemer ukentlig
- levere et rapportutkast til ledelsen for gjennomgang samt den endelige rapporten både elektronisk og på papir
- levere en internrapport til ledelsen med eventuelle generelle observasjoner og anbefalinger til vurdering

KPMGs attesteringstjenester er skreddersydd for din virksomhet

KPMGs vellykkede attesteringspraksis bygger på flere sentrale faktorer:

IT-attesteringstjenestene leveres av kvalifiserte fagfolk
KPMG har kompetente og erfarne ressurser med bakgrunn fra SOC og andre IT-attesteringstjenester. Vi bygger opp langsiktige relasjoner til kundene og bestreber oss på å vedlikeholde og utvikle dem.

Vi forstår virksomheten din
KPMGs fagfolk har omfattende kunnskap og erfaring med en lang rekke forretningsprosesser i mange bransjer, herunder IT-tjenester, bankvesen, energi, helse, forsikring, logistikk og produksjon.

Vi har en godt etablert strategi
KPMG har utarbeidet grundige metoder og strategier for levering av attesteringstjenester.

Vi bruker ledende metoder
Vi har utarbeidet en rekke kontrollmål og -aktiviteter og hjelper deg med å identifisere de målene og aktivitetene som møter kundenes og myndighetenes forventinger. I tillegg til rapporter kan KPMG levere observasjoner og anbefalinger til forbedring av organisasjonens miljø.

Anbefalingene våre er tilpasset din virksomhet og tar hensyn til relevante bransje- og myndighetsstandarder samt ledende praksiser.

Vi har effektive verktøy for prosjektledelse
KPMG samarbeider tett med deg for å planlegge alle attesteringsaktiviteter og bidra til å redusere avbrudd av den normale forretningsdriften. Vi involverer sentrale interessenter ved oppstart av et prosjekt for å fremme en klar forståelse av revisjonsprosessen og målene med den. Prosjektstatus, problemstillinger og effekten av dem kommuniseres gjennom hele oppdraget.

Kontakter

Gunnar Sotnakk
Partner, Audit

T: +47 4063 9279
E: gunnar.sotnakk@kpmg.no

Roland Fredriksen
Partner, Audit

T: +47 4063 9317
E: roland.fredriksen@kpmg.no

Sanna Suvanto
Director, Information Risk Management

T: +47 9526 0768
E: sanna.suvanto@kpmg.no

kpmg.com/socialmedia

kpmg.com/app

Download on the App Store