DOWNPASS-standaard annex 4 – Schema voor het uitvoeren van remote audits

- voorlopige versie -

Introductie:

Remote auditing (audit op afstand) is een van de auditmethoden die worden beschreven in ISO 19011:2018, bijlage A1. Het voordeel van remote auditing is de mogelijkheid om de auditdoelstellingen te bereiken middels maximale flexibiliteit. Om van deze auditmethode te kunnen profiteren, moeten alle betrokken partijen zich bewust zijn van hun rol in het proces, welke input zij moeten leveren, wat de verwachte output is en met welke risico's en mogelijkheden rekening moet worden gehouden om de auditdoelstellingen te bereiken.

Er zijn tal van redenen waarom een auditor niet aanwezig kan zijn voor een audit ter plaatse, bijvoorbeeld om veiligheidsredenen (toegangsbeperkingen), reisbeperkingen, pandemieën, enz.

Nieuwe informatie- en communicatietechnologieën (**ICT**) hebben auditing op afstand mogelijk gemaakt. Naarmate de toegang tot ICT is verbeterd, wordt auditing op afstand steeds gebruikelijker. Hierdoor kan de auditor communiceren met mensen over de hele wereld en toegang krijgen tot een breed scala van informatie en gegevens.

Deze technologieën veranderen de manier waarop werk wordt verricht. ICT bieden de mogelijkheid om locaties en mensen op afstand te auditen, waardoor afstanden, reistijden en kosten worden beperkt, het milieueffect van auditreizen wordt verminderd, aanpassing aan de behoeften van de klant wordt vergemakkelijkt en de kwaliteit van de producten wordt verbeterd.

ICT kunnen de reikwijdte of de kwaliteit van de steekproeven in het auditproces helpen vergroten, mits zij op de juiste wijze worden voorbereid, gevalideerd en gebruikt. Dit is bijvoorbeeld het geval wanneer videocamera's, smartphones, tablets, drones en satellietbeelden kunnen worden gebruikt om fysieke omstandigheden zoals productieprocessen of bos- en landbouwgrond te controleren.

Het gebruik van ICT maakt het ook mogelijk deskundigheid bij een audit te betrekken die anders wegens financiële of logistieke beperkingen niet mogelijk zou zijn. Zo kan de deelname van een technisch deskundige aan de analyse van een specifiek project voor korte perioden worden gepland (bijvoorbeeld twee uur). Met de beschikbare ICT kan de technische deskundige het proces op afstand analyseren, waardoor tijd en kosten worden bespaard en de kwaliteit van de resultaten wordt verbeterd.

Anderzijds moet bij het gebruik van ICT ook rekening worden gehouden met de beperkingen en risico's bij het bereiken van de controledoelstellingen. Dit betreft onder meer kwesties als informatiebeveiliging, gegevensbescherming, vertrouwelijkheid, waarheid en kwaliteit van het verzamelde objectieve bewijsmateriaal.

Er kunnen bijvoorbeeld vragen rijzen in verband met de videokwaliteit, de stabiliteit van de netwerkverbinding, de deskundigheid van de auditors in het gebruik van ICT, de kwaliteit van de beelden, enz.

Om de beslissing te nemen ICT in het auditproces te gebruiken moeten auditors, samen met het auditteam en de cliënt, de risico's en kansen identificeren die aan het gebruik van ICT verbonden zijn en besluitvormingscriteria vaststellen om het gebruik van ICT voor een audit op afstand goed te keuren.

Algemene aanbevelingen voor remote audits:

- Auditprogramma

1. *Fundamentele overwegingen*
Het gebruik van ICT voor auditing op afstand kan alleen plaatsvinden als aan de juiste voorwaarden is voldaan. Dit betekent dat de technologie beschikbaar moet zijn en dat zowel de auditor als de beoordeelde vertrouwd moeten zijn met het gebruik van de technologie. Indien niet aan deze voorwaarden is voldaan, mag geen remote audit worden uitgevoerd. Om de technologie in het auditproces te kunnen gebruiken, moet er een online-verbinding van constante hoge kwaliteit zijn. Zwakke bandbreedte of hardware maken het proces inefficiënt. Een auditproces dat reeds aan de gang is, moet worden afgebroken als dergelijke omstandigheden zich voordoen en kan pas worden uitgevoerd als de technische voorwaarden dienovereenkomstig zijn aangepast.

2. *Vertrouwelijkheid, veiligheid en gegevensbescherming (confidentiality, security and data protection (CSDP))*
Vertrouwelijkheid, veiligheid en gegevensbescherming zijn van cruciaal belang bij het gebruik van ICT. De auditor en het te auditen bedrijf moeten rekening houden met de wet- en regelgeving en eventueel aanvullende regelingen treffen om aan de eisen inzake vertrouwelijkheid, veiligheid en gegevensbescherming te voldoen. De functionaris voor gegevensbescherming (DPO) van beide partijen moet bij de beoordeling van deze kwesties worden betrokken. Bij de voorbereiding van het gebruik van ICT moeten zowel de eisen van de klant als de eisen van de auditors inzake vertrouwelijkheid, veiligheid en gegevensbescherming aan de orde komen en worden geëvalueerd. ICT mogen alleen worden gebruikt als alle maatregelen zijn genomen en beide partijen bevestigen dat aan de vereisten inzake vertrouwelijkheid, veiligheid en gegevensbescherming is voldaan en beide partijen instemmen met het gebruik van ICT. Het bewijs van deze overeenkomst moet schriftelijk worden vastgelegd en bij de auditdocumentatie worden gevoegd. Dit bewijs moet ook bij het auditverslag worden gevoegd.
Het auditteam moet toegang krijgen tot zowel de gedocumenteerde informatie als de bedrijfsruimten, boerderijen, opslagplaatsen, opfokruimten, stallen, enz. wanneer een audit op afstand wordt verricht. Deze records (gedocumenteerde informatie) moeten worden gedeeld in een beveiligd systeem, bijvoorbeeld in de cloud of een Virtual Private Network of een ander filesharing systeem. De gegevens moeten veilig worden opgeslagen. Auditors mogen geen screenshots maken van gecontroleerde personen als auditbewijs; screenshots van personen moeten onherkenbaar worden

gemaakt of verwijderd. Screenshots van documenten of dossiers of ander bewijsmateriaal moeten voor documentatiedoeleinden veilig worden bewaard.

3. *Risicobeoordeling*
De risico's die worden genomen om de auditdoelstellingen te bereiken, moeten door de auditor worden geanalyseerd, geïdentificeerd en beoordeeld.

- Uitvoerbaarheids- en risicoanalyse voor remote audits:

1. Vertrouwelijkheid, veiligheid en gegevensbescherming	
Alle partijen moeten ervoor zorgen dat er tussen de auditor en de beoordeelde overeenstemming bestaat over de kwesties vertrouwelijkheid, veiligheid en gegevensbescherming. Er moeten regelingen worden getroffen om de naleving van deze criteria te waarborgen.	
2. Gebruik van ICT	
Er is een stabiele verbinding met een goede online verbindingskwaliteit.	
ICT biedt toegang tot relevante gedocumenteerde informatie, waaronder software, databanken en records.	
Het is mogelijk de ondervraagde personen te authenticeren/identificeren, bij voorkeur met foto.	
Indien waarneming van voorzieningen, processen, activiteiten, enz. relevant is voor de verwezenlijking van de auditdoelstellingen, deze ook per video te verifiëren.	
Wijzigingen in het proces uit het verleden (bijvoorbeeld toepassing van een Corrective Action Plan) kunnen door middel van video worden geverifieerd.	
3. Mensen in de organisatie	
Het is mogelijk toegang te krijgen tot en interviews af te nemen met de personen die relevant zijn voor het kwaliteitsmanagementsysteem.	
4. Werking	
Indien het bedrijf wegens noodsituaties niet in normale werking is, zijn de processen/activiteiten die door middel van de remote audit worden gecontroleerd, representatief én maken zij het mogelijk de auditdoelstellingen te halen.	
5. Complexiteit van het bedrijf en het type audit	
In het geval van complexe bedrijfsstructuren, processen of producten en diensten moet de auditor zorgvuldig nagaan of het instrument van de remote audit geschikt is voor een volledige beoordeling van het bedrijf en de naleving van alle eisen van de DOWNPASS-standaard.	
6. Conclusies	

Indien de auditdoelstellingen kunnen worden bereikt met een audit op afstand: ➔ De audit op afstand voortzetten. Indien de auditdoelstellingen gedeeltelijk kunnen worden bereikt met een audit op afstand: ➔ Een remote audit kan gedeeltelijk worden uitgevoerd en later worden aangevuld met een audit ter plaatse. Indien de auditdoelstellingen niet kunnen worden bereikt met een audit op afstand: ➔ In plaats van de remote audit moet een audit ter plaatse worden uitgevoerd.	

- Criteria voor de beoordeling van de kwaliteit van de remote audit:

Alle informatie die nodig is om inzicht te krijgen in het bedrijf, de processen en de activiteiten ervan, moet schriftelijk aan de auditor worden verstrekt voordat ICT worden gebruikt, zodat de auditor kan beslissen of een dergelijke audit geschikt is om de auditdoelstellingen te bereiken. De auditor moet alle informatie krijgen over de grootte van het bedrijf, zijn activiteiten en processen. De vragen van de auditor moeten worden beantwoord. Als beide partijen besluiten tot een remote audit en het gebruik van ICT, moet de auditor op afstand toegang krijgen tot de operationele (productie)faciliteiten, processen en documenten, zodat de auditdoelstellingen kunnen worden bereikt. Ook moet worden vastgesteld welke personen aan een audit moeten worden onderworpen en moet ervoor worden gezorgd dat deze personen tijdens de remote audit beschikbaar zijn. Alvorens de remote audit uit te voeren, is het raadzaam een ICT-gebruikstest uit te voeren om na te gaan of er een stabiele internetverbinding bestaat en of het personeel is ingelicht over welke technologie wordt gebruikt en hoe deze wordt gebruikt.

- Auditplanning

De auditor heeft de mogelijkheid om via audit op afstand openings- en slotvergaderingen te houden met personen op verschillende locaties. Voorts heeft hij de mogelijkheid om tussentijdse vergaderingen met het auditteam te organiseren via telefoon, videoconferentie of webvergadering.
De verificatie van operationele processen, bedrijfsvoorzieningen en productieprocessen moet gebeuren aan de hand van videobeelden in real time, of anders door het gebruik van drones, mobiele of vaste videocamera's. Hiermee moet rekening worden gehouden bij de planning van de audit.

- Uitvoering van de audit

Bij het verrichten van de audit moet een openingsvergadering worden gehouden. Tijdens deze vergadering moeten de beschikbaarheid en de uitvoerbaarheid van het gebruik van ICT worden bevestigd. Ook moeten maatregelen ter waarborging van

vertrouwelijkheid en veiligheid worden gepresenteerd en afgesproken. Indien de auditor van plan is screenshots, kopieën van documenten en andere soorten opnamen te maken, moet daarvoor toestemming worden gevraagd, hetzij tijdens de openingszitting, hetzij wanneer ICT worden gebruikt. Wanneer ICT worden gebruikt om personen te ondervragen, moet het auditteam de naam en functie van de ondervraagde personen noteren en de ondervraagden meedelen welke informatie door de auditor zal worden bewaard. Wanneer de auditor interviews op afstand afneemt, moet hij feitelijke beweringen verifiëren aan de hand van ander bewijsmateriaal. Deze moeten door de auditor worden opgevraagd en geanalyseerd. Indien deze documenten per e-mail worden verzonden, dient de auditor voor de nodige vertrouwelijkheid te zorgen.
Tijdens de audit moet ervoor worden gezorgd dat de communicatie niet wordt verstoord door geluiden. Bij auditing op afstand moet de auditor ervoor zorgen dat er geen onderbrekingen of verstoringen zijn. Evenzo, als er pauzes zijn. Tijdens de pauzes moet het geluid worden afgezet en het beeld worden uitgezet om de privacy te waarborgen. Tijdens de audit moet ervoor worden gezorgd dat de communicatie niet wordt verstoord door geluiden. Bij auditing op afstand moet de auditor ervoor zorgen dat er geen onderbrekingen of verstoringen zijn. Evenzo, als er pauzes zijn. Tijdens de pauzes moet het geluid worden afgezet en het beeld worden uitgezet om de privacy te waarborgen.
Wanneer video wordt gebruikt om live online beelden van locaties op afstand te bekijken, is het belangrijk dat het bedrijf de waarheidsgetrouwheid van de beelden aantoont. Bij het uitzenden van live-beelden kan bijvoorbeeld de datum van een actuele krant worden weergegeven om aan te tonen dat deze beelden daadwerkelijk op die datum zijn genomen. Bij het bekijken van afbeeldingen van een (productie)faciliteit kunnen deze ook worden vergeleken met plattegronden. Wanneer beelden van een geografische locatie worden bekeken, kunnen deze worden vergeleken met beschikbare satellietbeelden of informatie van geografische informatiesystemen.
Al het bewijsmateriaal, alsmede de wijze waarop het bewijsmateriaal wordt verzameld, moet worden geregistreerd.
Bij een audit op afstand is het van belang rekening te houden met kleine onderbrekingen, zoals ook gewoonlijk bij een audit ter plaatse. De auditor en het personeel van de gecontroleerde onderneming moeten pauzes worden toegestaan. Een auditor mag de audit onderbreken, bijvoorbeeld om actuele informatie te lezen of om verstrekte informatie te analyseren. Na een dergelijke korte onderbreking kan de audit worden voortgezet. Beide partijen moeten ervoor zorgen dat alle relevante contactpersonen gedurende de geraamde audittijd beschikbaar zijn en dat de bedrijfsruimten toegankelijk zijn.

- Auditverslag

Het auditverslag (audit report) moet de omvang van het gebruik van ICT en de doeltreffendheid van het gebruik bij de verwezenlijking van de auditdoelstellingen beschrijven. In het verslag moet worden aangegeven welke processen niet konden worden geaudit, maar ter plaatse moeten worden geaudit. Dit is belangrijk voor het besluitvormingsproces en de aansluitende audits. De feedback van het auditteam over het gebruik van ICT moet aan de auditmanager worden doorgegeven, die deze zal gebruiken om de eerder vastgestelde risico's en mogelijkheden te actualiseren.

De voor het auditprogramma verantwoordelijke manager moet beslissen of de auditdoelstellingen kunnen worden bereikt met de audit op afstand, of er vervolgactiviteiten nodig zijn, of dat de remote audit moet worden aangevuld met een audit ter plaatse.

- Geldigheid van de audit

De geldigheidsduur van een remote audit is één jaar. Na een remote audit moet de volgende audit ter plaatse worden uitgevoerd.

Voorbeeld van de identificatie van risico's en mogelijkheden bij de toepassing van technieken voor remote audits[1]

Informatie- en communicatietechnologie (ICT)	Potentiële toepassing	Risico's	Mogelijkheden
Videogesprek (synchroon) (b.v.: Skype, WebEx, ZOOM, Hangouts)	Afnemen van interviews Begeleide locatie-rondleidingen	Inbreuken op de veiligheid en vertrouwelijkheid; Verschillen in tijdzones; Authenticatie van de persoon; Lage kwaliteit van de communicatie; De mogelijkheid om de organisatie op een meer autonome en vrije manier te observeren wordt verzwakt omdat de auditor de camera niet controleert; De mogelijkheid om reacties van verschillende gecontroleerde personen op de communicatie waar te nemen, kan zwakker zijn	Interview met relevante medewerkers die op afstand werken, bijv. home office, projectteams in design en ontwikkeling; Openings- en slotvergadering voor multisite audits; Verafgelegen locaties/activiteiten waar fysieke waarneming niet kritisch is; Vermindering van reistijd/kosten en daarmee gepaard gaande milieueffecten; Groter geografisch bereik
	Beoordeling van documenten met deelneming van de geauditeerde	Inbreuken op de veiligheid en vertrouwelijkheid; Mogelijke moeilijkheden bij het beantwoorden van verzoeken om documentatie; Meer nodige tijd (potentieel tijdrovend proces); Mogelijke manipulatie van gegevens; De interactie met de geauditeerden kan worden verzwakt; Verminderde kwaliteit van de verzamelde informatie	Documentenaudits wanneer reizen naar de locatie niet praktisch is, bijvoorbeeld audits in de eerste fase waarbij het bezoek ter plaatse niet van cruciaal belang is voor het bereiken van de doelstellingen en er beperkingen zijn wat tijd en reizen betreft; Cross-site - goed voor afgelegen locaties waar een bezoek aan de locatie kan worden overgeslagen of waar jaarlijkse bezoeken voor het auditprogramma niet nodig zijn, maar wel enige follow-up vereist is; Vermindering van reistijd/kosten en daarmee gepaard gaande milieueffecten
Enquêtes, applicaties	Invullen van checklists en vragenlijsten	Waarborgen van authenticiteit; Noodzaak om vooraf een checklist op te stellen en de ondervraagde eventueel voor te bereiden op de beantwoording, wat de kosten verhoogt	Betere kennis van de organisatie, toepasbaar in de voorbereidingsfase van de audit; Maakt de voorbereiding van auditwerk mogelijk dat tijdens de audit moet worden geverifieerd door het verzamelen van ander bewijsmateriaal; Stelt de organisatie in staat zich voor te bereiden op het bezoek ter plaatse

Informatie- en communicatietechnologie (ICT)	Potentiële toepassing	Risico's	Mogelijkheden
Document- en gegevenscontrole (asynchroon) (bijv.: webdocumenten controleren)	Bekijken van dossiers, procedures, arbeidsprocessen, schermen, enz.	Veiligheid en vertrouwelijkheid; Procedurele moeilijkheden bij het bekijken van documenten (bv. toegang op afstand en navigatie op de website van de organisatie); Meer tijd nodig (potentieel tijdrovend proces); Mogelijke manipulatie van gegevens; Gebrek aan interactie met gecontroleerden maakt het niet mogelijk kwesties te verduidelijken; Transparantie - De beoordeelde verliest zicht op wat geauditeerd wordt en de steekproef	Vergemakkelijkt het organiseren en maakt een flexibeler gebruik van de tijd door het auditteam mogelijk; Maakt het mogelijk informatie onafhankelijk van de gecontroleerde en diepgaander te onderzoeken; Mogelijkheid om deskundigheid in te schakelen die niet naar de locatie kon reizen; Biedt een goede basis om het kwaliteitsmanagementsysteem van de organisatie te begrijpen en kan auditprotocollen opleveren die de auditor kan gebruiken tijdens interviews
Video (synchroon) (b.v.: drone, livestream)	Toezicht op werk in afgelegen gebieden of met een hoog risico; Begeleide inspectie ter plaatse; Inspectie van processen of bewerkingen met een hoog risico; Observatie van lopende processen	Risico's in verband met het gebruik en de aanwezigheid van apparatuur, b.v. neerstorten van een drone, gebruik van apparatuur, slechte weersomstandigheden, kwaliteit van het beeld; Volledige beoordeling van de locatie, uitrusting en omstandigheden; Waarheidsgetrouwheid van de gegevens	Gemakkelijk toezicht op taken met een hoog risico; Verhoogde bemonstering; Ideaal voor audit activiteiten waar de veiligheidseisen niet toelaten dat het auditteam aanwezig is, of voor het observeren van locaties en faciliteiten waar de verhouding tussen reistijd en audittijd hoog is; Goed als aanvulling op veldbezoeken voor buitenactiviteiten (bijv. bos- en landbouwgebieden, mijnbouw)
Video (asynchroon) (b.v.: Bewakingscamera; video-opnamen speciaal gemaakt voor audits)	Toezicht op activiteiten die niet aan de gang zijn op het tijdstip van de audit; Proces video's; Callcenter stemopnames; Opgenomen opleidingswebinars	Veiligheid en vertrouwelijkheid; Kwaliteit van het beeld; Volledige beoordeling van locatie, uitrusting en omstandigheden; Waarheidsgetrouwheid van de gegevens	Hogere rentabiliteit (mogelijkheid om alleen de interessante momenten van de video te selecteren); Mogelijkheid om locaties en moeilijk bereikbare voorzieningen te observeren en de bemonstering te verbeteren; Indien de elektronische opname gevoelige gegevens bevat die volgens de CDO-criteria niet in aanmerking komen voor een remote audit, moet de auditor overwegen deze opnamecontrole te herbestemmen voor een audit ter plaatse