Readiness-checklist voor het Europese Trust Center

Een gescoorde zelfbeoordeling van uw op kopers gerichte Trust Center: 58 items over zes stakeholder-sporen — beveiligingsteams, juridische teams, complianceteams, inkoop, ontvangers van klantupdates en AI-agents — elk gemapt op een concrete Europese bewijsverwachting.

Dit PDF is de print- en reviewmetgezel. Het werkbestand is de XLSX (één werkblad per spoor plus een automatisch optellende scorekaart); een machine-leesbare Markdown-variant is er voor AI-agents. Alle drie zijn gratis op orbiqhq.com/templates/european-trust-center-readiness-checklist — geen e-mail vereist.

Juridische grondslagen: Richtlijn (EU) 2022/2555 (NIS2), art. 21, lid 2, onder d), en art. 23; Verordening (EU) 2022/2554 (DORA), art. 28–30; Verordening (EU) 2016/679 (AVG), art. 28, 32 en 33–34. Deze checklist is een hulpmiddel, geen juridisch advies.

Instructies

Een gescoorde zelfbeoordeling van uw op kopers gerichte Trust Center, getoetst aan Europese verwachtingen: 58 items over zes stakeholder-sporen.

ZO SCOORT U

1. Beoordeel van buitenaf: scoor wat een externe reviewer op het Trust Center kan vinden (openbaar + selfservice-afgeschermde niveaus), niet wat er intern bestaat.

2. Scoor elk item in de kolom Score: **Ja** = 2 punten (gepubliceerd, actueel, volledig en toegankelijk op het juiste toegangsniveau); **Deels** = 1 punt (bestaat, maar is verouderd >12 maanden, onvolledig, lastig te vinden of afgeschermd waar het openbaar zou moeten zijn); **Nee** = 0 punten (afwezig of onvindbaar).

3. De kolom Punten en het werkblad Scorekaart berekenen automatisch de scores per spoor, het totaalpercentage en uw readiness-band.

READINESS-BANDEN

Onder 40% — Foundational: het Trust Center is een brochure; reviewers vallen terug op e-mail-een-PDF. Pak eerst de twee zwakste sporen aan.

40–75% — Developing: het kernbewijs bestaat, maar ten minste twee sporen worden onderbediend; geef voorrang aan juridische transparantie en updatekanalen.

Boven 75% — Buyer-ready: alle zes sporen zijn selfservice; de beveiligingsreview loopt parallel aan de deal. Houd dit vast met een herscore per kwartaal.

EIGENAREN PER SPOOR (AANBEVOLEN)

Spoor 1 Beveiligingsteams — security lead / CISO · Spoor 2 Juridische teams — juridisch / FG · Spoor 3 Complianceteams — compliance- / GRC-lead · Spoor 4 Inkoop — sales / RevOps · Spoor 5 Klantupdates — customer success · Spoor 6 AI-agents — engineering / webteam. Eén coördinator (meestal de CISO of de compliance-lead) consolideert de Scorekaart.

RITME

Doorloop alle zes sporen elk kwartaal. Herscoor één spoor na elke wezenlijke wijziging: een nieuw certificaat of een nieuwe audit, een subverwerkerwijziging, een incident, een prijsaanpassing, een gewijzigd endpoint. Subverwerkerslijsten en de geldigheid van certificaten verouderen het snelst — controleer die maandelijks.

JURIDISCHE GRONDSLAGEN

NIS2 — Richtlijn (EU) 2022/2555 (art. 21, lid 2, onder d), beveiliging van de toeleveringsketen; art. 23 incidentmelding: 24 u / 72 u / 1 maand).

DORA — Verordening (EU) 2022/2554 (art. 28–30, risico's van ICT-derden), van toepassing sinds 17 januari 2025.

AVG — Verordening (EU) 2016/679 (art. 28 subverwerkers; art. 32 beveiliging; art. 33–34 melding van datalekken).

Spoor 1 — Beveiligingsteams (11 items, max. 22 punten)

Wat een beveiligingsreviewer nodig heeft om uw beheersmaatregelen te beoordelen zonder een gesprek.

ID	Item	Zo ziet goed eruit	Bewijsvoorbeeld	Score
SEC-01	ISO 27001-certificaat gepubliceerd	Het certificaat is zichtbaar met certificerende instelling, scopeverklaring, afgifte- en vervaldatum — niet alleen een badge	PDF of bewijskaart: "ISO/IEC 27001:2022, afgegeven door [instelling], geldig tot 2027-03-01, scope: SaaS-platform en ondersteunende infrastructuur"	Ja / Deels / Nee
SEC-02	Verklaring van toepasselijkheid op verzoek beschikbaar	De VvT (of een samenvatting van de beheersmaatregelen) is toegankelijk via een selfservice-afgeschermde flow met een vermelde doorlooptijd	Achter een NDA: "Verklaring van toepasselijkheid v4.2, 2026-01" in het beperkte niveau	Ja / Deels / Nee
SEC-03	Managementsamenvatting van de pentest, afgelopen 12 maanden	Een gedateerde samenvatting met het testbureau, de scope, de methodologie, het aantal bevindingen per ernst en de herstelstatus	"Externe pentest door [bureau], 2026-04; 0 kritiek, 2 hoog (hersteld 2026-05)"	Ja / Deels / Nee
SEC-04	Positie op het gebied van kwetsbaarhedenbeheer	De scanfrequentie, de patch-SLA's en de hersteltermijnen voor kritieke/hoge bevindingen zijn vermeld	"Wekelijkse scans van dependencies en infrastructuur; kritieke bevindingen gepatcht ≤ 72 u, hoge ≤ 14 dagen"	Ja / Deels / Nee
SEC-05	Encryptiepositie gedocumenteerd	Encryptie in rust en onderweg, met de algoritmen en een samenvatting van het sleutelbeheer	"AES-256 in rust, TLS 1.2+ onderweg, via KMS beheerde sleutels die jaarlijks roteren"	Ja / Deels / Nee
SEC-06	Samenvatting van het toegangsbeheer	Het afdwingen van MFA/SSO, het model van minimale rechten en het instroom-doorstroom-uitstroomproces zijn beschreven	"SSO + afgedwongen MFA voor alle medewerkers; toegangsreviews per kwartaal; RBAC"	Ja / Deels / Nee
SEC-07	Secure development lifecycle beschreven	Codereview, SAST/DAST, dependency scanning en releasebeheersmaatregelen zijn samengevat	"Alle wijzigingen collegiaal getoetst; SAST + dependency scanning in CI; gefaseerde deploys"	Ja / Deels / Nee
SEC-08	Scheiding van tenants/netwerken toegelicht (multitenant-SaaS)	Het model voor de logische scheiding tussen klantomgevingen is beschreven	"Tenantisolatie op rijniveau; encryptiecontexten per tenant; geen query's over tenants heen"	Ja / Deels / Nee
SEC-09	Samenvatting bedrijfscontinuïteit / uitwijk	Samenvatting van het BC-/uitwijkplan met RTO-/RPO-doelstellingen en de datum van de laatste test	"RTO 4 u / RPO 1 u; uitwijkoefening laatst uitgevoerd 2026-02"	Ja / Deels / Nee
SEC-10	Overzicht van de beveiligingsarchitectuur	Een architectuurbeschrijving of -diagram op hoofdlijnen (openbaar of afgeschermd) met de gegevensstromen en grenzen	Afgeschermd: "Overzicht architectuur & gegevensstromen, v3, 2026-03"	Ja / Deels / Nee
SEC-11	Route voor responsible disclosure	Een security.txt en/of een gepubliceerd beleid voor het melden van kwetsbaarheden, met een contactpunt	"/.well-known/security.txt met een security@-contact en een disclosurebeleid"	Ja / Deels / Nee

Spoor 2 — Juridische teams (10 items, max. 20 punten)

Wat juridische reviewers en FG's controleren voordat een verwerkersovereenkomst wordt getekend. Grondslagen: art. 28 en 32 AVG.

ID	Item	Zo ziet goed eruit	Bewijsvoorbeeld	Score
LEG-01	Verwerkersovereenkomst zonder drempels beschikbaar	Het actuele sjabloon van de verwerkersovereenkomst is te downloaden zonder registratie of salesgesprek	"Verwerkersovereenkomst v5.1 (2026-01), PDF, openbare download"	Ja / Deels / Nee
LEG-02	Openbare subverwerkerslijst	Elke subverwerker staat vermeld met naam, doel, verwerkte gegevenscategorieën en hostinglocatie — openbaar, niet achter een NDA (art. 28 AVG)	"AWS (eu-central-1, Frankfurt) — infrastructuurhosting — klantcontent"	Ja / Deels / Nee
LEG-03	Mechanisme voor wijzigingsmeldingen van subverwerkers	Een abonneerbaar meldkanaal plus de vermelde contractuele meldtermijn (doorgaans ~15 dagen; in grotere deals onderhandeld naar 30–60)	"Abonneer u op subverwerkerupdates; § 9 van de verwerkersovereenkomst geeft een meld- en bezwaartermijn"	Ja / Deels / Nee
LEG-04	Internationale doorgiftemechanismen gedocumenteerd	Per doorgifte is benoemd of een beroep wordt gedaan op SCC's of adequaatheid; het transfer impact assessment is op verzoek beschikbaar	"Doorgiften naar [leverancier] onder SCC's (2021/914 module 2) + TIA beschikbaar onder NDA"	Ja / Deels / Nee
LEG-05	Schriftelijke toezeggingen over gegevenslocatie	Waar klantgegevens (en metadata/back-ups) worden opgeslagen, per dienst, als schriftelijke toezegging	"Klantcontent wordt uitsluitend in EU-regio's opgeslagen en verwerkt; back-ups blijven in de regio"	Ja / Deels / Nee
LEG-06	Jurisdictie van de aanbieder bekendgemaakt	De exploiterende juridische entiteit, de plaats van oprichting en de blootstelling aan verstrekkingsbevelen van buiten de EU (bijv. de Amerikaanse CLOUD Act) zijn vermeld	"Geëxploiteerd door [entiteit] GmbH, opgericht in Duitsland; geen Amerikaanse moeder"	Ja / Deels / Nee
LEG-07	Selfservice-NDA-flow voor afgeschermde documenten	Een NDA die met één klik wordt ondertekend, met audittrail, geeft beperkte documenten binnen minuten vrij in plaats van dagen	"Toegang aanvragen → NDA in de browser ondertekenen → document ontgrendeld; handtekening gelogd"	Ja / Deels / Nee
LEG-08	Bewaar- en wisvoorwaarden gepubliceerd	Wat er met klantgegevens gebeurt bij beëindiging, met termijnen	"Klantgegevens worden binnen 30 dagen na afloop van het contract gewist; wisverklaring op verzoek"	Ja / Deels / Nee
LEG-09	Samenvatting van de technische en organisatorische maatregelen (TOM's)	De maatregelen van art. 32 AVG zijn gepubliceerd als gestructureerde samenvatting en worden vanuit de verwerkersovereenkomst aangehaald	"TOM-bijlage v3 (2026-02): toegangsbeheer, encryptie, weerbaarheid, testfrequentie"	Ja / Deels / Nee
LEG-10	Openbaarmaking van AI-gegevensgebruik	Of klantgegevens AI-modellen trainen; welke AI-subverwerkers toegang hebben; de opt-outroute	"Klantgegevens worden niet gebruikt om modellen te trainen; AI-subverwerkers: [lijst], gehost in de EU"	Ja / Deels / Nee

Spoor 3 — Complianceteams (11 items, max. 22 punten)

Wat GRC-reviewers bij gereguleerde klanten nodig hebben voor hun eigen NIS2-/DORA-/AVG-dossier.

ID	Item	Zo ziet goed eruit	Bewijsvoorbeeld	Score
COM-01	Frameworks getoond met scope en data	Elke certificering/verklaring toont de scope, de afgevende instelling, de auditdatum en de geldigheid — geen logostrook	"ISO 27001 (geldig tot 2027-03), ISO 27701 (geldig tot 2027-03), scopeverklaringen gelinkt"	Ja / Deels / Nee
COM-02	NIS2-positie gemapt	De beveiligingsmaatregelen zijn gemapt op de categorieën van art. 21, lid 2, NIS2, zodat essentiële/belangrijke klanten ernaar kunnen verwijzen in hun eigen ketendossier	"NIS2-readinesspagina: art. 21, lid 2, onder a)–j), gemapt op beheersmaatregelen en bewijs"	Ja / Deels / Nee
COM-03	Toezegging over incidentcommunicatie afgestemd op de NIS2-klokken	De toezegging om getroffen klanten snel genoeg te informeren om hun meldplichten van 24 u/72 u/1 maand te ondersteunen (art. 23 NIS2)	"Wij informeren getroffen klanten zonder onnodige vertraging, zodat zij de termijnen van art. 23 kunnen halen"	Ja / Deels / Nee
COM-04	DORA-datapunten voor ICT-derden beschikbaar	De contractuele en operationele datapunten die financiële entiteiten nodig hebben op grond van art. 28–30 DORA (dienstomschrijving, gegevenslocaties, onderaannemers, exitondersteuning) zijn ontsloten	"DORA-informatieblad: velden van het informatieregister vooraf ingevuld voor klanten"	Ja / Deels / Nee
COM-05	Certificeringsverlenging en verlopen nooit stilzwijgend	Verlengings-/vervaldata zijn zichtbaar; het vernieuwde bewijs wordt vóór de vervaldatum gepubliceerd	"De certificaatkaart toont de datum 'geldig tot'; de verlenging wordt 2 weken vóór het verlopen gepubliceerd"	Ja / Deels / Nee
COM-06	Bewijs geordend per framework en beheersmaatregel	Een navigeerbare structuur (framework → maatregel → bewijs), geen platte map met PDF's	"Blader op ISO 27001 / NIS2 / DORA / AVG; elke beheersmaatregel linkt naar het bijbehorende bewijs"	Ja / Deels / Nee
COM-07	Elk document voorzien van versie en datum	Een versienummer en de datum van de laatste wijziging op elk bewijsitem	"Informatiebeveiligingsbeleid v6.0 — bijgewerkt 2026-05-14"	Ja / Deels / Nee
COM-08	Route naar auditrapporten vermeld	Hoe klanten auditrapporten van derden verkrijgen (onder NDA) en of auditrechten worden ondersteund	"ISO-auditrapport beschikbaar onder NDA; auditrechtenbepaling ondersteund voor gereguleerde klanten"	Ja / Deels / Nee
COM-09	Kwetsbaarhedenafhandeling & adviezen (CRA-bewust)	Voor producten met digitale elementen: een gedocumenteerde kwetsbaarhedenafhandeling en een kanaal voor beveiligingsadviezen	"Pagina met beveiligingsadviezen, CVE-historie en een proces voor gecoördineerde openbaarmaking"	Ja / Deels / Nee
COM-10	Verklaring over exit en overdraagbaarheid	De exportformaten voor gegevens, de transitiehulp en de ondersteuning bij beëindiging zijn beschreven (ondersteunt de exitstrategie-eisen van DORA)	"Volledige export in open formaten binnen 30 dagen; bepaling over transitiehulp beschikbaar"	Ja / Deels / Nee
COM-11	Hergebruik van bewijs over frameworks heen	Hetzelfde bewijs van een beheersmaatregel wordt één keer gemapt op NIS2, DORA en de AVG in plaats van op drie parallelle antwoordsets	"De encryptiemaatregel wordt aangehaald door ISO A.8.24, art. 21, lid 2, onder h), NIS2, DORA en art. 32 AVG"	Ja / Deels / Nee

Spoor 4 — Inkoop (9 items, max. 18 punten)

Wat inkoop nodig heeft om de onboarding van een leverancier af te ronden zonder een discovery-gesprek.

ID	Item	Zo ziet goed eruit	Bewijsvoorbeeld	Score
PRO-01	Gepubliceerde, transparante prijzen	De prijzen (of ten minste het prijsmodel en de niveaus) zijn openbaar — geen muur met "neem contact op met sales"	"Prijspagina met functies per niveau en jaar-/maandtarieven"	Ja / Deels / Nee
PRO-02	Vendor-assuranceprofiel	De bedrijfsfeiten op één plek: juridische entiteit, registratienummer, hoofdkantoor, eigendom, belangrijkste contactpersonen	"Leveranciersprofiel: [entiteit], HRB [nummer], Berlijn; contactpersonen voor security & privacy"	Ja / Deels / Nee
PRO-03	Bewijs van cyberverzekering	De cyberaansprakelijkheidsverzekering is bevestigd met het dekkingsniveau (certificaat op verzoek)	"Cyberverzekering: € 5 mln dekking; certificaat beschikbaar onder NDA"	Ja / Deels / Nee
PRO-04	Uptime- en beschikbaarheidshistorie	Een openbare statuspagina en historische uptimecijfers	"status.[bedrijf].com — uptime over 12 maanden 99,97%"	Ja / Deels / Nee
PRO-05	Signalen over bedrijfscontinuïteit	Continuïteitsbewijs dat relevant is voor inkoop: escrow, opvolging en waar passend signalen over financiering/levensvatbaarheid	"Samenvatting bedrijfscontinuïteit + continuïteitstoezeggingen richting klanten"	Ja / Deels / Nee
PRO-06	Support- en escalatiemodel	De supportniveaus, de reactie-SLA's en een escalatiepad zijn gedocumenteerd	"Support-SLA: reactie op P1 ≤ 1 u; benoemde escalatieroute"	Ja / Deels / Nee
PRO-07	Voorwaarden voor onboarding/offboarding en gegevensuitvoer	Wat onboarding vereist en wat offboarding teruggeeft, inclusief eventuele kosten voor gegevensuitvoer	"Geen kosten voor gegevensuitvoer; exporttooling in selfservice; offboardingchecklist gepubliceerd"	Ja / Deels / Nee
PRO-08	Doorlooptijd voor documentaanvragen vermeld	Een vermelde SLA voor het afhandelen van documentaanvragen in het kader van due diligence	"Afgeschermde documenten worden ≤ 1 werkdag na de NDA vrijgegeven"	Ja / Deels / Nee
PRO-09	Belangrijkste afhankelijkheden bekendgemaakt	Materiële vierde partijen / concentratieafhankelijkheden zijn geïdentificeerd (cloudleverancier, kritieke leveranciers)	"Kritieke afhankelijkheden: AWS eu-central-1; [betaalprovider]; [authenticatieprovider]"	Ja / Deels / Nee

Spoor 5 — Ontvangers van klantupdates (8 items, max. 16 punten)

Of bestaande klanten via een gestructureerd kanaal over wijzigingen horen — en niet via een verrassingsmail.

ID	Item	Zo ziet goed eruit	Bewijsvoorbeeld	Score
UPD-01	Abonneerbare trust updates	Klanten kunnen zich abonneren op beveiligings-/compliance-updates vanuit het Trust Center	"Abonneerknop; updates per e-mail bezorgd, met een archiefpagina"	Ja / Deels / Nee
UPD-02	Gestructureerde incidentmeldingen	Incidentcommunicatie wordt via het Trust Center gepubliceerd met ernst, impact en status — geen ad-hoc e-mailthreads	"Incidentmelding 2026-03: ernst, getroffen diensten, tijdlijn, huidige status"	Ja / Deels / Nee
UPD-03	Wijzigingsmeldingen van subverwerkers met bezwaartermijn	Wijzigingen worden vóór de inschakeling aangekondigd, met verwijzing naar het meld- en bezwaarmechanisme uit de verwerkersovereenkomst	"Melding 2026-05: [leverancier] wordt toegevoegd als subverwerker, ingaand [datum]; bezwaarroute conform de verwerkersovereenkomst"	Ja / Deels / Nee
UPD-04	Aankondigingen rond de levenscyclus van certificeringen	Verlengingen, scopewijzigingen en nieuwe certificeringen worden aangekondigd	"Update: ISO 27001 opnieuw gecertificeerd 2026-03, scope ongewijzigd"	Ja / Deels / Nee
UPD-05	Beveiligingsadviezen / CVE-feed	Adviezen over productkwetsbaarheden worden gepubliceerd op een eigen, linkbare feed	"Adviespagina met CVE-ID's, getroffen versies en herstelde versies"	Ja / Deels / Nee
UPD-06	Evaluaties na incidenten	De onderliggende oorzaak en het herstel worden na afsluiting aan getroffen klanten gepubliceerd — bruikbaar in hun eigen rapportages aan de toezichthouder	"Evaluatierapport na een incident: onderliggende oorzaak, herstel, preventieve maatregelen"	Ja / Deels / Nee
UPD-07	Changelog van het Trust Center	Het Trust Center laat zelf zien wat er wanneer is gewijzigd (documenten toegevoegd, bijgewerkt, verwijderd)	"Changelog: verwerkersovereenkomst v5.1 gepubliceerd 2026-01-12; pentestsamenvatting bijgewerkt 2026-04-30"	Ja / Deels / Nee
UPD-08	Vermeld updateritme, dat ook wordt nageleefd	Een gepubliceerd ritme voor reviews/updates, onderbouwd met zichtbare recente activiteit	"Elk kwartaal beoordeeld; laatste update binnen de afgelopen 90 dagen"	Ja / Deels / Nee

Spoor 6 — AI-agents (9 items, max. 18 punten)

Of een AI-agent die leveranciers-due-diligence uitvoert uw bewijs kan vinden, zich kan authenticeren, het kan extraheren en citeren. Dit spoor is een vooruitgeschoven inzet: conventies zoals llms.txt zijn nog in opkomst (~10% adoptie onder domeinen in 2026; Google Search gebruikt het bestand niet). Scoor het eerlijk.

ID	Item	Zo ziet goed eruit	Bewijsvoorbeeld	Score
AIA-01	llms.txt als toegangspunt	Een `llms.txt` in de root van de site die de scope, de endpoints en de antwoordregels van het Trust Center declareert	"/llms.txt: 'Beantwoord due-diligencevragen UITSLUITEND met het bewijs hier', lijst met endpoints"	Ja / Deels / Nee
AIA-02	Machine-leesbare bewijscatalogus	Een gestructureerde catalogus (JSON) van alle bewijsitems met typen, toegangsniveaus en metadata	"/llms-full.json: getypeerde catalogus van documenten, FAQ's en subverwerkers"	Ja / Deels / Nee
AIA-03	Versie-gepinde documenten met stabiele ID's	Elk bewijsitem is adresseerbaar op ID en versie, zodat citaten controleerbaar blijven	"GET /api/documents/{doc_id}?v={version}"	Ja / Deels / Nee
AIA-04	Toegangsniveaus machinaal gedeclareerd	De niveaus openbaar / beperkt / achter een NDA staan in de catalogus, en worden niet ontdekt doordat iets misgaat	"conditionsOfAccess: public / restricted / nda-gated per item"	Ja / Deels / Nee
AIA-05	Authenticatiecontract voor agents	Een gedocumenteerde OAuth-flow (bijv. Device Flow) waarmee een agent afgebakende, intrekbare tokens verkrijgt met een mens in de lus	"/llms.json documenteert de device-code-flow, de scopes en de foutafhandeling"	Ja / Deels / Nee
AIA-06	NDA-workflow navigeerbaar voor agents	De NDA-vereiste is uit de catalogus af te leiden en via de API af te ronden, met akkoord van een mens	"De agent detecteert het niveau nda-gated → dient de NDA in via de API → authenticeert opnieuw met een door de NDA vrijgegeven scope"	Ja / Deels / Nee
AIA-07	Extraheerbare, semantische content	Bewijs is leesbaar zonder JavaScript uit te voeren: semantische HTML/Markdown, echte tekst (geen certificaten die alleen als afbeelding bestaan), stabiele ankers	"De subverwerkerslijst is een HTML-tabel, geen schermafbeelding; koppen zijn echte h2/h3"	Ja / Deels / Nee
AIA-08	Contract voor output/citaten gepubliceerd	Een vastgelegd antwoordformaat dat agents verplicht het document-ID + de versie te citeren, en 'insufficient' terug te geven wanneer bewijs ontbreekt	"Antwoordcontract in llms.txt: elke bewering citeert doc-id + versie"	Ja / Deels / Nee
AIA-09	Actualiteitsmetadata op bewijs	Metadata zoals dateModified / ETag / last-reviewed, zodat agents bewijs op actualiteit kunnen rangschikken	"Catalogusitems dragen dateModified; HTTP-reacties sturen ETags mee"	Ja / Deels / Nee

Scorekaart

Spoor	Items	Max. punten	Uw punten	Spoor %
1. Beveiligingsteams	11	22		
2. Juridische teams	10	20		
3. Complianceteams	11	22		
4. Inkoop	9	18		
5. Ontvangers van klantupdates	8	16		
6. AI-agents	9	18		
TOTAAL	**58**	**116**		

Readiness-band: totaal aantal punten ÷ 116 → < 40% Foundational · 40–75% Developing · > 75% Buyer-ready.

Na het scoren: benoem de twee laagst scorende sporen, zet elke Nee in die sporen om in een ticket met een eigenaar en een datum, en herscoor de sporen zodra de verbeteringen zijn doorgevoerd. Voer de volledige beoordeling elk kwartaal opnieuw uit.