

PROCEDUREBESCHRIJVING

VBDS AUDIT

Versie 4: januari 2025

Inleiding

Tegemoetkoming aan getoetste normen wordt verkregen door een toets van de archiveringsfunctionaliteiten in de omgeving waarin de softwareoplossing functioneert.

De getoetste normen stellen (dwingende) functionele eisen aan archivering en archiveringssoftware. De standaarden maken het mogelijk de *storage- en retrievalfunctionaliteit* zodanig in te richten dat alle juridische, bewijstechnische, verantwoordings- en bedrijfsvoeringsbelangen die binnen en buiten een (overheids-)organisatie een rol spelen op een verantwoorde wijze worden gediend. Dit dient het organisaties mogelijk te maken via *storage en retrieval* van data en documenten te waarborgen:

1. De rechtmatigheid van bedrijfsprocessen;
2. De kwaliteit van de verwerkte data en documenten gedurende de tijd dat ze worden bewaard;
3. De kwaliteit van het verwerkingsproces van de data en documenten;
4. De kwaliteit en doelmatigheid van het zoek- en *retrieval*-proces;
5. De kwaliteit en doelmatigheid van de opslag en het beheer van data en documenten gedurende de tijd dat ze worden bewaard

Applicaties met archiveringsfunctionaliteiten zorgen ervoor dat organisaties door de *storage en retrieval*-functionaliteit de Nederlandse wet- en regelgeving kunnen naleven. Een dergelijke applicatie behelst iedere infrastructuur die het beheer van archiefdocumenten gedurende door de Nederlandse wet- en regelgeving vastgestelde bewaartermijnen verzorgt. In de getoetste normen worden de vereiste systeem interfaces en zoekfunctionaliteiten beschreven die door deze applicaties dienen te worden ondersteund.

Aanvragers

Aanvragers van een Verklaring van Compliance kunnen ontwikkelaars en verkopers van applicaties zijn, maar ook organisaties die dit soort applicaties implementeren. De aanvragers zijn verantwoordelijk voor het organiseren van de toetsing en de inrichting van de testomgeving.

Auditor

De auditor is *Van Bussel Document Services* te Helmond.

De vier fasen van het auditproces

1. Overleggen geaccordeerde en vastgestelde documentatie
Het overleggen van (door de verantwoordelijke manager/producteigenaar) van geaccordeerde en vastgestelde documentatie (bv. systeem-, beheer- en gebruikershandleidingen, architectuur van de applicatie, softwarecomponenten, gebruikte third-party software, datamodel, metadata-schema, e.d.) Er dient bewijs te zijn van accordering c.q. vaststelling. Indien de toets plaats vindt op verzoek van een klantorganisatie, dient deze organisatie een verklaring te overleggen dat deze documentatie voor de klantorganisatie beschikbaar is. (e.g. system, management and

user manuals, application architecture, software components, overview of third-party software and their place in the architecture, data model, metadata scheme, etc.)

2. Nulmeting

De applicatie wordt eis voor eis op basis van het toetsingsschema doorlopen in een gezamenlijke sessie van de leverancier, de klantorganisatie en de auditor waarbij wordt aangegeven in hoeverre de eisen/opties kunnen worden ingevuld en waar nog lacunes kunnen worden geconstateerd. Er hoeft geen bewijs te worden overlegd. De auditor maakt een beknopt rapport op waarbij vooral de lacunes en onduidelijkheden worden benoemd.

3. Evaluatie

Het toetsingsformulier wordt door leverancier en organisatie ingevuld na het oplossen van geconstateerde lacunes in de nulmeting, waarbij bij iedere eis/optie wordt aangegeven hoe deze kan worden aangetoond. Hierbij wordt aangegeven hoe de eis wordt gedemonstreerd in de applicatie en welk (verder) bewijs hierbij wordt aangeleverd. De auditor ontvangt deze evaluatie, analyseert deze, checkt het (reeds) aangeleverde bewijs en stelt, indien noodzakelijk, vragen over onduidelijkheden of vraagt aanvullend bewijsmateriaal.

4. Audit

In de applicatie wordt de volledige werking van de gevraagde eisen aangetoond op basis van de in de evaluatie aangegeven wijze. De auditor kan, indien nodig, aanvullende vragen stellen of een aanvullende demonstratie vragen. Indien compliance kan worden aangetoond, wordt een Verklaring van Compliance afgegeven.

Procedure

1. De aanvrager verklaart bij het overleggen van geaccordeerde en vastgestelde documentatie/informatie alle gevraagde informatie naar waarheid te verstrekken. De auditor wordt formeel geautoriseerd tot het inzien en analyseren van deze documentatie/informatie. Als blijkt dat de aanvrager moedwillig onjuiste informatie heeft verstrekt, wordt de auditprocedure beëindigd. Indien een Verklaring van Compliance is verstrekt wordt deze door de auditor ingetrokken.
2. De auditor leest en analyseert alle gedeelde documentatie en andere informatie *voordat* de nulmeting wordt uitgevoerd.
3. De aanvrager stelt een (of meerdere) ter zake kundige medewerker(s) ter beschikking (van leverancier en klantorganisatie) voor het uitvoeren van een nulmeting.
4. De auditor stelt een beknopt rapport op van de nulmeting, waarbij de aanwezige lacunes worden benoemd.
5. Na het oplossen van de geconstateerde lacunes wordt door leverancier en klantorganisatie een evaluatie uitgevoerd op basis van het toetsingsformulier, waarbij zij aangeven hoe de betreffende eisen kunnen worden gedemonstreerd en welk bewijsmateriaal hiervoor kan worden overlegd. De auditor beoordeelt de evaluatie en checkt het bewijsmateriaal.
6. In het geval tijdens de evaluatie blijkt dat een eis niet kan worden aangetoond op grond van technische of organisatorische redenen, heeft de aanvrager de mogelijkheid als bewijs voor de realisatie van de specifieke eis technische en/of gebruikershandleidingen en een verklaring

ondertekend door de productmanager te overleggen, aangevuld met een verklaring door gebruikers van het product.

7. Na vaststelling van de evaluatie kan de daadwerkelijke audit plaatsvinden. De aanvrager realiseert (indien nodig) een testopstelling op basis waarvan het mogelijk is de applicatie, gebruikt voor het realiseren van de functionaliteiten gevraagd in de te toetsen standaard of richtlijn, te toetsen.
8. De aanvrager stelt een (of meerdere) ter zake kundige medewerker(s) ter beschikking om binnen de gerealiseerde testomgeving te demonstreren en te bewijzen dat de te toetsen omgeving de in de norm gestelde eisen/opties realiseert. Deze demonstratie gaat eis voor eis op een zodanige wijze dat er geen twijfel bestaat over het invullen van de in de norm gestelde eis, waarbij, indien noodzakelijk, nog ander aanvullend bewijsmateriaal mag worden aangeleverd.
9. De auditor genereert een voorlopig rapport, waarin bij iedere eis een beslissing over compliance of non-compliance wordt genomen, gebaseerd op argumenten. Dit voorlopig rapport wordt getoetst door de aanvrager op onjuistheden of onjuiste interpretaties.
10. De auditor genereert een definitief rapport met daarin een algemene conclusie gebaseerd op het voorlopig rapport. In deze conclusie is de beslissing:
 - a. Dat de software-oplossing compliant is (meer dan 95% van de eisen worden gerealiseerd) en een Verklaring van Compliance kan worden afgegeven.
 - b. Dat de software-oplossing grotendeels compliant is (meer dan 80% van de eisen worden gerealiseerd), maar dat er nog fundamentele problemen van non-compliance zijn voor wat betreft archiveringsprocessen. Deze problemen dienen te worden opgelost alvorens een Verklaring van Compliance kan worden afgegeven.
 - c. Dat de software-oplossing non-compliant is (minder dan 80% van de eisen worden gerealiseerd). Een Verklaring van Compliance kan niet worden toegekend.
11. Gebaseerd op de algemene conclusie:
 - a. Het auditrapport wordt gegenereerd in een definitieve versie, het audit portfolio wordt samengesteld en een Verklaring van Compliance toegekend.
 - b. De aanvrager zal alle problemen van non-compliance herstellen, waarna de betreffende eisen opnieuw worden getoetst. Wanneer meer dan 95 % van de eisen worden gerealiseerd, genereert de auditor het eindrapport in een definitieve versie, wordt het audit portfolio samengesteld en een Verklaring van Compliance toegekend.
 - c. De audit wordt afgesloten. De aanvrager kan alle problemen van non-compliance herstellen, maar een nieuwe audit op alle eisen is noodzakelijk.
12. De Verklaring van Compliance is gedurende een periode van drie (3) jaren geldig, waarna de software-oplossing opnieuw wordt getoetst.
13. Tenzij anders afgesproken wordt na afloop van de toetsing en samenstelling van het Portfolio Verklaring van Compliance de factuur van het toetsingstraject opgesteld en toegezonden.

Wanneer betaling van de factuur heeft plaatsgevonden wordt door de auditor het Portfolio Verklaring van Compliance, inclusief de opgestelde Verklaring van Compliance, aan de aanvrager ter beschikking gesteld.

14. Gedurende de periode van drie jaren worden wijzigingen in de applicatie gemeld bij de auditor. Dit dient met name te gebeuren indien nieuwe (of veranderingen in bestaande) archiveringsfunctionaliteiten worden geïmplementeerd die de compliance aan de in de normen gestelde eisen (kunnen) beïnvloeden.
15. Wanneer geen nieuwe (of veranderingen in bestaande) functionaliteiten zijn geïmplementeerd, wordt de verklaring van de aanvrager toegevoegd aan het audit portfolio en wordt de wijziging toegevoegd aan de Verklaring van Compliance. De aanvrager wordt een addendum toegezonden behorende bij de Verklaring van Compliance.
16. Indien nieuwe (of veranderingen in bestaande) functionaliteiten zijn geïmplementeerd, wordt een audit georganiseerd op de eisen die door deze veranderingen worden beïnvloed. Indien compliant, dan wordt het proces verder afgehandeld zoals beschreven is in No. 15. Indien non-compliant, dan wordt de nieuwe versie, update of upgrade niet toegevoegd aan de Verklaring van Compliance.
17. De aanvrager deelt met de auditor de contactinformatie (en veranderingen daarin) voor alle aangelegenheden met betrekking tot de getoetste applicatie.
18. Alle toegekende Verklaringen van Compliance worden vermeld op de website van de auditor (www.vbds.nl).