CERTIFICERINGSSCHEMA

INFORMATIEBEVEILIGING EN PRIVACY ROSA

Toezicht

DATUM	18 februari 2018
VERSIE	2.05
AUTEUR	Edustandaard werkgroep IBP

Inhoudsopgave

1 INLEIDING

Het certificeringsschema is een middel om organisaties die een ict-toepassing in de onderwijsketen leveren een eenduidige set aan maatregelen te geven op het gebied van informatiebeveiliging en privacy.

Onderwijsinstellingen moeten als afnemer en gebruiker van een ict-toepassing kunnen aantonen dat de leverancier “passende technische en organisatorische maatregelen” heeft getroffen om de beschikbaarheid, integriteit en vertrouwelijkheid van de ict-toepassing en de gegevens daarin te beschermen. Om dit te bewerkstelligen wordt in dit document beschreven op welke wijze dit aangetoond kan worden.

1.1 Niveaus van toezicht

Het certificeringsschema onderscheidt vier niveaus van toezicht. De toetsvorm van elk niveau zorgt voor een bepaalde mate van onafhankelijkheid van de rapportage:

Onafhankelijkheid	Toetsvorm	Omschrijving
Laag	Self-assessment	Leidt tot een zelfverklaring van de organisatie dat ze voldoen aan het certificeringsschema
Midden	Interne audit	Leidt tot zowel een zelfverklaring als een auditresultaat, maar wordt nog steeds uitgevoerd door de organisatie zelf
Midden	Peer review	Leidt tot een verklaring en auditresultaat van een externe organisatie, niet zijnde een professionele auditorganisatie
Hoog	Externe audit	Leidt tot een verklaring en auditresultaat van een professionele externe auditorganisatie

Deze vier niveaus worden in hoofdstuk 3 verder uitgewerkt.

1.2 Feedback certificeringsschema uit audits

Informatiebeveiliging en privacy zijn nooit af. De stand van de techniek en nieuwe inzichten vragen om een continue bijwerking van classificaties en maatregelen. Daarom kent ook het certificeringsschema een feedbackloop op basis van praktijkervaringen. Dit betekent dat het certificeringsschema op gezette tijden een herziening krijgt.

Een auditor kan bijvoorbeeld constateren dat een bepaalde maatregel, door technische vooruitgang of voortschrijdend inzicht, niet meer adequaat is. Dergelijke feedback moet worden teruggekoppeld richting Bureau Edustandaard, zodat de werkgroep IBP dit kan meenemen in het beheer en de doorontwikkeling van het certificeringsschema. Dit is niet afdwingbaar, maar draagt bij aan de verbetering van het certificeringsschema en is daardoor zeer wenselijk.

2 ALGEMENE UITGANGSPUNTEN

2.1 Informatieverstrekking

Op verzoek van een onderwijsinstelling dient de organisatie minimaal te verstrekken:

a) Een auditverklaring; een ondertekende verklaring waarin de organisatie verklaart te voldoen aan het certificeringsschema informatiebeveiliging en privacy ROSA (zie Bijlage A) met daarin aangegeven welke toetsvorm is uitgevoerd;
b) Een onderbouwing van deze verklaring door middel van een standaard rapportage (zie Bijlage B).

Het staat de onderwijsinstelling vrij om op basis van de verklaring en onderbouwing meer informatie op te vragen of controlevragen te stellen.

De maatregelen in het toetsingskader zijn niet uitputtend. Er zijn altijd meer maatregelen die een organisatie kan treffen. Tevens houdt het toetsingskader niet expliciet rekening met het feit dat veel organisaties voor sommige activiteiten en producten een externe leverancier hebben (bijvoorbeeld een externe hosting partij of cloud-leverancier). In zo'n situatie dienen de maatregelen die relevant zijn voor die externe leverancier doorgezet te worden naar die externe leverancier en door de organisatie getoetst/gecontroleerd te worden.

2.2 Frequentie

De organisatie dient ten minste 1x per jaar aan te tonen dat zij informatiebeveiliging en privacy onder controle heeft. Dit betekent in de praktijk dat de toetsing niet ouder mag zijn dan 1 jaar wanneer de auditverkaring opgevraagd wordt.

De versie van het certificeringsschema die courant[1] was op de datum van toetsing dient gebruikt te zijn. Het staat de onderwijsinstelling vrij om op basis van een nieuwere versie meer informatie op te vragen of aanvullende vragen te stellen.

Wanneer een organisatie, gedurende het jaar waarin de verklaring geldig is, grote wijzigingen aanbrengt in de betreffende ict-toepassing kan de opdrachtgever (onderwijsinstellingen of onderwijsraden) de organisatie gelasten om een tussentijdse verklaring, vergezeld van een nieuwe onderbouwing, te overleggen.

[1] De laatste courante versie is altijd te vinden op https://www.edustandaard.nl/standaarden/afspraken/afspraak/certificeringsschema/

3 SELF-ASSESSMENT

Een self-assessment is een toetsvorm die is uitgevoerd door de organisatie zelf en mensen die direct betrokken zijn bij de ict-toepassing. Daarom heeft deze toetsvorm de minste onafhankelijkheid.

3.1 Auditor

Bij een self-assessment wordt vaak niet gebruik gemaakt van een enkele auditor, maar is het een samenwerking die het procesdocument volgt.

3.2 Vastlegging

Verbeterpunten ten behoeve van de organisatie worden vastgelegd.

Een auditverklaring en onderbouwing zoals vermeld in de algemene uitgangspunten worden opgesteld, in de vorm van Bijlage A en Bijlage B.

3.3 Feedback richting Bureau Edustandaard

Opmerkingen en verbeterpunten ten opzichte van (de toepassing van) het certificeringsschema kunnen in elke gewenste vorm worden gestuurd naar Bureau Edustandaard.

4 INTERNE AUDIT

Een interne audit is een toetsvorm met een gedetailleerde vastlegging, die de organisatie zelf uitvoert, maar wel door een persoon die aantoonbaar onafhankelijk is.

4.1 Auditor

In dit geval moeten zodanige waarborgen bestaan dat de auditor aantoonbaar onafhankelijk zijn werkzaamheden moet kunnen uitvoeren, ten minste maar niet beperkt tot:

a) Functiescheiding tussen de persoon die de audit uitvoert en de personen die de ict-toepassing ontwikkelen of exploiteren;
b) Een expliciete vastlegging van de opdracht door en rapportage aan het management van de organisatie.

4.2 Vastlegging

Van de interne audit wordt een schriftelijke rapportage opgesteld. In deze rapportage is minimaal opgenomen:

c) Per norm een mening van de auditor of de maatregelen die horen bij deze norm effectief zijn;
d) Per norm de bewijsvoering die tijdens het onderzoek is geraadpleegd;
e) Een samenvattend oordeel of het geheel van maatregelen van de organisatie afdoende is, dit oordeel is gebaseerd op de professionele mening van de auditor.

Verbeterpunten ten behoeve van de organisatie worden vastgelegd.

Een auditverklaring en rapportage zoals vermeld in de algemene uitgangspunten worden opgesteld, in de vorm van Bijlage A en Bijlage B.

4.3 Feedback richting Bureau Edustandaard

Opmerkingen en verbeterpunten ten opzichte van (de toepassing van) het certificeringsschema kunnen in elke gewenste vorm worden gestuurd naar Bureau Edustandaard.

5 PEER REVIEW

Een peer review is een toetsvorm met een gedetailleerde vastlegging, die uitgevoerd wordt door een andere organisatie, waardoor de toetsing aantoonbaar onafhankelijk is.

5.1 Auditor

De auditor is een persoon van een andere organisatie in de onderwijssector, anders dan een professionele auditorganisatie is. Uit oogpunt van kostenbesparing en/of domeinkennis kan de organisatie besluiten tot deze tussenvorm van toetsing ten opzichte van interne- en externe audit.

5.2 Vastlegging

Van de peer review wordt een schriftelijke rapportage opgesteld. In deze rapportage is minimaal opgenomen:

a) Per norm een mening van de auditor of de maatregelen die horen bij deze norm effectief zijn;
b) Per norm de bewijsvoering die tijdens het onderzoek is geraadpleegd;
c) Een samenvattend oordeel of het geheel van maatregelen van de organisatie afdoende is, dit oordeel is gebaseerd op de professionele mening van de auditor.

Verbeterpunten ten behoeve van de organisatie worden vastgelegd.

Een auditverklaring en rapportage zoals vermeld in de algemene uitgangspunten worden opgesteld, in de vorm van Bijlage A en Bijlage B.

5.3 Feedback richting Bureau Edustandaard

Opmerkingen en verbeterpunten ten opzichte van (de toepassing van) het certificeringsschema kunnen in elke gewenste vorm worden gestuurd naar Bureau Edustandaard.

6 EXTERNE AUDIT

Een externe audit is een toetsvorm met een gedetailleerde vastlegging, die uitgevoerd wordt door een professionele auditorganisatie.

6.1 Auditor

De auditor is een persoon van een professionele auditorganisatie. De auditor moet dan ook aangesloten zijn bij een beroepsvereniging zoals bijvoorbeeld NOREA.

6.2 Vastlegging

Van de externe audit wordt een schriftelijke rapportage opgesteld. In deze rapportage is minimaal opgenomen:

a) Per norm een mening van de auditor of de maatregelen die horen bij deze norm effectief zijn;
b) Per norm de bewijsvoering die tijdens het onderzoek is geraadpleegd;
c) Een samenvattend oordeel of het geheel van maatregelen van de organisatie afdoende is, dit oordeel is gebaseerd op de professionele mening van de auditor.

Verbeterpunten ten behoeve van de organisatie worden vastgelegd.

Een auditverklaring en rapportage zoals vermeld in de algemene uitgangspunten worden opgesteld, in de vorm van Bijlage A en Bijlage B.

6.3 Feedback richting Bureau Edustandaard

Opmerkingen en verbeterpunten ten opzichte van (de toepassing van) het certificeringsschema kunnen in elke gewenste vorm worden gestuurd naar Bureau Edustandaard.

7 CONTROLE DOOR ONDERWIJSINSTELLING

De onderwijsinstelling moet vast kunnen stellen of de ict-toepassing voldoet aan het certificeringsschema. Ook dit kan op verschillende niveaus. Elke extra controle vergroot de zekerheid. De benodigde zekerheid moet de onderwijsinstelling zelf bepalen en deze moet in ieder geval in relatie staan tot de mogelijke risico's die gepaard gaan met het gebruik van de ict-toepassing. Bijvoorbeeld moet een onderwijsinstelling meer controle-stappen nemen voor een ict-toepassing die zeer gevoelige persoonsgegevens bewerkt.

7.1 Opzoeken organisatie via Privacyconvenant

De onderwijsinstelling kan via het Privacyconvenant.nl kijken of de organisatie is aangesloten bij het Privacyconvenant. Wanneer een organisatie dit is, committeert die zich ook via de bijsluiter van de bewerkingsovereenkomst aan het certificeringsschema of een soortgelijke standaard.

7.2 Opvragen auditverklaring

De onderwijsinstelling kan bij de organisatie een auditverklaring opvragen voor de betreffende ict-toepassing. Dit geeft aan wanneer welke vorm van toetsing wanneer heeft plaatsgevonden op de normen en uitgangspunten in het certificeringsschema.

Wanneer een externe audit is uitgevoerd door een professionele auditorganisatie, kan de onderwijsinstelling controleren of de auditor is aangesloten bij een beroepsvereniging voor auditors.

7.3 Opvragen rapportage ten behoeve van auditverklaring

De onderwijsinstelling kan bij de organisatie de rapportage ten behoeve van de auditverklaring opvragen. Deze geeft de BIV-classificatie aan die de organisatie bepaald heeft, geeft per aandachtsgebied aan in welke mate de ict-toepassing voldoet aan het certificeringsschema en eventuele afwijkingen hierop.

7.4 Opvragen details toetsing

De onderwijsinstelling kan bij de organisatie specifieke vragen stellen over de onderwerpen in de rapportage. Bijvoorbeeld op welke wijze de BIV-classificatie is vastgesteld, of op welke wijze een specifieke maatregel is uitgevoerd. Hiermee kan de onderwijsinstelling steekproefsgewijs toetsen of de auditresultaten in lijn zijn met de werkelijkheid.

A Auditverklaring

AUDITVERKLARING CERTIFICERINGSCHEMA

Verklaring behorend bij het certificeringsschema informatiebeveiliging en privacy ROSA

Inleiding

In deze Auditverklaring legt de organisatie vast dat de hieronder genoemde ict-toepassing voldoet aan het certificeringsschema. Het oordeel is tot stand gekomen na toetsing van de ict-toepassing aan de normen en uitgangspunten zoals beschreven in het certificeringsschema.

Verklaring

_____ *(naam organisatie)*, verklaart dat de ict-toepassing, genaamd _____ *(naam ict-toepassing)*, voldoet aan de normen en uitgangspunten zoals genoemd in het certificeringsschema, versie _____ *(versienummer)*. De toetsing is uitgevoerd middels self-assessment/interne audit/peer review/externe audit *(weghalen wat niet van toepassing is)*, door _____ *(organisatie, naam en functie auditor)* op _____ *(datum)*.

De organisatie heeft een onderbouwing van deze verklaring een rapportage ingevuld waarop is aangegeven of en in welke mate aan de beschreven normen wordt voldaan, of op termijn aan zal voldoen. Deze rapportage is op aanvraag beschikbaar.

<u>Aanvrager verklaart voorts dat:</u>

Een nieuwe Auditverklaring zal worden ingediend in geval van ingrijpende wijzigingen of updates aan de ict-toepassing, indien die aanpassingen van invloed (kunnen) zijn op de normen en uitgangspunten zoals opgenomen in het certificeringsschema.

Aldus opgemaakt en getekend op _____ *(datum)* te _____ *(plaats)*,

_____ *(handtekening)*

_____ *(naam voluit)* _____ *(functie)*

B Rapportage ten behoeve van de auditverklaring

Inleiding

Dit is een mogelijke rapportagevorm waarmee gedetailleerd inzicht gegeven wordt in de mate waarmee een organisatie voldoet aan het certificeringsschema. Het bevat de minimale onderdelen die een dergelijke rapportage moet bevatten. Het staat de organisatie vrij om de vorm en opmaak naar eigen behoeften aan te passen.

Rapportageonderdelen

Organisatie			
Ict-toepassing			
Omschrijving	(Korte omschrijving van functionaliteit en bewerkte gegevens)		
Datum			
Toetsvorm	(Self-assessment/interne audit/peer review/externe audit)		
Uitvoerder toets	(Organisatie, naam en functie uitvoerder)		
BIV-classificatie	(Beschikbaarheid=1/2/3, Integriteit=1/2/3, Vertrouwelijkheid=1/2/3)		
Categorie	**Maatregelen**	**Compliance**	**Uitleg**
		Voldaan/ niet voldaan/ alternatieve maatregel	(Bij niet voldaan aangeven hoe/wanneer dit wordt gecorrigeerd. Bij alternatieve maatregel deze beschrijven)
Beschikbaarheid	Overbelasting		
	Business continuity		
	Ontwerp		
	Monitoring		
	Testen		
	Software		
	Actuele dreigingen		
Integriteit	Herleidbaarheid (gebruikers)		
	Backup		
	Application controls		
	Onweerlegbaarheid		
	Herleidbaarheid (technisch beheer)		
	Controle integriteit		
	Onweerlegbaarheid		
	Actuele dreigingen		

Vertrouwelijkheid	Levenscyclus gegevens		
	Logische toegang		
	Fysieke toegang		
	Netwerk toegang		
	Scheiding omgevingen		
	Transport en fysieke opslag		
	Logging		
	Toetsing		
	Actuele dreigingen		