CERTIFICERINGSSCHEMA

INFORMATIEBEVEILIGING EN PRIVACY ROSA

Algemene beschrijving

DATUM	18 februari 2018
VERSIE	2.05
AUTEUR	Edustandaard werkgroep IBP

INHOUDSOPGAVE

1 INLEIDING

1.1 Achtergrond

Binnen het onderwijs vervult ict een belangrijke rol. Op verschillende manieren wordt gebruik gemaakt van ict-toepassingen voor onderwijskundige of onderwijsondersteunende producten en diensten. De aard en inhoud van deze ict-toepassingen kunnen onderling sterk verschillen, maar zij hebben als gemeenschappelijk kenmerk dat de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevensbewerking cruciaal is. Ook de toegenomen aandacht en strengere wetgeving rondom privacy dwingt alle partijen in de onderwijsketen expliciet aandacht te besteden aan informatiebeveiliging en privacy (IBP). Onderwijsinstellingen moeten erop kunnen vertrouwen dat (publieke of private) organisaties die ict-toepassingen leveren in het onderwijs persoonsgegevens op een veilige manier bewerken.

Voor onderwijsinstellingen is het echter niet eenvoudig om vast te stellen of een leverancier de juiste maatregelen heeft genomen. Omgekeerd is het voor leveranciers niet eenvoudig om aan te tonen dat zij tenminste aan de minimale eisen voldoen. Het hanteren van een eenduidige meetlat moet dit probleem oplossen. Bestaande ‘normenkaders’ bieden hierbij niet de helderheid en transparantie die nodig is om met partijen in een keten afspraken te maken. Dit wordt in detail uitgelegd in paragraaf 2.2 ‘relatie met andere normenkaders’.

Daarom hebben ketenpartijen in het onderwijsdomein gezamenlijk het ‘certificeringsschema informatiebeveiliging en privacy ROSA’ opgesteld. Deze standaard is onderdeel van de Referentie Onderwijs Sector Architectuur (ROSA[1]) en wordt binnen Edustandaard beheerd door de werkgroep IBP. Deze werkgroep bestaat uit IBP-specialisten uit de onderwijsketen en vertegenwoordigt zowel onderwijs als leveranciers. Via deze werkgroep kunnen alle partijen in de onderwijsketen invloed uitoefenen op de inhoud van de standaard.

1.2 Doelgroep

Het certificeringsschema is enerzijds bedoeld voor organisaties die ict-toepassingen leveren in de onderwijsketen. Deze kunnen op een eenduidige manier aantoonbaar maken dat ze informatiebeveiliging en privacy op orde hebben.

Anderzijds is het certificeringsschema bedoeld voor onderwijsinstellingen. Bij het specificeren van informatiebeveiligingseisen kunnen zij eenvoudig verwijzen naar het certificeringsschema, in plaats van specifieke eisen te stellen met betrekking tot (veelal technische) maatregelen. Ook kunnen zij met het toetsingskader eenvoudiger (laten) toetsen of een organisatie die ict-toepassingen levert de informatiebeveiliging op orde heeft.

[1] http://www.wikixl.nl/wiki/rosa

1.3 Doel

Het certificeringsschema is beoogd als een algemeen geldende baseline voor informatiebeveiliging in het onderwijsdomein, dat de toegankelijkheid en betrouwbaarheid van onderwijs gerelateerde informatie bevordert. Het is in de eerste plaats een hulpmiddel om in de onderwijsketen tot een passend niveau van informatiebeveiliging te komen.

Het certificeringsschema moet voor onderwijsinstellingen en leveranciers duidelijk maken zijn wat voor een ict- toepassing in het onderwijs een passend niveau van informatiebeveiliging is. Deze eisen zijn voor alle partijen gelijk en transparant.

Het certificeringsschema is daarmee een instrument om ICT-toepassingen mee te toetsen. Het legt de meetlat waartegen getoetst wordt vast. De wijze van toetsing (intern of extern) en de garanties die daarbij nodig zijn liggen niet vast. Afhankelijk van het belang van een toepassing of vanwege afspraken die erover in een keten zijn gemaakt, kan worden gekozen om de toetsing zwaarder aan te zetten. Dit is nader uitgewerkt in het document 'Certificeringschema_toezicht'.

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.

Tot slot is voor leveranciers – die nog geen managementsysteem voor informatiebeveiliging hebben ingericht – het certificeringsschema een hulpmiddel om daar een start mee te maken. Bij het doorlopen van de stappen uit procesdocument (zie certificeringsschema_proces) wordt namelijk een compacte verbetercyclus voor informatiebeveiliging uitgevoerd. Het toetsingskader biedt daarbij de concrete maatregelen waaraan moet worden voldaan.

1.4 Onderdelen van het certificeringsschema

Het certificeringsschema is een generiek instrument binnen de onderwijssector en bestaat uit de volgende onderdelen:

1. Certificeringsschema_algemene_beschrijving (dit document).
2. Certificeringsschema_proces; dit beschrijft de toepassing van het certificeringsschema voor een enkele organisatie.
3. Certificeringsschema_classificatie; Deze spreadsheet helpt een organisatie om het gewenste niveau van informatiebeveiliging te bepalen.
4. Certificeringsschema_toetsingskader.xlsx; Deze spreadsheet helpt een organisatie en/of auditor om te toetsen of de juiste maatregelen zijn getroffen op basis van de classificatie.

5. Certificeringsschema_toezicht; dit document beschrijft verschillende niveaus van audit op het toetsingskader en ondersteunt zowel de organisatie als de onderwijsinstelling.

1.5 Samenhang met andere initiatieven

Onderdeel van de ROSA-architectuur is het thema informatiebeveiliging en privacy, waarin principes en beheersmaatregelen zijn opgenomen waar ketenpartijen, dus ook onderwijsinstellingen aan dienen te voldoen. Het certificeringsschema is een nadere uitwerking van deze principes en beheersmaatregelen die interne maatregelen voorschrijft die organisaties moeten nemen om hun informatie voldoende te beveiligen.

Sinds 2014 is het certificeringsschema al onlosmakelijk verbonden aan de 'Edukoppeling Transactiestandaard'. De 'Edukoppeling Transactiestandaard' beschrijft de veilige gegevensuitwisseling tussen toepassingen. Het certificeringsschema wordt daarbij gebruikt om informatiebeveiligingseisen te specificeren voor toepassingen die middels Edukoppeling zijn aangesloten.

In juni 2016 is het Convenant Digitale Onderwijsmiddelen en Privacy 2.0 vastgesteld. In dit convenant worden afspraken gemaakt over de bescherming van persoonsgegevens en waarborgen voor de zorgvuldige omgang met Persoonsgegevens die worden verwerkt in het kader van het gebruik van Digitale Onderwijsmiddelen door Onderwijsinstellingen, waaronder het gebruik van leermiddelen, toetsen, administratie- en informatiesystemen. Onderdeel van deze afspraken is dat er, middels bijlage 2 van de bewerkersovereenkomst, de genomen technische en organisatorische kunnen worden aangetoond. Het certificeringsschema is een goede manier om de maatregelen aan te tonen. De formele afspraak om het certificeringsschema te koppelen aan het convenant is nog niet gemaakt.

Voor een onderwijsinstelling zijn er diverse initiatieven waar aan een hoger niveau van informatiebeveiliging en privacy wordt gewerkt. De zorg voor IBP kan alleen goed worden geregeld als scholen en leveranciers daar samen aan werken. Zie voor een overzicht: https://www.kennisnet.nl/artikel/wat-is-informatiebeveiliging-en-privacy-en-hoe-regel-ik-dit-op-school/ en https://www.surf.nl/themas/beveiliging

1.6 Taken en verantwoordelijkheden

Het eigenaarschap van het normenkader is belegd binnen Edustandaard, waar ook andere afspraken binnen het onderwijsdomein worden beheerd. De Edustandaard werkgroep IBP voert het beheer en de doorontwikkeling uit.

Naast de inhoud van het certificeringsschema moet er ook draagvlak zijn voor het gebruik. Draagvlak kan voortkomen uit het actief betrekken van de partijen die beoogd zijn om het certificeringsschema te gaan implementeren en te gebruiken. Voor het certificeringsschema zijn dat in eerste instantie partijen in de educatieve keten. Afspraken over het toepassen van

het certificeringsschema in de educatieve keten worden onder andere gemaakt binnen Edu-K, in het tactisch overleg continuïteit en beveiliging (https://www.edu-k.nl/continuiteit/) .

Audits kunnen worden uitgevoerd in opdracht van onderwijsinstellingen, sectorraden of de organisaties zelf op basis van het toetsingskader in het certificeringsschema.
Er is nog geen centrale registratie van audits en auditresultaten voorzien. Wel wordt in het toezichtdocument (Certificeringsschema_toezicht) beschreven welke mate van transparantie geboden kan worden door verschillende auditvormen.

2 TOETSINGSKADER

2.1 Toelichting toetsingskader

Het toetsingskader is het centrale onderdeel van het certificeringsschema. Het toetsingskader bestaat uit een spreadsheet met daarin tabbladen voor de informatiebeveiligingsaspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid. Voor elk van deze aspecten moet een organisatie maatregelen treffen.

Ter illustratie een overzicht van mogelijke maatregelen per informatiebeveiligingsaspect:
Beschikbaarheid: Overbelasting, Business continuity, Afhankelijkheden, Software, Logging / monitoring / testen, Actuele dreigingen (DDoS, ransomware)
Integriteit: Herleidbaarheid, Functiescheiding, Backup, Application controls, Manual controls, Onweerlegbaarheid, Actuele dreigingen (DDoS, ransomware)
Vertrouwelijkheid: Levenscyclus gegevens, Fysieke toegang, Logische toegang, Opslag en transport, Logging, Toetsing, Actuele dreigingen (DDoS, ransomware)

De maatregelen zijn uitgewerkt op 3 niveau's: Laag, Midden en Hoog. Het benodigde niveau kan worden bepaald met het classificatie hulpmiddel (Certificeringsschema_classificatie). Op basis van deze zogenaamde BIV-classificatie kunnen in het toetsingskader de maatregelen worden geselecteerd die nodig zijn om het gewenste niveau van informatiebeveiliging te garanderen.

2.2 Relatie tussen het certificeringsschema en andere normenkaders

De standaarden ISO 27001 en ISO 27002 zijn internationaal algemeen geaccepteerde internationale standaarden voor een betrouwbare informatieverwerking; ze zijn in 2017 overgenomen als Europese norm. ISO 27001 is een standaard die beschrijft hoe een organisatie procesmatig met het beveiligen van informatie kan omgaan, met als doel om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie zeker te stellen. Een organisatie die ISO 27001 gecertificeerd is heeft aangetoond de omgang met informatiebeveiliging goed te hebben ingericht. Er zijn adequate processen, procedures, werkinstructies om voor de organisatie informatiebeveiligingsrisico's te identificeren en daar afdoende maatregelen op te nemen. Een organisatie bepaalt daarbij zelf wat de scope is van de certificering, is de hele organisatie gecertificeerd of bijvoorbeeld alleen de beheerafdeling. Ook bepaalt een organisatie zelf wat de belangrijkste risico's zijn en of daar maatregelen op worden genomen of dat (een deel van) het risico wordt geaccepteerd.
Aan de ISO 27001 standaard is een bijlage verbonden (Annex A) met tactische richtlijnen en maatregelen. Een organisatie bepaalt zelf welke maatregelen van toepassing zijn in een zogenaamd Statement of Applicability (SoA).

ISO 27002 is feitelijk de uitgebreide beschrijving van de annex A uit ISO 27001 en geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie. ISO 27002 kan dienen als een

praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en effectieve methoden voor het bereiken van deze veiligheid.

De genoemde ISO-normen geven echter zelf geen niveaus of baseline aan voor specifieke maatregelen. De zwaarte van de te nemen maatregelen is immers niet voorgeschreven. Het staat je daarmee vrij om te kiezen of en hoe je deze maatregelen implementeert.

Uit bovenstaande volgt dat zelfs als alle leveranciers ISO 27001 gecertificeerd zijn onderwijsinstellingen nog de nodige vragen moeten stellen. Wat is de scope van de certificering, wordt de toepassing die ik afneem wel gedekt door deze scope? Welke maatregelen acht de leverancier nodig voor de toepassing, wat is het Statement of Applicabilty? Welke risico's zijn er afgedekt en zijn de genomen maatregelen daarvoor wel afdoende?

Het certificeringsschema moet de meeste van deze vragen wegnemen. Bij opstellen van het certificeringsschema is uitgegaan van de algemeen geldende risicogebieden voor ict-toepassingen in de onderwijsketen. Het proces omschrijft een risicoanalyse waarmee het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid wordt vastgesteld. Op basis van de relevante maatregelen uit verschillende normenkaders, waaronder ISO 27002, zijn voor deze niveaus concrete maatregelen opgesteld. Deze concrete invulling maakt voor onderwijsinstellingen en leveranciers van ict-toepassingen duidelijk aan welke eisen precies voldaan moet zijn.

2.3 Beheer en doorontwikkeling

Binnen Edustandaard wordt periodiek (minimaal eenmaal per jaar) de opzet en de werking van het certificeringsschema besproken met alle relevante stakeholders die vertegenwoordigd zijn in de Standaardisatieraad. Hiertoe wordt input verzameld vanuit de Edustandaard werkgroep IBP en relevante ketensamenwerkingen zoals Edu-K.

De specifieke inhoud van het schema en het toetsingskader worden geëvalueerd door de Edustandaard werkgroep IBP. In eerste instantie wordt uitgegaan van een evaluatiefrequentie van viermaal per jaar, namelijk bij de bijeenkomsten van de werkgroep. Hiertoe wordt input verzameld vanuit Edu-K en individuele organisaties die het certificeringsschema gebruiken.

Aanpassingen aan het toetsingskader, bijvoorbeeld wegens optreden van nieuwe risico's of bijstelling van de maatregelen, worden direct gepubliceerd. Hiermee wordt een uitzondering gemaakt op het gebruikelijke standaardisatie proces. Jaarlijks wordt de standaard als geheel, dus toetsingskader en de overige onderdelen van het certificeringsschema, opnieuw formeel vastgesteld.

3 TOEPASSING

3.1 Toepassing door ketenpartijen

Een organisatie die ict-toepassingen levert voert een self-assessment uit of laat een externe toets uitvoeren, op basis van het procesdocument (Certificeringsschema_proces). Dit document legt uit welke stappen een organisatie moet ondernemen om te bepalen of zij voldoet aan het certificeringsschema.

3.2 Toetsing

Een auditor (intern of extern) voert een audit uit, op basis van het toezichtdocument (Certificeringsschema_toezicht). Dit document legt uit welke stappen en verslaglegging minimaal moeten plaatsvinden.

3.3 Toepassing door onderwijsinstellingen

Een onderwijsinstelling moet vast kunnen stellen of een 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. Een onderwijsinstelling kan bij het inkopen van ict aan een leverancier eisen dat de toepassing voldoet aan het certificeringsschema.