BIV-classificatie

De kwaliteitsaspecten die worden toegepast op informatiebeveiliging zijn Beschikbaarheid, Integriteit, en Vertrouwelijkheid. Deze termen worden hier inclusief de deelaspecten beschreven. Alle aspecten kunnen worden geclassificeerd in laag, midden en hoog.

Beschikbaarheid:

de mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening waarborgen.

Deelaspecten hiervan zijn:

• Continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is;
• Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is;
• Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

Voor de beschikbaarheid komt de classificatie *laag, midden en hoog* respectievelijk overeen met *niet vitaal, vitaal en zeer vitaal.*

Integriteit:

de mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.

Deelaspecten hiervan zijn:

• Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;
• Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
• Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Voor de integriteit komt de classificatie *laag, midden en hoog* respectievelijk overeen met *openbaar, intern en vertrouwelijk*

Vertrouwelijkheid:

de mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.

Deelaspecten hiervan zijn:

• Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is;
• Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is;
• Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn;
• Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

Voor de vertrouwelijkheid komt de classificatie *laag, midden en hoog* respectievelijk overeen met *openbaar, intern en vertrouwelijk*

Hoe bepaal ik het classificatie niveau?

Hiervoor maken we gebruik van de vragen, zoals deze zijn opgesteld voor het certificeringsschema. Praat over onderstaande vragen en maak een inschatting naar gewenst niveau. Het is misschien nog wel belangrijker om met een aantal mensen te praten over deze vragen, dan een exacte inschatting te maken. Door erover te praten kweek je bewustwording en ga je anders naar de processen kijken.

Beschikbaarheid

Uitleg *Bedenk welk **proces** (het onderwijsproces of een specifiek ondersteunend proces) de ict-toepassing ondersteunt. Vul aan de hand van onderstaande vragen een motivatie in en plaats een X in de bijbehorende kolom.*

Vragen	Motivatie	Laag	Midden	Hoog
Wat is de verwachtte belasting van de ict-toepassing? - Laag = weinig gelijktijdige gebruikers, weinig transacties (±1 per uur) - Midden = veel gelijktijdige gebruikers, normale hoeveelheid transacties (±10 per uur) - Hoog = veel gelijktijdige gebruikers, veel transacties (>100 per uur)				
Wanneer moet de dienst beschikbaar zijn? - Laag = regulier (kantooruren) - Midden = ruim (bijvoorbeeld 07:00 - 23:00) - Hoog = altijd (24x7x365)				
Zijn er contractuele of wettelijke verplichtingen voor de beschikbaarheid? - Laag = nee, of deze zijn regulier - Midden = er zijn contractuele verplichtingen en deze zijn ruim of hoog - Hoog = er zijn wettelijke verplichtingen				
Wat is de langste periode dat de ict-toepassing niet beschikbaar mag zijn? - Laag = maximaal enkele dagen - Midden = maximaal een werkdag - Hoog = maximaal een aantal uur				
Hoe erg is het als de data, informatie of de ict-toepassing niet beschikbaar zijn? - Laag = niet - Midden = het proces wordt belemmerd maar kan wel doorgaan - Hoog = het proces kan in zijn geheel niet doorgaan				
Leidt het niet beschikbaar zijn van de toepassing tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies wat opgevangen kan worden door tijdige communicatie - Hoog = langdurig imagoverlies				

Niveau 1: **Laag** Beschikbaarheid is onbelangrijk.	**Niveau 2:** **Midden** Beschikbaarheid is belangrijk	**Niveau 3:** **Hoog** Beschikbaarheid is noodzakelijk
Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende meerdere dagen brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een dag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.

Integriteit

Uitleg *Bedenk welke **gegevens** (bijvoorbeeld leerresultaten of leermateriaal) de ict-toepassing ondersteunt. Vul aan de hand van onderstaande vragen een motivatie in en plaats een X in de bijbehorende kolom.*

Vragen	Motivatie	Laag	Midden	Hoog
Kan er fraude met leerresultaten of financiële fraude plaatsvinden door fouten in de gegevens of ongeautoriseerde wijzigingen? - Laag = nee, de gegevens lenen zich niet voor fraude - Midden = beperkt, gegevens worden ook elders gecontroleerd - Hoog = ja, de ict-toepassing is de enige toepassing met deze gegevens				
Hoe erg is het als er fouten of ongeautoriseerde veranderingen in de gegevens zitten? - Laag = niet - Midden = het proces wordt belemmerd maar kan wel doorgaan - Hoog = het proces kan in zijn geheel niet doorgaan				
Hoeveel effect hebben fouten of ongeautoriseerde veranderingen in gegevens? - Laag = alleen intern - Midden = intern en bij een enkele ketenpartij - Hoog = in de hele keten				
Leiden fouten of ongeautoriseerde veranderingen tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies - Hoog = langdurig imagoverlies				
Zijn er contractuele of wettelijke verplichtingen voor de integriteit van gegevens? - Laag = nee - Midden = ja, deze eisen stelselmatige controle - Hoog = ja, deze eisen stelselmatige controle en bewijs van werking				
Kunnen er personen negatieve gevolgen ondervinden als gevolg van het niet correct zijn van gegevens? - Laag = niet - Midden = eventuele fouten zijn nog te corrigeren - Hoog = fouten veroorzaken ernstige of langdurige negatieve gevolgen				

Niveau 1: **Laag** Integriteit is onbelangrijk.	**Niveau 2:** **Midden** Integriteit is beschermd.	**Niveau 3:** **Hoog** Integriteit is noodzakelijk.
Blijvende juistheid van informatie (vanaf de bron tot het laatste gebruik) is gewenst, maar hoeft niet gegarandeerd te zijn. Indien informatie niet correct is, leidt dit tot beperkte schade.	Blijvende juistheid van informatie moet gewaarborgd zijn. Sommige toleranties zijn toelaatbaar. Juistheid van informatie is belangrijk, maar niet kritisch. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is kan de organisatie substantiële schade lijden.	Informatie moet gegarandeerd correct zijn. Informatie waarbij het noodzakelijk is dat de correctheid niet betwist kan worden, zoals de uitslagen van toetsen, examens, onomkeerbare financiële transacties. Indien informatie niet correct is, kan de organisatie ernstige schade lijden.

Vertrouwelijkheid

Uitleg *Bedenk welke **gegevens** (bijvoorbeeld leerresultaten of leermateriaal) de ict-toepassing ondersteunt. Vul aan de hand van onderstaande vragen een motivatie in en plaats een X in de bijbehorende kolom.*

Vragen	Motivatie	Laag	Midden	Hoog
Wat is de classificatie van de gegevens? - Laag = publiek of intern gebruik - Midden = vertrouwelijk - Hoog = geheim				
Worden personen waarvan gegevens lekken benadeeld door het lekken van gegevens? - Laag = nee - Midden = personen worden kortstondig benadeeld - Hoog = personen worden langdurig benadeeld				
Leiden datalekken tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies wat opgevangen kan worden door tijdige communicatie - Hoog = langdurig imagoverlies				
Zijn er contractuele of wettelijke verplichtingen voor de vertrouwelijkheid? - Laag = nee - Midden = ja, deze eisen bescherming - Hoog = ja, deze eisen bescherming, bewijs van werking en melding van inbreuk				
Welke type persoonsgegevens bevat de ict-toepassing? - Laag = geen - Midden = 'gewone' persoonsgegevens zoals NAW - Hoog = bijzondere persoonsgegevens (geloof, medisch, et cetera)				
Kunnen er personen in gevaar worden gebracht als gevolg van het uitlekken van gegevens? - Laag = niet - Midden = eventuele fouten zijn nog te corrigeren - Hoog = personen kunnen het slachtoffer worden van identiteitsfraude				

Niveau 1: **Laag** Informatie is voor intern gebruik	**Niveau 2:** **Midden** Informatie is vertrouwelijk.	**Niveau 3:** **Hoog** Informatie is geheim.
Openbaar worden van gegevens leidt tot weinig of geen schade voor een instelling of betrokkene.	De organisatie, instelling of betrokkene kan substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know basis). Hieronder vallen onder andere persoonsgegevens.	De organisatie, instelling of betrokkene kan ernstige schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag uitsluitend toegankelijk zijn voor een zeer geselecteerde groep personen. Hieronder vallen onder andere bijzondere persoonsgegevens.