Behorende bij het
Informatieclassificatieraamwerk
van de Vlaamse overheid

Vlaamse overheid

‘Pas toe of leg uit’ principe

Versie juni 2024

Bron: Team Informatieveiligheid

Doelpubliek: Leidend Ambtenaren, proceseigenaren

DIGITAAL VLAANDEREN

Voor een **veilige** digitale overheid

DIGITAAL
VLAANDEREN

Het **‘Pas toe of leg uit’ principe** is één van de **basisprincipes** van het **Vo-informatieclassificatieraamwerk** (ICR). Eenvoudig gezegd houdt dit de keuze in tussen het **toepassen van** een maatregel of **uitleggen waarom niet**. Met dit principe kunnen entiteiten erover waken dat maatregelen passend en proportioneel zijn in hun omgeving.

Raadpleeg het Informatieclassificatie raamwerk voor meer informatie **via deze QR:**

Maar wat betekent het 'Pas toe of leg uit' principe in het kader van het ICR?

DIGITAAL VLAANDEREN

Het **'Pas toe of leg uit' principe** is ***niet*** van toepassing op het **governance deel** van het ICR: de inventarisatie en informatieklassebepaling volgens de **impactschalen** zoals gedefinieerd in het ICR **zijn verplicht** te volgen (enkel 'pas toe'), **zo ook de spelregels rond eigenaarschap, rollen en verantwoordelijkheden en het feit dat een risicoanalyse moet uitgevoerd worden voor assets met klasse 3 of hoger.**

Waarop is 'Pas toe of leg uit' principe dan wel van toepassing? Het principe wordt gebruikt in de implementatie van de minimale en specifieke maatregelen van het ICR. Met andere woorden: **zodra je een informatieklassebepaling hebt uitgevoerd, bepaal je welke minimale/specifieke maatregelen hier tegenover staan.** Je kan hiervoor bijvoorbeeld de selectietool gebruiken, die geeft een overzicht van de maatregelen van toepassing op de bepaalde informatieklasse.

Dit overzicht toets je af op de vraag: heb ik deze maatregel al toegepast? Zo ja, dan voldoe je alvast aan **deel één van het principe, namelijk 'pas toe'**. Misschien is de maatregel nog niet ingevoerd maar heb je wel de intentie om dat te doen. Dan **zorg je ervoor** dat de **maatregel opgenomen wordt in je planning** (jaarplan informatieveiligheid of roadmap).

Een andere mogelijkheid bestaat erin dat je **de maatregel niet toepast** (en ook niet zal invoeren), **maar misschien heb je een alternatief. Nu zit je in het tweede deel van het principe, namelijk het 'leg uit' gedeelte**.

Belangrijk is dan dat je via risicoanalyse inschat wat het niet toepassen van de gevraagde maatregel of het gebruiken van een alternatief met het gewenste niveau van informatieveiligheid doet.

Als het risico dat hiermee ontstaat **significant** is, dan moet je leidend ambtenaar dit valideren (risico aanvaarding). Sowieso moet je dit alles ook documenteren.

Een overzicht van het 'Pas toe of leg uit' principe:

DIGITAAL VLAANDEREN