edustandaard

Voor:	Standaardisatieraad, Edustandaard
Van:	Architectuurraad, Edustandaard
Datum	29 juni 2017
Betreft	Positief advies inz. inbeheername Certificeringsschema
Bijlage	ROSA Architectuurscan/advies: Certificeringsschema 2017

Samenvatting

Het Certificeringsschema Informatiebeveiliging en Privacy ROSA versie 2017 (CS 2017) is voor inbeheername aangeboden aan Edustandaard. Op 22 juni 2017 heeft de Architectuurraad het CS 2017 besproken aan de hand van een door Bureau Edustandaard uitgevoerde ROSA architectuurscan. Op basis van deze bespreking en de uitkomsten van de architectuurscan heeft de Architectuurraad besloten een positief advies uit te brengen ten aanzien van inbeheername van het Certificeringsschema 2017 door Edustandaard.

ROSA Architectuurscan

De Architectuurraad is een adviserend gremium, waarin ketenpartijen op inhoudelijk niveau worden vertegenwoordigd. De leden van de raad adviseren de Standaardisatieraad over afspraken en standaarden en hun onderlinge samenhang. De voorzitter van de Architectuurraad is adviserend lid van de Standaardisatieraad.

Eén van de instrumenten waar de Architectuurraad over beschikt om aan deze adviserende rol invulling te geven, is de ROSA Architectuurscan. Met de ROSA Architectuurscan worden op systematische wijze alle architectuuraspecten van een bij Edustandaard ingebracht onderwerp in kaart gebracht en worden knelpunten en kansen gesignaleerd. De scan bepaalt de relatie tussen het CS 2017 en ROSA, en leidt tot drie soorten adviezen: 1) adviezen die sec het CS 2017 betreffen; 2) adviezen die betrekking hebben op de context waarin het informatiemodel toegepast gaat worden, en 3) adviezen die de ROSA zelf betreffen en leiden tot onderwerpen op de backlog van de Architectuurraad.

Op basis van de uitkomsten van de architectuurscan heeft de Architectuurraad een advies geformuleerd ten aanzien van de voorgenomen inbeheername van het CS 2017.

Positief advies

De Architectuurraad adviseert positief ten aanzien van de inbeheername van het CS 2017 door Edustandaard. Naar aanleiding van de uitgevoerde architectuurscan zijn er, vanuit de inhoudelijke expertise van de leden van de Architectuurraad, geen bezwaren geconstateerd die inbeheername in de weg staan.

De Architectuurraad adviseert de Standaardisatieraad tevens om de adviezen uit de architectuurscan die direct betrekking hebben op het certificeringsschema – in het adviesrapport gemarkeerd als ‘productadviezen’ - mee te geven aan de Werkgroep IBP met de oproep aan deze adviezen opvolging te geven zodra de voorbereidingen starten voor een nieuwe (jaarlijkse) versie van het Certificeringsschema. Deze adviezen hebben betrekking op:

- Het hanteren van dezelfde definities als het ROSA-katern IBP;
- Het verduidelijken van de samenhang tussen de maatregelen uit het Certificertingsschema en de doelen uit ISO 27001 zoals die zijn beschreven in het ROSA-katern IBP;
- Het mogelijk uitbreiden van de maatregelenset;
- De inrichting van ‘incident response’;
- Het verduidelijken van het begrip eigenaarschap van gegevens in termen van zeggenschappen over die gegevens;
- De relatie van het Certificeringsschema met de Edukoppeling transactiestandaard.

Ten slotte vraagt de Architectuurraad aan de Standaardisatieraad om kennis te nemen van de ‘context-adviezen’. Deze adviezen betreffen:

- De blijvende noodzaak voor organisaties om, in aanvulling op de maatregelen uit het Certificeringsschema, organisatorische (proces)maatregelen te nemen;
- Structurele afstemming tussen de werkgroepen IBP en Edukoppeling.