Leeswijzer voor het ‘Baseline Informatiebeveiliging Rijk (BIR) Coverage report’

Dit document helpt bij het interpreteren van het “Microsoft Office 365 and Azure BIR coverage report” zoals opgesteld door KPMG Advisory N.V.

Disclaimer

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

For the latest version of this document contact Martin Vliem, National Security Officer for Microsoft in The Netherlands, or Hans Bos, National Technology Officer for Microsoft in The Netherlands.

Introductie

Voordat u uw gegevens toevertrouwd aan de Microsoft Cloud, heeft u ongetwijfeld vragen. Wat Microsoft doet om uw gegevens te beschermen, hoe Microsoft aan regelgeving voldoet en hoe u kunt verifiëren dat Microsoft doet wat ze zegt.

Vertrouwen is de basis en voorwaarde voor het gebruik van informatietechnologie. Microsoft investeert internationaal in beveiliging en privacy maatregelen.

Over de Baseline Informatiebeveiliging Rijk

Adequate beveiliging van informatie is een voorwaarde vanuit onder meer de Wet Bescherming Persoonsgegevens (WBP). De Baseline Informatiebeveiliging Rijksdienst (BIR) geeft een normenkader voor informatiebeveiliging bij de Rijksdienst. Deze ‘baseline’ is sinds 2012 van kracht, en kan worden ingezet op een ‘comply or explain’ manier. De BIR ‘Operationele Handreiking’ stelt onder meer het volgende:

> *De normen en maatregelen in het BIR zijn gebaseerd op een niveau van vertrouwelijkheid, dat hoort bij de rubricering “Departementaal Vertrouwelijk” en het niveau WBP risicoklasse 2 verhoogd risico.*

Bij data met dit niveau van vertrouwelijkheid zal encryptie en sleutelmanagement zo geregeld moeten worden dat externe partijen (inclusief de leverancier van bijvoorbeeld een cloud) geen mogelijkheden hebben tot inzage van de data.
bron: BIR Operationele Handreiking

En het BIR Tactisch Normenkader (TNK) document schrijft:

De BIR is geheel gestructureerd volgens NEN/ISO 27001, bijlage A en NEN/ISO 27002. De overheid is verplicht om aan ISO 27001 en ISO 27002 te voldoen. Het college standaardisatie heeft deze voorschriften opgenomen in de lijst met verplichte standaarden voor de publieke sector, volgens het comply or explain principe. De BIR beschrijft de invulling van NEN/ISO27001 en 27002 voor de rijksoverheid. In de BIR zijn deze specifieke rijksnormen gemerkt met een [R]. NEN/ISO 27001 en 27002 beschrijven details voor implementatie (implementatierichtlijnen) en eisen voor de procesinrichting (o.a. het ISMS uit NEN/ISO 27001). Die documenten geven dus de details voor de toepassing, die niet in de BIR zijn beschreven en die nodig blijven voor een goede implementatie van de BIR.
bron: BIR Tactisch Normenkader (TNK) - titelpagina

De BIR beschrijft dat deze gebaseerd is op de ISO27001 en ISO27002. En dat (indien van toepassing) aan deze norm voldaan moet worden, inclusief een aantal aanvullende normen ('R-normen').

Meer informatie over de BIR en haar context is op internet beschikbaar.

- Beveiligingsvoorschrift Rijksdienst 2013 (BVR): http://wetten.overheid.nl/BWBR0033512/2013-06-01
- Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR): http://wetten.overheid.nl/BWBR0022141/2007-07-01
- Baseline Informatiebeveiliging Rijk (BIR): http://www.earonline.nl/index.php/Overzicht_Baseline_Informatiebeveiliging_Rijksdienst_(BIR_2012)
- Handreiking informatiebeveiliging: http://www.earonline.nl/images/earpub/5/5c/BIR_Operationele_Handreiking_v1_0.pdf
- Comply or explain procedure: http://www.earonline.nl/images/earpub/a/a9/04._A_BIR_explainprocedure_1.0_voor_ICCIO-1-.pdf
- Quickscan: http://www.earonline.nl/images/earpub/9/90/04._B_QuickScan_BIR_20140121_v10-1-.pdf

Het 'coverage report'

Het gebruik van ISO27001 en ISO27002 als basis voor de BIR zorgt ervoor dat de BIR aansluit bij internationale en marktontwikkelingen. Het 'coverage report' geeft aan waar de BIR normen aansluiten op de ISO certificeringen die beschikbaar zijn voor de Microsoft Online Services. Waar sprake is van aanvullende BIR normen wordt verwezen naar andere geverifieerde normen, contractuele waarborgen en/of documentatie. Op deze manier ondersteunt het 'coverage report' een overheid organisatie het onderbouwen van de 'comply' met de BIR, bij gebruik van Microsoft Online Services.

Er is gekozen voor een optimale aansluiting bij de wereld van de open en geaccepteerde standaarden, ISO 27001:2005 en ISO 27002:2007. Indien een organisatieonderdeel of een toeleverancier haar zaken op orde heeft volgens ISO 27001:2005, rekening houdend met de implementatiemaatregelen uit ISO 27002:2007, dan hoeft die organisatie slechts te controleren op de aanvullende bepalingen voor de rijksdienst. Die aanvullende bepalingen voor de Rijksdienst zijn in de BIR:2012 gemarkeerd met (R) zodat ze herkenbaar en apart toetsbaar zijn.
Bron: BIR Tactisch Normenkader (TNK) - 1.2. Aansluiting bij open standaarden

Microsoft kan een overheidsorganisatie verdere ondersteuning en medewerking verlenen ter verkrijging van een zogeheten 'in control' verklaring.

Veel gestelde vragen

V: Is Microsoft BIR gecertificeerd?
A: De Baseline Informatiebeveiliging Rijk (BIR) kan door (rijks)overheid worden gebruikt om te onderbouwen dat informatie op een veilige (vertrouwelijkheid, integriteit en beschikbaarheid) manier wordt verwerkt. Een overheidsinstelling kan aangeven dat ze Microsoft software en Microsoft

online diensten heeft ingericht en gebruikt om een manier die in overeenstemming is met de eisen in de BIR.
Microsoft is dan ook niet zelf BIR gecertificeerd. Het doel van het 'coverage report' is om te onderbouwen dat de beschikbare waarborgen en de functionele mogelijkheden van de Microsoft producten en diensten, een overheid organisatie in staat stellen deze te gebruiken op een manier die in overeenstemming is met de eisen in de BIR.

V: Voldoe ik als Microsoft Online Services gebruiker automatisch aan de BIR?
A: De Baseline Informatiebeveiliging Rijk (BIR) gaat over de inrichting en het praktische gebruik van informatie verwerkende voorzieningen. De Microsoft producten en online diensten voldoen aantoonbaar aan diverse (internationale) standaarden rond beveiliging. De overheidsinstelling kan die producten en online diensten vervolgens op een manier inrichten en gebruiken die aan de eisen uit de BIR voldoen. De operationele inrichting en het praktische gebruik is in handen van de overheidinstelling.

V: Het 'coverage report' toont geen 100% 'coverage' voor Microsoft online services, geeft dat aan dat volledige BIR 'compliance' onhaalbaar is?
A: De Microsoft Online Services bieden veel waarborgen rond veiligheid en bieden veel keuzemogelijkheden aan de gebruikende organisatie. Omdat de BIR (ook) gaat over het inrichten en gebruik van de online services, zal de overheid organisatie ook zelf een aantal keuzes moeten maken die aansluiten bij de BIR. Daarnaast zijn een beperkt aantal normen in de BIR niet direct te projecteren op moderne internationale normen of raamwerken. Daar kan het 'coverage report' voor die BIR normen geen 'coverage' bevestigen in die internationale normen. Microsoft geeft voor die situaties meer informatie over hoe aangesloten wordt of kan worden bij de BIR norm.

V: Is het 'coverage report' een juridisch document?
A: Het 'coverage report' is alleen beschrijvend ter ondersteuning van een discussie en proces richting de 'comply or explain' van een BIR 'in control' verklaring. Het 'coverage report' is geen juridisch bindend document.

V: Mag ik het 'coverage report' delen met anderen?
A: Zowel de BIR als de waarborgen en functionaliteit van de Micrsooft Online Services vallen onder de voorwaarden van een Non-Disclosure Agreement (NDA). Het 'coverage report' wordt beschikbaar gemaakt via de Microsoft Service Trust Portal (https://www.microsoft.com/en-us/TrustCenter/STP/default.aspx).
U kunt het document gebruiken voor uw eigen interne en externe audit, en als onderdeel van uw 'compliance' en risico management proces.