Ministerie van Justitie en Veiligheid

Cloud Security & Privacy Control Framework

Versie 1.2 15-12-2024

Ministerie van Justitie en Veiligheid

Inleiding

Beveiliging in Public Cloud-omgevingen vereist een andere beveiligingsbenadering in vergelijking met traditionele on-premise en Private Cloud-omgevingen. De belangrijkste redenen zijn dat het bedreigingslandschap voor de public cloud anders is, waarbij de public cloud nieuwe beveiligingsmogelijkheden biedt.
Het Cloud Security & Privacy Control Framework (in dit document verder benoemd als Cloud Control Framework of CCF) biedt een Raamwerk om deze beveiligingsbenadering te faciliteren.

Het Cloud Control Framework beschrijft het **WAT** van de security en privacy controls die moeten worden geïmplementeerd, **WANNEER** deze controls noodzakelijk zijn, en **HOE** deze controls moeten worden geïmplementeerd middels guidelines, waarbij vrijheid bestaat in de technische implementatie daarvan.

Controls in dit Framework richten zich op de Vertrouwelijkheid en Integriteit maatregelen en in beperktere mate op die voor Beschikbaarheid.

Gezien de gehanteerde begrippen rond cloud en beveiliging vaak Engelse naamgeving en woordgebruik kennen is de keuze gemaakt om het Raamwerk deels in het Engels op te stellen vanwege de leesbaarheid. Wij vragen uw begrip daarvoor. Er zullen echter ook enkele Nederlandstalige paragrafen in staan daar waar bijv. wordt gerefereerd aan de Algemene Verordening Gegevensbescherming (AVG) en de Baseline Informatiebeveiliging Overheid (BIO). De keuze is daar gemaakt om de Nederlandse beschrijving niet te vertalen naar het Engels.

Het Cloud Control Framework is een levend document, omdat de beschreven risico's en daarmee samenhangende beveiligingsmaatregelen kunnen wijzigen. Het Cloud Control Framework wordt om die reden jaarlijks geëvalueerd en zo nodig aangepast.

Versie

Versie	Auteurs	Datum	Wijzigingen	Status
1.0	Anabel Mocanu, Florens Vossen, Chris Eyzenga, Arjan Deij, Sander Dopmeijer, Remco Boersma	**20-04-2022**	**Intiele versie**	**Goedgekeurd door** - **ArchitectuurForum JenV** - **CTO-overleg** - **CISO-Board**
1.1	Ben de Haan , Inga van Doormalen, Remco Boersma	**21-07-2023**	**1ste Aanpassingen Privacy Board**	
1.1	Ben de Haan , Inga van Doormalen, Remco Boersma	**15-08-2023**	**2de Aanpassingen Privacy Board**	
1.2	Toevoeging Susanne Pronk Adviseur Servicecentrum Privacy en Veiligheid	**15-12-2024**	**Aanpasingen** Privacy hoofdstuk 7	**Goedgekeurd door** **Privacy-Board**

1. Inhoud

1. Cloud Control Framework

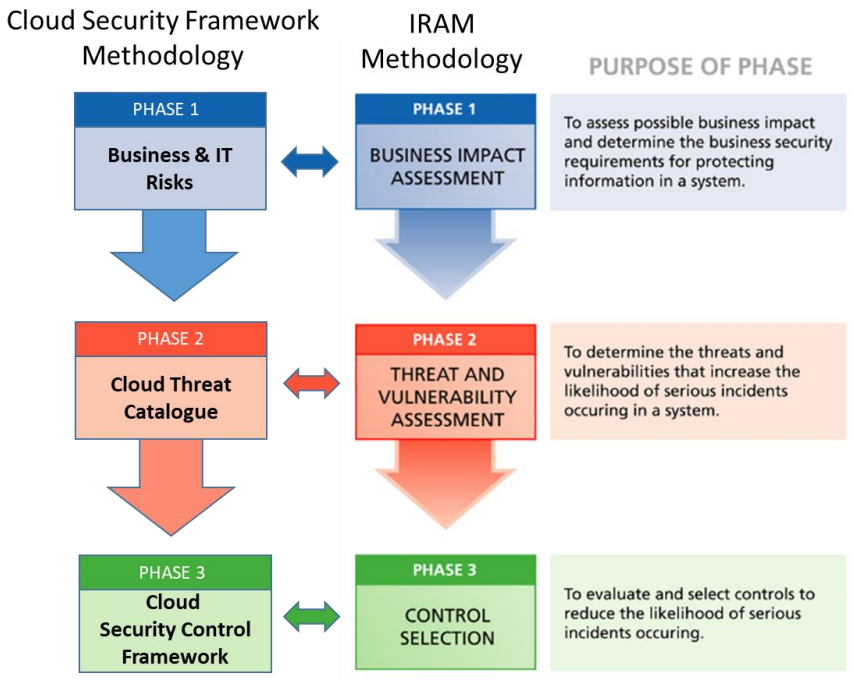
1.1 Doelstellingen

De Doelstellingen van het Cloud Control Framework (CCF) zijn:

- Om antwoord te geven op het ''Wat'' (controledoelstellingen), ''Waarom'' (dreigingen en risico's) en "Wanneer", zodat de focus kan worden gelegd op het "Hoe": het ontwerpen en implementeren van de controls op basis van de in het CCF onderkende risico's;
- Creëren van een 'Shift-left in beveiliging en privacy, waarmee wordt bedoeld om zo vroeg mogelijk in het ontwikkelproces en de implementatiefase rekening te houden met privacy en security maatregelen;
- Ondersteuning te leveren bij het implementeren van een 'security & privacy by design and default' benadering;
- Om duidelijkheid te creëren over wie verantwoordelijk is voor welke controls en ondersteuning te leveren middels implementatie richtlijnen:
- De basis te leveren voor zicht op naleving (compliancy) van de noodzakelijk controls;
- Het verbinden van de stappen, van dreigingen en risico's tot controle-implementatie en validatie daarvan. Deze end-to-end traceerbaarheid geeft vertrouwen in het vermogen om de JenV cloudplatforms te beschermen en te beveiligen.

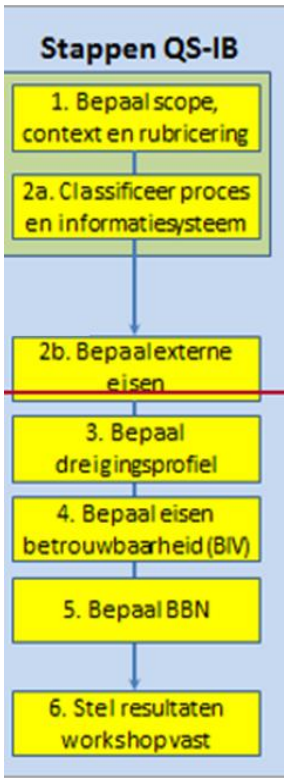
1.2 Cloud Control Framework (CCF) versus IRAM

Op de vraag hoe de methodiek van het Cloud Control Framework zich verhoudt tot de Information Risk Assessment Methodology (IRAM), is het antwoord dat de methodieken behoorlijk op elkaar lijken, zoals hieronder weergegeven.
Het CCF volgt dus de IRAM-benadering.



Het belangrijkste verschil zit in de eerste fase. Waar het Cloud Control Framework zich richt op algemene Cloud Business en IT-Risico's, begint de IRAM met een Business Impact Assessment die naast de meer algemene 'statische' business kwetsbaarheden ook de specifieke individuele Business kwetsbaarheden meeneemt.

1.3 Quick-Scan Informatie Beveiliging (QS-IB)



De Quick-Scan IB is bedoeld voor het bepalen van het Basis Beveiligings Niveau (BBN) alsmede de eventuele (rest)risico's die overblijven na beoordeling van de toegepaste maatregelen. Het Cloud Control Framework richt zich middels de Foundation-, Environment- en Standard controls zich op de controls die noodzakelijk zijn voor BBN2. De geavanceerde controls in het Cloud Control Framework gaan in op de controls die naast de Foundation- en Enviroment-controls ingezet kunnen worden voor BBN3.

1.4 Aanleiding

Met de inzet van Clouddiensten ontstaan relaties met externe, meestal particuliere IT-providers die afhankelijkheden veroorzaken. Dergelijke afhankelijkheden beperken de digitale soevereiniteit van JenV. De toenemende concentratie van IT-leveranciers op de markt zal dergelijke afhankelijkheden nog verder vergroten. Om die reden wordt ingezet op een JenV 'Trusted Cloud', waarbij eigen maatregelen in de publieke cloud deze soevereiniteit moeten beschermen en garanderen. Door inrichting van de cloud controls met inzet van de beveiligde JenV 'Trusted Cloud' in de publieke cloud zorgt ervoor dat de onafhankelijkheid, zelfbeschikking en beveiliging van JenV met inzet van de publieke clouddiensten kan worden vormgegeven. De implementatie van een JenV Trusted cloud bestaat uit de inzet van eigen controls in de publieke cloud op zowel het gebied van netwerkbeveiliging, identiteitscontrole, privacy bescherming als data-encryptie. In het JenV 'Trusted Cloud' concept worden de volgende aspecten centraal binnen JenV geregeld:

- De koppelingen met verschillende cloud providers ('multi cloud') zal worden ingericht als gemeenschappelijke dienst. Deze worden centraal gerealiseerd (via de internettoegangsdienst JUBIT), zodat onderdelen van JenV daar eenvoudig op kunnen aansluiten;
- Generieke infrastructuur beveiligingsmaatregelen conform BIO BBN2 zullen centraal worden aangebracht. Deze zijn in het CCF opgenomen als Foundation Controls;
- Onderdeel van de 'JenV Trusted Cloud' zijn centrale beveiligingsdiensten t.a.v. netwerk, toegang, monitoring;
- Inrichting van monitoring en logging is een federatief model op verschillende niveaus;
- Er is met Microsoft een Rijksbrede overkoepelende overeenkomst gesloten waardoor een deel van de Microsoft producten en diensten, te weten Office Pro Plus als ook Windows 10 Enterprise, in overeenstemming met de AVG gebruikt kunnen worden zoals in de kamerbrief van 1 juli 2019 gerapporteerd (MBSA). Recent (1 juni 2023) is de vergelijkbare overeenkomst met Amazon Web Services via SLM Rijk tot stand gekomen;
- Met andere Cloudleveranciers (o.a. Google) worden gelijksoortige overkoepelende overeenkomsten gesloten om zo te borgen dat die aanbieders de gegevens uitsluitend inzetten met de benodigde AVG waarborgen.

2. Dataclassificatie en betrouwbaarheidseisen

Om vast te stellen welke data in de publieke Cloud geplaatst kan/mag worden, moet inzichtelijk zijn over welke data de organisatie beschikt en welke betrouwbaarheidseisen daaraan worden gesteld. Deze betrouwbaarheidseisen kunnen op basis van een business impact assessment worden bepaald. Data moet daarom zijn geclassificeerd en gerubriceerd, zodat deze wordt voorzien van het juiste beveiligingsniveau. Hierbij zijn wet- en regelgeving en de betrouwbaarheidseisen die de organisatie aan deze gegevens stelt, een belangrijk uitgangspunt. Op basis van deze classificatie en rubricering moet de organisatie vaststellen, welke gegevens wel en welke niet in de Cloud geplaatst mogen worden.

2.1 Beschikbaarheid, integriteit en vertrouwelijkheid (classificatie)

Onder de betrouwbaarheidseisen worden beschikbaarheid, integriteit en vertrouwelijkheid verstaan, vaak afgekort met BIV. Op basis van de toegekende BIV-classificatie wordt vastgesteld of er voldoende adequate maatregelen genomen kunnen worden voor het plaatsen van de data in de Cloud. Om deze BIV-classificaties eenduidig te kunnen bepalen zijn de volgende drie belangrijkste wet- en regelgevingen van belang, die hieronder kort worden toegelicht:

1. Het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013), met betrekking tot vertrouwelijkheid van informatie binnen de Rijksoverheid
2. De Baseline informatiebeveiliging Overheid 2018 (BIO) De BIO beschrijft de invulling van de NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017 voor de overheid, maar vervangt deze normen niet..
3. De (Uitvoeringswet) Algemene verordening gegevensbescherming ((U)AVG) en de Richtlijn Gegevensbescherming Opsporing en Vervolging. De belangrijkste regels voor de omgang met persoonsgegevens zijn hierin vastgelegd, naast de sectorspecifieke wet- en regelgeving. De wetgeving om persoonsgegevens te beschermen schrijft in het kader van beveiliging, betrouwbaarheid, integriteit, beschikbaarheid en veerkracht voor.
   Hierbij geeft de UAVG uitvoering aan de Algemene Verordening Gegevensbescherming.

Het classificeren van gegevens conform BIV classificatie wordt bepaald door analyse van de kans dat onzorgvuldig of onrechtmatig gebruik zich voordoet en door de schade die daaruit voortvloeit. De uitkomst van die analyse bepaalt de risicoklasse en daarmee het vereiste niveau van maatregelen en procedures. Hogere klassen geven additionele normen aan die passen bij die hogere risicoklasse. De gegevensverantwoordelijke dient zorgvuldig af te wegen in welke risicoklasse de gegevens vallen.

Dit is een belangrijke notie bij het toepassen van de afweging welke data waar mag worden opgeslagen en verwerkt. Daarnaast zijn de volgende begrippen en de invulling daarvan van belang:

2.2 Betrouwbaarheid en betrouwbaarheidseisen

Betrouwbaarheid is de mate waarin een organisatie voor de informatievoorziening kan rekenen op een informatiesysteem. De betrouwbaarheid van een informatiesysteem is de verzamelterm voor drie aspecten van beveiliging die binnen het vakgebied informatiebeveiliging algemeen zijn geaccepteerd: beschikbaarheid, integriteit en vertrouwelijkheid. De betrouwbaarheidseisen geven weer aan welke eisen het informatiesysteem moet voldoen met betrekking tot deze drie aspecten.

Zonder zicht op de data die in de cloud wordt opgeslagen kunnen geen effectieve beheersmaatregelen worden getroffen om de data op een adequate en kostenefficiënte wijze te beschermen tegen onrechtmatig gebruik. Tevens dient bij de transitie naar de publieke cloud rekening te worden gehouden met contractuele en wettelijke vereisten. Zicht op het type data dat naar de cloud wordt verzonden is derhalve essentieel voor een optimale beveiliging van de data.

Aandachtspunt: Data is vaak (nog) niet conform de BIV criteria geclassificeerd, soms is niet duidelijk van welke classificaties sprake is.

Maatregelen: Data dient te worden geïnventariseerd en geclassificeerd.

Eisen vanuit de BIO (Baseline Informatiebeveiliging Overheid)

BIO 8.1.1 Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.

BIO 8.2.1 Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.

BIO 8.2.2 Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.

BIO 8.2.3 Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.

3. Control Classification

3.1 Introduction

The Cloud Control Framework prescribes security control objectives ("The What") to mitigate organizational and IT risks that are caused by cloud specific threats as described in the Threat Catalogue (Chapter 6). Mitigating controls must meet the risk appetite, the general level of risk a company accepts while pursuing its business objectives before it decides to take any action to reduce that risk (the organization's risk capacity), and risk tolerance, the aggregate degree of variance from that risk appetite that the organization is willing to tolerate, by raising the attacker cost to an acceptable risk level for expected attacks. Because organizational/IT risks and impact are dependent on the environment and data classification that is subject to threats, the security level that controls must provide will vary per environment and data classification.

For example: the required security level for a sandbox environment with anonymized data will require a lower security level and control objectives than a production environment that processes confidential data. To differentiate CCF control sets over environments and data classification, CCF controls are grouped in "Control Containers" by using control classification. Control classification prescribes "When" controls must be applied.

The CCF uses four types of control classifications (for graphical overview see next page):

- **Foundation control classification**
- **Environment control classification**
- **Data control classification which are categorized in Standard and Advanced**
- **Privacy control classification**

3.2 Foundation control classification

Foundation is a single classification that contains the security controls that apply to all environments, subscriptions and platform workloads/applications, regardless of their purpose or data classification of the data that is stored and processed. This means that Foundation Controls are fully fledged to provide the required security levels for even the most critical data classification.

3.3 Environment control classification

Because environment control classifications are used to define control sets that provide a distinct level of security per environment, two sub-classifications are defined:

Production & Non-Production controls

- All Development, Test, Acceptance and Production (DTAP) environments are considered as a single classification called PROD & NON-PROD
- From a security control perspective, no distinction is made between environments that are part of a production context. This is because threats apply to all stages of the development lifecycle and can exploit weaknesses of a less secured environment to propagate to other environments or conduct lateral movement.

Data control classification

Data control classification defines control sets that provide the required security level for single or multiple data classification levels, where Restricted Data requires a higher level of security and is subject to more strict security controls than for example Public Data. The data classification levels of JenV are distributed over two CCF control classifications, named **STANDARD** (Dep-V-BBN2) and **ADVANCED** (Dep-V-BBN3). Based on the data classification level, only one CCF control classification will apply, Standard (Dep-V-BBN2) control or Advanced (Dep-V-BBN3) control.

STANDARD controls must be applied on workloads and applications that store and process:

- Public Data (Openbaar)
- Internal Use Data (Bedrijfsvertrouwelijk)
- Confidential Data (Departementaal vertrouwelijk)

ADVANCED controls must be applied on workloads and applications that store and process:

- Restricted Data (Bijzondere informatie - Departementaal vertrouwelijk)

Examples

- A standard workload/application requires FOUNDATION Controls + ENVIRONMENT (PROD & NON-PROD) Controls + STANDARD Controls
- An advanced workload/application requires FOUNDATION Controls + ENVIRONMENT (PROD & NON-PROD) Controls + ADVANCED Controls

3.3 Privacy Control classification

The Privacy controls are the controls implemented based on performing a Data Protection Impact Assessment (DPIA) by the Business Owner depending on the data classification, the needed level of security and privacy restrictions.

Sandbox

- Sandbox environments are meant for incubation, exploring cloud capabilities, hackathons, proof of concept, and learning use cases only.
- Use of sandbox environments for development and test purposes in a production context, or even characteristics like resource naming or branding that can be traced back to the customer or one of its brands, is strictly prohibited.
- Sandbox environments have a short and hard limited lifecycle, and a minimal set of controls in order to support sandbox use cases.
- Sandbox environments are isolated from the other customer virtual private cloud networks and if needed isolated from on-premises network in that case only accessible from Internet.

Some aspects of Foundation controls may not be applicable or feasible for a Sandbox environment. If a Foundation control is not applied to its full extent on a Sandbox environment, the omission must be documented and approved. This to prevent multiple variants of the same control per environment.

Overview of controls - Cloud Security & Privacy Control Framework One Pager

The figure below shows the controls per layer of the Cloud Security & Privacy Control Framework.
The Foundation Controls (**F**) are implemented centrally as common controls and are obligatory
The Environment Controls (**E**) are also obligatory and need to be implemented by the responsible JenV Business representative
The Standard (**S**) and Advanced (**A**) Controls are depending on the type of workload (read, sort of system, application or data)
The Privacy Controls (**P**) are based on protection of personal data as a result of the DPIA.

<table>
<tr><th>Privacy</th><th>Standard (DEP-V BBN2)</th><th>Advanced (DEP-V BBN3)</th></tr>
<tr><td>P1: PRI 01 - DPIA
P4: PRI 04 - Pseudonymisation/Anonymisation</td><td>S1: IAM 05 - Secure Secret and Key Management
S2: IAM 06 - Identity Provider Protection
S3: IAM 07 - Identity Protection
S4: DATA 06 - JenV Managed Encryption Keys
S5: DATA 07 - Provider Managed Encryption Keys</td><td>A1: IAM 06 - Identity Provider Protection
A2: DATA 02 - Encryption of data in transit using virtual private networks
A3: DATA 04 - Encrypt data in use using Application-Level Encryption
A4: DATA 05 - Protect data in use using a Trusted Execution Environment (TEE)
A5: DATA 06 - JenV Managed Encryption Keys</td></tr>
<tr><th colspan="3">Environment (Prod & Non-Prod)</th></tr>
<tr><td colspan="2">E1: AUD 02 - Resource Auditing
E2: IAM 01 - Identity Access Management on all Resources
E3: IAM 02 - IAM on all Accounts
E4: IAM 03 - MFA on all User Accounts
E5: IAM 04 - Privileged Access Management
E6: DATA 01 - Encryption of data in transit using public networks
E7: DATA 03 - Encrypt data at rest</td><td>E8: NETW 04 - Outbound Connectivity from CSP Private Networks
E9: NETW 05 - Connectivity to and from CSP Public networks
E10: NETW 06 - Network Segmentation
E11: TVM 01 - Technical Vulnerability Management
E12: TVM 02 - Virus and Malware Protection
E13: TVM 03 - Threat Protection</td></tr>
<tr><th colspan="3">Foundation</th></tr>
<tr><td colspan="3">F1: NETW 01 - Internal Connectivity to and from CSP Private Networks
F2: NETW 02 - External connectivity to and from CSP Private Networks
F3: NETW 03 - Connectivity between Private and Public Endpoints
F4: PRI 02 - Contractering CSP
F5: PRI 03 - Waarborgen internationale doorgifte - Data processing in European Economic Area
F6: TVM02 - Virus and Maleware Protection
F7: AUD 01 - Platform Auditing</td></tr>
</table>

4. Control Responsibility & Accountability

4.1 Introduction

The Cloud Control Framework prescribes the security and privacy control objectives ("The What") to mitigate organizational, IT and privacy risks that are caused by cloud specific threats as described in the Security Threat Catalogue. The CCF controls are grouped in "Control Classifications". Besides that these classifications describe when the control must be applied, it also distinguish who is responsible for implementing the control and accountable for the implementation.

The CCF uses four types of control classifications:

- **Foundation controls**
- **Environment controls**
- **Data controls which are categorised in Standard and Advanced**
- **Privacy Controls**

4.2 Foundation controls

Responsibility
The Foundation controls are implemented on a generic level as part of the concept of the JenV Trusted Cloud. This is part of the service agreement of the JUBIT-service. These controls are obligatory for all JenV organizations using the Trusted Cloud concept. These control are implemented by the JUBIT service provider (Solvinity) under the responsiblity of DI&I. The Foundation Controls are implementated during the onboarding proces of the tenant of a specific JenV entity.

Accountability Although the foundation controls are implemented on a generic level, the business owner of an individual Azure Tentant is still capable to bypass or disable these Foundation Controls based on their digital sovereignty. So the Accountabilty to use and safeguard the implementation of these controls still resides by the Business.

4.3 Environment controls

Responsibility and **Accountability**
The Environment controls are being implemented on Azure Tenant level. Each Tenant has the obligation to implement these controls to be in line with the BIO (Baseline Informatiebeveiliging Overheid). The Responsibilty as well as the Accountability lies with the Business Owner. This accounts for the Sandbox controls as well as the Production & Non- Production controls.

4.4 Data controls

Responsibility and **Accountability**
The implementation of the Data based controls is a Responsibilty of the Business Owner. These controls are implemented based on a Risk Analysis performed by the Business Owner depending on the data classification and the needed level of security and privacy restrictions. Based on the classification standard controls are needed for Dep-V-BBN2 and advanced controls for Dep-V-BBN3.

4.5 Privacy controls

Responsibility and **Accountability**
The implementation of the Privacy controls is a Responsibilty of the Business Owner. These controls are implemented based on a Risk Analysis performed by the Business Owner depending on the data classification, the needed level of security and privacy restrictions.

5. Risk Register

The Cloud Control Framework focuses on general IT- and Organizational-Risks, the more general 'static' business vulnerabilities and not on specific individual Business vulnerabilities. In order to define control objectives, it must be clear how cloud native threats can lead to IT Risks and Business and Organizational Risks. The more general 'static' IT and Orgnanizationale Risks that are regonized are;

5.1 IT Risks

Loss or unauthorized access to personal identifiable information (PID)/ departementaal vertrouwelijke informatie
Tampering of system configuration
Loss of integrity of information
Unapproved / untested system configuration or functionality
Reduced or disruption of system availability
Untimely critical business process recovery

5.2 Organizational Risks

Reputational and/or financial damage
Loss of trust in government
Reduced ability to provide basic organizational services
Loss or unauthorized disclosure of confidential information
Disruption of service delivery (business continuity)
Data breaches containing user data
Attackers could compromise accounts and gain access to confidential information
Attackers could gain access to confidential information about internal operations
Loss of (sensitive) data
Data breaches containing PID

6. Threat Catalogue

6.1 Introduction

The control objectives in the Cloud Control Framework (CCF) are threat and risk based. These objectives are defined in such a way that the implementation of controls mitigate cloud native threats to establish the required security level that corresponds with the risk profile for a cloud-based workload. As a result, the residual risk must meet the risk appetite of JenV.

In order to define these control objectives, it must be clear how cloud native threats can lead to IT Risks and Business/Organizational Risks. For this purpose, the CCF contains a Security Threat Catalogue with cloud native threats which is the actual starting point for defining threat and risk based CCF control objectives.

Securing the JenV Trusted Cloud and JenV cloud workloads requires a cloud native approach for defining and implementing security controls due to the changing cloud threat landscape, and how cloud native threats lead to risks in cloud environments. The CCF Security Threat Catalog consists of cloud native threats that are applicable to cloud-based workloads and that are considered as information security threats. Therefore, CCF Threat Catalog is limited to threats (attack tactics and techniques) that are limited to public cloud environments only. Hence, threats that apply to resources that are beyond the perimeter and control boundary of public cloud infrastructure (such as on-premises systems or end-user devices) are out of scope of the CCF Threat Catalog.

The CCF Threat Catalog contains adversary tactics and techniques used by threat actors and is based on real-world observations. The CCF Threat Catalogue is based on two primary sources:

- The MITRE ATT&CK® knowledge base of adversary tactics and techniques. Because the CCF is targeted towards public cloud-based workloads only, the CCF Threat Catalogue specifically uses the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques
- The OWASP Top Ten Web Application Security Risk for web applications specific security threats

The CCF Threat Catalogue is not meant to provide a thorough analysis of threats or a comprehensive cloud native threat list. The goal is to have a consolidated list of threats that reflect the cloud native threat landscape on a global level to provide a basis for mapping IT Risk and Business Risk to threats and defining mitigating control objectives. This consolidated threat list is derived from practical CCF cases from customer environments across different industries and has been validated and tuned by the JenV Security Operations Center to make sure it reflects the threat landscape for JenV and the Public Sector Industry.

From a security and risk management perspective, all applicable tactics and techniques (not limited to the CCF consolidated Threat Catalogue) in MITRE ATT&CK® must be addressed when building a threat model to assess, design, and implement security controls. Use basic threat modeling techniques to identify applicable threats:

- Decompose the solution
- Understand the information flow between the different components
- Identify threat actors and map these to exposed components/attack surface and information flows
- Assess which threats in the CCF Threat Catalogue can be exploited by these threat actors, and complement these threats with applicable tactics and techniques in MITRE ATT&CK®
- Use these insights to define and interpret the CCF controls that are linked to these threats and how to design and implement these controls

6.2 Threats Overview

Threat 1 Compromised Accounts through Brute Force Attacks

Description

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Occasionally, large numbers of username and password pairs are dumped online when a website or service is compromised, and the user account credentials accessed. The information may be useful to an adversary attempting to compromise accounts by taking advantage of the tendency for users to use the same passwords across personal and business accounts. The information may be useful to an adversary attempting to compromise accounts by taking advantage of the tendency for users to use the same passwords across personal and business accounts.

Mitre Reference

Brute forcing passwords can take place via interaction with a service by using different sub-techniques such as password guessing, password cracking, password spraying, credential stuffing. As described in Brute Force, Technique T1110 - MITRE ATT&CK®

- Password Guessing
- Password Cracking
- Password Spraying
- Credential Stuffing

IT Risks

- Loss or unauthorized access to personal identifiable information/ departementaal vertrouwelijke informatie
- Tampering of system configuration
- Loss of integrity of information
- Reduced or disruption of system availability

Organizational Risks

- Reputational damage
- Loss of trust in government
- Reduced ability to provide basic organizational services

Threat 2 Security Misconfiguration resulting in Unauthorized Access and Subdomain Hijacking

can be linked with Adversaries obtain unauthorized access to data from improperly secured Cloud Storage Objects

Description

Attackers will often attempt to exploit unpatched flaws, default accounts, unprotected files and directories, and DNS entries that point to non-existent or deprovisioned resources, to gain unauthorized access or knowledge of the system, gain control over content, or abuse of authentic-looking subdomains for phishing campaigns.

Mitre Reference

A05 Security Misconfiguration - OWASP Top 10:2021. Subdomain hijacking is one of the frequent threats overserved that is caused by misconfiguration.

IT Risks

- Loss or unauthorized disclosure of confidential information
- Loss of integrity of information

Organizational Risks

- Financial and reputational damages
- Loss or unauthorized disclosure of confidential information

Threat 3 Exposed Cloud Service Dashboard

Description

An adversary may use a Cloud Service Provider (CSP) portal/dashboard GUI with stolen credentials to gain useful information from an operational cloud environment, such as specific services, resources, and features. For example, the CSP control plane can be used to view all assets, findings of potential security risks, and to run additional queries, such as finding public IP addresses and open ports (like AKS API). Depending on the configuration of the environment, an adversary may be able to enumerate more information via the graphical dashboard than an API. This allows the adversary to gain information without making any API requests.

Mitre Reference

This is a discovery tactic.

IT Risks

- Loss or unauthorized disclosure of confidential information
- The integrity of information is compromised
- Unapproved / untested system configuration or functionality
- Reduced or disruption of system availability

Organizational Risks

- Loss or unauthorized disclosure of confidential information
- Disruption of service delivery (business continuity)

Threat 4 Leaked Secrets through Source Code repository

Description

Malicious users can steal API keys, tokens, or any other form of credentials embedded in configuration files hosted on proprietary code that has been made public accidentally through public forks in source code repositories such as GitHub.

Mitre Reference

Adversaries may leverage code repositories to collect valuable information. Code repositories are tools/services that store source code and automate software builds. They may be hosted internally or privately on third party sites such as Github, GitLab, SourceForge and BitBucket. Users typically interact with code repositories through a web application or command-line utilities such as git.

Once adversaries gain access to a victim network or a private code repository, they may collect sensitive information such as proprietary source code or credentials contained within software's source code. Having access to software's source code may allow adversaries to develop Exploits, while credentials may provide access to additional resources using Valid Accounts.

IT Risks

- Loss or unauthorized disclosure of confidential information
- The integrity of information is compromised
- Unapproved / untested system configuration or functionality

Organizational Risks

- Reputational damages
- Loss or unauthorized disclosure of confidential information
- Data breaches containing user data

Threat 5 Account Compromise through Social Engineering

Description

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. Social engineering attacks happen in one or more steps.

Mitre Reference

Adversaries may compromise accounts with services that can be used during targeting. For operations incorporating social engineering, the utilization of an online persona may be important. Rather than creating and cultivating accounts (i.e. Establish Accounts), adversaries may compromise existing accounts. Utilizing an existing persona may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona. See Compromise Accounts, Technique T1586 - MITRE ATT&CK® for more information.

IT Risks

- Loss or unauthorized disclosure of confidential information
- The integrity of information is compromised
- Unapproved / untested system configuration or functionality

Organizational Risks

- Financial and reputational damages
- Attackers could compromise accounts and gain access to confidential information

Threat 6 Legitimate Privilege Abuse

Description

Adversaries may abuse legitimate privileged accounts or tokens for gaining higher-level permissions and unauthorized access.

Example: consider an internal healthcare application used to view individual patient records via a custom Web Application. The Web application user authorization model normally limits users to viewing an individual patient's healthcare history – multiple patient records cannot be viewed simultaneously, and electronic copies are not allowed. However, a rogue user might be able to circumvent these restrictions by connecting to the database using an alternative client such as MS-Excel. Using Excel and their legitimate login credentials, the user could retrieve and save all patient records to their laptop. Once patient records reach a client machine, the data then becomes susceptible to a wide variety of possible breach scenarios.

Mitre Reference

No direct reference however can be linked to Privilege Escalation

IT Risks

- Loss or unauthorized disclosure of confidential information
- The integrity of information is compromised

Organizational Risks

- Reputational damages
- Loss or unauthorized disclosure of confidential information

Threat 7 Account Discovery

Description

Adversaries may attempt to get a listing of accounts on a system or within an environment. This information can help adversaries determine which accounts exist to aid in follow-on behavior.

Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application.

Mitre Reference

This is a discovery tactic. Account Discovery: Cloud Account, Technique T1087.004 - MITRE ATT&CK®

IT Risks

- Loss of information confidentiality or disclosure of confidential information

Organizational Risks

- Reputational damages
- Loss or unauthorized disclosure of confidential information
- Data breaches
- Attackers could gain access to confidential information about internal operations

Threat 8 Compromised Application Tokens through Spear Phishing and Social Engineering

Description

Adversaries can steal user application access tokens as a means of acquiring credentials to access remote systems and resources. This can occur through social engineering and typically requires user action to grant access.

Mitre Reference

Within this tactic, adversaries have been seen targeting Gmail, Microsoft Outlook, and Yahoo Mail users.

IT Risks

- Loss or unauthorized disclosure of confidential information
- The integrity of information is compromised

Organizational Risks

- Loss of sensitive data
- Data breaches containing PID
- Reputational damages

Threat 9 Malware

Description

Software that performs a malicious task on a target device or network, e.g. corrupting data or taking over a system. This can include ransomware, or trusted, pre-installed system tools to spread malware.

Mitre Reference

Adversaries may develop malware and malware components that can be used during targeting. Building malicious software can include the development of payloads, droppers, post-compromise tools, backdoors (including backdoored images), packers, C2 protocols, and the creation of infected removable media. Adversaries may develop malware to support their operations, creating a means for maintaining control of remote machines, evading defenses, and executing post-compromise behaviors. See https://attack.mitre.org/datasources/DS0004/

IT Risks

- The integrity of information is compromised
- Reduced or disruption of system availability
- Untimely critical business process recovery

Organizational Risks

- Attackers could gain access to confidential information
- Data breaches containing user data
- Reputational damages

Threat 10 Man in the Browser

Description

Adversaries can take advantage of security vulnerabilities and inherent functionality in browser software to change content, modify behavior, and intercept information as part of various man in the browser techniques.

Mitre Reference

A specific example is when an adversary injects software into a browser that allows them to inherit cookies, HTTP sessions, and SSL client certificates of a user then use the browser as a way to pivot into an authenticated intranet. Executing browser-based behaviors such as pivoting may require specific process permissions, such as SeDebugPrivilege and/or high-integrity/administrator rights.

IT Risks

- Loss or unauthorized disclosure of confidential information or personal identifiable data
- (PID) The integrity of information is compromised
- Unapproved / untested system configuration or functionality

Organizational Risks

- Reputational damages
- Data breaches
- Access to confidential data

Threat 11 Endpoint Denial of Service

Description

Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources those services are hosted on or exploiting the system to cause a persistent crash condition. Example services include websites, email services, DNS, and web-based applications. Adversaries have been observed conducting DoS attacks for political purposes and to support other malicious activities, including distraction, hacktivism, and extortion.

Mitre Reference

Botnets are commonly used to conduct DDoS attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global internet. Adversaries may have the resources to build out and control their own botnet infrastructure or may rent time on an existing botnet to conduct an attack. In some of the worst cases for DDoS, so many systems are used to generate requests that each one only needs to send out a small amount of traffic to produce enough volume to exhaust the target's resources. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult. Botnets have been used in some of the most high-profile DDoS attacks, such as the 2012 series of incidents that targeted major US banks.

IT Risks

- Reduced or disruption of system availability

Organizational Risks

- Reputational damages
- Disruption of business operations

Threat 12 Network Sniffing (hybrid cloud)

Description

Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network or use span ports to capture a larger amount of data.

Cloud based network fabrics often abstract layer 2 network traffic and have protective measures in place like packet filters and anti-spoofing for DHCP and ARP. As this may mitigate traditional network sniffing techniques, adversaries must switch to cloud specific techniques like traffic mirroring services and manipulating routing tables to redirect and intercept traffic to compromised virtual machines.

Mitre Reference

Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol. Techniques for name service resolution poisoning, such as LLMNR/NBT-NS Poisoning and SMB Relay, can also be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary. Network sniffing may also reveal configuration details, such as running services, version numbers, and other network characteristics (e.g. IP addresses, hostnames, VLAN IDs) necessary for subsequent Lateral Movement and/or Defense Evasion activities.

IT Risks

- Loss or unauthorized disclosure of confidential information

Organizational Risks

- Reputational damages
- Attackers could gain access to confidential information about internal operations
- Data breaches containing user data

Threat 13 Lateral Movement

Description

Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network, conduct network reconnaissance to find other targets and subsequently gaining access to it. Adversaries might install their own remote access tools or malware to accomplish Lateral Movement, to compromise other targets and to elevate privileges.

Mitre Reference

Constitutes of (but not limited to) malware and elevation of privilege tactics.

For examples:

- A compromised application or virtual machine is abused to target other applications that are reachable in the same network segment
- A compromised application tier is abused to gain unauthorized access to a data tier

IT Risks

- Unapproved / untested system configuration or functionality
- Loss or unauthorized disclosure of confidential information

Organizational Risks

- Reputational damages
- Loss or unauthorized disclosure of confidential information

Threat 14 Unauthorized Access through Unsecured Credentials

Description

Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. Bash History), operating system or application-specific repositories (e.g. Credentials in Registry), or other specialized files/artifacts (e.g. Private Keys).

Mitre Reference

This is a credential access tactic.

IT Risks

- Loss or unauthorized disclosure of confidential information
- The integrity of information is compromised
- Unapproved / untested system configuration or functionality

Organizational Risks

- Reputational damages
- Loss or unauthorized disclosure of confidential- or personal identifiable data (PID)

Threat 15 Man in the Middle

Description

Adversaries may attempt to position themselves between two or more networked devices using a man-in-the-middle (MiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary-controlled system so they can collect information or perform additional actions.

Mitre Reference

Adversaries may leverage the MiTM position to attempt to modify traffic, such as in Transmitted Data Manipulation. Adversaries can also stop traffic from flowing to the appropriate destination, causing denial of service.

IT Risks

- Loss or unauthorized disclosure of confidential information
- The integrity of information is compromised
- Unapproved / untested system configuration or functionality

Organizational Risks

- Financial and reputational damages
- Data breaches
- Loss or unauthorized disclosure of confidential information

Threat 16 Forced Authentication

Description

Adversaries may gather credential material by invoking or forcing a user to automatically provide authentication information through a mechanism in which they can intercept. Example: The Server Message Block (SMB) protocol is commonly used in Windows networks for authentication and communication between systems for access to resources and file sharing. When a Windows system attempts to connect to an SMB resource it will automatically attempt to authenticate and send credential information for the current user to the remote system. This behavior is typical in enterprise environments so that users do not need to enter credentials to access network resources. Adversaries may take advantage of this behavior to gain access to user account hashes through forced SMB/Web Distributed Authoring and Versioning (WebDAV) authentication.

Mitre Reference

This falls under the credential access tactic.

IT Risks

- Unapproved / untested system configuration or functionality
- Disclosure of sensitive information
- Compromise the of integrity of data.

Organizational Risks

- Financial and reputational damages
- Attackers could gain access to confidential information about internal operations
- Data breaches containing sensitive or personal identifiable data

Threat 17 Software Discovery

Description

Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from Software Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Mitre Reference

Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable to Exploitation for Privilege Escalation.

IT Risks

- Tampering of system configuration
- Loss or unauthorized access to personal identifiable information/ departementaal vertrouwelijke informatie

Organizational Risks

- Financial and reputational damages
- Loss or unauthorized disclosure of confidential information
- Data breaches containing user data

Threat 18 Arbitrary Code Execution due to Vulnerable and Outdated Components

Description

Systems or components such as Virtual Machines, Containers, API's, Network Protocols and Encryption Algorithms that are used in component-heavy application development patterns might be vulnerable, unsupported, or out of date. Attackers can exploit these vulnerabilities for remote code execution vulnerabilities that enables execution of arbitrary code that could lead to compromised system.

Mitre Reference

Execution, Tactic TA0002 - Enterprise | MITRE ATT&CK® See OWASP Vulnerable and Outdated Components

IT Risks

- Loss or unauthorized disclosure of confidential information
- The integrity of information is compromised
- Reduced or disruption of system availability
- Unapproved / untested system configuration or functionality

Organizational Risks

- Reputational damages
- Loss or unauthorized disclosure of confidential information
- Disruption of service delivery (continuity)
- Untimely critical business process recovery

Threat 19 Network Denial of Service

Description

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes and to support other malicious activities, including distraction, hacktivism, and extortion.

Mitre Reference

To perform Network DoS attacks several aspects apply to multiple methods, including IP address spoofing, and botnets. Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. See https://attack.mitre.org/techniques/T1498/

IT Risks

- Reduced or disruption of system availability

Organizational Risks

- Reputational damages
- Disruption of business operations

Threat 20 Internal Network Threat

Description

Like external network threats, where adversaries may sniff network traffic to capture information about an environment, this risk/threat applies in a zerotrust environment as well on the internal network. Such as network sniffing using the network interface on a system to monitor or capture information sent over a wired or wireless connection. Or internal malicous person may place a network interface into promiscuous mode to passively access data in transit over the network or use span ports to capture a larger amount of data. Adversaries may attempt to position themselves between two or more networked devices using a man-in-the-middle (MiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary-controlled system so they can collect information or perform additional actions.

Mitre Reference 1

Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol. Techniques for name service resolution poisoning, such as LLMNR/NBT-NS Poisoning and SMB Relay, can also be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary. Network sniffing may also reveal configuration details, such as running services, version numbers, and other network characteristics (e.g. IP addresses, hostnames, VLAN IDs) necessary for subsequent Lateral Movement and/or Defense Evasion activities.

Mitre Reference 2

Adversaries may leverage the MiTM position to attempt to modify traffic, such as in Transmitted Data Manipulation. Adversaries can also stop traffic from flowing to the appropriate destination, causing denial of service.

IT Risks

- Loss or unauthorized disclosure of confidential information
- The integrity of information is compromised
- Unapproved / untested system configuration or functionality

Organizational Risks

- Reputational damages
- Attackers could gain access to confidential information about internal operations
- Data breaches containing user data

Threat 21 Compromised Privileged Accounts

Description

Attackers or malicious users getting access to privileged accounts such as Admins account credentials without good detection of these attacks after the fact. The attempt to compromise accounts by taking advantage of the tendency for users to use the same passwords across personal and business accounts.

Mitre Reference

Brute forcing passwords can take place via interaction with a service by using different sub-techniques such as password guessing, password cracking, password spraying, credential stuffing.

IT Risks

- Loss or unauthorized access to personal identifiable information/ departementaal vertrouwelijke informatie
- Tampering of system configuration
- Loss of integrity of information
- System availability

Organizational Risks

- Reputational damage
- Loss of trust in government
- Reduced ability to provide basic organizational services

Threat 22 Unauthorized Access to Data from Improperly Secured Cloud Storage Objects

Description

Misconfiguration and improperly secured cloud storage can lead to unauthorized data access and compromised data. This is typically caused by unintentionally allowing public access by unauthenticated users or overly broad access by all users. Adversaries may also obtain leaked credentials in source repositories, logs, or other means as a way to gain access to cloud storage objects that have access permission controls.

Mitre Reference

Data from Cloud Storage Object, Technique T1530 - Enterprise | MITRE ATT&CK®

IT Risks

- Loss of personal identifiable information/ departementaal vertrouwelijke informatie
- Loss of integrity of information

Organizational Risks

- Reputational damage
- Loss of trust in government

Threat 23 Data Exfiltration

Description

Adversaries may perform data exfiltration techniques to steal JenV data from CSP private networks. After the data has been collected, adversaries often package it to avoid detection while exfiltrating. Techniques for getting data out of a target network typically include transferring it over a command and control channel or an alternate channel and may also include putting size limits on the transmission.

Mitre Reference

Attack techniques to transfer data out Volvo Group managed cloud environments are described in Transfer Data to Cloud Account, Technique T1537 - Enterprise | MITRE ATT&CK®

IT Risks

- Loss of personal identifiable information/ departementaal vertrouwelijke informatie

Organizational Risks

- Reputational damage
- Loss of trust in government

7. Controls

This chapter describes the naming convention of the Security and Privacy Controls. The actual Controls within the CCF are explained and how these related to each other, and how they are being updated based on feedback and new insights.

7.1 Control Naming Convention

Control Naming Convention	Naming	Example
Auditing	AUD-xx	AUD-01-Resource Auditing
Data	DATA-xx	DATA-01-Encryption of data in transit using public networks
Identity & Access Management	IAM-xx	IAM-01-IAM on all Resources
Networking	NETW-xx	NETW-01-Internal Connectivity to and from CSP Private Networks
Privacy	PRI-xx	PRI-01-Data Processing in Europe
Threat Vulnerability Manangement	TVM-xx	TVM-01-Technical Vulnerability Management

7.2 Auditing Controls

De transitie naar de cloud heeft impact op de identificatie en het beheer van informatiebeveiligingsgebeurtenissen (incident response). Cloudproviders zijn huiverig met het delen van allerlei logbestanden en data, zeker wanneer deze gegevens bevatten van andere klanten. Het is daarnaast niet vanzelfsprekend dat wanneer zich een incident voordoet in de cloudomgeving van de cloudprovider dit incident (of een melding ervan) ook de weg zal vinden naar het Ministerie van Justitie en Veiligheid. Het verschilt per cloudprovider en per service model (IaaS, PaaS of SaaS) wat wel en niet mogelijk is. De migratie van applicaties en diens data naar de systemen van de cloudprovider leidt veelal tot (een gevoel van) verlies van controle en zicht op logdata. Aanvullende maatregelen dienen te worden getroffen om dit gat te dichten. Het is daarom van belang goed stil te staan bij de impact die de transitie naar de cloud heeft op logging en monitoring om vervolgens hierop in te spelen, bijvoorbeeld door aanvullende maatregelen te treffen in het huidige beleid omtrent logging en monitoring.

Maatregelen

- Aansluiting op JenV SIEM/SOC Tooling is noodzakelijk voor de incident en event monitoring.
- Het is aan te bevelen om duidelijke communicatiepaden met de cloudprovider op te zetten die in het geval van incidenten direct kunnen worden benut. Een duidelijke communicatie van verantwoordelijkheden en rollen is hierbij tevens essentieel.
- Het interne beheerproces omtrent incidenten behoort te worden aangepast om aansluiting te vinden met de aanpak van de cloudprovider.
- Er dienen duidelijke afspraken te worden gemaakt met de cloudprovider omtrent incidentbeheer. Deze afspraken dienen te worden vastgelegd in de Service Level Agreement en moeten betrekking hebben op alle fases van het incident response plan, te weten: detectie, analyse, beheersing, schoning, en herstel.
- Het is aan te raden om te onderzoeken in hoeverre reeds afspraken zijn gemaakt met desbetreffende cloudprovider omtrent incidentbeheer.

Eisen Baseline Informatiebeveiliging Overheid

- BIO 6.1.3 (BBN 2) Contact met overheidsinstanties. Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.
- BIO 12.4.1 (BBN 1) Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
- BIO 12.4.2 (BBN 1) Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
- BIO 12.4.3 (BBN 1) Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.
- BIO 12.4.4 (BBN 1) De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.
- BIO 16.1.1 (BBN 1) Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.
- BIO 16.1.2 (BBN 1) Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
- BIO 16.1.4 (BBN 1) Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.
- BIO 16.1.5 (BBN 1) Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
- BIO 16.1.7 (BBN 2) De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.

AUD 01 - Platform Auditing

Status	Concept
Control Classification	Foundation
Version	0.1
Owner Control Definition	DI&I
Owner	SOC JenV

Control Objectives

Platform Auditing provides insight into the operations that were performed on the control/management plane of the cloud platform to manage resources in CSP subscriptions.

Control Sub-Objectives

Sub- Control #	Sub-Control Description
AUD- 01-01	Provide audit logs to perform security monitoring and auditing on a platform level
AUD- 01-02	Audit logs must provide insight into: What operations were taken on resources; Who initiated the operation; When the operation occurred; The status/result of the operation; Values of other object properties that might help to research the operation (e.g. level of the event such as “Warning” or “Informational”)
AUD- 01-03	Audit logs must be protected from being tampered
AUD- 01-04	Access to audit logs must be must be restricted to only those individuals who are responsible for monitoring operations on the control/management plane
AUD- 01-05	Audit Logs must be retained online for a specified period

Link to Threat Catalogue

Threat ID
Threat 3: Exposed Cloud Service Dashboard
Threat 9: Malware
Threat 15: Man in the Middle
Threat 12: Network Sniffing

Implementation Guidelines

AUD-01-01

- Configure central audit log management using Azure Monitor
- Use Microsoft Defender for Cloud or equal functionality from other provider and Microsoft
- Sentinel or other/own SIEM-tooling to enable alerts and detect threats See Security logs and alerts using Azure services for further guidance

AUD-01-02 & AUD-01-03

- These capabilities are provided by the Microsoft Azure cloud platfom natively
- See Overview of Azure platform logs and Azure Active Directory reports for more information

AUD-01-04

- Access to audit logs must be based on the applicable roles and required permissions within JenV using access control
- See Roles, permissions, and security in Azure Monitor and Manage access to Log Analytics workspaces on how to manage these access permissions

AUD-01-05

- See Configure data retention and archive policies in Azure Monitor Logs to configure retention settings

AUD 02 - Resource Auditing

Status	Concept
Control Classification	Environment
Version	0.1
Owner Control Definition	DI&I
Owner	JenV Onderdeel

Control Objectives

The purpose of Resource Auditing is to collect, correlate and analyze security log data from cloud resources to detect security threats. Resource Audit Logs provide security insights into operations that were performed within cloud resources (data plane) such as:

- Sign-in activity and audit trail of changes made in CSP provided identity and directory services
- Data access to a PaaS based database
- Syslog and event log data that provide insight into security operations and security events within IaaS based Virtual Machines

Control Sub-Objectives

Sub- Control #	Sub-Control Description
AUD- 02-01	Resource audit logs must be protected from being tampered with
AUD- 02-02	Resource audit logs must be consolidated through connecting cloud services to centralized log spaces to enable analysis, correlation and alert logic of all resource logs together
AUD- 02-03	Resource audit logs must be retained for a specified period of time
AUD- 02-04	Access to resource audit logs must be restricted to only those individuals who are responsible for monitoring operations on the data plane

Link to Threat Catalogue

Threat ID
Threat 1: Compromised Accounts through Brute Force Attacks
Threat 3: Exposed Cloud Service Dashboard
Threat 5: Account Compromise through Social Engineering
Threat 6: Legitimate Privilege Abuse
Threat 9: Malware
Threat 13: Lateral Movement
Threat 17: Software Discovery
Threat 18: Arbitrary Code Execution due to Vulnerable and Outdated Components

Implementation Guidelines

AUD-02-02

- Use Azure resource logs to gain insight into operations that were performed within an Azure resource
- Use Azure Policies to enforce that resource logs are enforced for all deployed resources

AUD-02-01 & AUD-02-04

- Access to audit logs must be based on the applicable roles and required permissions within JenV using access control
- See Roles, permissions, and security in Azure Monitor and Manage access to Log Analytics workspaces on how to manage these access permissions

AUD-02-03

- See Configure data retention and archive policies in Azure Monitor Logs to configure retention settings

7.3 Data Controls

Dataversleuteling

Inherent aan het gebruik van een publieke cloudoplossing is het concept van multi-tenancy, waarbij middelen in de cloud zoals opslag en rekenkracht worden gedeeld door meerdere klanten van de cloudprovider. Om te voorkomen dat de klanten bij elkaars data kunnen komen, worden de verschillende klantomgevingen van elkaar gescheiden door middel van isolatie op de virtuele laag. Om het risico tot oneigenlijke toegang tot data te verkleinen is het noodzakelijk om data-at-rest te versleutelen en implementatie van daarbij horend sleutelbeheer (key-management).

Maatregelen

Een effectieve maatregel tegen misbruik van data in de cloud is dataversleuteling. Alvorens data wordt verzonden naar de cloud behoort deze in het meest optimale geval te worden versleuteld, waarbij de cryptografische sleutels ten behoeve van het versleutelen van de data in eigen beheer blijven (zie ook norm EKM-04 van de CSA Cloud Control Matrix).

Cloud leveranciers bieden diverse mogelijkheden zoals HSM protected vaults/key stores (FIPS 140-2 level 2) of dedicated vaults/key stores van dit type (FIPS 140-2 level 3). Tevens bieden Cloud leveranciers mogelijkheden voor BYOK (Bring-Your-Own-Key), BYOE (Bring-Your-Own-Encryption) of HYOK (Hold-your-Own-Key).

Sleutels in eigen beheer

Onder sleutels in eigen beheer en bij de cloud provider wordt verstaan, de sleutels waarover men zelf controle heeft (zelf kan creëren, verwijderen), die in FIPS 140-2 level 2 of hoger HSM of protected cloud vaults/key stores worden opgeslagen waarover men controle heeft. Welke we kunnen aanmaken/verwijderen in de cloud, toegangsrechten kunnen beheren, e.d.
Onder sleutels in eigen beheer vallen uiteraard ook sleutels in eigen on-premise vaults/key stores.

Sleutels niet in eigen beheer

Onder sleutels niet in het eigen beheer en opgeslagen bij de cloud provider worden verstaan alle standaard sleutels, gebruikt door de cloud provider en opgeslagen in cloud vaults/key stores waarover de afnemer geen controle heeft.

Wat het best passend is hangt af van de context en het BBN-niveau van het informatiesysteem en de risico-analyse (indien van toepassing). In generieke zin kan worden uitgegaan:

- BBN1 → een non-HSM backed key vault / key management dienst volstaat.
- BBN2 → een FIPS 140-2 level 2 HSM backed key vault / key management dienst volstaat.
- BBN3 → een dedicated FIPS 140-2 level 3 HSM backed key vault / key management dienst zou kunnen volstaan, BYOK of HYOK indien risicoanalyse dit noodzakelijk maakt.

Voor BBN1 volstaat het encrypten van data middels AES256 middels encryptie mechanisme van de cloudleverancier. Voor het niveau tot en met BBN2 mag gebruik worden gemaakt van Key Vaults die worden ondersteund middels een Cloud HSM (Hardware Security Module) voor de generatie en opslag van sleutels waarbij de beheersmaatregelen zijn opgenomen. Voor BBN3 dient een gerichte analyse van opslag van sleutels te worden onderzocht en afgewogen.

Eisen Baseline Informatie Beveiliging Overheid

- BIO 8.1.2 (BBN 1) Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben (zoals cryptografische sleutels).
- BIO 10.1.1 (BBN 2) Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd ter bescherming van ‘data in transit’ en ‘data at rest’.
- BIO 10.1.2 (BBN 1) Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.
- BIO 18.1.5 (BBN 1) Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving. Maatregelen Policies en procedures zijn aanwezig voor het cryptografische sleutel management, waaronder voor lifecycle management van sleutels, van generatie tot intrekking en vervanging. Gebruik van publieke sleutel infrastructuur, cryptografische protocollen en algoritmen (AES256), access control voor sleutel generatie en uitwisseling inclusief segregatie van sleutels ten behoeve van versleutelde data en sessies.

DATA 01 - Encryption of data in transit using public networks

Status	Concept
Control Classification	Environment
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

The purpose of encryption of data in transit is to protect data from being intercepted while data moves between on-premises and the CSP (Inter-Cloud Connectivity). This protection is achieved by encrypting the data before transmission, authenticating the endpoints and decrypting and verifying the data on arrival. For example, Transport Layer Security (TLS) is often used to encrypt data in transit for transport security, and Secure/Multipurpose Internet Mail Extensions (S/MIME) is used often for email message security. So control objective is to prevent that adversaries may sniff network traffic to capture data or information about an environment, including authentication material passed over the network. This Control objective is to prevent that adversaries may attempt to position themselves between two or more networked devices using a man-in-the-middle (MiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation.

This control relates to Advanced Control DATA-02 Encryption of data in transit using virtual private and public networks.
The following table shows this control compared to Standard and Advanced:

Control Sub-Objectives

Sub- Control #	Sub-Control Description
DATA- 01-01	**All data in transit using public connectivity such as Internet, and inter-cloud connectivity between CSP managed cloud networks and on-premises, must be encrypted. All data in transit using intra-cloud connectivity (within CSP network boundary) must be encrypted unless this is practically infeasible. The following scenarios classify as practically infeasible:**
	1. Traffic remains within the logical boundaries of the cloud resource type and the cloud resource type does not natively support encryption and requires additional 3rd party solutions that cause disproportional complexity, cost, or performance impact. E.g. implementing a Service Mesh specifically for node to node transit encryption within a Kubernetes Cluster
	2. Traffic remains within the logical boundaries of the cloud resource type and enabling resource type native encryption requires a complex deployment model or pricing plan that leads to cost explosion. E.g. encryption in transit between front-end and back-end nodes that belong to a single logical Cloud Application PaaS service
	3. The CSP private network hosts a legacy IaaS workload for which it is technically impossible to encrypt data in transit
	If the above scenarios do not apply and data in transit using intra-cloud connectivity is not encrypted, a request for an exemption must be submitted, and the exemption must be approved by a Security Officer
DATA- 01-02	**Ensure proper management and renewal of SSL certificates**

Link to Threat Catalogue

Threat ID	Justification
Threat 8: Compromised Application Tokens	**Expiring auth.tokens forces you to request new tokens**
Threat 12: Network Sniffing	

Threat 14: unauth. access through unsecured cred's	**Prevents leaking account details from HTTP headers**
Threat 15: Man in the Middle	
Threat 21: compromised Privileged Accounts	**Prevents leaking account details from HTTP headers**

Implementation Guidelines

- Data encryption in transit must ensure that data cannot be eavesdropped (sniffing/snooping) and intercepted (man-in-the-middle)
- Encryption must preferably be done on the Application and Presentation layers (HTTPS, TLS) instead of lower layers such as the Network layer (IPSec)
- Encryption protocols and certificate rotation must follow best security practices.
- Encryption is preferably done at the presentation layer level (HTTPS, TLS) rather than at the lower network level (such as IPsec).
- Cypher Suites compliant with TLS1.2 should be used

DATA 02 - Encryption of data in transit using virtual private networks

Status	Final
Control Classification	Advanced
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

The purpose of encryption of data in transit is to protect data from being intercepted while data moves within the network boundary of the CSP (Intra-Cloud Connectivity). This protection is achieved by encrypting the data before transmission, authenticating the endpoints and decrypting and verifying the data on arrival. So the control objective is to prevent that the CSP may sniff network traffic to capture data or information about an environment, including authentication material passed over the network. To prevent that adversaries may attempt to position themselves between two or more networked devices using a man-in-the-middle (MiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation.

This control relates to Standard Control DATA-01 Encryption of data in transit using public networks.

Control Sub-Objectives

Sub- Control #	Sub-Control Description
DATA- 02-01	All data in transit must be encrypted, regardless of the type of connectivity used: public (internet), inter-cloud (between CSP and on-premises) or intra-cloud (within CSP network boundary). This also applies to: peered virtual cloud networks, traffic between VM's (such as an application VM that connects to a database VM, even when these VMs are in the same subnet and virtual cloud network), node-to-node traffic between nodes that belong to a single logical Cloud PaaS instance or Kubernetes Cluster
DATA- 02-02	Ensure proper management and renewal of SSL certificates

Link to Threat Catalogue

Threat ID	Justification
Threat 12: Network Sniffing	
Threat 14: unauth. access through unsecured cred's)	Prevents leakage of account details from HTTP headers
Threat 15: Man in the Middle	

Implementation Guidelines

- Data encryption in transit must ensure that data cannot be eavesdropped (sniffing/snooping) and intercepted (man-in-the-middle)
- Encryption must preferably be done on the Application and Presentation layers (HTTPS, TLS) instead of lower layers such as the Network layer (IPSec)
- Encryption protocols and certificate rotation must follow best security practices.
- Encryption is preferably done at the presentation layer level (HTTPS, TLS) rather than at the lower network level (such as IPsec).
- Cypher Suites compliant with TLS1.2 should be used

DATA 03 - Encrypt data at rest

Status	Concept
Control Classification	Environment
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

Control objective is to prevent that data can be read by adversaries or own employees that have no need to known. By encrypting the data, the privacy, confidentiality and integrity of the data is protected. Or when the data is confiscated it can't be used or being interpreted. So to guard the confidentialty as well as the integrity of the data.

Control Sub-Objectives

Control	Classification	Data Classification	Data at rest	Storage Encryption	Application Level Encryption
DATA- 03	Standard	Public, Confidential, Internal use	Must be encrypted	Must be encrpyted	May be encrypted
DATA- 03	Advanced	Restricted	Must be encrypted	Must be encrypted	Must be encrypted

Sub- Control #	Sub-Control Description
DATA- 03-01	When data is encrypted by the application before it is transferred to a storage service the control objective is to protect against unauthorized access, even if someone has obtained access to the storage service or the file system used by the application for storing data

Link to Threat Catalogue

Threat ID	Justification
Threat 6: Legitimate Privilege Abuse	
Threat 14: Unauthorized Access through Unsecured Credentials	
Threat 22: Data from Cloud Storage Object	
Threat 23: Data Exfiltration	

Types of Encryption

https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview

Service Level Encryption

The CSP is responsible for encryption and key management (for example via Storage Service Encryption for Storage Accounts and Transparent Data Encryption for Azure SQL). This is independent of whether the service is running on a public endpoint or on a private endpoint or connectivity is limited by network controls.

Server Level Encryption

Encryption of data at rest on IaaS VM (virtual server) level where encryption is performed by the server operating system by encrypting the VHDs (virtual hard drives) that are attached to the virtual machine. Hence, protect data on a VHD level. **This type of encryption uses customer managed keys**. In case of Microsoft Azure, this type of encryption is called Azure Disk Encryption.

Application Level Encryption

Application-Level Encryption is the level of encryption that is provided by the application that is using storage services. Programmatically encrypt data in a JenV application before it is transported to and stored in cloud storage, and programmatically decrypt data after retrieving it from cloud storage. Hence, this also provides encryption of data in transit. **This type of encryption requires customer managed keys**. Application Level Encryption is the most secure level of encryption but requires programmatic changes to applications. It also impacts scalability (load on application level) and data integration scenarios with cloud native data services.

Implementation Guidelines

Data encryption at rest is the default, this can be achieved at various levels. The implementation depends on whether the data regards a cloud service or an own application, as well as the desired level of risk.

- Data at rest is encrypted at private endpoint level - application or server level (Virtual Machine), hereby JenV is responsible for encryption and key management.
- Storage encryption: data at rest is protected by storage layer encryption. This means, encryption at the disk or database level. This protects against attackers trying to steal files, records, or disk drives.

DATA 04 - Encrypt data in use using Application Level Encryption

Status	Concept
Control Classification	Advanced
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

Application-Level Encryption is the level of encryption that is provided by the application that is using storage services. Regardless of the type of storage service, data is programmatically encrypted in the JenV application before it is transported to and stored in storage services, and programmatically decrypted after retrieving data from storage services. Application-Level Encryption is the most secure level of encryption but requires programmatic changes to applications and requires customer managed keys. It also impacts scalability (load on application level) and data integration scenarios with cloud native data services.
https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview

Control Sub-Objectives

Sub- Control #	Sub-Control Description
DATA- 04-01	To prevent unauthorized access to data on physical storage devices (disks/spindles, SSD) and logical access to data on storage level and data in use must be encrypted on application level

Link to Threat Catalogue

Data at rest on disks that is subject to Application Level Encryption is automatically encrypted and decrypted when it enters and leaves the storage service. Given that, Service Level Encryption provides protection against someone gaining access to the physical hardware hosting the data. Mitigating these physical disk access and disk walkout attack vectors is the sole responsibility of the CSP. Therefore, the Threat Catalogue does not contain a threat description that applies to these attack vectors. However, Application Level Encryption will help to meet advanced organizational security and compliance commitments.

Threat ID	Justification
Threat 10: Man-in-the-Browser	The application encrypts its traffic itself (separately), this does not happen at an earlier, possibly compromised phase.
Threat 12: Network sniffing	The encryption in the isolated TEE-environment makes the data and its handling less sensitive for compromizing
Threat 14: unauth. access through unsecured cred's	The encryption by the application makes it less sensitive to access to keys by hacked accounts.
Threat 15: Man-in-the-Middle	The application encrypts its traffic itself (separately), this does not happen at an earlier, possibly compromised phase.

Implementation Guidelines

JenV departments can encrypt data in use, taking advantage of security technology offered by modern CPUs (carrying the Secure Encrypted Virtualization extension) together with confidential computing cloud services. This increases confidence that data will stay private and encrypted even while being processed.

As data-in-use encryption comes with higher costs, much impact, its usage is advised mainly for applications which are highly secret, or applications where no encryption is possible other than Data-in-Use encryption. Access to data by (malicious) administrators and privileged software (such as hypervisors) is restricted by placing the data and application code together in an 'enclave', separated from the host. For data-in use, according to the CAF, you're required to maintain data ownership separate from the underlying cloud platform at all times, even at the RAM and CPU level.

DATA 05 - Protect data in use using a Trusted Execution Environment (TEE)

Status	Concept
Control Classification	Advanced
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

To protect data which is stored and processed unencrypted in a non-persistent digital state like computer random-access memory (RAM), CPU caches, or CPU registers, unencrypted data must be processed in an isolated execution environment.

A Trusted Execution Environment (TEE) is an environment for executing code with a high level of trust that provides a higher level of security for trusted applications. TEE provides the following security capabilities:

- Mitigates data access by cloud operators, malicious admins, and privileged software such as the hypervisor
- Data access is fully in the control of JenV regardless of whether in rest, transit, or use (even though the infrastructure is not)
- JenV code running in the cloud is protected and verifiable by JenV
- Data and code are not readable to the CSP when inside the Trusted Computing Base (TCB)

Control Sub-Objectives

Sub-Control #	Sub-Control Description
DATA-06-01	Code and data must be stored in and isolated and trusted execution environment
DATA-06-02	Decrypted code and data must only be exposed to an environment that is approved by the data owner

Link to Threat Catalogue

The use of this Advanced Control must be assessed on a per workload basis. Every Advanced Workload must undergo a threat model and security assessment to determine which attack vectors aim to be mitigated with TEE. If all data-in-use computation desires to have added defense in depth with TEE, then the components processing the data by the CSP should be running on confidential infrastructure. There are other considerations to assess what is in the Trusted Computing Base (TCB) of a solution, typically with trade-offs of usability and cost in order to have more control and confidentiality.

The Trusted Execution Environment (aka Confidential computing) protects a.o. against

Threat ID	Justification
Threat 10: Man in the Browser	The application encrpts its data itself (separately), encryption (e.g. in-flight) isn't taking place in an earlier, possible compromise phase
Threat 15: Man in the Middle	The application encrpts its data itself (separately), encryption (e.g. in-flight) isn't taking place in an earlier, possible compromise phase

Threat actors

- Malicious privileged admins or insiders
- Hackers exploiting bugs in the Hypervisor/OS of cloud fabric
- Third parties accessing data without customer consent

For the implementation of this control, this basic threat modeling can be used to assess whether these threat actors are applicable for a specific advanced workload or not.

Implementation Guidelines

JenV departments can encrypt data in use, taking advantage of security technology offered by modern CPUs (carrying the Secure Encrypted Virtualization extension) together with confidential computing cloud services. Access to data by (malicious) administrators and privileged software (such as hypervisors) is restricted by placing the data and application code together in an 'enclave', separated from the host. For data-in use, according to the CAF, you're required to maintain data ownership separate from the underlying cloud platform at all times, even at the RAM and CPU level.

A Confidential VM is a type of Compute Engine VM that ensures that your data and applications stay private and encrypted even while in use. You can use a Confidential VM as part of your security strategy so you do not expose sensitive data or workloads during processing. At the moment of writing (August 2022), only four types of VMs support TEE, providing the strong, hardware-enforced boundary. Also O/S support is limited.

Preparation starts at https://docs.microsoft.com/en-us/azure/confidential-computing/confidential-vm-overview

DATA 06 - JenV Managed Encryption Keys

Status	Concept
Control Classification	Advanced
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

Secure key management is essential for generating, protecting and managing encryption keys that are used to encrypt data at rest as specified in DATA-03-Encrypt data at rest using Application Level Encryption and DATA-04-Encrypt data at rest using Service Level Encryption .

With Managed Keys, Min. J&V has full and granular control over usage and management of encryption keys. Cloud Foundation teams and Platform/Application Teams are responsible for managing the lifecycle of encryption keys that are used for encryption of data at rest.

Control Sub-Objectives

Sub- Control #	Sub-Control Description
DATA- 05-01	Use the procedure that is built-in into the Storage/Database service to generate and store encryption keys
DATA- 05-02	For storage, usage, rotation and access control of encryption keys, the same Control Sub-Objectives apply as described on IAM-04-Secure Secret and Key Management

Link to Threat Catalogue

Threat ID	Justification
Threat 06: Legitimate Privilege Abuse	
Threat 22: Data from Cloud Storage Object	
Threat 23: Data Exfiltration	

Implementation Guidelines

Rather than using Azure provided keys, using JenV generated keys further protects data. These keys can be stored in a standard Key Vault, in an Azure provided HSM or even in a JenV owned HSM. Decide how much protection is needed and at which costs (billing and management).

References: https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview
https://docs.microsoft.com/en-us/azure/key-vault/keys/byok-specification

In the Europese Aanbesteding (EA) JUBIT3 the following criteria are asked for the implementation of HSM (Hardware Security Module). The scope of this HSM is also extended into the cloud. The link to the presentation gives insight in the requirements asked for Cloud HSM's HSM.pptx

DATA 07 - Provider Managed Encryption Keys

Status	Concept
Control Classification	Standard
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

Secure Secret and Key Management entails encrypted and secured storage of secrets & keys, management of secrets & keys, access control to secrets & keys, and logging and monitoring the use of secrets & keys in order to protect and control access.

Secrets are used to provide authentication and authorization to resources and data. Examples of secrets are: passwords, API keys, access keys/tokens, authentication certificates.

Keys are encryption keys that are used to encrypt data at rest as defined in DATA-03 Encrypt data at rest and DATA-04 Encrypt data in use using Application Level Encryption. Furthermore the working of the HSM is described in FIPS 140-2 Level 1/2/3.

Control Sub-Objectives

Sub- Control #	Sub-Control Description
DATA-07-01	Ensure that all secrets are encrypted and stored in a secured and protected vault. If secrets can be automatically created, secured and managed by the CSP, and are not exposed or used by Cloud Foundation teams or Application Platform teams, it is not applicable to store and secure these secrets in Min. J&V's vaults
DATA-07-02	Ensure that access to secrets and access granted through secrets follow IAM-04 Privileged Access Management and are bound to a specific use case, service or application
DATA-07-03	Establish rotation of secrets on a regular basis. The secret expiration date is based on the risk profile of the application and the level of exposure of secrets. The Platform Security Officer will provide advice and guidance on how to determine the secret expiration period/date.
DATA-07-04	Ensure that access to the vaults (control plane) and access to the secrets stored in a vault (data plane) are governed through Access Control Lists.
DATA-07-05	Ensure that access to the vaults (control plane) and access to the secrets stored in a vault (data plane) are logged and monitored to detect suspicious and abnormal access patterns

Link to Threat Catalogue

Threat ID	Justification
Threat 1: Compromised Accounts through Brute Force Attacks	The threats (mentioned in this table) which are mitigated by encryption are also valid for this control objective. Our reasoning is that if the keys are not protected well the encryption is not working well and the threats is nt mitigated.
Threat 4: Leaked Secrets through Source Code Repository	

Threat 7: Account discovery	
Threat 8: Compromised Application Tokens through Spear Phishing and Social Engineering	
Threat 9: Malware	
Threat 12: Network Sniffing	
Threat 13: Lateral Movement	
Threat 14: Unauthorized Access through Unsecured Credentials	
Threat 16: Forced Authentication	
Threat 20: Internal Network threat	
Threat 21: Compromised Priveledged Accounts	

Implementation Guidelines

- It is not allowed to store secrets in (source) code, configuration files, templates, and connection stings
- Secrets must not be shared among multiple systems or application instances, as compromising one instance would endanger the whole service
- Secrets must be used to tightly control access
- Dedicated HSM must be used instead of Azure Key Vault protected through a secure mechanism provided by the cloud service provider (CSP) for advanced workloads

7.4 Identity & Access Management Controls

Bij de inzet van Cloud Producten worden eisen gesteld, waarbij sprake is van een risicoafweging voor de inzet van onderstaande maatregelen. Voor die gevallen waarbij sprake is van betrouwbaarheidsniveau DepV BBN2 en/of persoonsgegevens zijn onderstaande eisen van toepassing. Voor lagere rubricering is dit sterk gewenst maar kunnen uitzonderingen middels een 'explain' worden toegepast.

1. Identiteiten 'ontstaan' in de interne JenV omgeving (eigen on-prem AD) en worden gefedereerd/gesynchroniseerd met de betreffende Cloud- leverancier. Dit betekent dat als een medewerker uit dienst gaat en daarmee zijn identiteit verdwijnt uit de interne AD, deze ook verdwijnt t.b.v. de Cloud-toepassing en daarmee toegang wordt geblokkeerd.
2. Gebuik van 2-factor authenticatie is verplicht. Het betrouwbaarheidsniveau van identiteit en authenticatiemiddel is conform het JenV-Trustframework, passend bij de voorziening en bepaald op basis van een risicoafweging.
3. Data welke wordt gebruikt door de SAAS-toepassing is altijd versleuteld zowel in Rest als in Transit.
4. Er wordt een analyse uitgevoerd welke AD-attributen noodzakelijk zijn om te worden gefedereerd met de Cloud-aanbieder.
5. Er wordt gebruik gemaakt van een CASB (Cloud Access Security Broker). Logging daarvan wordt beschikbaar gesteld en ook auditing daarop is mogelijk.

Aandachtspunt

De exploitatie van verschillende cloudplatformen en cloudproviders leidt op den duur tot een versnippering van accounts en het beheer ervan, hetgeen de accountbeveiliging niet ten goede komt. Elk platform kent dan zijn eigen set aan accounts, accountinstellingen en beveiligingseisen, die op hun beurt kunnen afwijken van het organisatiebrede beveiligingsbeleid.

Aansluiting op JenV Toegangs-landschap is essentieel in het kader van toekomstvastheid en hergebruik toegangsmanagement en toegangsgebruik voorzieningen, processen en controls.

Eisen Baseline Informatiebeveiliging Overheid

De JenV Identiteiten en het beheer zijn leidend voor de Cloudidentiteit. Dat betekent dat de user identiteit en toegangsrechten binnen JenV worden gecreëerd en worden gefedereerd/gesynchroniseerd naar de cloud.

- BIO 9.1.1 (BBN 1) Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.
- BIO 9.1.2 (BBN 1) Gebruikers behoren alleen toegang te krijgen tot de (netwerk)diensten waarvoor zij specifiek bevoegd zijn.
- BIO 9.2.1 (BBN 1) Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
- BIO 9.2.3 (BBN 1) Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.
- BIO 9.2.4 (BBN 1) Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces, bijvoorbeeld middelen ten behoeve van multi-factor authenticatie.
- BIO 9.2.5 (BBN 1) Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
- BIO 9.4.2 (BBN 1) Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.
- BIO 9.4.3 (BBN 1) Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.

IAM 01 - Identity Access Management on all Resources

Status	Concept
Control Classification	Environment
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

To ensure that legitimate parties have the right access to the right resources at the right time essential to perform its intended function while keeping unauthorized parties out of systems.

Access to resources include:

- Deploying and managing resources through the CSP (Cloud Solution Provider) resource manager (control plane)
- Access to data within cloud resources like PaaS databases and IaaS VMs (data plane)
- Access to applications (SaaS) that leverage cloud services

Control Sub-Objectives

Sub- Control #	Sub-Control Description
IAM- 01-01	Ensure the identity of legitimate parties with Min. JenV's identity provider before granted access to resources
IAM- 01-02	Establish a central Authentication/Authorization service to resources
IAM- 01-03	Ensure the removal of access as soon as access is no longer required or changed, for example for an employee leaving the company
IAM- 01-04	Manage and control the access to resources (IaaS, PaaS) and to applications that are registered with the CSP in a way that they align with established protocols and technology used and applied by Min. J&V
IAM- 01-05	Ensure that access to Azure resources and applications that are registered with the Azure AD as the Identity Provider are assigned to Resource Security Groups adhering to the principle of least privilege
IAM- 01-06	Ensure that users do not have standing or unneeded permissions by auditing and reviewing assignments of access permissions to Resource Security Groups on a regular basis
IAM- 01-07	Ensure that RBAC (Role Based Access Control) with an attribute ABAC (Attribute Based Access Control) is implemented on the control and data plane for each cloud service
IAM- 01-08	Admit only owned non-personal accounts for system authentication

Link to Threat Catalogue

Threat ID	Justification
Threat 2: Security Misconfiguration resulting in Unauthorized Access and Subdomain Hijacking	
Threat 13: Lateral Movement	
Threat 14: Unauthorized Access through Unsecured Credentials	
Threat 17: Software Discovery	
Threat 20: Internal Network Threat	

Implementation Guidelines

- When granting permissions, use the principle of least privilege
- Comply with various regulatory requirements for identification, suspicious activity and identity theft prevention
- RBAC must be deployed on the control plane of each cloud service
- RBAC must be deployed on the data plane of each cloud service Access to a cloud resource is always based on an attribute (e.g. based on group membership)
- Non-Personal accounts know an owner and are only allowed for system (process) authentication
- IAM must comply with the established protocols, processes and technology used and applied by Min. J&V, See "domein architectuur Toegang"

IAM 02 - IAM on all Accounts

Status	Concept
Control Classification	Environment
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

Ensure that management / system owner identify users or systems and grant access based on their role.

Control Sub-Objectives

Sub- Control #	Sub-Control Description
IAM- 02-01	Ensure that all personal accounts are based on JenV identities supplied via the generic IAM service of JenV.
IAM- 02-02	Ensure that based on the risks accounts of citizens only granted access via Digi-D or E-herkenningsmiddelen or similar
IAM- 02-03	Establish management of user accounts and of role groups populated by sets of users with similar roles in the organization are delivered and managed by the the generic IAM service of JenV.
IAM- 02-04	Ensure that modifications on accounts and groups are logged and monitored and deviations are documented and approved by an management or system owner
IAM- 02-05	Ensure that designated managers in the organization can perform a periodic review / evaluation of the permissions
IAM- 02-06	Ensure that application specific non-personal/service accounts are provisioned upon the request of an application owner and the ownership of these accounts as part of the provisioning procedure.
IAM- 02-07	Ensure that the use of non-personal accounts (NPA) is restricted to service to service authentication and break-glass accounts.
IAM- 02-08	Ensure that privileged non-personal accounts are used by e.g., a VM scanning agent, are unique per VM instance and must not have access to other VM instances
IAM- 02-09	Setup monitoring system that allows identification or presence of accounts, expired accounts or accounts that should be disabled (e.g default accounts)
IAM- 02-10	Ensure that break-glass accounts can be used in case of emergencies with or without the generic IAM service of JenV
IAM- 02-11	Establish a federated services for JenV organisations and external partners

Link to Threat Catalogue

Threat ID	Justification
Threat 5: Account Compromise through Social Engineering	
Threat 13: Lateral Movement	

Threat 14: Unauthorized Access through Unsecured Credentials	
Threat 20: Internal network threats	
Threat 23: Data Exfiltration	**indirectly mitigated**

Implementation Guidelines

- Access is based on the need to know / need to have principle and adhere to the rules of segregation of duties
- Accounts are based on JenV supplied identities
- Non-personal accounts must not be shared among multiple services
- Accounts for non-JenV identities (partners, customers) are given access via Digi-D or E-herkenning or similar, or via B2B and B2C options.
- Accounts and groups are provided and managed by the JenV managed IAM system
- Modifications on accounts and groups are logged and checked.
- Permissions are based on minimum necessary permissions.
- Permissions are regularly reviewed, at least with role change and reassignment.
- Temporary 'higher' permissions are allowed for only a certain period of time.
- Break glass accounts are implemented outside the scope of IAM in case of calamities
- Use of separate/local accounts must be avoided
- IAM integrations should be coordinated with Min. JenV's IAM team

IAM 03 - MFA on all User Accounts

Status	Concept
Control Classification	Environment
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

De publieke cloud biedt brede netwerktoegang via het internet tot de data die zijn opgeslagen in de cloud en verschillende beheerportalen waarmee de cloudomgeving kan worden geconfigureerd. De toegang hiertoe is doorgaans beveiligd met accounts en wachtwoorden. Door de brede netwerktoegang dienen er aanvullende beveiligingsmaatregelen te worden getroffen om de cloudaccounts (die toegang geven tot de cloud) te beschermen tegen misbruik.

Maatregelen

Het is noodzakelijk om vanaf DEP-V informatie gebruik te maken van een vorm van multi-factor authenticatie ter versterking van de beveiligingsmaatregelen rondom toegang tot de cloud, onafhankelijk van de BIO BBN-score van het informatiesysteem. Pas hier het data afwegingskader toe voor vaststelling van gewenst authenicatie niveau (EIDAS laag, substantieel of hoog) en de gewenste vorm van MFA (SMS, Token, PKI). De huidige Trusted cloud hanteert per default 2FA op het niveau substantieel.

Control Objectives

Ensure that Multi Factor Authentication (MFA) with a token is used during the authentication process to grant access to cloud resources or cloud related functionality. The used factor is based on the JenV Trust framework (EIDAS: low, Substantial and High)

Control Sub-Objectives

Sub- Control #	Sub-Control Description
IAM-03-01	Ensure that MFA is used for all privilegd and non-privileged user accounts, irrespective of device, device ownership or network location
IAM-03-02	Ensure that external partners or citizens use MFA via DigiD or E-herkenningsmiddelen or similar
IAM-03-03	Ensure that MFA is used to authenticate access to both the cloud control plane and the cloud data plane
IAM-03-04	Ensure a break-glass emergency procedure to enable authentication when MFA is not possible due to service disruption
IAM-03-05	Ensure that (risk based) additional security measures if MFA can not be used

Link to Threat Catalogue

Threat ID	Justification
Threat 1: Compromised Accounts through Brute Force Attacks	
Threat 3: Exposed Cloud Service Dashboard	
Threat 5: Account Compromise through Social Engineering	

Threat 9: Malware	
Threat 13: Lateral Movement	
Threat 14: Unauthorized Access through Unsecured Credentials	
Threat 20: Internal network threats	

Implementation Guidelines

- Multi Factor Authentication (MFA) is mandatory for all own user Accounts
- MFA must comply with the established protocols, processes and technology used and applied by Min. J&V's IAM MFA.
- The determination of the MFA asset is derived from the JenV Trust Framework (EIDAS; Low, Substantial, High)
- Accounts for non-JenV identities (partners, customers) use the MFA means from the DigiD or E-herkenning or possibly iDIN and similar.
- Protect against compromise of a single authentication factor and provide defense in depth by leveraging multiple authentication factors.
- For non-interactive authentication processes such as non-personal accounts for service-to-service authentication, other measures must be in place to secure the authentication mechanism.
- Access to cloud resources (management/development) or functionality realized in the cloud is required multi-factor, preferably attribute or claim based and conditional.
- Additional security measures are necessary if MFA cannot be used (eg password validity, monitoring).

IAM 04 - Privileged Access Management

Status	Concept
Control Classification	Environment
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

Privileged Access Management (PAM) refers to the process and technology that is used to provide secured privileged access. This entails not only securing, monitoring and managing privileged identities (PIM), but also the end-to-end access path from device to interface, including intermediary components such as jump servers, PIM/PAM solutions and connectivity. Privileged Access Management must provide a holistic solution that protects against multiple attacker entry points. Access to any interface making it possible to modify and/or circumvent security controls or access controls are considered as privileged access.

Examples of interfaces and privileged access:

- Cloud management portal (cloud control plane), allowing to modify the components deployed
- Remote desktop or secure shell of virtual machines, allowing to modify the security posture of the virtual machine
- The privileged service connection to the cloud control plane of a CI/CD environment

Control Sub-Objectives

Sub- Control #	Sub-Control Description
IAM- 04-01	Activity Monitoring must be applied on privileged access, for example by implementing central session recording or by using logging mechanisms combined with *just in time* access mechanism and/or *dual control* access mechanisms
IAM- 04-02	It must be possible to provide audit history reports for internal and external audits. For the retention of audit history, the retention time described in AUD-01-03 applies
IAM- 04-03	It must be possible to relate (trace back) all privileged actions (commands/changes) to an individual
IAM- 04-04	An approval workflow must be in place to manage privileged access to cloud resources; the responsible manager should be aware which authorizations (s)he provides when (s)he consents a workflow
IAM- 04-05	All administrative Tier-0 activities must be performed by dedicated administrative accounts. Designated security groups/user accounts that have top-level privileges assigned must have break-glass authentication procedures
IAM- 04-06	Separate and limit highly privileged/administrative users
IAM- 04-07	Avoid standing access for user accounts and permissions
IAM- 04-08	Manage lifecycle of identities and entitlements
IAM- 04-09	Review and reconcile user access regularly
IAM- 04-10	Set up emergency access
IAM- 04-11	Use privileged access workstations
IAM- 04-12	Follow just enough administration (least privilege) principle
IAM- 04-13	Determine access process for cloud provider support

Link to Threat Catalogue

Threat ID	Justification
Threat 2: Security Misconfiguration resulting in Unauthorized Access and Subdomain Hijacking	**indirectly mitigated by sub-objective 04- 04**
Threat 5: Account Compromise through Social Engineering	
Threat 13: Lateral Movement	
Threat 21: Compromised Priveledge Accounts	

Implementation Guidelines

Adhere to the applicable control objectives in the CCF controls listed below:

- IAM-01 IAM on all Resources following the IAM of the relevant JenV-organization
- IAM-02 IAM on all Accounts following the IAM of the relevant JenV-organization
- Privileged access to interfaces must adhere to IAM-03 MFA on all User Accounts following the IAM of the relevant JenV-organization
- Privileged approval process and assignments must be managed or delegated through established the IAM processes of the relevant JenV-organization .
- The attack surface of interfaces providing Privileged Access must be minimized, for instance by blocking direct access from EUC networks and/or by JIT NSGs (just-in-time enabled network Security Groups).
- Intermediaries add a link to the chain of Zero Trust assurance for the privileged access path and must sustain (or improve) the Zero Trust security assurances in the access path
- Intermediaries such jump servers or session managers must provide an isolated virtual zone where privileged identities can operate in with low risk
- Primary access layer of jump servers must be hardened to protect against zero-day exploits

IAM 05 - Secure Secret and Key Management

Status	Concept
Control Classification	Standard
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

Secure Secret and Key Management entails encrypted and secured storage of secrets & keys, management of secrets & keys, access control to secrets & keys, and logging and monitoring the use of secrets & keys in order to protect and control access.

Secrets are used to provide authentication and authorization to resources and data. Examples of secrets are: passwords, API keys, access keys/tokens, authentication certificates.

Keys are encryption keys that are used to encrypt data at rest as defined in DATA-03 Encrypt data at rest using Application-Level Encryption and DATA-04 Encrypt data at rest using Service Level Encryption. Furthermore the working of the HSM is described in FIPS 140-2 Level 1/2/3.

Control Sub-Objectives

Sub- Control #	Sub-Control Description
IAM- 05-01	Ensure that all secrets are encrypted and stored in a secured and protected vault. If secrets can be automatically created, secured and managed by the CSP, and are not exposed or used by Cloud Foundation teams or Application Platform teams, it is not applicable to store and secure these secrets in Min. J&V's vaults
IAM- 05-02	Ensure that access to secrets and access granted through secrets follow IAM-04 Privileged Access Management and are bound to a specific use case, service or application
IAM- 05-03	Establish rotation of secrets on a regular basis. The secret expiration date is based on the risk profile of the application and the level of exposure of secrets. The Platform Security Officer will provide advice and guidance on how to determine the secret expiration period/date.
IAM- 05-04	Ensure that access to the vaults (control plane) and access to the secrets stored in a vault (data plane) are governed through Access Control Lists.
IAM- 05-05	Ensure that access to the vaults (control plane) and access to the secrets stored in a vault (data plane) are logged and monitored to detect suspicious and abnormal access patterns

Link to Threat Catalogue

Threat ID	Justification
Threat 1: Compromised Accounts through Brute Force Attacks	The threats (mentioned in this table) which are mitigated by encryption are also valid for this control objective. Our reasoning is that if the keys are not protected well the encryption is not working well and the threats is nt mitigated.

Threat 4: Leaked Secrets through Source Code Repository	
Threat 7: Account discovery	
Threat 8: Compromised Application Tokens through Spear Phishing and Social Engineering	
Threat 9: Malware	
Threat 12: Network Sniffing	
SThreat 13: Lateral Movement	
Threat 14: Unauthorized Access through Unsecured Credentials	
Threat 16: Forced Authentication	
Threat 20: Internal Network threat	
Threat 21: Compromised Priveledged Accounts	
Threat 22: Data from Cloud Storage Object	

Implementation Guidelines

- It is not allowed to store secrets in (source) code, configuration files, templates, and connection stings
- Secrets must not be shared among multiple systems or application instances, as compromising one instance would endanger the whole service
- Secrets must be used to tightly control access
- Vault must be protected through a secure mechanism provided by the cloud service provider (CSP)

IAM 06 - Identity Provider Protection

Status	Concept
Control Classification	Advanced
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

Protect personal accounts and non-personal accounts/service accounts that are provided by a non-CSP managed Identity Providers such as Microsoft Active Directory Service (ADS) or other Identity Providers or services that are deployed on non-CSP managed IaaS. Identity Provider Protection is used to protect against compromise of credentials through detecting brute force attacks, failed authentications, user group membership changes, and other anomalies that indicate suspicious activities and events.

Control Sub-Objectives

Sub-Control #	Sub-Control Description
IAM-06-01	Identify, detect and investigate advanced threats, compromised identities, and malicious insider actions
IAM-06-02	Monitor account usage, entity behavior and activities with learning-based and behavioral baseline analytics
IAM-06-03	Identify and investigate suspicious account activities and advanced attacks throughout the kill chain
IAM-06-04	Detect malicious attempts to compromise identities, move laterally and gain persistency

Link to Threat Catalogue

Threat ID	Justification
Threat 1: Compromised Accounts through Brute Force Attacks	
Threat 5: Account Compromise through Social Engineering	
Threat 7: Account Discovery	
Threat 8: Compromised Application Tokens through Spear Phishing and Social Engineering	
Threat 13: Lateral Movement	
Threat 14: Unauthorized Access through Unsecured Credentials	

Implementation Guidelines

- IAM-06-01,
- IAM-06-02,
- IAM-06-03,
- IAM-06-04

- Implement Microsoft Defender for Identity to protect Microsoft Active Directory Service (ADS) domain controllers.
- Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions.

IAM 07 - Identity Protection

Status	Concept
Control Classification	Standard
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

Protect personal accounts and non-personal accounts/service principals/identities by automatically analyzing daily signals to identify and protect against threats. Improve the security of accounts by leveraging contextual information (device, location etc.) to determine the risk level of the session.

Control Sub-Objectives

Sub- Control #	Sub-Control Description
IAM- 07-01	Detect account sign-ins from: atypical locations based on the account recent-sign-ins, anonymous IP address from platforms such as Tor or/and Anonymizer VPN's, accounts with unfamiliar sign-in properties which have not be given to the account and are suddenly used, malware linked IP address (e.g., Command and Control identified Domain), excessive number of failed login attempts, and deprecated accounts in the subscription
IAM- 07-02	Detect account Password Spray attacks
IAM- 07-03	Detect user's valid credentials that have been leaked outside the organization
IAM- 07-04	Detect the use of break glass accounts as described in IAM-02-IAM on all accounts, following Min. J&V's IAM and integrate detection with Security Management & SIEM solution
IAM- 07-05	Manage application identities securely and automatically. (Use managed application identities instead of creating human accounts for applications to access resources and execute code. Managed application identities provide benefits such as reducing the exposure of credentials. Automate the rotation of credential to ensure the security of the identities.)
IAM- 07-06	Authenticate server and services. (Authenticate remote servers and services from your client side to ensure you are connecting to trusted server and services. The most common server authentication protocol is Transport Layer Security (TLS), where the client-side (often a browser or client device) verifies the server by verifying the server's certificate was issued by a trusted certificate authority.
IAM- 07-07	Use single sign-on (SSO) for application access, to simplify the user experience for authenticating to resources including applications and data across cloud services and on-premises environments.
IAM- 07-08	Use strong authentication controls (strong passwordless authentication or multi-factor authentication) with your centralized identity and authentication management system for all access to resources. Authentication based on password credentials alone is considered legacy, as it is insecure and does not stand up to popular attack methods.
IAM- 07-09	Restrict resource access based on conditions (explicitly validate trusted signals to allow or deny user access to resources, as part of a zero-trust access model). Signals to validate should include strong authentication of user account, behavioral analytics of user account, device trustworthiness, user or group membership, locations and so on. Conditional access policies in place to evaluate sign-in/user risk during the authentication procedure.

IAM- 07-10	Restrict the exposure of credential and secrets: ensure that application developers securely handle credentials and secrets by (1) avoidance of embedding the credentials and secrets into the code and configuration files; (2) the use of a key vault or a secure key store service to store the credentials and secrets; (3) scanning for credentials in source code.
IAM- 07-11	Secure user access to existing applications. In a hybrid environment, where you have on-premises applications or non- native cloud applications using legacy authentication, consider solutions such as cloud access security broker (CASB), application proxy, single sign-on (SSO) to govern the access to these applications for the following benefits: (1) enforce a centralized strong authentication; (2) monitor and control risky end-user activities; (3) monitor and remediate risky legacy applications activities; (4) detect and prevent sensitive data transmission

Link to Threat Catalogue

Threat ID	Justification
Threat 1: Compromised Accounts through Brute Force Attacks	
Threat 3: Exposed Cloud Service Dashboard	
Threat 5: Account Compromise through Social Engineering	
Threat 8: Compromised Application Tokens through Spear Phishing and Social Engineering	
Threat 9: Malware	
Threat 13: Lateral Movement	
Threat 14: Unauthorized Access through Unsecured Credentials	

Implementation Guidelines

IAM-07-01, IAM-07-02, IAM-07-03

- Implement Azure Active Directory Identity Protection to identify and address identity risk

IAM-07-04

- Leverage Microsoft Sentinel User and Entity Behavior Analytics (UEBA) to identify anomalous activity

IAM-07-05

- Use Azure Managed identities to provide automatically managed identity in Azure Active Directory for applications when connecting to resources that support Azure Active Directory (Azure AD) authentication
- See Managed Identities for Azure resources for more information

7.5 Network Controls

NETW 01 - Internal Connectivity to and from CSP Private Networks

Status	Concept
Control Classification	Foundation
Version	0.1
Owner Control Definition	DI&I
Owner	DI&I - Solvinity

Control Objectives

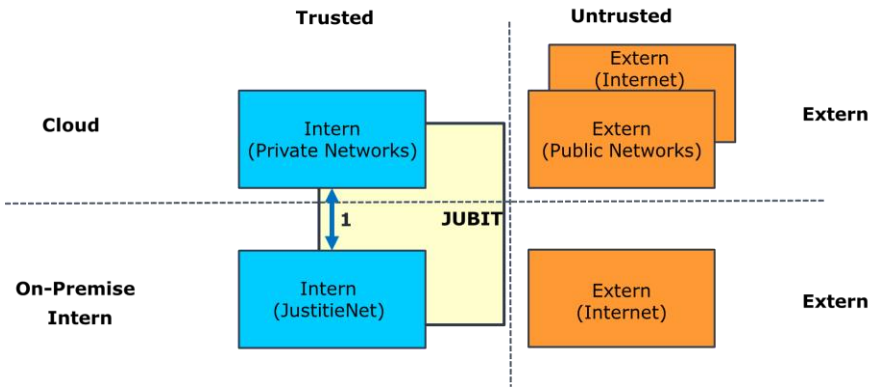
To prevent that internal network traffic between Justitienet and the CSP private networks is routed incorrectly or unwanted traffic over the internal network bypassing the implementations of the JenV Trusted Cloud Controls.

Control Sub-Objectives

Sub- Control #	Sub-Control Description
NETW- 01-01	Control inbound/outbound connectivity by using techniques like layer 3 network access control list; hostname whitelisting; TCP/UDP port filtering and ICMP filtering.
NETW- 01-02	Network polices and connectivity controls must be based on least possible connectivity and must be maintained/reviewed periodically
NETW- 01-03	Inbound and outbound traffic must be logged (meta data)

Link to Threat Catalogue

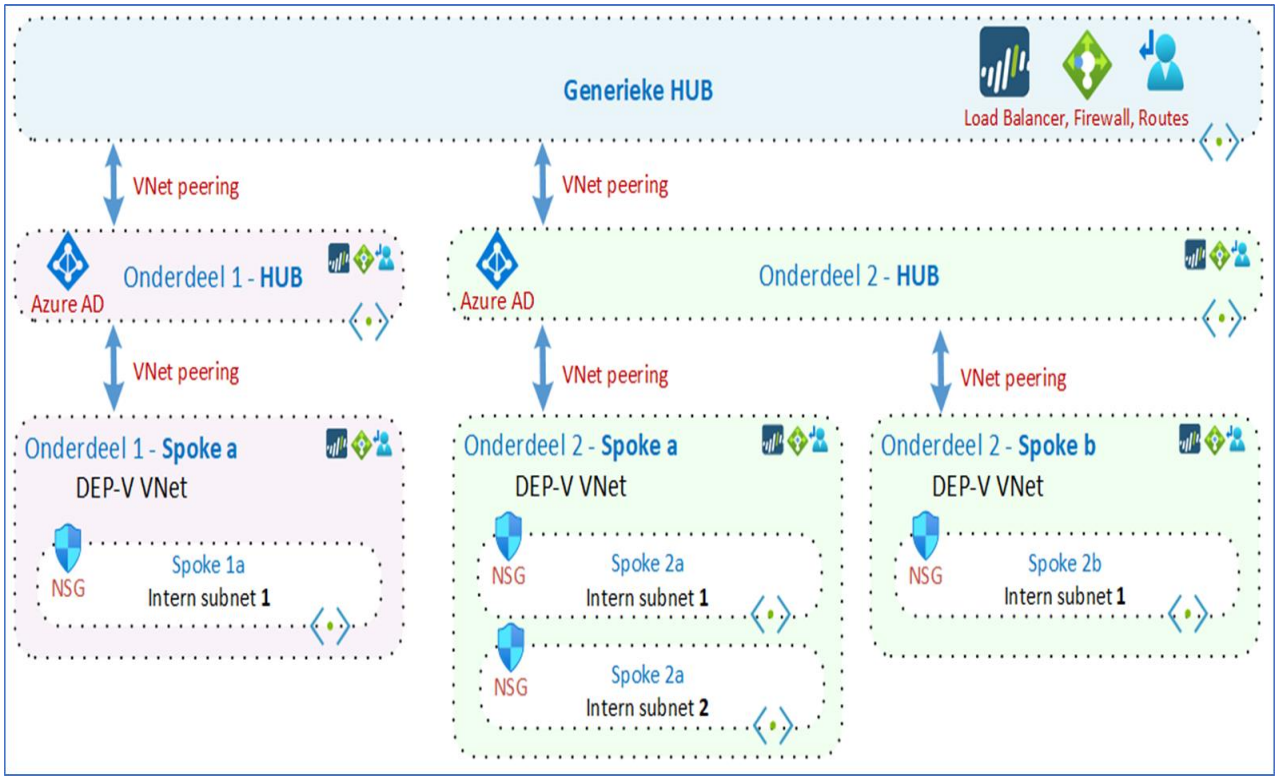
Threat ID	Justification
Threat 20: Internal network threats	
Threat 22: Data from Cloud Storage Object	assuming zero-trust principle
Threat 23: Data Exfiltration	assuming zero-trust principle



Implementation Guidelines

- Private Virtual Networks have a peering relationship with the sector hub where connectivity between Cloud VNET's is required to the internal Justitie network.
- Virtual Networks have a peering relationship with the hub where connectivity between Cloud VNET's is required.
- Traffic to and from the JenV Trusted Cloud is routed over the Cloudinterconnect (Express Route) to and from the internal Justitie network.
- Traffic to and from the JenV Trusted Cloud to and from the internal Justitie network runs through the secure interface Palo Alto Firewall (at least Layer 3 protection) within the Cloud tenant of 'het JenV Onderdeel', whereby the application is provided with appropriate IP addresses within the JenV-IP numbering plan.
- Private Virtual Networks are controlled by 'het JenV onderdeel' and host IAAS resources such as VM's and PAAS services which are VNET-integrated.
- Inspection is preferably at layer 7 specific application level (behavioural inspection).
- Private Virtual Networks are controlled by JenV and host IAAS resources such as VM's and PAAS/SAAS services which are VNET-integrated.

For the above protection, routing to the Private networks to on-premise is enforced over the Express Route and Hub-spoke model provided under the JUBIT service.



NETW 02 - External connectivity to and from CSP Private Networks

Status	Concept
Control Classification	Foundation
Version	0.1
Owner Control Definition	DI&I
Owner	DI&I - Solvinity

Control Objectives

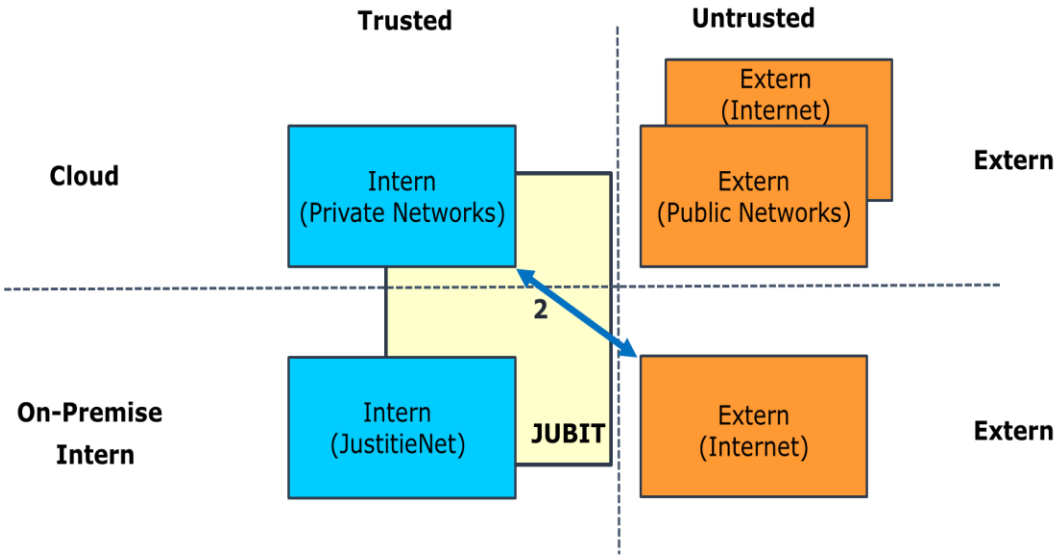
To prevent that external network traffic to the CSP private networks is routed incorrectly or unwanted traffic over bypassing the implementations of the JenV Trusted Cloud Controls. To prevent that Adversaries may sniff network traffic to capture data or information about an environment, including authentication material passed over the network. To prevent that adversaries may attempt to position themselves between two or more networked devices using a man-in-the-middle (MiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation.

CSP Private networks are virtual private cloud networks that are controlled by Min. J&V and host IaaS resources such as VMs and injected PaaS/SAAS services.

Inbound and outbound traffic from (source):

- Internet
- or other external networks including other CSP's (inter-cloud connectivity)

to CSP Private networks must be controlled and secured to protect IaaS/PaaS resources and IaaS/Paas based applications. The level of control depends on the source of the traffic and related security impact.



Control Sub-Objectives

Sub- Control #	Sub-Control Description
NETW- 02-01	Network interfaces in the private networks must have a private IP address (RFC1918) and not have a public IP address by default
NETW- 02-02	'All' inbound traffic must be logged

NETW- 02-03	'All' outbound traffic must be logged
NETW- 02-04	Web based applications running in CSP Private networks must be published through secured protocols (HTTPS over TLS1.2 or according the latest NIST standards)
NETW- 02-05	It must be possible to detect attacks using signatures, network behavior analysis, or other mechanisms to analyse traffic
NETW- 02-06	Web based applications running in CSP Private networks must be secured by a layer 3 network access control list in combination with SSL/TLS termination and inspection
NETW- 02-07	Use threat intelligence-based filtering to alert and deny traffic from known malicious IP addresses and domains
NETW- 02-08	All services, applications and API's published towards internet must be protected against Endpoint DDoS attacks or Layer 7 DDoS attacks (Botnet attacks)
NETW- 02-09	It must be possible to inspect encrypted traffic (SSL/TLS termination) to detect data leakage, data exfiltration, or malicious traffic. SSL/TLS termination might not be applicable for every workload, e.g., when breaking the SSL/TLS end-to-end trust between host and destination is not desirable or not allowed
NETW- 02-10	Control inbound connectivity by using techniques like FQDN whitelisting or layer 3 network access control list when FQDN whitelisting is not feasible; hostname whitelisting; TCP/UDP port filtering and ICMP filtering; threat intel based or reputation based filtering
NETW- 02-11	Inbound network polices and connectivity controls must be based on least possible connectivity and must be maintained/reviewed periodically

Link to Threat Catalogue

Threat ID	Justification
Threat 9: Malware	
Threat 11: Endpoint Denial of Service	
Threat 12: Network Sniffing	
SThreat 13: Lateral Movement	
Threat 15: Man-in-the-Middle	
Threat 19: Network Denial of Service	

Implementation Guidelines

- Private Virtual Networks have a peering relationship with the hub where connectivity between Cloud VNET's is required.
- Traffic to and from the JenV Trusted Cloud is routed over the Cloudinterconnect (Express Route) to the internal Justitie network.
- Traffic to and from the JenV Trusted Cloud and External networks (internet e.a.) runs via dedicated JenV cloud connections, via the secure interface (preferable via a Layer 7 Firewall) within Jubit, where the application is provided with IP-addresses appropriate within the JenV IP-numbering plan.
- Virtual Private Networks are controlled by JenV and host IAAS resources such as VM's and PAAS services which are VNET-integrated.

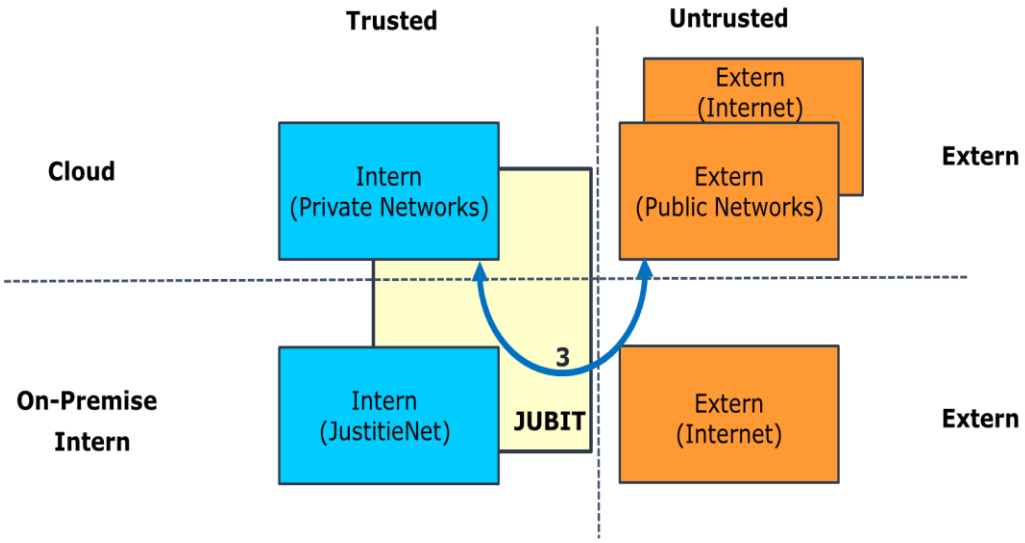
For the above protection, routing to the Private networks to external networks is enforced over the Express Route and Hub-spoke model provided under the JUBIT service. Connectivity from and to Internet, from and to the private networks is routed via JUBIT.

NETW 03 - Connectivity between Private and Public Endpoints

Status	Concept
Control Classification	Foundation
Version	0.1
Owner Control Definition	DI&I
Owner	DI&I - Solvinity

Control Objectives

To prevent that Adversaries may sniff network traffic to capture data or information about an environment, including authentication material passed over the network. To prevent that adversaries may attempt to position themselves between two or more networked devices using a man-in-the-middle (MiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation.



Control Sub-Objectives

Sub- Control #	Sub-Control Description
NETW- 03-01	It must be possible to inspect encrypted traffic (TLS-termination) to detect data leakage, data exfiltration, or malicious traffic. TLS-termination might not be applicable for every workload, e.g., when breaking the TLS end-to-end trust between host and destination is not desirable or not allowed
NETW- 03-02	Control inbound connectivity by using techniques like FQDN whitelisting or layer 3 network access control list when FQDN whitelisting is not feasible; hostname whitelisting; TCP/UDP port filtering and ICMP filtering; threat intel based or reputation based filtering
NETW- 03-03	Inbound network polices and connectivity controls must be based on least possible connectivity and must be maintained/reviewed periodically
NETW- 03-04	In- and outbound traffic must be logged (meta data)

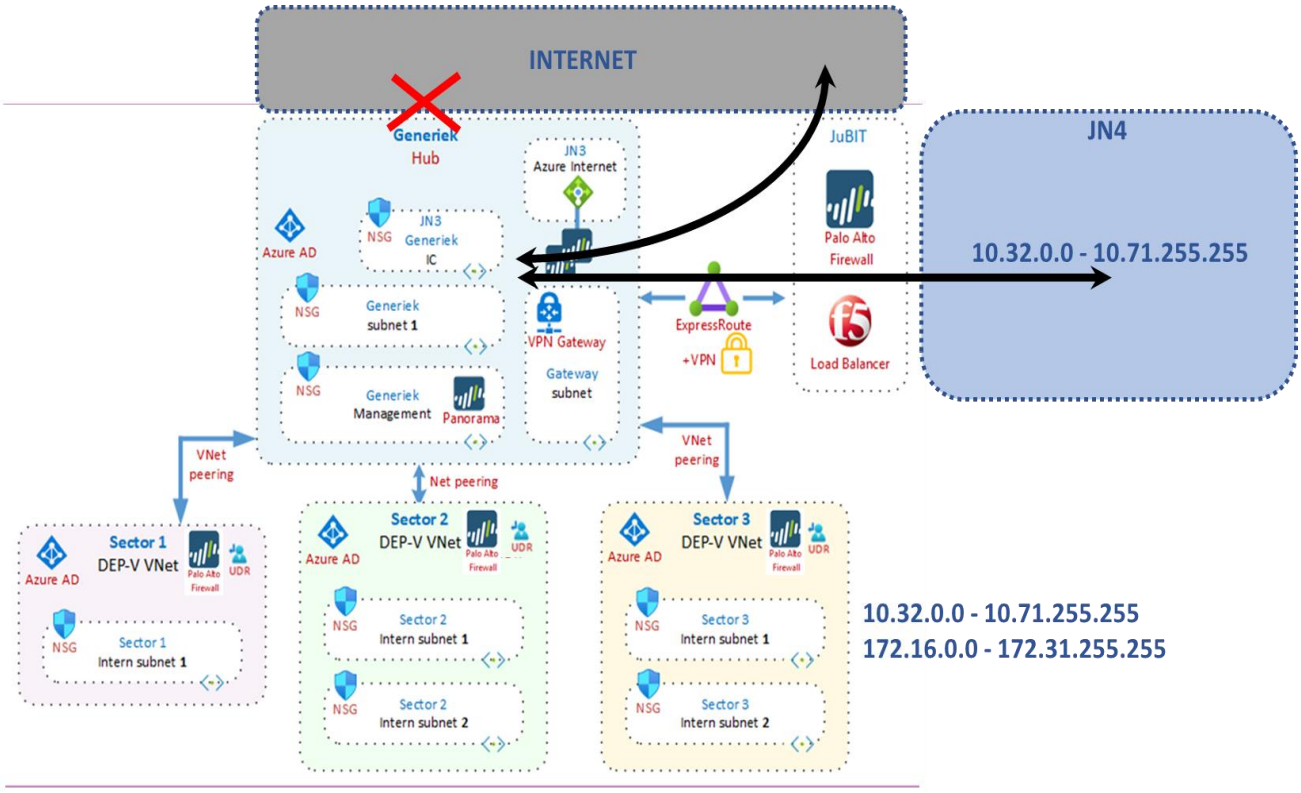
Link to Threat Catalogue

Threat ID	Justification
Threat 9: Malware	
Threat 11: Endpoint Denial of Service	
Threat 12: Network Sniffing	
Threat 13: Lateral Movement	
SThreat 15: Man in the Middle	
Threat 19: Network Denial of Service	

Implementation Guidelines

- Private Virtual Networks have a peering relationship with the hub where connectivity between Cloud VPNs is required.
- Traffic to and from the JenV Trusted Cloud is routed over the Cloudinterconnect (Express Route) to the internal Justitie network.
- Traffic to and from the JenV Trusted Cloud and External networks (internet e.a.) runs via dedicated JenV cloud connections, via the secure interface (preferable via a Layer 7 Firewall) within Jubit, where the application is provided with IP-addresses appropriate within the JenV IP-numbering plan.
- Private VNET's are controlled by JenV and host IAAS resources such as VM's and PAAS services which are VNET- integrated.

For the above protection, routing to the Private networks to external networks is enforced over the Express Route and Hub-spoke model provided under the JUBIT service. Connectivity from and to Internet, from and to the private networks is routed via JUBIT.

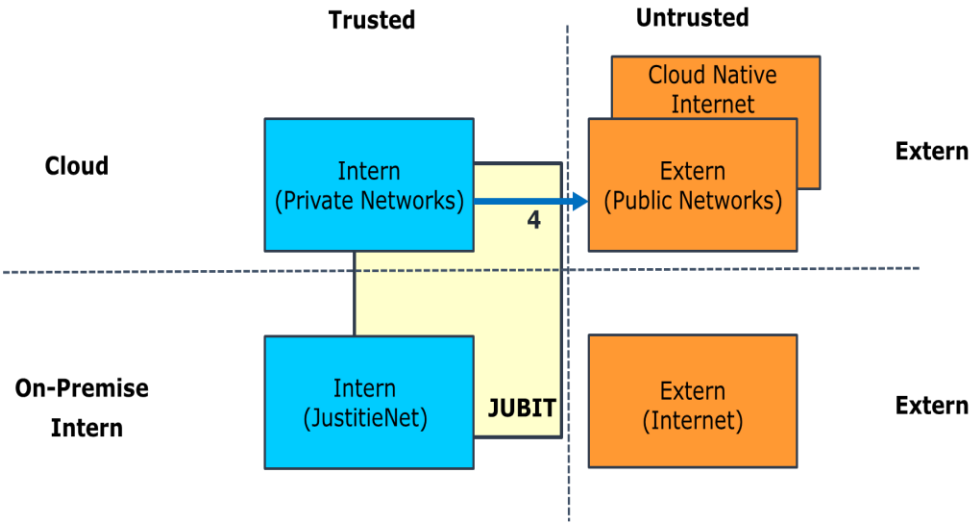


NETW 04 - Outbound Connectivity from CSP Private Networks

Status	Concept
Control Classification	Environment
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

To prevent that Adversaries may sniff network traffic to capture data or information about an environment, including authentication material passed over the network. To prevent that adversaries may attempt to position themselves between two or more networked devices using a man-in-the-middle (MiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation.



Control Sub-Objectives

Sub- Control #	Sub-Control Description
NETW- 04-01	It must be possible to inspect encrypted traffic (SSL/TLS termination) to detect data leakage, data exfiltration, or malicious traffic. TLS termination might not be applicable for every workload, e.g., when breaking the SSL end-to-end trust between host and destination is not desirable or not allowed
NETW- 04-02	Control outbound connectivity by using techniques like FQDN whitelisting or layer 3 network access control list when FQDN whitelisting is not feasible; hostname whitelisting; TCP/UDP port filtering and ICMP filtering; threat intel based or reputation based filtering
NETW- 04-03	Outbound network polices and connectivity controls must be based on least possible connectivity and must be maintained/reviewed periodically
NETW- 04-04	Outbound traffic must be logged (meta data)

Link to Threat Catalogue

Threat ID	Justification
Threat 9: Malware	
Threat 12: Network Sniffing	
Threat 15: Man in the Middle	
Threat 23: Data Exfiltration	

Implementation Guidelines

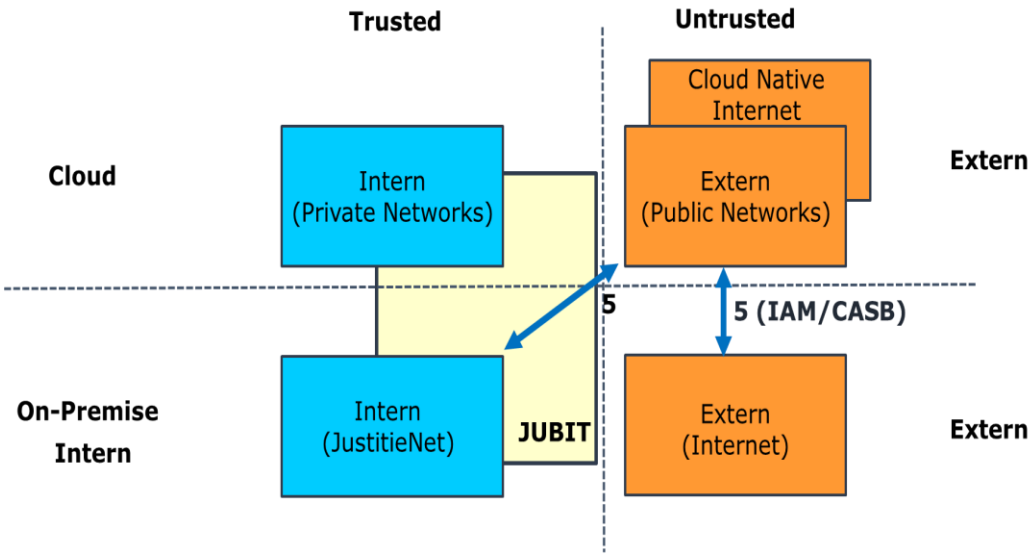
- Data traffic is inspected on viruses, maleware and other attacks.
- Inspection is preferably at specific application level (behavioural inspection).
- Connection is via the Palo Alto (PA) Firewall in the hub of the tenant and the outbound (unsecure) defined zone implemented on the PA Firewall.

NETW 05 - Connectivity to and from CSP Public networks

Status	Concept
Control Classification	Environment
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

For native PAAS/SAAS services, which cannot be integrated with the VNET/Private Endpoint technique in the JenV Trusted Cloud, the CSP is responsible for the protection of these public endpoints (by default reachable from Internet) and JenV can only take responsibility on the User Authentication and Authorization. These services reside in CSP Public and often have IAM controls including strong authentication as the primary control plane for securing access to these services. The CSP is responsible for protection (e.g. DDOS protection) of public endpoints, where Min. J&V has the possibility to enforce complementary connectivity controls and build defense in depth.



Control Sub-Objectives

Sub- Control #	Sub-Control Description
NETW- 05-01	Where possible, inbound connectivity to CSP Public Endpoints must be limited to: customer managed services (e.g. Webservices) and CSP managed cloud services (PaaS/SAAS services)
NETW- 05-02	When a public endpoint lacks sufficient IAM-controls, additional controls are mandatory, such as CASB and limiting inbound connections. The following IAM-controls are considered as sufficient: IAM-controls that comply with IAM-01 IAM on all Resources; Service Principals that comply with IAM-02 IAM on all Accounts following Min. J&V's IAM and IAM-04 Secure Secret and Key Management, CSP Managed Identities
NETW- 05-03	Inbound network polices and connectivity controls must be based on least possible connectivity and must be maintained/reviewed periodically

Link to Threat Catalogue

Threat ID	Justification
Threat 1: Compromised Accounts through Brute Force Attacks	
Threat 6: Legitimate Privilege Abuse	
Threat 11: Endpoint Denial of Service	
Threat 19: Network Denial of Service	
Threat 22: Data from Cloud Storage Object	

Implementation Guidelines

Mechanisms for controlling inbound connectivity can include:

- Cloud Access Security Broker (CASB)
- Correct IAM controls
- Cloud Application Gateways with Web Application Firewall capabilities (in case of webservices)
- Network based Access Control List

NETW 06 - Network Segmentation

Status	Concept
Control Classification	Environment
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

Network Segmentation is used to contain a set of applications, individual applications or application tiers in dedicated network segments, and control the connectivity between these network segments. This approach implements the zero trust principles on IaaS and PaaS, is used to limit the attack surface of applications and application tiers, and to protect against lateral movement.

Control Sub-Objectives

Sub- Control #	Sub-Control Description
NETW- 06-01	Applications and services must only expose those interfaces, or service endpoints, that are required to use the application or service. This applies to both inbound connectivity from public networks as from (virtual) private VNET's
NETW- 06-02	Network segmentation policies are used to control connectivity between application tiers or prevent undesired connectivity such as a publicly exposed fronted tier connecting to a data tier.
NETW- 06-03	Logging information about the IP traffic (metadata) between resources of an application must be captured and retained. The retention period is specified in CCF-AUD-01-03

Link to Threat Catalogue

Threat ID	Justification
Threat 6: Legitimate Privilege Abuse	
Threat 11: Endpoint Denial of Service	
Threat 13: Lateral Movement	
Threat 19: Network Denial of Service	

Implementation Guidelines

- Application and network configuration must restrict the connectivity based on least possible connectivity and must be maintained/reviewed periodically.
- Connectivity with an application must be isolated from the connectivity with other applications.

- Segmentation is based on the tier model of the application (e.g., frontend tier, application tier, data tier).
- Front-end applications must be placed in another network segment than backend applications such as API's.
- Inbound connectivity to back-end application should be restricted to only the front-end application that handles the back-end application logic.
- Outbound connectivity from back-end application should be restricted to only the front-end application that handles the application logic.
- Front-end applications should in principle never connect directly to Database tier.
- Database tier should never allow inbound our outbound connectivity from the Internet.
- Outbound and Inbound connectivity to database tier within Advanced workloads must be strongly controlled and monitored at the different layers.

7.5 Technical Vulnerability Management Controls

TVM 01 - Technical Vulnerability Management

Status	Concept
Control Classification	Environment
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

Vulnerability Management entails continuous monitoring, identifying and mitigating software vulnerabilities, misconfigurations and excessive permissions to reduce the likelihood of those being exploited and prevent compromise of endpoints.

Vulnerability Management applies to:

- Virtual Machines (Operating System software and third-party software/applications)
- Container registry images
- PaaS based database and storage services

Control Sub-Objectives

Sub- Control #	Sub-Control Description
TVM-01-01	Cloud endpoints must be automatically scanned for known vulnerabilities and misconfigurations at deployment and during the lifecycle
TVM-01-02	Identified vulnerabilities must be timely assessed and remediated or mitigated to decrease the associated risks to an acceptable level
TVM-01-03	Cloud endpoints must be up to date with the latest operating system, network protocol and application security updates to patch known vulnerabilities
TVM-01-04	Virtual Machine images must be hardened
TVM-01-05	What is detected via Vulnerability Management is enforced with Platform Hardening

Link to Threat Catalogue

Threat ID	Justification
Threat 1 Compromised Accounts through Brute Force Attacks	
Threat 2 Security Misconfiguration resulting in Unauthorized Access and Subdomain Hijacking	
Threat 5 Account Compromise through Social Engineering	

Threat 7 Account Discovery	
Threat 9 Malware	
Threat 13 Lateral Movement	
Threat 18- Arbitrary Code Execution due to Vulnerable and Outdated Components	

Implementation Guidelines

- Vulnerability scanning and detection must be based on X standards
- Virtual Machine hardening must be in accordance with JenVs' Security Architecture hardening benchmarks

Control Identifier	Control Sub-Objective
TVM-01-01	Defender for Cloud integrated Qualys vulnerability scanner
TVM-01-02	Defender for Cloud vulnerability assessment
TVM-01-03	Update Management in Azure Automation
TVM-01-04	Apply Azure security baselines to machines

TVM 02 - Virus and Malware Protection

Status	Concept
Control Classification	Environment
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

To protect resources from virus, ransomware or malicious files that can be identified through the use of Anti-virus which classifies them through digital signatures.

Control Sub-Objectives

Sub- Control #	Sub-Control Description
TVM-02- 01	Protect the integrity/confidentiality of the data processed/stored in all cloud services through the detection and blocking of viruses, ransomware and other malware
TVM-02- 02	Ensure that the solution and the data used to recognize malware (signature file) is kept up to date
TVM-02- 03	Ensure that records describing the detection of malware are captured and forwarded to a central log

Link to Threat Catalogue

Threat ID	Justification
Threat 4 Leaked Secrets through Source Code repository	
Threat 7 Account Discovery	
Threat 9 Malware	
Threat 10 Man in the Browser	
Threat 12 Network Sniffing (hybrid cloud)	
Threat 13 Lateral Movement	
Threat 15 Man in the Middle	
Threat 16 Forced Authentication	

Implementation Guidelines

Enable the correlation of malware detection records with signals indicating suspicious patterns from all components in an
- application chain.

The fundemental guideline is that of inspection and cleaning of incoming and outgoing traffic flows. This involves various traffic flows, including web traffic, e-mail, DNS traffic, message traffic, file transfers, API traffic, etc. Where the cleaning can be performed by various anti-malware, anti-Spam, ATP/APT scan/filter appliances.

Inspection and cleaning of traffic flows should provide protection against all known attacks (known signatures including: anti-spoofing, denial of service, routing attacks, intrusion, eavesdropping, etc). Inspection and cleaning of traffic flows should also provide protection against zero-day attacks using modern means such as behavior analysis and artificial intelligence.

- Security; malicious content (viruses, malware, ransomware, etc.) are detected and removed or cleaned;
- Filtering of websites; on the basis of URLs, content, domains, networks, etc., websites can be blocked or allowed per Participant for certain users or user groups;
- Traceability; to monitor the integrity, all actions must be traceable to the responsible user and/or digital identity;
- Transparency; all actions and attempted actions are recorded. This includes logging of established viruses, malware, etc.;
- Manageability; Logging, policies, filter lists, etc. are manageable;
- Granularity; it can be set that certain connections are, partially or not inspected and secured. For example, privacy-sensitive information can be excluded from inspection, for example home banking and health insurance companies or connections to update systems from suppliers such as Microsoft, ESET, Symantec, etc.

TVM 03 - Threat Protection

Status	Concept
Control Classification	Environment
Version	0.1
Owner Control Definition	DI&I
Owner	JenV onderdeel

Control Objectives

Provide protection, detection and response capabilities to protect against potential threats before they have the opportunity to access critical data or breach systems.

Control Sub-Objectives

Sub- Control #	Sub-Control Description
TVM- 03-01	For Iaas Endpoints Implement Endpoint Detection and Response (EDR) capabilities to: - Contain malware before this can cause any damage to target systems; - Prevent the propagation of malicious viruses or malware; - Identify suspicious files before these are uploaded or stored in JenV's Azure cloud environments; - Quickly detect lateral movement and reconnaissance, misdirect attacks, and gain engagement-based alerts on threats
TVM- 03-02	For Paas Endpoints Leverage CSP provided advanced threat protection and security capabilities to protect cloud resources like: Storage, SQL Databases, Open-Source Relational Databases, Containerized Application Infrastructure, Container Registries, Key Vaults, CSP Control & Management Plane (Cloud Resource Manager), DNS and dangling DNS Detection, Internet Connected Devices (IoT), Virtual Networks, Web Application Services, Virtual Machine Endpoint Security

Link to Threat Catalogue

Threat ID	Justification
Threat 1- Compromised Accounts through Brute Force Attacks	
Threat 2- Security Misconfiguration resulting in Unauthorized Access and Subdomain Hijacking	
Threat 3- Exposed Cloud Service Dashboard	
Threat 5- Account Compromise through Social Engineering	
Threat 6- Legitimate Privilege Abuse	
Threat 7- Account Discovery	
Threat 9- Malware	
Threat 10- Man in the Browser	

Threat 11- Endpoint Denial of Service	
Threat 12- Network Sniffing (hybrid cloud)	
Threat 13- Lateral Movement	
Threat 15- Man in the Middle	
Threat 16- Forced Authentication	
Threat 17- Software Discovery	
Threat 18- Arbitrary Code Execution due to Vulnerable and Outdated Components	
Threat 19- Network Denial of Service	
Threat 22- Unauthorized Access to Data from Improperly Secured Cloud Storage Objects	
Threat 23- Data Exfiltration	

Implementation Guidelines

Azure offers built in threat protection functionality through services such as Azure Active Directory (Azure AD), Azure Monitor logs, and Microsoft Defender for Cloud (documentation).

Control Identifier	Control Sub-Objective
TVM-03-01 and TVM-03-02	Enable Azure Defender for Cloud for each subscription and activate Azure Defender for all Azure resource types that have this enabled (documentation).

7.6 Privacy Controls

7.6.1. Inleiding en doelstelling

In dit hoofdstuk worden de privacy controls uiteengezet. Het doel van de privacy controls is ondersteuning te bieden aan medewerkers van JenV door maatregelen aan te bieden die de privacy en bescherming van persoonsgegevens kunnen waarborgen bij de verwerking van persoonsgegevens in een cloud omgeving.

De privacy controls bevatten voorbeelden van maatregelen die kunnen worden gebruikt om te zorgen dat privacy en bescherming van persoonsgegevens voldoende zijn geborgd en persoonsgegevens in de cloud in overeenstemming worden verwerkt met de wet, waaronder de AVG en de Richtlijn gegevensbescherming bij rechtshandhaving (hierna: Richtlijn 2016/680)[1], en (interne) kaders en richtlijnen en beleid. Tevens kunnen de privacy controls worden gebruikt om te toetsen én te evalueren in hoeverre reeds getroffen maatregelen adequaat zijn om naleving (blijvend) te waarborgen.

7.6.2 Privacy controls

De overheid verwerkt grote hoeveelheden (gevoelige) persoonsgegevens. Persoonsgegevens waarvoor de overheid verantwoordelijk is en verplicht is veilig te houden. Het verwerken van persoonsgegevens in een cloud omgeving brengt nieuwe privacyrisico's met zich mee. Privacyrisico's die in kaart moeten worden gebracht, zodat maatregelen getroffen kunnen worden om ook persoonsgegevens die verwerkt worden in de cloud veilig te houden.

Onderstaande privacy controls bieden handvatten om risico's in kaart te brengen, maar tevens een aantal maatregelen tegen reeds bekende risico's bij de verwerking van persoonsgegevens in de cloud. Deze zijn enerzijds gebaseerd op verplichtingen uit de AVG, de eerder uitgevoerde DPIA op de Microsoft producten Office365 en Azure online services[2], aanbevelingen uit de door EDPB - in samenwerking met de Europese toezichthouders - uitgevoerde Coordinated Enforcement Action (CEF)[3] en uitgebracht advies van de Autoriteit persoonsgegevens[4]. Let op, wanneer het gaat om persoonsgegevens die worden verwerkt in het politie en justitie domein is de Richtlijn 2016/680 van toepassing. Deze richtlijn is geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Bij de verwerking van politiegegevens of gegevens onder de Wjsg dient aan de verplichtingen van de Wpg respectievelijk de Wjsg te zijn voldaan.[5] De privacy controls kunnen aangepast worden naar aanleiding van ontwikkelingen op deze gebieden. Zoals aangegeven in de inleiding is het Cloud Control Framework een levend document. Risico's en maatregelen kunnen wijzigen door gewijzigde regelgeving en veranderde technieken en dreigingen, maar ook (nieuw uit te brengen) adviezen en richtlijnen van toezichthouders spelen hier een belangrijke rol in.

Privacy en security controls zijn twee verschillende concepten, maar zijn toch onlosmakelijk met elkaar verbonden. Beiden hebben tot doel risico's te verkleinen. Privacy controls ten aanzien van persoonsgegevens en security controls ten aanzien van alle vormen van informatie van een organisatie ofwel data in algemene zin. Zie onderstaande afbeelding ter illustratie.

---

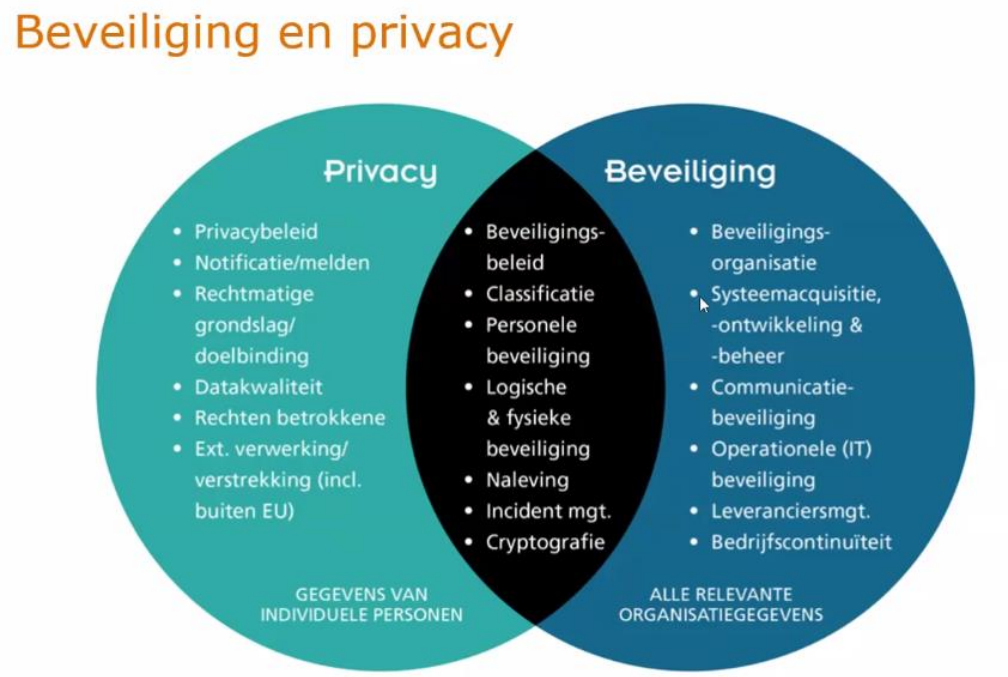
[1] Waar in dit document verwezen wordt naar 'persoonsgegevens' worden hiermee ook gegevens bedoeld die onder de Richtlijn 2016/680 worden beschermd.

[2] DPIA Microsoft Teams, Onedrive Sharepoint and Azzure AD. June 2022. DPIA Microsoft Teams

[3] European data Protection Board. 2022 Coordinated Enforcement Action: Use of cloud-based services by the public sector. Adopted on 17 January 2023. https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf

[4] Autoriteit Persoonsgegevens. Inzet van Cloud Service Providers, 11 november 2022.
https://www.autoriteitpersoonsgegevens.nl/uploads/imported/brief_over_inzet_cloud_service_providers.pdf
Autoriteit Persoonsgegevens. Rijksbreed cloudbeleid 2022. 14 november 2022.
AP: kabinet moet privacyrisico's cloudbeleid aanpakken | Autoriteit Persoonsgegevens

[5] Zie voor meer informatie over privacywetgeving voor politie en justitie de website van de Autoriteit Persoonsgegevens.



Bron: Privacy Board JenV

Uit de afbeelding valt tevens op te maken dat het borgen van de privacy deels afhankelijk is van het uitvoeren van beveiligingsmaatregelen ofwel de security controls dragen bij aan het bevorderen van privacy. Het toepassen van security controls is echter niet voldoende om alle privacyrisico's te beheersen. Ten aanzien van de verwerking van persoonsgegevens in de cloud dienen de volgende privacy controls meegenomen te worden:

Privacy control 01 – DPIA

Alvorens met een CSP in zee te gaan en met een verwerkingsactiviteit in de cloud aan te vangen dienen de privacy risico's in kaart te worden gebracht. Indien een verwerking leidt tot een hoog risico dient voorafgaand aan de verwerking een DPIA te worden uitgevoerd.[6] Het kan worden aangenomen dat een verwerking binnen de cloud door de publieke sector waarschijnlijk leidt tot de verplichting een DPIA uit te voeren gezien de doorgaans op grote schaal verwerking van - onder meer - bijzondere persoonsgegevens en/of strafrechtelijke persoonsgegevens door de overheid.[7] Naast de wettelijke criteria uit artikel 35 lid 3 AVG hebben zowel de Autoriteit Persoonsgegevens als de Europese toezichthouders criteria geformuleerd om in te schatten of een DPIA uitgevoerd dient te worden. Een overzicht waaruit blijkt wanneer wel of geen DPIA uitgevoerd dient te worden, is te vinden op de website van de Autoriteit Persoonsgegevens. Rijksbreed is een Pre-scan DPIA beschikbaar waarmee bepaald kan worden of het verplicht is om een DPIA uit te voeren en op welke aspecten van de gegevensverwerking mogelijke risico's zijn voorzien.[8] Let op, indien een DPIA niet vereist is, is op basis van artikel 32 AVG alsnog vereist dat er adequate technische en organisatorische maatregelen worden getroffen bepaald op basis van een risicobeoordeling.

Op basis van de uitgevoerde DPIA – dan wel risicobeoordeling - kunnen er technische en organisatorische maatregelen getroffen worden om de vastgestelde risico's te mitigeren. Denk hierbij bijvoorbeeld aan het risico op de doorgifte van persoonsgegevens naar een derde land zoals de Verenigde Staten (zie privacy control 03) en het gebrek aan controle op welke derde partijen persoonsgegevens worden gedeeld. Dit zijn risico's waar tegen maatregelen genomen kunnen worden.

Indien er reeds een DPIA op de verwerking is uitgevoerd schrijft artikel 35 lid 11 AVG voor dat bij een wijziging van de risico's van de verwerking deze DPIA opnieuw getoetst moet worden. De overgang naar verwerking in

[6] Artikel 35 lid 1 AVG en artikel 27 Richtlijn 2016/680.

[7] European data Protection Board. 2022 Coordinated Enforcement Action: Use of cloud-based services by the public sector. Adopted on 17 January 2023. https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf

[8] Pre-scan DPIA. Relevante documenten - Rijksportaal (overheid-i.nl)

de cloud kan een wijziging van de risico's inhouden en vereisen dat de DPIA opnieuw moet worden beoordeeld op de specifieke risico's die verwerking in de cloud met zich meebrengt.

Is er reeds een DPIA uitgevoerd op een gegevensverwerking die sterk lijkt op de aan te vangen gegevensverwerking dan hoeft er geen DPIA op worden uitgevoerd. Eén DPIA mag namelijk meerdere gegevensverwerking bestrijken indien deze vergelijkbare hoge risico's inhouden. Dit volgt uit artikel 35 lid 1 AVG. Dit zou mogelijk zijn in het geval er een vergelijkbare technologie wordt gebruikt om dezelfde soort gegevens voor dezelfde doeleinden te verzamelen bijvoorbeeld bij gebruik van een gezamenlijke database door verschillende onderdelen van de overheid.

Indien de uitvoer van een DPIA verplicht is (en een DPIA nog niet is uitgevoerd), is er een gebruiksvriendelijk cloud specifiek DPIA-model ontwikkeld die JenV-organisaties kunnen gebruiken voorafgaand aan de ingebruikname van de clouddienst.[9]

Gezien de razendsnelle ontwikkelingen in het cloudlandschap, veranderingen in regelgeving en richtlijnen omtrent dit onderwerp, maar ook veranderingen met betrekking tot verwerkingsactiviteiten dient de DPIA geregeld geëvalueerd te worden. Risico's en daarmee de bijbehorende maatregelen kunnen wijzigen en dienen in dat geval te worden geactualiseerd.

Stappenplan privacy control 01 - DPIA

- Breng risico's in kaart (uitvoer DPIA, tenzij..).
- Tref maatregelen om risico's weg te nemen.
- Evalueer en actualiseer.

Privacy control 02 – Contractering CSP

Mede gebaseerd op de uitkomsten van de DPIA (of risicobeoordeling) is het van groot belang afspraken met de CSP contractueel stevig vast te leggen. Dit is ook verplicht op grond van artikel 28 AVG en artikel 22 Richtlijn 2016/680 in een zogenoemde verwerkersovereenkomst. SLM Rijk heeft een DPIA uitgevoerd op de Microsoft producten Office 365 en Azure online services. Op basis van de uitkomst van de DPIA zijn aanvullende afspraken vastgelegd in de overeenkomst met Microsoft onder meer toeziend op de rollen van partijen, het gebruik van metadata en het recht van audit. [10]

De punten waar afspraken over moeten worden gemaakt worden opgesomd in artikel 28 lid 3 AVG. De exacte afspraken zijn echter maatwerk afhankelijk van de specifieke verwerkingsactiviteit die uitbesteed gaat worden. Dit kan onder meer afgeleid worden uit de specificaties van de gegevensverwerking en de bijbehorende risico's die in een DPIA zijn vastgesteld. Contractuele afspraken kunnen (privacy)risico's omtrent verwerking in de cloud mitigeren. Grote (cloud) software providers werken vaak met standaardovereenkomsten. In dit geval kan het nodig zijn aanvullende afspraken te maken met de CSP. Het van belang om daarbij (minimaal) onderstaande punten onder de aandacht te houden.

- Rollen van partijen

Het is van belang om de rollen van partijen, verwerkingsverantwoordelijke en verwerker, duidelijk vast te stellen en vast te leggen. In dit kader dienen alle verwerkingsactiviteiten in de cloud te worden gespecificeerd. Ook mogelijke verwerkingsactiviteiten door de CSP voor eigen doeleinden. Het is niet wenselijk dat een CSP data van burgers - toevertrouwd aan de overheid - voor eigen doeleinden gebruikt. Dit zou de CSP verwerkingsverantwoordelijke maken. CSP's werken vaak met standaard contracten waar het gebruik van data voor eigen doeleinden vaak is toegestaan. Hier dienen aanvullende afspraken over te worden gemaakt.

- Inzetten van subverwerkers

In het verlengde van voorgaande punt is het tevens van belang om alle subverwerkers te identificeren en te duiden, bijvoorbeeld welke verwerkingsactiviteiten de subverwerker uitvoert en vanuit welke (vestigings)locatie. Daarnaast dienen afspraken gemaakt te worden welke subverwerkers en onder welke voorwaarden toegevoegd mogen worden. Het moet mogelijk zijn bezwaar te maken tegen het toevoegen van een subverwerker om naleving van de AVG te kunnen blijven borgen. Dit dient in het contract met de CSP te worden te worden vastgelegd.

[9] Cloud DPIA-model JenV architectuurdocumentatie repository - Docs (eminjenv.nl) zie bijlage.

[10] SLM Rijk overeenkomst Microsoft. Downloads - DPIAs - SLM Microsoft, Google Cloud en Amazon Web Services (slmmicrosoftrijk.nl)

- Maak afspraken over de verwerkingsactiviteiten

Het is van belang dat de CSP alleen namens de verwerkingsverantwoordelijk en volgens de instructies van verwerkingsverantwoordelijke handelt. Naast het vaststellen van de rollen van partijen (inclusief subverwerkers) is het identificeren en beoordelen van alle verwerkingsactiviteiten (inclusief van CSP) van belang. Kwalificeert de CSP zichzelf als verwerkingsverantwoordelijke voor bepaalde verwerkingsactiviteiten en voldoen deze verwerkingen aan de AVG zijn punten die verhelderd moeten worden. Een CSP kan bepaalde gegevens nodig hebben om de dienst te leveren (telemetrische gegevens/diagnostische gegevens) of kan in de standaardovereenkomst het gebruik van metadata voor eigen doeleinden toestaan. Hier dienen mogelijk aanvullende afspraken over te worden gemaakt.

- Modelcontract/standard contractual clauses (SCC)

Indien er sprake is van doorgifte naar een derde land en er is geen adequaatheidbesluit voor dat land genomen dient er een modelcontract te worden afgesloten (zie verder privacy control 03).

- Technische en organisatorische beveiligingsmaatregelen

Een verwerkingsverantwoordelijke is verplicht om passende technische en organisatorisch maatregelen te treffen. Indien een verwerking wordt uitbesteed aan een CSP moeten er ook specifieke afspraken worden gemaakt in het contract met de CSP over de te nemen technische en organisatorische maatregelen afgestemd op de risico's van de verwerkingen. Bijvoorbeeld over het gebruik van encryptie (zie privacy control 04).

- Periodieke controle of partij zich aan de afspraken houdt

Op grond van 28 lid 3 sub h AVG dient de verwerkingsverantwoordelijk na te gaan of een verwerker zich aan de gemaakte afspraken houdt en dient een verwerker informatie beschikbaar te stellen en audits toe te staan om dit voor verwerkingsverantwoordelijke mogelijk te maken. Met een CSP dienen afspraken te worden gemaakt over periodieke controles (al dan niet gekwalificeerd als een audit) van de CSP en de uitgevoerde verwerkingsactiviteiten. Let op, in een standaardovereenkomst van een CSP worden audits geregeld uitgesloten. Hier dienen dan aanvullende afspraken over te worden gemaakt.

- Exit strategie

Het is van belang afspraken te maken met de CSP over de teruggave en vernietiging van de gegevens bij contractbeëindiging. Dit behoeft ook een zeker mate van uitwerking. Niet alleen om de continuïteit van bedrijfsprocessen te borgen, maar ook omdat het (tijdelijk) niet beschikbaar zijn van gegevens tot een risico voor de privacy van betrokkenen kan leiden. Neem hier ook ontwikkelingen uit de in januari 2024 geeimplemneteerde Data Act in mee die neiuwe regels geeft voor onder meer het overstappen tussen clouddiensten.

- Werk samen in onderhandeling en contractering CSP

Als het gaat om contractonderhandelingen hebben grote CSP's doorgaans een sterkere onderhandelingspositie. Dit zie je terug in de standaardovereenkomsten die CSP's gebruiken met de voor deze partij meest gunstige voorwaarden (zie voorgaande punten ter illustratie). Het samenwerken met andere overheidsinstellingen stelt de overheid beter in staat goede voorwaarden te onderhandelen. Illustrerend is de SLM Rijk overeenkomst Microsoft.

Let op, ook kleinere CSP werken vaak met standaardovereenkomsten. In dit geval kan het ook nodig zijn aanvullende dan wel afwijkende afspraken te maken om de bescherming van persoonsgegevens goed te borgen. Ook hier kan samenwerking tussen overheidsinstellingen de onderhandelingspositie versterken.

Om bovenstaande punten (contractueel) te waarborgen is het van belang een privacy functionaris te betrekken bij het contracteren van een CSP.

Stappenplan privacy control 02 - *Contractering CSP*

- Breng gegevensverwerking en risico's in kaart.
- Leg (maatwerk)afspraken vast met CSP.
- Evalueer of CSP afspraken nakomt.

Privacy control 03 – Waarborgen bij internationale doorgifte

Bij gebruik van de cloud is de kans aanwezig dat je met een CSP in zee gaat die buiten de Europese Economische Ruimte (EER) is gevestigd en/of bepaalde (verwerking)activiteiten vanuit een land buiten de EER uitvoert. Let op, dit kan ook via een subverwerker die de CSP heeft ingezet. In het geval dat er

persoonsgegevens naar een land buiten de EER worden doorgegeven is er sprake van doorgifte van persoonsgegevens naar een derde land. De AVG en de Richtlijn 2016/680 stellen speciale voorwaarden aan doorgifte naar landen buiten de EER. Dit is alleen toegestaan als het betreffende land een passend beschermingsniveau heeft ofwel op een gelijkwaardige manier worden beschermd als binnen de EER; de Richtlijn 2016/680 voegt daar nog bevoegde categorieën ontvangers aan toe[11]. Dit kan door de Europese Commissie (EC) worden vastgesteld met een adequaatheidsbesluit, bijvoorbeeld onder de AVG voor het Verenigd Koninkrijk, Argentinië, Japan en (onder voorwaarden) de VS en onder de Richtlijn 2016/680 alleen voor het Verenigd Koninkrijk.

Dit is ook toegestaan indien er passende waarborgen getroffen worden conform artikel 46 AVG, zoals het gebruik van het door de EC vastgestelde modelcontract ofwel SCC.[12] Dit contract kan worden gebruikt om met de CSP een passend beschermingsniveau te borgen voor de doorgifte van persoonsgegevens naar een derde land. In dit geval dient tevens beoordeeld te worden of deze waarborg daadwerkelijk een passend beschermingsniveau biedt voor de doorgifte naar het betreffende land. Op basis van deze beoordeling, ook wel een data transfer impact assessment (DTIA) genoemd, kan het noodzakelijk zijn om aanvullende maatregelen treffen (bijvoorbeeld encryptie en pseudonimisering) en deze ook contractueel vast te leggen.[13] Zie voor het uitvoeren van een DTIA het Toetsingskader Doorgifte persoonsgegevens Rijksoverheid.

Alvorens met een CSP in zee te gaan is het nodig om vast te stellen of er met gebruik van de betreffende clouddienst doorgiften naar derde landen plaatsvinden. Breng hiervoor de infrastructuur, leveranciers, partners en overige derden én landen waar deze partijen gevestigd zijn of van waaruit ze opereren in kaart. Indien er doorgiften naar derde landen plaatsvinden moeten deze voldoen aan bovengenoemde vereisten van een passend doorgifte. Indien dit niet mogelijk is, bijvoorbeeld door de onwil van een CSP om bepaalde zaken contractueel vast te leggen, het niet kunnen treffen van passende aanvullende maatregelen, de onmogelijkheid de doorgifte te stoppen voor gebruik van cloud, kan er geen gebruik worden gemaakt van de betreffende CSP. In dit geval zal er voor een andere CSP moeten worden gekozen.

Daarnaast dient rekening te worden gehouden met de mogelijke intrekking van een adequaatheidsbesluit of dat als gevolg van wetswijzigingen in een land van doorgifte de getroffen waarborgen niet langer passend zijn. Dit is met name een risico voor doorgiften naar de VS. een doorgifte die eerder was toegestaan kan dan mogelijk niet langer plaatsvinden.

Stappenplan privacy control 03 – *Waarborgen internationale doorgifte*

- Stel vast of er doorgiften naar derde landen plaatsvinden.
- Indien er geen passend beschermingsniveau is tref passende waarborgen (o.a. modelcontract, DTIA, etc).
- Indien dit niet mogelijk is stop met gebruik CSP.

[11] Vaak zal er sprake zijn van een CSP die als (sub)verwerker optreedt, dan zijn voor de Richtlijn 2016/680 de doorgifteartikelen niet van toepassing.

[12] Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 4 juni 2021 betreffende Standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad. Publications Office (europa.eu). Let op, voor de Richtlijn 2016/680 is tot op heden nog geen modelcontract opgesteld.

[13] European Data Protection Board. Aanbevelingen inzake maatregelen ter aanvulling op doorgifte instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen. 18 juni 2021. EDPB_Recommendations_202001(Vo.2.0)_NL.docx (europa.eu)

Privacy control 04 – Pseudonimiseren en anonimiseren

Hoewel in verband met de bruikbaarheid van gegevens niet altijd geschikt om toe te passen voor alle verwerkingen in de cloud kunnen persoonsgegevens, ter bescherming, gepseudonimiseerd of geanonimiseerd worden.

Pseudonimiseren is een goede maatregel om persoonsgegevens te beveiligen. Het is een maatregel waarbij identificerende gegevens worden gescheiden van niet-identificerende gegevens en worden vervangen voor kunstmatige identificatoren. Persoonsgegevens worden getransformeerd in een dataset die niet meer herleidbaar is naar een persoon. Omdat er wel nog een koppeling kan worden gemaakt tussen de gepseudonimiseerde gegevens en de identificerende gegevens (middels een sleutel) blijven gepseudonimiseerde gegevens persoonsgegevens. Er is in dit geval sprake van (de mogelijkheid tot) omkeerbaarheid. De AVG is in dit geval van toepassing. Ook indien de gepseudonimiseerde gegevens verstrekt worden aan een derde (bijvoorbeeld een CSP). Door de kunstmatige indentificatoren kan de derde geen koppeling maken met een geïdentificeerde persoon. Op deze manier vermindert pseudonimiseren – mits op correcte wijze uitgevoerd – het privacyrisico van betrokkenen.[14] In het kader van het pseudonimiseren is het aan te raden de ontwikkelingen van Privacy Enhancing Technologies (PET) te volgen en waar relevant in te zetten. Ook onder de Richtlijn 2016/680 wordt pseudonimiseren als passende maatregel gezien om persoonsgegevens te beschermen.[15]

Bij het anonimiseren van persoonsgegevens worden gegevens zodanig veranderd dat de gegevens niet langer herleidbaar zijn naar een individu. Let op, het proces van anonimiseren is een verwerking van persoonsgegevens. Anonieme gegevens zijn echter niet langer persoonsgegevens. De AVG dan wel Richtlijn 2016/680 zijn in dit geval niet langer van toepassing. De gegevens moeten wel daadwerkelijk anoniem zijn en redelijkerwijs op geen enkele manier herleidbaar zijn of alsnog gekoppeld kunnen worden. In dit geval is het proces onomkeerbaar. Bij volledig anonieme gegevens bestaat er niet langer een privacyrisico voor betrokkenen.[16]

Verbreek indien mogelijk, ook bij verwerking in de cloud, de link tussen personen en gegevens door de gegevens te anonimiseren of pseudonimiseren. In dit geval worden er minder (of geen persoonsgegevens) verwerkt en verminderen door deze maatregelen de risico's voor betrokkenen. Ter aanvulling, de EDPB ziet pseudonimisering als doeltreffende aanvullende maatregel bij de doorgifte van persoonsgegevens naar derde landen (zie privacy control 03).

Let op, in de praktijk is er regelmatig discussie of gegevens wel of niet identificeerbaar zijn. Discussies of gegevens gepseudonimiseerde gegevens, dan wel geanonimiseerde gegevens, of persoonsgegevens zijn. Toezichthouders en gerechten lijken hier dikwijls over van mening te verschillen. In dit kader is het aan te raden ontwikkelingen met betrekking tot de definitie van geanonimiseerde dan wel gepseudonimiseerde gegevens goed te blijven volgen waaronder uitspraken van de het Europe Hof van Justitie die op dit punt een meer ruime definitie hanteren.[17]

Stappenplan privacy control 04 – *Pseudonimiseren en anonimiseren*

- Indien mogelijk anonimiseer of pseudonimiseer de persoonsgegevens.
- Controleer of er sprake is van daadwerkelijk gepseudonimiseerde dan wel geanonimiseerde gegevens.

[14] Zie artikel 4 sub 5 AVG en overweging 26 en 27 AVG.

[15] Artikel 20 Richtlijn 2016/680.

[16] Zie overweging 27 AVG.

[17] HvJ EU 26 april 2023, T-557/20, ECLI:EU:T:2023:219

Tot slot

Om bovenstaande privacy controls te borgen is het van essentieel belang om in het proces van overgang naar de cloud een privacy functionaris te betrekken. Dit is nog meer van belang indien de Wpg of de Wjsg van toepassing is. Voor verwerkingen onder de Richtlijn 2016/680 (geïmplementeerd in de Wpg en Wjsg) zijn niet altijd richtlijnen en/of modellen (o.a. modelcontract) beschikbaar zoals voor verwerkingen onder de AVG. Daarnaast verschilt de systematiek van de Richtlijn 2016/680 en zijn gegevensverwerkingen per definitie gevoelig van aard. Het proces van overgang naar de cloud kan wezenlijk verschillen voor verwerkingen onder de Richtlijn 2016/680 en behoeft speciale aandacht en ervaring.

Bijlage Cloud DPIA

Concept Cloud PIA Model v3.12_Extend

Bijlage Toetsingskader doorgifte persoonsgegevens Rijksoverheid