1. Bijlage bij Zelfverklaring

Deze bijlage wordt door iedere leverancier ingevuld als onderbouwing bij de zelfverklaring.

De gedachte achter de zelfverklaring is dat de leverancier transparant is over de mate waarin aan de eisen wordt voldaan. Dit in tegenstelling tot de een onafhankelijke toetsing, waarin deze vaststelling door een derde plaatsvindt. De leverancier dient daarom voor zichzelf te bepalen hoe hij een bepaalde control voor de eigen dienstverlening zou moeten toepassen.

De formuleringen in kolommen ‘Control Domain’, ‘Control ID’ en ‘Control Specification’ zijn overgenomen uit de Cloud Security Agency (CSA) Cloud Control Matrix (CCM) versie 3.0.1 De controls waarvan het ‘control id’ eindigt op een a en de ‘control specification’ in het Nederlands is geschreven zijn specifiek toegevoegd.

Toelichting kolom ‘Eis’

* Daar waar een control is gemarkeerd met ‘volledig’ betekent dit dat de leverancier volledig aan deze control moet voldoen en dat er geen verbeterpunten meer mogen zijn.
* Daar waar een control is gemarkeerd met ‘deels’ betekent dit dat verbeterpunten zijn toegestaan. De leverancier moet op termijn aan deze control moet voldoen en op dit moment al deze control in een bepaalde mate moet hebben ingericht.

Voor alle controls geldt daarmee dat het niet acceptabel is als er nog helemaal geen maatregelen zijn getroffen om aan deze control te voldoen.

De kolom ‘Interpretation note’ is toegevoegd door de schemabeheerder en dient als illustratie / achtergrondbeschrijving van de betreffende control.

In de kolom ‘Beschrijving conformiteit, eventueel aangevuld met toelichting’ geeft de leverancier aan in welke mate aan de eis wordt voldaan. Hier zijn twee situaties mogelijk:

1. Daar waar volledig aan een eis moet worden voldaan geeft leverancier aan dat hij volledig aan de eis voldoet.
2. Daar waar een leverancier deels aan een eis mag voldoen wordt:
   1. Als leverancier aan de eis voldoet, kan worden volstaan met het opnemen van ‘voldaan’.
   2. Als leverancier deels aan de eis voldoet moet de leverancier ‘deels’ aangeven, aangevuld met een onderbouwing van hetgeen wel is geregeld en dat wat nog niet is geregeld.
   3. Als leverancier geen maatregelen heeft getroffen voor de betreffende eis dan dient hij aan te geven: ‘geen maatregelen getroffen’.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Control Domain** | **Control ID** | **Control Specification** | **Eis** | **Interpretation note** | **Beschrijving conformiteit, eventueel aangevuld met toelichting** |
| **Application & Interface Security** *Application Security* | AIS-01 | Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations. | Deels |  | Volledig / deels, omdat … |
|  | AIS-01.a | Daar waar partijen kiezen voor een gegevensuitwisseling conform Edukoppeling moet de thans geldende versie van de transactiestandaard zijn toegepast. | Volledig | Toegevoegd als specifieke eis vanuit de schema eigenaar. | Volledig |
| **Application & Interface Security** *Data Security / Integrity* | AIS-04 | Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alteration, or destruction. | Deels |  | Volledig / deels, omdat … |
| **Audit Assurance & Compliance** *Information System Regulatory Mapping* | AAC-03 | Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected. | Deels | Organisatie houdt bij wat de impact is van nieuwe wet- en regelgeving. Ten aanzien van de impact van nieuwe privacy wetgeving is de organisatie pro-actief. Met pro-actief wordt bedoeld dat een organisatie niet alleen nieuwsbrieven maar ook met gespecialiseerde adviseurs of gesprekspartners afstemt hoe nieuwe richtlijnen zich vertalen naar implementatie in de eigen bedrijfsvoering. | Volledig / deels, omdat … |
|  | AAC-03a | Onderdeel van deze norm is dat een passende bewerkersovereenkomst is afgesloten, conform het geldende model. | Volledig | Toegevoegd als specifieke eis vanuit de schema eigenaar. | Volledig |
|  | AAC-03b | Onderdeel van deze norm is dat persoonsgegevens door de leverancier op geen enkele wijze aan derden ter beschikking worden gesteld. | Volledig | Toegevoegd als specifieke eis vanuit de schema eigenaar. | Volledig |
| **Business Continuity Management & Operational Resilience** *Retention Policy* | BCR-11 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness. | Deels | Minimaal onderdeel van een retention policy moet zijn:   * welke data is onderdeel van de backup * hoe lang mag welk type data worden bewaard * op welke manier moet data worden vernietigd / verwijderd als deze data niet langer wordt gebruikt / mag worden gebruikt | Volledig / deels, omdat … |
| **Data Security & Information Lifecycle Management** *Data Inventory / Flows* | DSI-02 | Policies and procedures shall be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, providers shall ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds. | Deels | Doel van de policies en procedures moet zijn dat vermenging van gegevens met die van andere klanten wordt voorkomen.  Het is hierbij belangrijk om dit enerzijds te bezien in de relatie tussen School en cloud leverancier, maar ook in de relatie tussen cloud leverancier en onderwijsketen. | Volledig / deels, omdat … |
| **Data Security & Information Lifecycle Management** *Handling / Labeling / Security Policy* | DSI-04 | Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data. | Deels | Het labelen moet worden geïnterpreteerd als fysiek of elektronisch markeren van data. | Volledig / deels, omdat … |
| **Data Security & Information Lifecycle Management** *Non-Production Data* | DSI-05 | Production data shall not be replicated or used in non-production environments. | Volledig |  | Volledig |
| **Data Security & Information Lifecycle Management** *Ownership / Stewardship* | DSI-06 | All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated. | Deels | Het moet helder zijn wie de ‘steward’ is van de data. Dit is een randvoorwaarde om vermenging van gegevens met die van andere klanten te kunnen voorkomen. | Volledig / deels, omdat … |
| **Data Security & Information Lifecycle Management** *Secure Disposal* | DSI-07 | Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements. | Deels |  | Volledig / deels, omdat … |
| **Datacenter Security** *Off-Site Authorization* | DCS-04 | Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises. | Deels |  | Volledig / deels, omdat … |
| **Datacenter Security** *Unauthorized Persons Entry* | DCS-08 | Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss. | Deels |  | Volledig / deels, omdat … |
| **Datacenter Security** *User Access* | DCS-09 | Physical access to information assets and functions by users and support personnel shall be restricted. | Deels |  | Volledig / deels, omdat … |
| **Encryption & Key Management** *Key Generation* | EKM-02 | Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control. | Deels | Deze eis is specifiek van toepassing voor de Key die de cloud leverancier zelf gebruikt om gegevens met de keten uit te wisselen. | Volledig / deels, omdat … |
| **Encryption & Key Management** *Sensitive Data Protection* | EKM-03 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations. | Deels |  | Volledig / deels, omdat … |
|  | EKM-03.a | Toegang tot (gegevens in) de clouddienst verloopt altijd via een HTTPS (SSL/TLS)-verbinding. | Volledig |  | Volledig |
| **Governance and Risk Management** *Baseline Requirements* | GRM-01 | Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business need. | Deels | De cloud leverancier stelt voor intern gebruik dergelijke baselines op. | Volledig / deels, omdat … |
| **Governance and Risk Management**  *Data Focus Risk Assessments* | GRM-02 | Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:  • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure  • Compliance with defined retention periods and end-of-life disposal requirements  • Data classification and protection from unauthorized use, access, loss, destruction, and falsification | Deels |  | Volledig / deels, omdat … |
| **Governance and Risk Management** *Policy Enforcement* | GRM-07 | A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures. | Volledig |  | Volledig |
| **Governance and Risk Management** *Risk Assessments* | GRM-10 | Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance). | Deels |  | Volledig / deels, omdat … |
| **Human Resources** *Background Screening* | HRS-02 | Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk. | Deels | Deze eis geldt specifiek in relatie tot de eis dat misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school moet worden voorkomen. | Volledig / deels, omdat … |
| **Human Resources** *Employment Agreements* | HRS-03 | Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets. | Deels | Deze eis geldt specifiek in relatie tot de eis dat misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school moet worden voorkomen. | Volledig / deels, omdat … |
| **Human Resources** *Employment Termination* | HRS-04 | Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. | Deels | Deze eis geldt specifiek in relatie tot de eis dat misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school moet worden voorkomen. | Volledig / deels, omdat … |
| **Human Resources** *Non-Disclosure Agreements* | HRS-07 | Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. | Deels | Deze eis geldt specifiek in relatie tot de eis dat misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school moet worden voorkomen. | Volledig / deels, omdat … |
| **Human Resources** *Roles / Responsibilities* | HRS-08 | Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. | Deels |  | Volledig / deels, omdat … |
| **Identity & Access Management** *Audit Tools Access* | IAM-01 | Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data. | Deels | Doel hiervan is dat vermenging van gegevens met die van andere klanten wordt voorkomen.  Doel hiervan is tevens om vast te stellen dat cloud-leverancier afdoende maatregelen heeft getroffen om per klantomgeving een log of audittrail vast te leggen om het uitvoeren van digitaal en/of forensisch onderzoek en audits te ondersteunen. | Volledig / deels, omdat … |
| **Identity & Access Management** *Credential Lifecycle / Provision Management* | IAM-02 | User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following:  • Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships)  • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems)  • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant))  • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation)  • Account credential lifecycle management from instantiation through revocation  • Account credential and/or identity store minimization or re-use when feasible  • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets)  • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to  data and sessions  • Adherence to applicable legal, statutory, or regulatory compliance requirements, | Deels | Deze eis geldt specifiek in relatie tot de eis dat misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school moet worden voorkomen.  Met (oud-) medewerkers wordt specifiek gedoeld op de (oud-) medewerkers van de cloud leverancier.  Wel dient hier te worden vermeld welke generieke waarborgen leverancier heeft getroffen ter ondersteuning van het beheer van gebruikersrechten door aangesloten onderwijsinstellingen. Denk bijvoorbeeld aan bijvoorbeeld blokkeren van inactieve accounts, specifieke aanvraag- / wijzigings- / intrekkingsprocedures en het mogelijk maken periodieke review toegangsrechten door het verstrekken van overzichten. | Volledig / deels, omdat … |
| **Identity & Access Management** *Policies and Procedures* | IAM-04 | Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity. | Deels | Deze eis geldt specifiek in relatie tot de eis dat misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school moet worden voorkomen. | Volledig / deels, omdat … |
| **Identity & Access Management** *Segregation of Duties* | IAM-05 | User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest. | Deels | Deze eis geldt specifiek in relatie tot de eis dat misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school moet worden voorkomen. | Volledig / deels, omdat … |
| **Identity & Access Management** *Third Party Access* | IAM-07 | The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access. | Deels | Deze eis geldt specifiek in relatie tot de eis dat misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school moet worden voorkomen. | Volledig / deels, omdat … |
| **Identity & Access Management** *Trusted Sources* | IAM-08 | Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary. | Deels | Deze eis geldt specifiek in relatie tot de eis dat misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school moet worden voorkomen. | Volledig / deels, omdat … |
| **Identity & Access Management** *User Access Authorization* | IAM-09 | Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user  access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control. | Volledig | Deze eis geldt specifiek in relatie tot de eis dat misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school moet worden voorkomen. | Volledig |
| **Identity & Access Management** *User Access Reviews* | IAM-10 | User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures. | Deels | Deze eis geldt specifiek in relatie tot de eis dat misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school moet worden voorkomen. | Volledig / deels, omdat … |
| **Identity & Access Management** *User Access Revocation* | IAM-11 | Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control. | Deels | Deze eis geldt specifiek in relatie tot de eis dat misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school moet worden voorkomen. | Volledig / deels, omdat … |
| **Identity & Access Management** *User ID Credentials* | IAM-12 | Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:  • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)  • Account credential lifecycle management from instantiation through revocation  • Account credential and/or identity store minimization or re-use when feasible  • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets) | Deels | Deze eis geldt specifiek in relatie tot de eis dat misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school moet worden voorkomen. | Volledig / deels, omdat … |
| **Infrastructure & Virtualization Security** *Audit Logging / Intrusion Detection* | IVS-01 | Higher levels of assurance are required for protection, retention, and lifecyle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach. | Deels | Doel hiervan is vast te stellen dat cloud-leverancier afdoende maatregelen heeft getroffen om per klantomgeving een log of audittrail vast te leggen om het uitvoeren van digitaal en/of forensisch onderzoek en audits te ondersteunen. | Volledig / deels, omdat … |
| **Infrastructure & Virtualization Security** *Production / Non-Production Environments* | IVS-08 | Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties. | Volledig |  | Volledig |
| **Infrastructure & Virtualization Security** *Segmentation* | IVS-09 | Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:  • Established policies and procedures  • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance  • Compliance with legal, statutory and regulatory compliance obligations | Deels | Doel hiervan is dat vermenging van gegevens met die van andere klanten wordt voorkomen.  Doel hiervan is tevens vast te stellen dat cloud-leverancier afdoende maatregelen heeft getroffen om per klantomgeving een log of audittrail vast te leggen om het uitvoeren van digitaal en/of forensisch onderzoek en audits te ondersteunen. | Volledig / deels, omdat … |
| **Security Incident Management, E-Discovery & Cloud Forensics** *Incident Management* | SEF-02 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures. | Deels | Doel hiervan is vast te stellen dat cloud-leverancier afdoende maatregelen heeft getroffen om per klantomgeving een log of audittrail vast te leggen om het uitvoeren van digitaal en/of forensisch onderzoek en audits te ondersteunen. | Volledig / deels, omdat … |
| **Security Incident Management, E-Discovery & Cloud Forensics** *Incident Response Legal Preparation* | SEF-04 | Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation. | Deels | Doel hiervan is vast te stellen dat cloud-leverancier afdoende maatregelen heeft getroffen om per klantomgeving een log of audittrail vast te leggen om het uitvoeren van digitaal en/of forensisch onderzoek en audits te ondersteunen. | Volledig / deels, omdat … |
| **Supply Chain Management, Transparency and Accountability** *Supply Chain Agreements* | STA-05 | Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms:  • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations)  • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships  • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts  • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain)  • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit  report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed  • Expiration of the business relationship and treatment of customer (tenant) data impacted  • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence | Deels |  | Volledig / deels, omdat … |
|  | STA-05a | Specifiek ten aanzien van het eerste punt en de interpretatie van “physical geographical location of hosted services”: de leverancier geeft volledige transparantie over de locatie van de data door aan te geven in welke plaats / land de data zich bevindt. | Volledig | Toegevoegd als specifieke eis vanuit de schema eigenaar. | Volledig |
| **Supply Chain Management, Transparency and Accountability** *Supply Chain Metrics* | STA-07 | Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream).  Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships. | Deels |  | Volledig / deels, omdat … |
| **Supply Chain Management, Transparency and Accountability** *Third Party Audits* | STA-09 | Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements. | Deels |  | Volledig / deels, omdat … |
| **Threat and Vulnerability Management** *Vulnerability / Patch Management* | TVM-02 | Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identfied weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control. | Deels |  | Volledig / deels, omdat … |