

Cloud services

BIO Theme elaboration

October 2021 [version 2.1 final]

The CIP exercises due care in compiling its publications. It is possible that there are omissions, inaccuracies and / or datedness. It is always the responsibility of the reader to assess this himself and, if desired, to correct it if he relies on or uses a CIP publication. The CIP is happy to receive correction requests and suggestions.

© Centre for Information Security and Privacy Protection. The CIP has granted creative commons attribution-sharealike 4.0 international (CC BY-SA 4.0) license for this publication. For more information see: [https://creativecommons.org/licenses/by-sa/4.0/deed.nl.](https://creativecommons.org/licenses/by-sa/4.0/deed.nl)



|  |  |
| --- | --- |
| Title | BIO Theme development Cloud services |
| Date | October 2021 |
| Version | 2.1 final |
| Client | Director CIP |
| Regime | Commented practice |
| Authors | Wiekram Tewarie (UWV) and Jaap van der Veen (CIP) |
| Reviewers | Version 1.0: Professionals from the CIP network and the CIP core team  Version 2.0: CIP Core Team Version 2.1: CIP Core Team |

**Consideration**

CIP products rely on knowledge from professionals from different organizations active in the CIP network, both from the government and the market.

Comments and additions can be reported on [cip](https://www.cip-overheid.nl/contact/) [overheid.nl/contact.](https://www.cip-overheid.nl/contact/)

**Reading guide**

Prior to chapter 3 Policy domain, 4 Implementation domain and 5 Control domain, the core of this document, each BIO Theme elaboration has an introduction with a standard paragraph format.

In addition:

* For the designation of persons, the male form is used (he/him/his) regardless of the sex.
* The controls and measures mentioned in this thematic elaboration are organized in the policy, implementation and control domain, with which they can be addressed to the corresponding officers. These officers are not appointed because this is organization-dependent.
* Attachments are included only for specific information from Chapter 3 Policy Domain, 4 Implementation Domain and/or 5 Control Domain.
* Of best practices (open standards, whether or not accessible with a license), the most current versions are abbreviated, unless the current version is not sufficient.
* For an overview of all best practices, abbreviations and concepts used and a generic explanation of the design of the theme elaborations, see the Structure Guide BIO Theme Elaborations.

**Table of contents**

 Introduction 8

* 1. Objective 9
  2. Set-up BIO Theme elaboration 9
  3. Context relationship between CSC and CSP 10
  4. Context and global structure of cloud services 12

 Policy area 13

 Implementation domain 13

 Control domain 13

* 1. Scope and limitation of cloud services 13
  2. Reason to use cloud services 14
  3. Application BIO Thematic elaboration 15

 Risks related to cloud services 16

* 1. Threats/vulnerabilities 16
  2. CSC-oriented points of attention 17
  3. Security objects for cloud services 18

 Policy area 20

* 1. Objective 20
  2. Risks 20
  3. Objects, controls and measures 20

 B.01 Laws and regulations 21

 B.02 Cloud Security Strategy 22

 B.03 Exit strategy 23

 B.04 Cloud Services Policy 24

 B.05 Transparency 25

 B.06 Risk management 26

 B.07 IT functionality 27

 B.08 Business continuity management 28

 B.09 Privacy and protection of personal data 30

 B.10 Security organisation 31

 B.11 Cloud services architecture 33

 Implementation domain 34

4.1 Objective 34

4.2 Risks 34

4.3 Objects, controls and measures 34

 U.01 Standards for Cloud Services 35

 U.02 Risk assessment 36

 U.03 Business Continuity Services 37

 U.04 Data and Cloud Service Recovery 37

 U.05 Data protection 38

 U.06 Data retention and data destruction 39

 U.07 Data separation 40

 U.08 Separation of services 40

 U.09 Malware Protection 41

 U.10 Access to IT services and data 42

 U.11 Cryptoservices 43

 U.12 Interfaces 44

 U.13 Service Orchestration 45

 U.14 Interoperability and portability 46

 U.15 Logging and monitoring 47

 U.16 Cloud Services Architecture 48

 U.17 Multi-tenant architecture 48

 Control domain 50

5.1 Objective 50

5.2 Risks 50

5.3 Objects, controls and measures 50

 C.01 Service management policy and evaluation guideline 51

 C.02 Risk control 51

 C.03 Compliance and assurance 53

 C.04 Technical vulnerability management 54

 C.05 Security monitoring report 55

 C.06 Management organisation cloud services 56

 Justification 58

 Explanation of objects in the policy area 60

|  |  |  |
| --- | --- | --- |
|  | Explanation of objects in the execution domain | 63 |
|  | Explanation of objects in the control domain | 66 |
|  | Decision tree for risk assessment IV services | 69 |
|  | Summary of the AIVD's position and policy outlook for the BZK | 72 |

**Foreword**

This document contains a frame of reference for the BIO Theme Elaboration Cloud Services, drawn up by the CIP to give government organizations a picture of the most relevant topics when acquiring secure cloud services. The document is intended as a guide, related to the application of the Baseline Information Security Government (BIO) and provides an overview of the elaboration of cloud service objects from the point of view of the CSC (Cloud Service Consumer). To limit the scope of this document, the identified objects are related to general cloud services. This document makes no statements about whether cloud may be used. That choice is subject to the current policy. When choosing cloud, this document can be used in the provisioning.

The BIO has been declared mandatory for the government parties. Due to the rapid developments of cloud services, government parties have a great need for overview and insight into the most crucial components that require attention when acquiring cloud services. All the more so because specific security objects aimed at cloud services are missing from the BIO. This is because the BIO is based on a generic baseline NEN-EN-ISO/IEC 27002:2017 (hereinafter referred to as ISO 27002). In addition to this ISO standard, NEN-EN-ISO/IEC has drawn up a number of implementation frameworks and there are frameworks such as the Cybersecurity Framework (CSW) of the National Institute of Standards and Technology (NIST) and the Cloud Control Matrix (CCM) of cloud Security Alliance (CSA), aimed at the security of cloud services. Also the The Standard of Good Practice (SoGP) 2018, standards of the Bundesamt für Sicherheit in der Informationstechnik (BSI), International Telecommunication Union

(ITU) and the ICT Security Guidelines for Web Applications of the National Cyber Security Centre

(NCSC) contain relevant controls and measures for cloud services. A problem for government parties is that there is no handy overview for a summary of all relevant matters about cloud services, unambiguously related to the BIO. A frequently heard statement is: 'We can no longer see the forest for the trees.'

The writing group has organized various workshops in which various government parties have participated. These parties have made their policy documents available and shared their vision, risks and problems with which they are confronted in practice. With this information and risks associated with cloud services, the disk group has drawn up this document and offered it to the government parties for review. Version 1.1 contains a complete picture of topics that require attention for information security and privacy when acquiring cloud services. The privacy aspects are elaborated in the Cloud Computing and Privacy guide of the Information Security Service (IBD).

For the structuring of this document, the same system has been chosen as for the other BIO Theme Elaborations. The description of the system is briefly presented in this document.

This document is limited to those matters that are important from the CSC to the Cloud Service Provider (CSP), including the interfaces between the CSC and the CSP. Of course, the CSC plays an important role in the information chain and must have its IT management in order. Only then can there be good cooperation between the CSC and the CSP. This fact is an important starting point for stakeholders within the government parties.

Many substantive suggestions and responses have been received. The intention of this document is to help the reader with questions about cloud services. Where improvements can be made, this theme elaboration can be enriched with supplied texts.

# Introduction

The application of cloud [[1]](#footnote-1)computing services, or cloud services for short, is a method for delivering the ICT. Cloud computing is a term that stands for the environment in which CSPs offer functionality or services in the form of a technological black box. This means that cloud services are chosen with a predetermined 'service menu'. The CSC may require that the effective level of security for the CSC concerned is not affected by maintenance and release work for other CSCs.

In general, there are 3 types of IT clouds:

1. Private (with a dedicated infrastructure)

The IT facilities are set up for one CSC and set up with the standards of the CSP.

1. Private/shared (with a fully or partially shared infrastructure)

The IT facilities are accessible to a single CSC and, in order to save costs, they share the underlying infrastructure with other CSCs (e.g. storage and network).

1. Public

The IT facilities are accessible via the Internet. The facilities are usually shared with other CSCs.

The most well-known cloud services are:

* Software as a Service (SaaS)

With SaaS, the application is fully under the control of the service provider.

* Platform as a Service (PaaS)

With PaaS, the platforms and infrastructure are managed by the CSP and not the applications.

* Infrastructure as a Service (IaaS)

With IaaS, only the infrastructure is managed by the CSP and not the applications and platforms.

The application of cloud services fits in with the shift from customized solutions to standard solutions. Some government organizations already use certain types of cloud services. Other organizations are still considering using cloud services. Some have also developed their own cloud policy for this. However, many government organizations are uncertain about:

* acquiring cloud services, because many activities take place out of sight;  storing data with a third party.

Another important point of attention for the government organization is that with an increase in the number of services and service providers (CSPs), the management effort for the customer (CSC) can increase further.

Especially when CSPs engage other CSPs for the services to be provided.

Despite the fact that there are different baselines for cloud services, organizations are wondering which topics[[2]](#footnote-2) they should focus on.

Governments that want to tender IT services should, from their special responsibility, ask themselves the question, which data of employees, citizens and companies can be stored in the (public) cloud and which data must remain within the protection of the government's data centers . Leading in this are the answers[[3]](#footnote-3) of Minister Plasterk to questions from the House of Representatives, May 2014. The positions of the General Intelligence and Security Service (AIVD) and the exploration of Cloud Policy of the National Service and the IBD guidelines for cloud services are also guiding factors in the risk analysis, as elaborated later in this thematic elaboration.

# 1.1 Objective

The aim of this BIO Theme elaboration is to give government organizations a systematic picture of the main objects of cloud services, with which they are supported in a well-balanced use of cloud services and the recognition of the aspects that are important when entering into a cloud service. The focus of this theme elaboration is on availability, integrity, confidentiality and controllability of the data and the reliability of the business processes.

The elaboration of the BIO Theme elaboration Cloud services serves as a guide for the purchase of cloud services. The choice of objects should take place with the context of the organization and risk analysis.

# 1.2 Set up BIO Theme elaboration

The BIO Theme Elaboration Cloud Services is developed along two lines: structure and objects. The structure of the BIO Theme Elaboration Cloud Services consists of a division of policy, implementation and control. The security objects are the substantive topics that, from the point of view of the CSC, are important. By first focusing on the objects, insight is gained into and the relationship between the necessary objects. After the insight gained, controls and underlying criteria for measures are defined for each object. The objects and the associated criteria for measures are structured via the policy, implementation or control domain.

A standard set-up for BIO Theme elaborations is followed. Because of the special character of this theme elaboration, a number of topics have been added for better understanding. This thematic elaboration follows the following set-up:

* Context of the relationship between the CSC and the CSP (see section 1.3)
* Context and overall structure of this thematic elaboration (see section 1.4)
* Scope and limitation of the thematic elaboration (see section 1.5)
* Reason to use cloud services (see section 1.6)
* Threats/vulnerabilities (see section 2.1)
* CSC-oriented considerations (see section 2.2)
* Security objects for cloud services in the policy, execution and control domain (see section 2.3) related to basic elements (see Chapter 3, Chapter 4 and Chapter 5)

# 1.3 Context relationship between CSC and CSP

In the relationship between the CSC and the CSP, there are three issues that organizations always focus on. Reasoned by the CSC, these are:

1. On-going

In terms of performance, does the CSC get the right services on a daily basis? In other words, do the services provided meet price, quality, safety and continuity requirements? So what about the performance?

1. Continuous monitoring (near real time)

Does the CSC get the assurance that it regularly receives the right services in accordance with contracts, business requirements and security requirements? So what about the intended conformity?

1. Compliancy (periodic measurements and evaluations)

Does the CSC get the assurance that it has received the right services in the past period, in accordance with laws and regulations, contracts, business requirements and security requirements? So what about the intended compliance?

When purchasing cloud services, the CSP not only provides the contracted cloud services (ICT service delivery), but also the necessary continuous monitoring, compliance and assurance reports, see Figure 1.

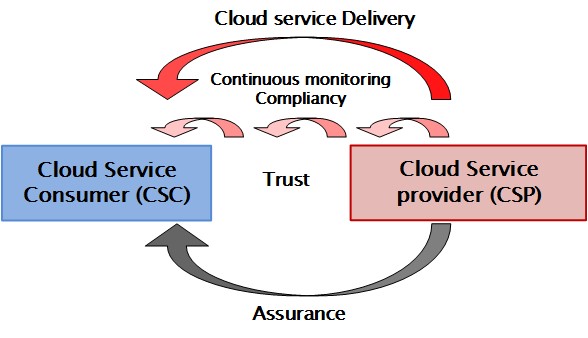


Figure 1: Two deliverables of a CSP

Figure 1 is further elaborated is figure 2.



Figure 2: Two CSP deliverables and CSC requirements/wishes

ICT service delivery

This concerns the public or private cloud services actually requested by the CSC, which must meet certain functional and security requirements. The delivery is accompanied by performance measurements of the services provided and the necessary improvement measures for deliveries and security.

Assurance

This is an annual report based on a survey conducted by a third party. With the assurance report, the CSP provides assurance to the CSC that the services provided have met the contractual requirements. The assurance report is established with a research process in which a frame of reference is used as a means of testing.

Trust

The purchase of cloud services is accompanied by a supported and feasible ICT service contract. However, there will always be aspects that are overlooked in contract formation. A lasting relationship therefore requires a relationship of trust between the CSC and the CSP, otherwise they always run the risk of becoming embroiled in a legal battle.

Both on the CSC side and on the CSP side, different aspects play a role. In the relationship between the CSC and CSP, each party has its own role. The relevant aspects are described below.

CSC (demand side)

Initially, the CSC establishes a Program of Requirements and Wishes (PvEeW) for the cloud services to be acquired and communicates this with the potential CSPs. When the CSC and the chosen CSP reach agreement, cloud services are provided. An important question for public service provision is: 'Is the application of Cloud service permitted in view of the risks accepted by the House of Representatives?' 4. Annex 5 Decision trees for risk assessment IV services includes tools, in the form of decision trees, that allow organisations to decide whether or not to use cloud services.

CSP (delivery side)

With the PvEeW, the CSP creates a functional and technical design. The service is then built, tested and put into production.

These services provided must always comply with the conditions set in the form of legal and business requirements. In addition, the parties agree that the services provided:

* be measurable and predictable;
* be compliant with laws and regulations, business and security requirements of the CSC;  be secure and controlled.

Services provided

These services must always comply with the conditions set in the form of legal and business requirements. In addition, the parties agree that the services provided:

* be measurable and predictable;
* be compliant with laws and regulations, business and security requirements of the CSC;  be secure and controlled.

# 1.4 Context and global structure of cloud services

Figure 2 can be summarized with the policy, implementation and control domain. This is illustrated in Figure 3.

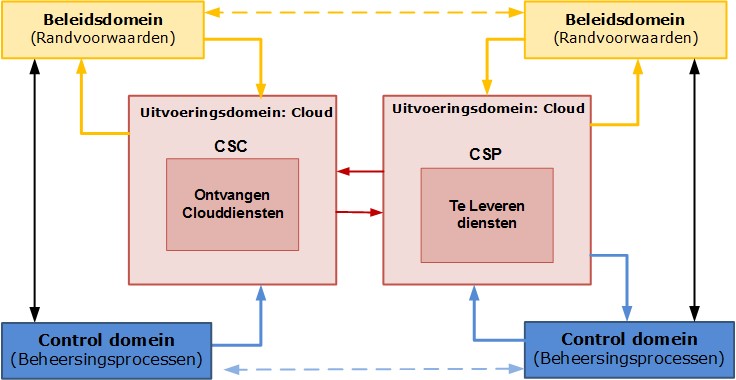


Figure 3: Context CSC and CSP relationship in cloud services acquisition

4 Mail: J.L.M. Kuijpers (AIVD), concerns: Public cloud services and classified information of 9 September 2019.

Concept for alignment: Exploration of cloud policy for the Dutch National Service, version 0.96, dated 12 August 2019, [https://www.earonline.nl/images/earpub/8/86/Quickscan\_BIR2017\_versie\_1.pdf.](https://www.earonline.nl/images/earpub/8/86/Quickscan_BIR2017_versie_1.pdf)

Policy framework: Privacy and information protection 2019, version 1.0 of 20 January 2019.

Letter: Ferd Grapperhaus (Ministry of Justice and Security), Subject: CLOUD act of October 2018.

# Policy area

The CSC draws up a PvE(eW), which is a precondition. For both the CSC and the CSP, the PvE(eW) is a keyboard instrument. They may ask the following questions:

* CSC: have I received the correct service(s)?
* CSP: How can I prove that I have provided the right services?

# Field of execution

Within this domain, it concerns the operational delivery of cloud services. There must be transparency on both sides about the requested and actual deliveries.

# Control domain

Within this domain, the control processes have been set up. For the intended service provision, the control processes on the CSC and CSP side must be aligned.

# 1.5 Scope and limitation of cloud services

The scope of the BIO Theme Elaboration Cloud Services is the set of specific topics (objects) that organizations must pay attention to when purchasing cloud services. This theme elaboration mainly focuses on the 'what' aspect.

It is also important to know along which route organizations can go to the cloud. This is based on migration strategies. The migration strategies will not be described. The so-called 'how' aspect is not elaborated in this document. In practice, different baselines are available for this.

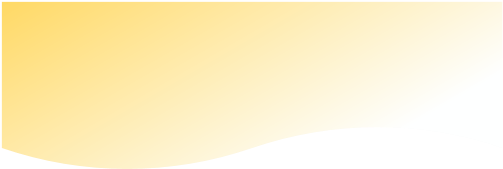
The general requirements of the BIO and ISO 27001 and ISO 27002 remain unaffected. This theme elaboration concerns specific additional objects that are related to cloud services. The measures related to these objects must be realistic and implementable for a CSP.

Privacy aspects: Data Protection Impact Assessments (DPIAs) are not explicitly included in this document because DPIAs from the General Data Protection Regulation (GDPR) must be carried out generically with every project.

The boundary of this document is shown in Figure 4 below.

**Normative level**

**Application level**



Etc

.



BIO Theme

-

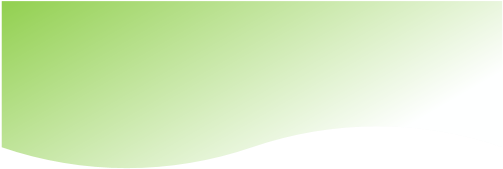
elaboration C



BIO Theme

-

elaboration B

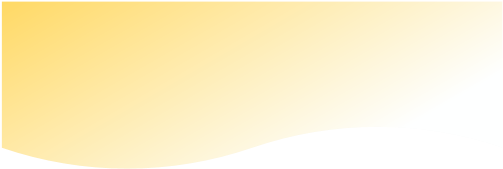


BIO Theme

-

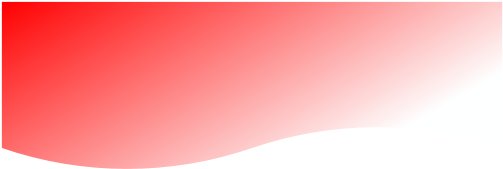
effect

Cloud services



Etc

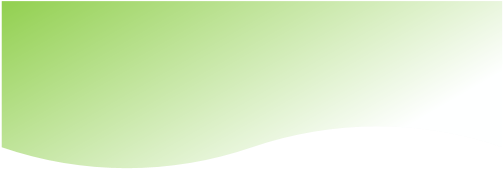
.



Best practices C

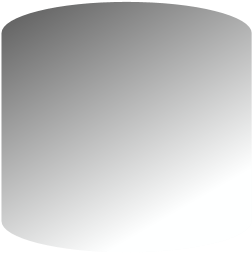
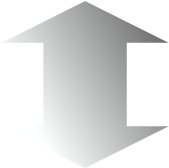
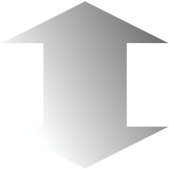


Best practices B



Best practices

Cloud services



Information

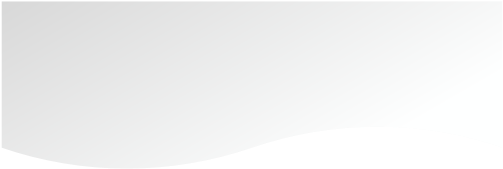
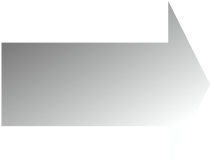
Security Object

Repository

(

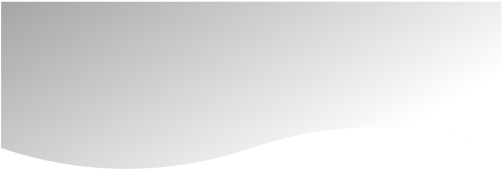
ISOR

)



Etc

.

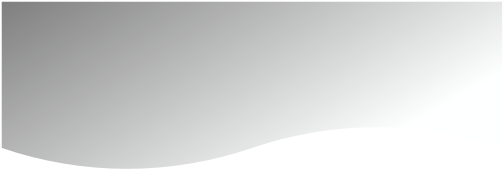


Standard

/

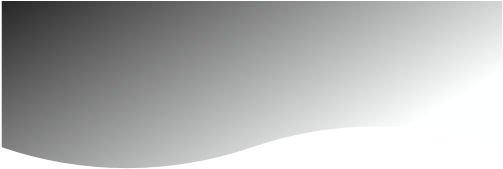
best practice

3

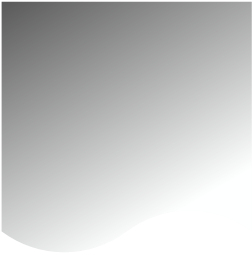
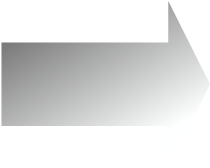


. .ISO

27002



Bio



Referral

-

matrix BIO

–

Bio

-

Practices

Figure 4: Relationship between BIO Theme development Cloud services with adjacent documents

# 1.6 Reason to use cloud services

Some important arguments from governments to use cloud services are:

* the focus on core tasks;
* efficient business operations and reducing overall costs;
* being able to have access to new IT functionality within a short period of time and thus being able to adapt the services to citizens and businesses more quickly to the (changing) needs;
* the assurance of qualified personnel;
* reducing IT complexity in specific situations;
* improving security/availability;
* a revised business strategy and required specific security requirements for processes and data.

In addition, organizations with external factors can consider using cloud services, such as:

* Applicable laws and regulations for:
* a reliable service and the safe handling of data from citizens and companies;
* government policy on data in the cloud and the influence of international treaties;
* the need for a resilient government against cybercrime and state actors;
* Technological developments

The CSC wants to be able to respond to innovations that can lead to more efficient business operations and a reduction in total costs.

# 1.7 Application BIO Thematic elaboration

This document is a tool for choosing a number of cloud objects to address when acquiring cloud services. In the design of this theme elaboration, the topic of cloud was approached functionally and not elaborated on the technical layering of SaaS, PaaS and IaaS. In acquiring cloud services, this document can serve as a tool. This implies the following steps:

* First, determine the context of the case and the type of service to be acquired.
* Next, identify the operational security objects. Consult the objects in the execution domain (see chapter 4 Execution domain).
* After that, identify the conditional objects. Consult the objects in the policy domain (see chapter 3 Policy domain).
* Finally, identify the control objects. Consult the objects in the control domain (see chapter 5 Control domain).
* Include the security objects in the PvEeW for the cloud service, so that these objects can be related by the CSP to the specifications of existing 'standard services' or translated into measures for the specific services offered.

# Risks related to cloud services

Relevant risks associated with cloud services can be grouped into 2 risk groups:

1. Data

Data of the citizen or CSC have been lost or misused.

1. IT services

The reliable service to the citizen and CSC is at risk.

Risks are determined by threats and vulnerabilities and the likelihood that damage will occur as a result. Both threats and vulnerabilities are made concrete below. The 'probability' factor is not calculable for cloud services, but can be estimated by research from the CSC's own context and the developing market of CSPs.

# 2.1 Threats/vulnerabilities[[4]](#footnote-4)

The professional literature mentions various threats/vulnerabilities that a CSC must take into account when acquiring cloud services. After the acquisition, the CSC may be confronted with issues about contracts and performance of the cloud service and about support by and the relationship with the CSP. When identifying objects for cloud services, both the aforementioned risk groups were used as an angle. Table 1 Cloud Computing Vulnerabilities CSA and Greer and Jackson, 2017 and Figure 5 provide an overview of the most important vulnerabilities and common consequences. Appendix 2 Explanation objects in the policy domain, Appendix 3 Explanation objects in the implementation domain and Appendix 4 Explanation objects in the control domain contain detailed elaborations of the threats. Table 1 Cloud Computing Vulnerabilities CSA and Greer and Jackson, 2017 and Figure 5 are limited to the set of CSA and Greer and Jackson.

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Cloud Computing Vulnerabilities CSA and Greer and Jackson, 2017 | | |
| 1 | Data | Data breaches | Data disruptions |
| 2 | Data loss or data leakage | Data loss or data leaks |
| 3 | Cloud services | Account or service traffic hijacking | Hijacking account or service traffic |
| 4 | Denial of service | Denial of service |
| 5 | Malicious insiders | Malicious insiders |
| 6 | Abuse of nefarious use of cloud computing | Misuse or criminal use of cloud computing |
| 7 | Insufficient due diligence | Insufficient due diligence |
| 8 | Shared technology vulnerabilities | Shared technology vulnerabilities |
| 9 | Insecure interfaces and application programming interfaces (APIs) | Insecure interfaces and APIs |
| 10 | Unknown risk profile | Unknown risk profile |
| 11 | Hardware failure | Hardware failure |
| No. | Cloud Computing Vulnerabilities CSA and Greer and Jackson, 2017 | | |
| 12 |  | Nature disasters | Natural disasters |
| 13 | Closure of cloud service | Disconnection of the cloud service |
| 14 | Cloud related malware | Cloud related malware |
| 15 | Inadequate infrastructure design and planning | Inadequate infrastructure design and planning |

Table 1: Cloud Computing Vulnerabilities CSA and Greer and Jackson, 2017

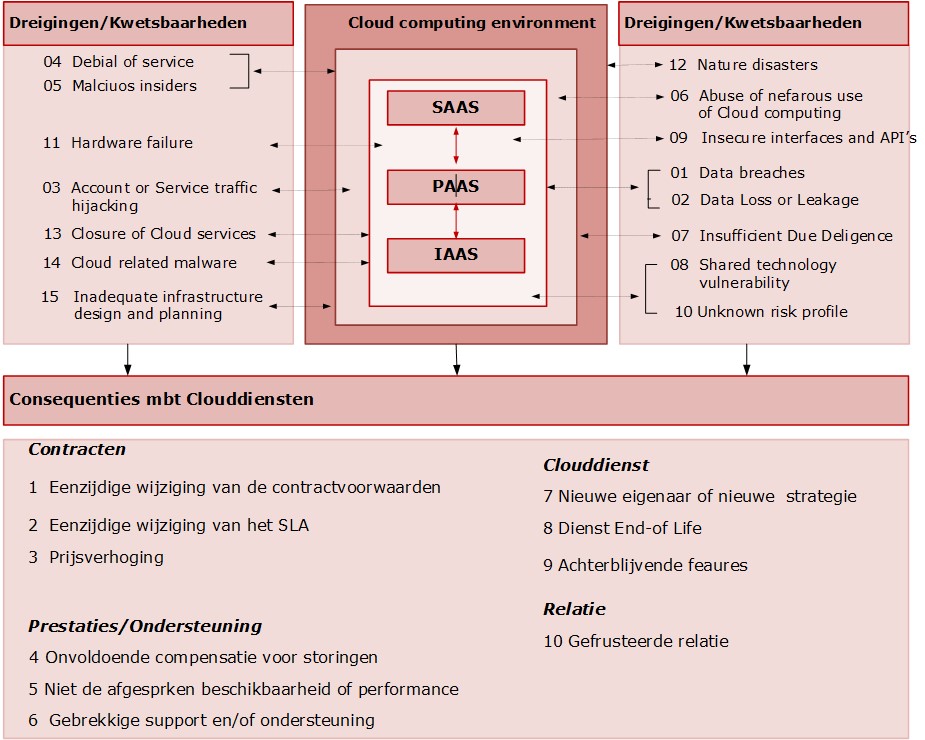


Figure 5: Cloud-related threats and vulnerabilities

# 2.2 CSC-oriented points of attention

For cloud services, the writing group had various conversations with CSCs and CSPs. Also, the writing group has received several policy documents from CSCs. In the discussions and the study of the documents, 2 questions are central:

1. What cloud service issues play a role in CSCs?
2. What are CSCs most concerned about when acquiring cloud services?

The identified issues are broadly divided into a number of generic topics: policy and strategy, processes/functions (technical and organizational), interactions, infrastructure and structure.

(architecture and organizational structure). Figure 6 gives an overview of the classified topics.

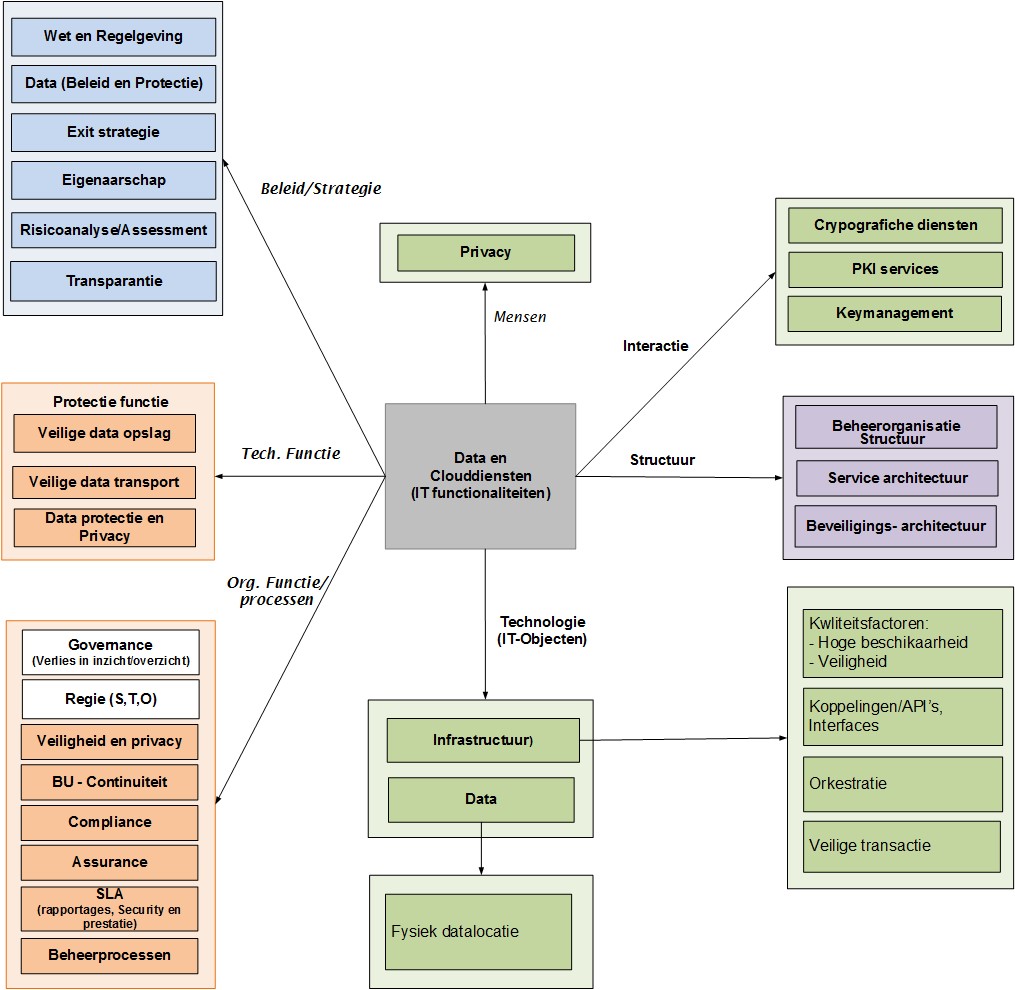


Figure 6: CSC-oriented points of interest

# 2.3 Security objects for cloud services

Objects are identified with research questions and risk areas. The objects aim to mitigate risks. They are derived from the general security requirements: availability, integrity, confidentiality and auditability which are then classified in the policy, implementation and control domain. The questions that play a role from the point of view of these domains are:

* Which peripheral elements play a role in the design of the cloud services and what is the consequence of the absence of one or more of these elements?
* Which elements play a role in the design of the cloud services and what is the consequence of the absence of one or more of these elements?
* Which elements play a role in the control of cloud services and what is the consequence of the absence of one or more of these elements?

The contextual analysis shows that several topics do not appear in the BIO. For the subjects for which the BIO has not formulated a control, controls from other baselines have been adopted.

# Policy area

# 3.1 Objective

The purpose of the policy domain is to identify the conditional elements that are preconditions for setting up, securing and controlling cloud services.

# 3.2 Risks

If the right policy aspects for the design and maintenance of cloud services are lacking, there is a risk that insufficient guidance will be given to the safe design and operation of these services. As a result, the information provision of the organization as a whole is endangered and there is a real chance that data leaks will occur. Annex 2 Explanation of objects in the policy domain indicates for each focus area which risks are relevant.

# 3.3 Objects, controls and measures

The topics that play a role specifically for cloud services in the policy domain are shown in Figure 7. If an object block is coloured yellow, the corresponding control occurs in the BIO. If it concerns a white marked object block, the BIO has not defined a control, but this object is necessary for this BIO Theme elaboration.

**Angle**

Intention

Function

Behavior

Structure

**Law**

**-**

**and regulations**

Law

B

.

01

**Cloud Security Strategy**

Strategy

B

.

02

**Exit**

**-**

**strategy**

Strategy

B

.

03

**Cloud Services Policy**

(

Operational

)

policy

B

.

04

**Transparency**

(

Operational

)

policy

B

.

05

**Risk management**

Assessment

B

.

06

**IT**

**-**

**Functionality**

Technical function

B

.

07

**Business continuity**

**-**

**management**

Lawsuit

B

.

08

**Privacy and protection**

**personal data**

Quality factor

B

.

09

**Security organization**

IT

-

Organisational structure

B

.

10

**Cloud services architecture**

IT

-

architecture

B

.

11

Figure 7: Overview of objects for cloud services in the policy domain

For each specific security object, the control (main standard) and measures (sub-standards) are described in the following paragraphs.

# B.01 Laws and regulations

### Object definition

Includes applicable national and international laws and regulations applicable to cloud services.

### Object explanation

National and international laws and regulations that apply to cloud services, such as the GDPR in particular, relate to the organizational and technical measures to be taken, such as awareness, people and physical resources. The CSP will translate these into specific requirements for cloud components.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Preventing violations of any law, legal and regulatory or contractual obligations and security requirements. | | |
| Risk | Damage due to legal liability. | | |
| Control | All relevant **legal, statutory, regulatory**, **contractual requirements** and the **CSP's approach** to meeting these requirements should be explicitly identified, documented and kept up to date for each cloud service and the organisation. | | BIO 2019: 18.1.1 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Legal, statutory, regulatory requirements | 1. | The CSP informs the CSC which laws and regulations apply to cloud services. | ISO 27017 2015: 18.1.1 |
| 2. | The CSP identifies its own relevant legal requirements (such as GCU requirements and encryption application) in order to protect personal data. | ISO 27017 2015: 18.1.1 |
| 3. | The requirements applicable to the CSC arising from laws and regulations have been identified, especially with regard to geographically distributed processing, storage and communications for which different legislation exists, such as measures arising from the GDPR. | ISO 27017 2015: 18.1.1 |
| 4. | The CSP provides the CSC with assurance (evidence-based compliancy reporting) about (compliance with) the applicable legal and contractual requirements. | ISO 27017 2015: 18.1.1 |
| Contractual requirements | 5. | For cloud services, in order to be able to meet the legal and contractual requirements, specific measures have been taken and responsibilities have been appointed. | ISO 27002 2017: 18.1.1 |
| Approach | 6. | In order to be able to meet the requirements of the CSC, the CSP has adopted all laws and regulations that apply to it for the provision of cloud services. | ISO 27002 2017: 18.1.1 |

# B.02 Cloud Security Strategy

### Object definition

Includes the CSP's plan of action that will enable it to achieve its security objectives for cloud service delivery.

### Object explanation

Organizations are faced with the question of which cloud services they should acquire and where and how they can use them safely. To this end, the IT stakeholders of CSCs need to develop a decision framework, with which the possible scenarios can be systematically examined. This framework focuses in particular on types of applications and technical characteristics. A strategy includes statements about the objectives in the deployment of the cloud services that the organization wants to pursue and the ways in which this should take place.

In order to serve CSCs, the CSP has developed a cloud security strategy from its own point of view. This strategy gives the CSCs sufficient opportunities to relate their cloud strategy to the strategy of a specific CSP. This offers the CSC the opportunity to adjust its choices or to impose additional requirements on the CSP.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Determining in advance what the CSC wants to pursue with the security of cloud services and how that will be achieved. | | |
| Risk | Not having an agreed guideline/global approach to securing cloud services. | | |
| Control | The CSP should have developed a **cloud security strategy** that **is consistent** with the strategic objective of the CSP and that demonstrably supports information security. | | SoGP 2018: SG2.1 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Cloud Security Strategy | 1. | The CSP's cloud security strategy outlines how it supports the business objectives of CSC(s) by describing, among other things:   * a balanced set of security measures, focusing on risk management; * how (functional) cloud security achieves resilience to high impact incidents. | SoGP 2018: SG2.1.2 |
| 2. | The CSP's cloud security strategy:   * indicates, inter alia, how it protects CSCs from threats; * pays attention to the current security context of the CSP, including skills, capabilities and information security function. | SoGP 2018: SG2.1.3  SoGP 2018: SG2.1.6 |
| Related | 3. | The coherence of security measures of the CSP supports the achievement of the business goals of the CSC. It indicates:   * to what extent the CSP's cloud security strategy is aligned with the CSC's organization-wide objectives; * how the CSC's cloud security governance is supported by the CSP's management; * that the cloud services are documented and reviewed regularly. | SoGP 2018: SG2.1.1 |

# B.03 Exit strategy

### Object definition

Includes the plan of action for the termination of service with an existing CSP, as well as being able to transfer data and IT services to a new CSP.

### Object explanation

Because no contract lasts forever, a CSC must be able to say goodbye to the CSP at some point. If no binding agreements have been made about saying goodbye when the cloud service is shut down, it can become very difficult or expensive to migrate data to another CSP.

The organization must take into account a 'vendor lock-in'. It is therefore important to develop an exit strategy even before entering into an agreement with a CSP. The exit strategy should include the conditions for data changes. It is also possible to include the practical elaboration of the exit strategy in a Service Level Agreement (SLA).

For various reasons, a CSC may want to terminate the services of the CSP. On the one hand, in a planned manner, such as at the end of the contract term, otherwise for various reasons, such as non-compliance with the agreements, taking over the CSP by another organisation. The non-planned termination is related to the exit strategy, which is part of business continuity management (BCM). The planned termination of the service provision affects the transition and is part of Service Level Management (SLM).

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Determining in advance what the organization wants to pursue when terminating cloud services and how that will be achieved. | | |
| Risk | Failure to have an agreed guidance/global approach in the event of termination of supplier contracts. | | |
| Control | The cloud services agreement between the CSP and CSC should include an exit strategy that includes both a number of **provisions[[5]](#footnote-5)** on exit and a number of **conditions6** that may give rise to an exit. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Provisions | 1. | The CSC lays down a number of provisions about the exit scheme in the agreement, such as:   * The exit provision applies both at the end of the agreement and for valid reasons submitted by the CSC (see conformity indicator Conditions). * The agreement (and any processing agreement) continues until the exit scheme has been fully implemented. * The notice period gives sufficient time to be able to migrate. * Data and configuration data (if relevant) may only be deleted after successful migration. * An independent party checks and determines that all data has been migrated. * The exit scheme will be adjusted/filled in differently if the software used for the cloud service has changed. | BSI C5 2020: PI-02 |
| Conditions | 2. | The CSC may decide to exit outside the expiry of the contract period if there are aspects related to:   * Contracts: * are not available for agreed performance; * unilateral amendment by the CSP of the SLA;  price increase. * Performance/Support provided: * insufficient compensation for malfunctions; * failure to deliver the agreed availability or performance;  lack of support. * Cloud service(s): * new owner or new strategy; * end-of-life of cloud service(s);  omitted features. | CIP network |

# B.04 Cloud Services Policy

### Object definition

Includes the outcome of a decision on which security goals for cloud services should be achieved.

### Object explanation

The topic of cloud services should be a specific part of the CSC's information security policy. A CSC can also opt for a specific cloud services policy, whereby the general information security policy specifically for cloud services is elaborated or filled in in the information security section. The policy will have to contain starting points on how, within what time frame and with what means cloud services should achieve the objectives. This policy will also have to pay attention to archiving policies, cryptography policies, certifications and declarations.

In order to operate the CSC, the CSP will have developed a cloud security policy from its own point of view. This policy gives the CSC the opportunity to relate its cloud policy to the strategy of the CSP and offers the CSC the opportunity to adjust the choices or to set additional requirements for the CSP.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Mastering cloud services; that cloud services contribute to the delivery of products with which the organization can achieve its objectives. | | |
| Risk | Insufficient ability to direct efforts for cloud services, as a result of which they do not or insufficiently contribute to the objectives of the organization. | | |
| Control | The CSP should extend its information security policy with a **cloud security policy** to address the features and use of cloud services. | | ISO 27017 2015: 5.1.1 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Cloud Security Policy | 1. | The cloud security policy includes:   * Organic oriented measures: * information security requirements applicable to the design and deployment of cloud services; * communication with the CSC in relation to and during changes; * communication of security breaches and sharing of information; * guidelines for the support of (forensic) investigations; * compliance measures on laws and regulations. * Technically oriented measures: * multi-tenancy and isolation of the CSC; * access procedures, e.g. strong authentication for access to cloud services; * access to and protection of the data of the CSC; * lifecycle management of CSC accounts; * risks related to unauthorized insiders; * virtualization security; * security architecture and measures to protect data, applications and infrastructure. | ISO 27017 2015: 5.1.1 |

# B.05 Transparency

### Object definition

Includes the visibility of the relationships and coherence of organization, technology and contracts thereof between CSC and CSP.

A clear communication, with which the CSP gives the responsible officers within the CSC and CSP insight into the status of the implementation and the functioning of the cloud services. Transparency is an important item in the relationship between the CSC and CSP, which is supported by the cloud services architecture. In it, the CSP describes the relationships between the components of the cloud services (how they are linked to each other). It provides insight and overview about ICT components and their interrelationships. The cloud services architecture shows how the components support the business processes of the CSC.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Provide the responsible officers within the CSC and CSP with insight into the status of the implementation and functioning of cloud services. | | |
| Risk | The CSP can provide a service that is not or incompletely tailored to the needs of the CSC. | | |
| Control | The CSP provides the CSC with a **system description** in which the cloud services are clearly and transparently specified and in which the **jurisdiction**, **research possibilities** and **certificates** are addressed. | | BSI C5 2020: BC-01  BSI C5 2020: BC-05  BSI C5 2020: BC-06 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| System-  description | 1. | The system description includes the following aspects:   * types and scope of cloud services displayed with SLAs; * principles, procedures and measures to reflect development and operationalisation; * description of the infrastructure components that are part of the development and operationalisation of cloud services; * how security incidents are handled; * roles and responsibilities of the CSP and CSC, including the obligation to cooperate; * (which) parts of the cloud services and/or functions have been assigned or outsourced to sub-contractors. | BSI C5 2020: 3.4.4.1 |
| Jurisdiction | 2. | The SLA or system description provides for a specification of jurisdiction over data storage, processing and backup location, even if it (or parts thereof) is outsourced to subcontractors. | BSI C5 2020: BC-01 |
| Research opportunities | 3. | The SLA or system description provides a specification for publication requirements and research opportunities. | CIP network |
| Certificates | 4. | The SLA or system description provides a specification on the availability of valid certificates. | BSI C5 2020: BC-06 |

# B.06 Risk management

### Object definition

Concerns a control process for a methodical approach to security risks.

Cloud services are constantly subject to threats, weaknesses and risks. It is important to set up a risk management process and to identify the responsibilities for this, whereby a risk management approach (method) and the scope to be used are determined. This involves identifying and quantifying risks to cloud services and establishing control measures. Control measures are the activities that limit the chance of occurrence and/or the consequences of an incident.

The risk management process is part of an Information Security Management System

(ISMS), as described in the ISO 27001 Management Systems for Information Security - Requirements and is elaborated in the ISO 27005 Information security risk management.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | To enable persons responsible for cloud services to effectively and in a timely manner identify, evaluate and determine the treatment necessary to keep these risks within acceptable limits. | | |
| Risk | The security measures taken are beyond the acceptable limits. The cloud services are under- or over-secure. | | |
| Control | The CSP should have established and maintained the organization and **responsibilities** for the **risk management process** for the security of cloud services. | | ISO 27005 2018: 7.4 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Responsibilities | 1. | The responsibilities of the CSP include:   * developing the information security risk management process that focuses on the CSP's environment; * identifying stakeholder analyses; * defining the roles and responsibilities of internal and external parties; * establishing the required relationships between the own organization and stakeholders and the relationship with the high-level risk management function and with relevant projects or activities. | ISO 27005 2018: 7.4 |
| 2. | The organization of the risk management process has been approved by managers of the CSP. | ISO 27005 2018: 7.4 |
| Risk management process | 3. | The risk management process is systematically described with attention to policies, procedures and guidelines for activities about communicating, advising, determining the context of investigations, treating, monitoring, reviewing, recording and reporting risks. | ISO 31000 2019: 6.1 |

# B.07 IT functionality

### Object definition

Includes application features provided by cloud services.

IT services provide functionalities with technology related to the Internet. Examples of such services are: generic services, such as: application services (SaaS), storage services, Cloud Virtual Private Server, infrastructure, Global Positioning System (GPS) information service, but also specific services, such as: GPS Customs services. These cloud services can also be exposed to threats. That is why these IT services must meet the required security aspects.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Ensure that IT functionalities meet the required security aspects. | | |
| Risk | IT functionalities are a weak link in security. | | |
| Control | **IT functionalities** should be provided from a **robust and secure system chain** from the CSP to the CSC. | | SoGP 2018: BC1.3 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| IT functionalities | 1. | For the security of IT functionalities (processing, storage, transport and retrieval of information), availability, integrity and confidentiality measures have been taken. | CIP network |
| 2. | Technical security measures in the form of strong access security, encryption and data analysis methods have been taken against infrastructure protection. | ITU-T FG Cloud TR Part 5  2012: 8.5 |
| 3. | In order to provide secure cloud services, the IT infrastructure is continuously monitored and controlled to protect against threats. | ITU-T FG Cloud TR Part 5  2012: 8.8 |
| Robust and secure system chain | 4. | The infrastructure is set up with reliable hardware and software components. | SoGP 2018: BC1.3.1 |
| 5. | There are documented standards and procedures to deal with advanced cyberattacks. | SoGP 2018: TM1.5.1 |

# B.08 Business continuity management

### Object definition

Concerns a control process for activities that protect organizations from disruptive events.

### Object explanation

BCM describes the requirements for a management system to protect organizations from disruptive events, to reduce the likelihood of these events and to ensure that an organization can fully recover from them. Among other things, the organization will focus on the development, implementation and maintenance of policies, strategies and programs in order to be able to control the effects of potentially disruptive events on the organization. In the cloud environment, the CSC trusts the CSP as a third party. The CSP will need to give the CSC assurance on asset and resource documentation, incident management, business continuity, recovery plans, policies, management processes and backup management.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Resuming critical business processes within critical timeframes. | | |
| Risk | The failure to respond effectively to the manifestness of major malfunctions and (un)known risks (disaster/emergency situations). The threat is not stopped as soon as possible and the consequential damage is not limited as much as possible. | | |
| Control | The CSP should have adequately organized its BCM process, addressing the following aspects: **responsibility for BCM**, **policies and procedures**, **business continuity planning**, **verification and updating**, and **computer centers**. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Responsibility for  Bcm | 1. | The CSP has appointed a process owner for the BCM process and has given him responsibility for shaping BCM and compliancy with the outlined policy. | BSI C5 2020: BCM-01 |
| 2. | The person responsible for BCM ensures that adequate resources are available to carry out an effective BCM process. | BSI C5 2020: BCM-01 |
| 3. | The management of the CSP commits to the established BCM requirements. | BSI C5 2020: BCM-01 |
| 4. | The BCM policy and policy for business impact analyses have been established and communicated. | BSI C5 2020: BCM-02 |
| Policies and procedures | 5. | Policies and procedures for determining the impact of cloud service outages have been documented and communicated, paying attention to:   * availability of data and functionality in relation to vendor lock-in and transition to other CSPs or exit strategy (for the possible risk-based scenarios); * identification of critical products and services; * identifications of dependencies, processes, and business partners and third parties; * consequences of disruptions; * estimates of resources required for recovery. | BSI C5 2020: BCM-02 |
| Business continuity planning | 6. | The CSP has a documented framework for business continuity planning that addresses, among other things:   * defining the scope taking into account the dependencies; * accessibility of these plans for responsible officials; * assigning a person responsible for the review, update and approval; * defining communication channels; * recovery procedures; * method for implementing the BCM plan; * continuous improvement process of the BCM plan;  relationships with security incidents. | BSI C5 2020: BCM-03 |
| Verification and updating | 7. | Business impact analyses and continuity plans are verified, updated and regularly tested. | BSI C5 2020: BCM-04 |
| 8. | During testing, attention is paid to the influence of CSCs (tenants) and third parties. | BSI C5 2020: BCM-04 |
| Computer Centers | 9. | The facilities of the computer centers are secured and are monitored (monitored), maintained and regularly tested. | CIP network |

# B.09 Privacy and protection of personal data

### Object definition

Privacy concerns personal freedom, the right to be left alone. Protection of personal data concerns the process of protecting this data.

### Object explanation

The data to which threats and privacy-protecting rules are related. Both data and privacy protection must meet the security requirements set by law and by the CSC. Data and privacy includes the inventory and classification of data according to a specific labeling policy. Data protection takes place in three states of data: at rest, in processing and on transport. Data in devices can be controlled by focusing on three moments: deletion, transport and movement. Data can be related to company data and personal data. The necessary measures are taken to protect personal data. Data security can be approached from different aspects. Figure 8 identifies the main aspects.

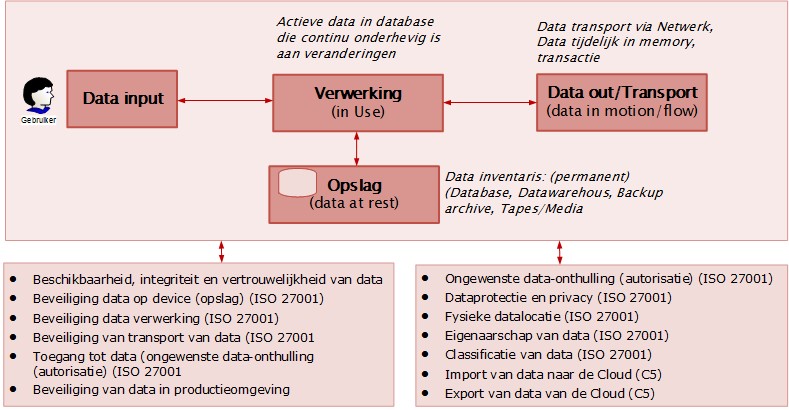


Figure 8: Data in different operating states

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Obtaining a thorough set of security measures. | | |
| Risk | The company and personal data is under-protected. | | |
| Control | In order to protect company and personal data, the CSP should have security measures in place from different dimensions: **security aspects and stages**, **access and privacy**, **classification/labelling**, **ownership** and **location**. | | ITU-T FG Cloud TR Part 5  2012: 8.5 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Security aspects and stages | 1. | Availability, integrity and confidentiality measures have been taken for the storage, processing and transport of data. | NIST CFW 2018: PR. DS-1  NIST CFW 2018: PR. DS-2 |
| Access and privacy | 2. | To protect data and privacy, security measures have been taken, in the form of data analysis, DPIA, strong access security and encryption. | CIP network |
| Classification/ labelling | 3. | Data and resources in which/on which data is contained are assigned a classification by the controller based on the data type, value, sensitivity and critical content for the organization. | CSA CCM 2019: DSI-01 |
| 4. | Data related to e-commerce and sent over public networks is adequately classified and protected against fraud, unauthorized access and data corruption. | CSA CCM 2019: DSI-03 |
| 5. | The CSP applies a uniform classification for information and resources relevant to the development and provision of cloud services. | BSI C5 2020: AM-06 |
| Ownership | 6. | Ownership of resources that are part of cloud services has been established. | CIP network |
| 7. | The agreement between the CSP and the CSC establishes ownership of the use, return and deletion of data (data objects) and the physical means containing data when terminating the cloud service. | ISO 19086-1 2016:  10.7.1.2 |
| Location | 8. | The CSP specifies and documents at which location (in which country/region) the data is stored. | ISO 27018 2020: A.12.1 |

# B.10 Security organisation

### Object definition

Concerns a targeted pooling of knowledge and skills between persons with tasks, responsibilities and powers for the relational coherence of security.

### Object explanation

The security feature includes the formalized tasks and responsibilities for cloud services. Within the security function, it is arranged that contact is maintained with those responsible within the CSC organization when there are security incidents.

The security organization of the CSP ensures/supervises compliance with the information security policy, cloud services policy and other related policies. Although a 'Security function' can be considered as an independent object, simplicity has been chosen to integrate it with the organization in this BIO Theme elaboration.

Where necessary, the security organization intervenes. The tasks, responsibilities, powers and resources that the security organization has for this purpose are explicitly named and determined in advance, in relation to the CSC. It must also be established in advance how the reporting lines between the security managers are organized.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | To establish a defined, approved, understood and working structure for the design, existence and operation management of information security within the CSP. | | |
| Risk | The ineffective expression of the cloud services policy. | | |
| Control | The CSP should have appointed a **security function** and set up a security organisation, which sets out the **organisational position, the tasks, responsibilities and powers** of the **officers** involved and the **reporting lines**. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Security function | 1. | The security function, which is led by a Chief Security Officer (CSO), supports the CSP in establishing and promoting cloud security policies by:   * developing and maintaining a security strategy and policy; * developing security standards, procedures and guidelines; * defining a set of security services; * coordinating security throughout the organization; * monitoring the effectiveness of cloud service regulations; * providing oversight of and conducting investigations into security services. | SoGP 2018: SM2.1.2 |
| 2. | The security feature provides proactive support for:   * cloud risk assessment activities; * classifying information and systems; * use of encryption; * securing related projects; * developing business continuity program and security audits. | SoGP 2018: SM2.1.4 |
| Organisational position | 3. | The CSP has given the information security organization a formal position within the entire organization. | CIP network |
| Tasks, responsibilities and powers | 4. | The CSP has described and assigned information security responsibilities for defining, coordinating and evaluating to specific officers. | BIO 2019: 6.1.1 |
| 5. | The tasks, responsibilities and powers are laid down in an authorisation matrix. | CIP network |
| Officials | 6. | The most important officers (stakeholders) for information security have been appointed and the mutual relationships have been made transparent with an organizational chart. | CIP network |
| Reporting-  lines | 7. | The accountability and reporting lines between the officials concerned have been established. | ~trust services |
| 8. | The type, frequency and requirements for the substantive reports have been determined. | ~trust services |

# B.11 Cloud services architecture

### Object definition

Concerns a model-based description of a technical and organizational coherence, in which the

CSP establishes the relationships between the components of the cloud services and the support of the CSC.

### Object explanation

In the cloud services architecture, the CSP records how the IT functionalities are related to each other and how they are interrelated. The cloud services architecture shows how IT functionalities support the business processes of the CSC.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Offering a cloud service landscape and thereby giving direction to the cloud service and guaranteeing a reliable operation of the cloud service. | | |
| Risk | Have no or insufficient control over the cloud services. The operation of the cloud services is unreliable. | | |
| Control | The CSP has established an up-to-date architecture that provides a **framework** for the interrelationships **and dependencies** of the  IT functionalities. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Framework | 1. | The framework includes the following aspects:   * security policy of the CSP with principles and laws and regulations; * Functional; types and scope of cloud services; * zoning model for separation between CSCs; * trust framework (agreements and measures to promote the relationship of trust); * SLAs and valid certificates;  risk management. | CIP network |
| Coherence and dependencies | 2. | The interrelationship between IT functionalities involved, used and maintained cloud services is identified and described. | NCSC 2015: B.06.05 |

# Field of execution

# 4.1 Objective

The purpose of the implementation domain of cloud services is to ensure that, in accordance with specific policy principles, a reliable and secure service is provided and that the operation meets the requirements set by the CSC.

# 4.2 Risks

If, when entering into or during the application of cloud services, adequate security functions, naming these functions in the contracts and the control of compliance with the agreements are missing, then continuity risks arise and possibly data leaks or misuse of sensitive data. Appendix 3 Explanation of objects in the implementation domain indicates for each focus area which risks are relevant.

# 4.3 Objects, controls and measures

Figure 9 shows the objects that play a role specifically for the execution domain. If an object block is coloured orange, the corresponding control appears in the BIO. If it concerns a white marked object block, the BIO has not defined a control, but this object is necessary for this BIO Theme elaboration.



Figure 9: Overview of objects for cloud services in the execution domain

# U.01 Standards for Cloud Services

### Object definition

Includes a set of documents with recognized agreements, specifications, or criteria that support the conditioning, provisioning, and control of cloud services.

### Object explanation

The application of (open) industry standards by CSPs, especially at the interface with the CSC, makes it possible for data and IT functionalities, offered via cloud services, to be delivered to the CSC more easily, reliably and securely. Thanks to these standards , IT functionalities and data can easily be transferred to a new CSP after an agreed termination of the contract between the CSC and the CSP.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Achieving the necessary coordination of activities for the design, provision of services and control of cloud services. | | |
| Risk | Generic risks are not or insufficiently mitigated. | |  |
| Control | The CSP applies demonstrably relevant **national standards** and **international standards** for the design and operation of the services and the interaction with the CSC. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| National standards | 1. | The CSP makes its services transparent, so that the CSC can demonstrably meet the bio and 'apply or explain' standards that are mandatory for it. | CIP network |
| International standards | 2. | The CSP takes security measures based on international standards, such as:   * BSI-Standard 200-4 Business Continuity Management * ITU-T FG Cloud TR 1.0 2012 Part 5 Cloud security * NEN-ISO/IEC 17788 Overview and vocabulary * NEN-ISO/IEC 17789 Reference architecture * NEN-ISO/IEC 19941 Interoperability and portability * NEN-ISO/IEC 19944 Cloud services and devices * NEN-ISO/IEC 27017 Code of practice for cloud services * NEN-ISO/IEC 27018 Personally identifiable information (PII) in public clouds * NIST SP 800-145 Definition of Cloud Computing | ISO 27017 2015: 2.1 |

# U.02 Risk assessment

### Object definition

Concerns an investigation into the possibility of a certain risk occurring and into the harmful effects if the risk occurs.

### Object explanation

Risk assessment is part of risk management and involves identifying threats and vulnerabilities. The risk management process is part of the management system for information security, as described in the ISO 27001 'Management systems for information security' and risk management is elaborated in the ISO 27005 'Information security risk management'.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Identify potential risks that may affect cloud services and determine how the risks can be managed or reduced to an acceptable level. | | |
| Risk | Have no or insufficient insight into the risks that affect cloud services. | | |
| Control | The CSP should carry out a risk assessment consisting of a **risk analysis** and **risk assessment** with the criteria and objective for cloud services of the CSP. | | ISO 27005 2018: 8.1 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Risk analysis | 1. | The risks to the resources covered by the scope of cloud services are identified, valued (quantified or qualified) and described by risk assessment criteria and objectives of the CSP. | ISO 27005 2018: 8.1 |
| Risk assessment | 2. | The identified risks are evaluated with risk acceptance criteria. | ISO 27005 2018: 8.4 |

# U.03 Business Continuity Services

### Object definition

Includes measures that ensure the recovery of the data and the service during normal operation and in the event of occurring calamities, within the agreed maximum downtime, whereby data loss is prevented.

### Object explanation

Because the CSC relies heavily on the CSP and external factors for its business operations, business continuity services are essential. Business continuity services include the package of measures, which ensures both for normal operation (with Quality of Service (QoS)) and for situations of calamities, such as natural disasters, within the agreed maximum downtime Recovery Time Objective (RTO), the recovery of data and the critical service, whereby data loss is limited to the agreed maximum data loss. Well-known continuity measures are redundancy, disaster recovery and periodically demonstrating that recovery functions work.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | During normal operation and in the event of frequent calamities, ensure the recovery of the data and the service within the agreed maximum downtime, whereby data loss is prevented. | | |
| Risk | Data in the cloud is not available for longer than the agreed maximum downtime. | | |
| Control | Information processing facilities should be implemented with sufficient **redundancy** to meet **continuity requirements** . | | BIO 2019: 17.2.1 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Redundancy | 1. | The agreed continuity is guaranteed by sufficiently logical or physically multiple system functions. | ISO 27002 2017: 17.2.1 |
| Continuity requirements | 2. | The continuity requirements for cloud services agreed with the CSC organization are ensured by specific measures described in the system architecture. | ISO 27002 2017: 17.2.1 |

# U.04 Data and Cloud Service Recovery

### Object definition

Concerns the recovery of CSC data and the provision of services after interruptions or destruction of data and IT resources.

### Object explanation

One of the most important requirements for the reliability of cloud services is the recoverability of the data and/or the service after interruption or destruction of the data and assets due to malfunctions or calamities: disaster recovery.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Ensuring that cloud services and the data can be restored, within the agreed period, after interruption of the service and / or destruction of the data. | | |
| Risk | Exceeding the maximum data loss and/or downtime. | | |
| Control | The **recovery function** of the data and cloud services, aimed at supporting business processes, should be facilitated with infrastructure and IT services, which are robust and periodically **tested**. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Restore function | 1. | In the event of calamities, the data and cloud services are restored within the agreed period and maximum data loss and made available to the CSC. | SoGP 2018: BC1.3.9 |
| 2. | The continuous process of recoverable protection of data is monitored. | CIP network |
| Tested | 3. | The adequate functioning of recovery functions is periodically tested by qualified personnel and the results are shared with the CSC. | BSI C5 2020: BCM-04 |

# U.05 Data protection

**Object definition**

Concerns the protection of the confidentiality and integrity of CSC data.

### Object explanation

Data 'on transport' are company data that is exchanged with the CSP via the cloud service. Data 'in processing' refers to data that is processed. Data 'at rest' concerns data that has been stored for a short or longer period of time (with the CSP). The government imposes strict requirements on these three situations.

For the application of public cloud services, a Secretary General grants prior permission for the processing of Basic Security Level (BBN) 2-classified information in the public cloud. This requirement also applies to personal data.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Ensuring that BBN2 or higher classified data is protected with cryptographic measures and complies with Dutch legislation. | | |
| Risk | Data with the classification BBN2 or higher is insufficiently protected. | | |
| Control | Data ('on transport', 'in processing' and 'at rest') with the classification BBN2 or higher should be protected with **cryptographic measures** and comply with Dutch legislation. | | ISO 27040 2016: 6.3.2.1 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Cryptographic measures | 1. | Data transport is secured with cryptography to the latest state of the art (in accordance with the Forum for Standardization), whereby the key management is carried out by the CSC itself if possible. | CIP network |
| 2. | Data stored in the cloud service shall be protected to the latest state of the art with encryption and with a key length sufficient at least for the purpose, whereby the key management is not purchased as a cloud service if possible and is carried out by the CSC itself. | CIP network |

# U.06 Data retention and data destruction

**Object definition**

Includes the storage and controlled erasure or destruction of CSC data.

### Object explanation

Data retention concerns the sustainable and technology-independent storage and archiving of data, whereby the integrity and readability of the data is not compromised during the entire retention period. (Personal) data must be deleted or destroyed as soon as they are no longer required or at the end of the retention period. After the retention period, the data must be returned to the CSC, to another CSP to be determined by the CSC or to be deleted/destroyed.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | The availability of data if necessary for, for example, accountability and if data is no longer archive-worthy, it will be deleted/destroyed in a timely manner. | | |
| Risk | The availability and integrity of the data is compromised during archiving and archiving for longer than necessary. | | |
| Control | Archived data should be stored during the agreed **retention period**, **technology-independent**, **consultable**, **immutable** and with integrity and can be destroyed at the direction of the CSC/data owner. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Retention period | 1. | The guaranteed storage period agreed with the CSP is contractually stipulated and complies with the Archives Act. | ISO 27040 2016: 6.7.1 |
| Technology-independent consultable | 2. | Data can be consulted independently of the technology used by the CSP during the entire retention period. | ISO 27040 2016: 6.7.1 |
| Immutable | 3. | If possible, data is archived using Write Once Read Many (WORM) technology, which guarantees the integrity of the data. | ISO 27040 2016: 6.7.1 |
| Destroyed | 4. | Prior to modifying storage media for maintenance purposes, the CSC's data, including the backup of data and metadata, is securely erased or destroyed. | ISO 27040 2016: 6.7.1 |
| 5. | Upon termination of the contractual relationship, the data of the CSC, including the backup of data and the metadata, is securely erased to prevent the CSC data from being restored by the CSP afterwards, for example with forensic tools. | ISO 27040 2016: 6.7.1 |

# U.07 Data separation

**Object definition**

Concerns the sustainable isolation of CSC data from other CSCs.

### Object explanation

Isolating data (in processing or at rest) from the CSC, from all data from the CSP and from the data from other CSCs. Sustainable separation of CSC data and of the data of other companies (secure multi-tenancy), both during transport, in processing and storage, is a precondition for purchasing secure cloud services.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Ensure that the data of or under the management of the CSC is only accessible to this CSC. | | |
| Risk | Other CSCs and the CSP get access to the data or managed by the CSP and vice versa. | | |
| Control | CSC data should be sustainably **isolated** during transport, processing and storage from **management functions** and data from and other services to other CSCs, which the CSP manages. | | ISO 27040 2016: 7.7.4 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Isolated | 1. | Permanent isolation of data is realized within a multi-tenant architecture. Patches and adjustments of applications and infrastructure are realized in a controlled manner for all cloud services that the CSC purchases. | CIP network |
| 2. | Isolation of CSC data is ensured by separating it at least logically from the data of other CSCs under all operating conditions. | CIP network |
| Management features | 3. | The privileges to view or modify CSC data and/or encryption keys by management functions and administrators are granted in a controlled manner and the use of these rights is logged. | CIP network |

# U.08 Separation of services

### Object definition

Concerns the permanent isolation by the CSP of the services to be provided between the different CSCs and between CSCs and the CSPs.

### Object explanation

Isolating services/services from/for the CSC, from all services/services that are not required for that specific service, such as those of/for other CSCs. The service, which is specifically provided to a particular CSC, is separate from services provided by the CSP to other CSCs and is separate from the internal information provision of the CSP. Unwanted influence or communication that can cause data leaks must be prevented.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Preventing unwanted influence or communication of data between the CSC and CSP and other CSCs. | | |
| Risk | Influencing or communicating data. | | |
| Control | The cloud infrastructure is set up in such a way that the services to users of information services are **separated**. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Divorced | 1. | The CSP achieves the following separation of cloud services:   * separation of cscs in a multi-tenant environment; * separation between the purchased cloud service and the internal information provision of the CSP; * the CSP makes it possible to verify the intended separation of cloud services. | CIP network |

# U.09 Malware Protection

**Object definition**

Includes continuously protecting CSC data from malicious software.

### Object explanation

Data in the information chain of the CSC and CSP is continuously protected against malware, such as viruses.

When outsourced, the CSP will apply malware protection, including to the virtual machines.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Ensuring that information in the chain of the CSC and CSP is continuously protected against malware. | | |
| Risk | Malware is not detected or detected too late and malware found is not or sufficiently recovered. | | |
| Control | To protect against malware, **controls** should be implemented for **detection, prevention and recovery** combined with appropriate user awareness. | | BIO 2019: 12.2.1 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Controls | 1. | The CSP specifies, as part of the agreement, which measures (for malware protection, among other things) should be taken at which position in the information chain of the CSC and CSP. | ISO 27017 2015: 15.1.2 |
|  | 2. | The CSP has equipped the IT systems and network perimeters for which it is responsible for the development and operation of cloud services with malware protection and removal tools. | CIP network |
| Detection, prevention and recovery | 3. | The malwareprotection is carried out on various environments, such as on mail servers, (desktop) computers and when accessing the organization's network. The scan for malware includes:   * all files received over networks or through any form of storage medium, even before use; * all attachments and downloads even before use; * virtual machines;  network traffic. | BIO 2019: 12.2.1.5  ISO 27002 2017:  12.2.1g.1 and 2 |

# U.10 Access to IT services and data

### Object definition

Includes processes and resources for granting and monitoring access rights to CSC data and business processes.

### Object explanation

Access to data and business processes of all possible users both the CSC and the CSP is provided exclusively with identification, authentication and authorization. Note: The granting of access has a direct relationship with the 'Bring Your Own Device' (BYOD) policy of an organization.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Prevent unauthorized access to business processes/data in cloud services. | | |
| Risk | Misuse and loss of (sensitive) data. | | |
| Control | **Users** should only have access to IT services and data for which they are specifically **authorized** . | | BIO 2019: 9.1.2 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Users | 1. | The CSP shall only provide the CSC with access to services, IT services and data for which it is specifically authorised, whereby:   * Technical measures prevent users and administrators from accessing services, IT services and data beyond what is formally permitted. * Users with emergency access rights (during calamities, when actions cannot be performed by authorized administrators) are documented by management, approved and performed with segregation of functions. Emergency access is activated for as long as necessary for the corresponding task(s). | CIP network |
|  | 2. | Under the responsibility of the CSP, administrators shall be granted access:   * to data with the least privilege principle;  to data with the need-to-know principle; * with multi-factor authentication; * to data and application functions via technical measures. | CIP network |
|  | 3. | Only users with authenticated equipment can access IT services and data. | BIO 2019: 9.1.2.1 |
| Competent | 4. | Under the responsibility of the CSP, privileges (system authorisations) for users are granted through formal procedures. | BSI C5 2020: IDM-03 |
| 5. | Access to IT services and data is limited by technical measures and has been implemented, for example with the role and rights concept. | CIP network |

# U.11 Cryptoservices[[6]](#footnote-6)

### Object definition

Includes technical functions for encrypting and decrypting data, creating electronic signatures and being able to apply enhanced authentication.

### Object explanation

The technical functions for encryption and decryption of data, electronic signature and enhanced authentication, whether or not via Public-Key-Infrastructure (PKI) technology. Key management is a part of cryptoservices. If desired, the CSC can specify in its Program of Requirements (PvE), the crypto requirements of the National Office for Connection Security (NBV).

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Protecting the availability, integrity and confidentiality of sensitive data during transport over networks and storage. | | |
| Risk | Data can be accessed by unauthorized persons during transport via networks and storage. | | |
| Control | Sensitive data of the CSC should be **encrypted** in accordance with the agreed **policy** on **cryptographic measures** during transport over networks and when stored at CSP. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Policy | 1. | The cryptography policy includes at least the following topics:   * when cryptography is used; * who is responsible for the implementation of cryptology; * who is responsible for key management; * which standards serve as a basis for cryptography and the way in which the standards of the Standardisation Forum are applied; * the way in which the level of protection is determined; * in the case of communication between organizations, the policy is determined among themselves. | BIO 2019: 10.1.1.1 |
| Cryptographic measures | 2. | In the case of PKIoverheid certificates: apply the PKIoverheid requirements with regard to key management. In other situations: use the ISO 11770 standard for managing cryptographic keys. | BIO 2019: 10.1.2.1 |
| Encrypted | 3. | Sensitive data (on transport and at rest) is always encrypted, with private keys managed by the CSC. The use of a private key by the CSP is based on a controlled procedure and must be jointly agreed with the CSC organisation. | BSI C5 2020: CRY-03 |

# U.12 Interfaces

**Object definition**

Concerns connections at interfaces in the chain between CSC and CSP.

### Object explanation

An interface is the organizational or technical connection at the interface in the chain of the CSC and the CSP. This BIO Theme elaboration is limited to the technical connection. Limiting the number of interfaces requires the necessary attention and supervision to limit the risks of data loss.

Controlling the number of interfaces is therefore necessary to limit the risks of data loss.

Interconnector systems fall under the ISO 270xx category network services.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Monitoring and controlling interfaces in the chain of the CSP and the CSC. | | |
| Risk | Data from or managed by the CSP comes into the hands of the CSP via the interfaces. | | |
| Control | The **interconnected network connections** (interfaces) in the chain from the CSC to the CSP should be **monitored** and **controlled** to limit the risks of data breaches. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Network connections | 1. | In connection points with external or untrusted zones, measures have been taken to identify and respond to possible attacks that negatively affect the availability of information (e.g. Distributed Denial of Service attacks (DDos) attacks). | BIO 2019: 13.1.2.4 |
|  | 2. | Physical and virtualized network components are designed and configured in such a way that network connections between trusted and untrusted networks are limited and monitored (monitored). | CIP network |
|  | 3. | Management activities of the CSP are strictly separated from the data of the CSC. | CIP network |
|  | 4. | Data traffic for CSCs is separated in jointly used network environments according to a documented concept for the network-level (logical) segmentation of CSCs, in order to ensure the integrity and confidentiality of the transmitted data. | BSI C5 2020: COS-06 |
| Monitored | 5. | The data traffic entering or leaving the CSP is monitored in relation to the nature of the data/information systems to be protected and analyzed for malicious elements by means of detection facilities. | BIO 2019: 13.1.2.1 |
| 6. | The CSP has Intrusion Detection Prevention (IDP) and Intrusion  Detection System (IDS) integrated into a comprehensive Security Information and Event Management (SIEM), so that security events and unknown equipment are detected from the necessary technical measures and corrective measures can be taken. | BSI C5 2020: COS-01 |
| Composed | 7. | In the event of discovered new threats, taking into account applicable legal frameworks, these are mandatory shared within the government, including with the NCSC (only for government organizations) or the sectoral Computer Emergency Response Team (CERT), preferably by automated mechanisms (threat intelligence sharing). | BIO 2019: 13.1.2.2 |

# U.13 Service Orchestration

### Object definition

Concerns the arranging, assessment and adjustment by the CSC of the set of services provided by a CSP.

### Object explanation

The CSP orchestrates the cloud services. This means that it arranges (assesses and adjusts) the cloud services and that the information can be exchanged with standard messages between the cloud services of the CSP and the CSCs, so that the quality of the cloud service to be provided to the CSC corresponds to the agreed QoS, information security and costs.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | The quality of the cloud service to be provided to the CSC corresponds to the agreed QoS, information security and costs. | | |
| Risk | No or insufficient coordination, aggregation and composition of the service components of the cloud service. | | |
| Control | Service orchestration provides **coordination**, aggregation, and composition of the **service components** of the cloud service provided to the CSC. | | ISO 17789 2014: 9.2.3.4 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Coordination | 1. | Cloud orchestration technology works with heterogeneous systems and potentially global cloud deployment (in different geographic locations and with different CSPs). | CIP network |
| Service components | 2. | The functional coherence of the service components is described. | CIP network |
| 3. | Orchestration of cloud services requires the following information:   * the CSC identity; * the business relationship of the CSC within the cloud network;  the IP address of the CSC. | ITU-T: FG Cloud TR 1.0  Part 5 Cloud security  2012: II.2.3 |

# U.14 Interoperability and portability

### Object definition

Concerns the ability to operate services and exchange of data without special tools or adjustments with other organizations and systems.

### Object explanation

In order to avoid the risk of vendor lock-in and dependencies on external IT facilities, the CSP, in dialogue with the CSC, should ensure that cloud services are designed in such a way that they are interoperable and that the CSC dataset is transferable, without the need for particularly costly or complex tools or laborious adjustments per cloud service.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Ensuring that cloud services are usable across IT platforms and data can easily be passed on to another CSP without compromising integrity and confidentiality. | | |
| Risk | Cloud services cannot be applied to other IT platforms and data cannot be transferred to another CSP. | | |
| Control | Cloud services can be used (**interoperability**) on different IT platforms and can use standards to connect different IT platforms and transfer data (**portability**) to other CSPs. | | BSI C5 2020: COS-02  ISO 19941 2017: 7.1.7 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Interoperability | 1. | To ensure the interoperability of cloud services, data is available in accordance with recognized industry standards and documented input and output interfaces. | BSI C5 2020: PI-01 |
| Portability | 2. | To ensure the portability of the data, the CSP uses secure network protocols for the import and export of data, ensuring integrity and confidentiality. | BSI C5 2020: PI-01 |

# U.15 Logging and monitoring

### Object definition

Includes recording information security-related events and monitoring and recognizing deviations from policies.

### Object explanation

The intended functioning of IT functions in the information chain should be monitored through logging and monitoring. Monitoring is aimed at identifying any deviations from policy rules and logging is aimed at recording events, as evidence and for improvement and/or recovery.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | The timely detection and recording of unauthorized and/or incorrect activities of employees and malfunctions of IT functions in the information chain. | | |
| Risk | Deviations from normal behavior are not visible and cannot be investigated and remedial actions cannot be taken in time. | | |
| Control | Log files in which **events** that record user activities, exceptions, and information security events should be created, retained, and reviewed regularly. | | BIO 2019: 12.4.1 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Events logged | 1. | The violation of the policy rules is recorded by the CSP and the CSC. | CIP network |
| 2. | The SIEM and/or Security Operation Centre (SOC) have clear rules about when an incident must be reported to the responsible management. | BIO 2019: 12.4.1.5 |
| 3. | The CSP maintains a list of all assets that are critical in terms of logging and monitoring and regularly reviews this list for correctness. | CIP network |
| 4. | Strict requirements are imposed on logs and monitoring. Advanced protections for logging and monitoring have been defined for the critical components. | CIP network |
| 5. | Access to and management of the logging and monitoring functionality is limited to selected and authorized employees of the CSP. | CIP network |
| 6. | Changes in logging and monitoring are checked by independent and authorized employees. (Log rules should never be changed; after all, they are intended to be used as a burden of proof.) | CIP network |

# U.16 Cloud Services Architecture

### Object definition

Concerns a model-based description of a technical and organizational coherence, in which the

CSP establishes the relationships between the components of the cloud services and the support of the CSC.

### Object explanation

In the cloud services architecture, the CSP establishes the functional relationships between IT components throughout the chain of the CSC and the CSP. This architecture describes how the IT components should be set up to support the CSC's business processes.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Providing a cloud landscape to support the CSC business processes that is secured in conjunction and provides insight into their design. | | |
| Risk | Have no or insufficient control over cloud services. | | |
| Control | The cloud services architecture specifies the **coherence** and security of the services and the interconnection between the CSC and the CSP and provides transparency and oversight of edge conditional environment parameters, for both the design, delivery and portability of CSC data. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Cohesion | 1. | The architecture shall specify at least the following:   * IT services in relation to functionality for business processes; * the level of trust of the security of the cloud services; * the description of the infrastructure, network and system components used for the development and operation of the cloud service(s); * roles and responsibilities of the CSP and the CSC, including the duties to cooperate and the associated controls at the CSC; * IT functions assigned or outsourced by the CSP to subcontractors. | CIP network |

# U.17 Multi-tenant architecture

### Object definition

Concerns a specification in which a CSP describes the interrelationships of CSCs and the durable separation between the CSCs from cloud services.

### Object explanation

The system of cloud services offered on common infrastructure, whereby CSCs can never read or influence each other's data due to a strict (logical and/or physical) separation of data and services. CSCs should not be affected by peak loads from other organisations (other CSCs and/or CSPs).

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Providing a multi-tenant landscape that is secured in conjunction and provides insight into its design. | | |
| Risk | Have no or insufficient control. | | |
| Control | With multi-tenancy, the CSC data within cloud services, which are purchased by multiple CSCs, is **encrypted** at rest and processed **separately** on **hardened** (virtual) machines. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Encrypted | 1. | CSC data on transport and at rest is encrypted. | ITU-T FG Cloud TR Part 5  2012: S12 |
| Divorced | 2. | Virtual machine platforms for CSCs with special/increased security requirements are set up separately. | ITU-T FG Cloud TR Part 5  2012: S12 |
| Hardened | 3. | Virtual machine platforms are hardened. | ITU-T FG Cloud TR Part 5  2012: S12 |

# Control domain

# 5.1 Objective

The purpose of the control domain is to determine to what extent:

* controls are sufficiently set up and functioning to ensure the intended availability, integrity and confidentiality of the cloud services;
* infrastructural services, functional and technical, are kept at the agreed level.

This means, among other things, that an adequate management organization has been set up within the CSP, in which the management processes have been designed.

# 5.2 Risks

In the absence of the necessary measures within the CSP, it is not certain whether the development and maintenance of the IT components meets the intended organisational and security conditions and that the governance of the cloud services is adequately designed. Nor can it be determined whether the desired measures are being complied with. Appendix 4 Explanation of objects in the control domain indicates for each focus area which risks are relevant.

# 5.3 Objects, controls and measures

Figure 10 shows the topics that play a role specifically for the control domain. If an object block is colored blue, the corresponding control occurs in the BIO. If it concerns a white marked object block, the BIO has not defined a control, but this object is necessary for this BIO Theme elaboration.

**Angle**

Intention

Function

Behavior

Structure

**Service Management Policy**

**and evaluation directive**

(

Operational

)

policy

C

.

01

**Risk**

**-**

**Control**

Assessment

C

.

02

**Compliance and assurance**

Assessment

C

.

03

**Technical**

**vulnerability management**

Lawsuit

C

.

04

**Security**

**-**

**monitoring**

**-**

**Reporting**

Event

/

history

C

.

05

**Management organisation**

**cloud services**

IT

-

Organisational structure

C

.

06

Figure 10: Overview of objects for cloud services in the control domain

The objects, for cloud services, that play a role specifically within the control domain, are elaborated in the paragraphs below.

# C.01 Service management policy and evaluation guideline

### Object definition

Concerns the result of decision-making for setting up management processes and the systematically developed recommendations for evaluating and carrying out control activities for cloud services.

### Object explanation

The service management policy guides how the cloud services management organization should be set up and how it should function. Guidelines and procedures exist to support the specific management processes. The management organisation structure reflects the coherence of the set-up processes.

Cloud services consist of different components and different interfaces. It is of great importance that cloud services, due to risk management, are periodically evaluated. Evaluation activities should be supported by evaluation guidelines, procedures and instructions in order to avoid the risk that the results of the control activities do not meet the requirements.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Give direction to the way in which the management organization for cloud services should be set up and the way in which it should function. | | |
| Risk | The results of audit activities carried out on cloud services do not meet the set requirements. | | |
| Control | The CSP has formulated a service management policy for cloud services containing **guidelines** for the control processes, **control activities and reports**. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Directives | 1. | For cloud services, the CSP has guidelines for the design of the service management organization. | CIP network |
| 2. | The CSP has described relevant management processes and effectively set them up in accordance with an established cycle, including: registration, status measurement, monitoring, analysis, reporting and evaluation. | CIP network |
| Control activities and reports | 3. | For cloud services, the CSP has guidelines for:   * carrying out control activities, including penetration and vulnerability testing; * evaluate and report on performance, conformance and delivery performance. | CIP network |

# C.02 Risk control

### Object definition

Concerns the assessment of continuous research into threats and vulnerabilities and the assessment of the management of identified risks.

### Object explanation

Risk control is the monitoring and review of risk assessment activities in relation to risk management. Monitoring and reviewing risks is necessary because risk factors: value of assets, impact, threats, weaknesses and likelihood of occurrence are constantly changing. Risk control can be supported by externally obtained information about threats and weaknesses.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Check in good time whether there are changes that affect the outcome of the risk assessment. | | |
| Risk | Not anticipating risk factors that influence the outcome of the risk assessment or anticipating them too late. | | |
| Control | Risk management and the risk assessment process should be continuously **monitored and reviewed** and, if necessary, improved. | | ISO 27005 2018: 12.1  ISO 27005 2018: 12.2 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Monitored and reviewed | 1. | The CSP regularly verifies the criteria used to measure the risks and to determine whether they are always consistent with the organization's objectives, strategy, policy and/or context. | ISO 27005 2018: 12.2 |
| 2. | Identified risks should be monitored and evaluated in relation to the factors: value of the assets, threats, weaknesses, probability of occurrence and impact, in order to maintain a complete risk picture and to (be able to) determine changes in a timely manner. | ISO 27005 2018: 12.1 |
| 3. | For the monitoring of risks, the CSP will continuously focus on:   * new assets that should be part of the scope of a risk assessment; * changes in the value of assets; * the possibility that new or increased weaknesses may lead to threats; * the possibility that previously identified weaknesses may be exposed to new threats; * increased impact or consequences of the assessed risks and weaknesses resulting in an unacceptable level of risk;  information security incidents. | ISO 27005 2018: 12.1 |
| 4. | The CSP regularly carries out the monitoring activities and mitigates the identified risks. | ISO 27005 2018: 12.1 |
| 5. | When monitoring and reviewing, the following elements are addressed, among others:   * laws and regulations and organisational/technical context; * risk assessment approach; * value of assets and categories; * risk assessment criteria; * risk acceptance criteria. | ISO 27005 2018: 12.2 |

# C.03 Compliance and assurance

### Object definition

Concerns the control of compliance with the applicable laws and regulations, policies, guidelines and procedures and the independent assessment of compliance with them.

### Object explanation

Compliance indicates that the CSP works in accordance with the applicable laws and regulations and the outlined cloud security policy. The CSC is offered certainty about the intended security level of the cloud service offered. For this, the CSP will need to have set up a compliance function that assists the management of the CSP in keeping the CP organization in control in order to work in accordance with the applicable laws and regulations and the agreed security policy.

Assurance is providing assurance about compliance with laws and regulations through independent review. This provides the CSC with certainty of the intended security level of the cloud service offered. This takes place with an assurance report.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Preventing violations of laws and regulations, security policies, guidelines and procedures and providing assurance about the intended level of security of the cloud service. | | |
| Risk | The uncontrolled deviation from what is stated in laws and regulations, the security policy, the guidelines and the procedures and having no certainty about the security level entered. | | |
| Control | The CSP should regularly review compliance with the cloud security agreements for **compliance**, issue an annual **assurance** statement to the CSC, and ensure that the results of these two exercises are aligned. | | ISO 27002 2017: 18.2.1  ISO 27002 2017: 18.2.2 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Compliancy | 1. | For the governance of the cloud services to the CSC, the CSP has set up a compliance process, which ensures continuous compliance with laws and regulations and the agreed cloud security policy. | CIP network |
| 2. | The CSP registers the regularly issued performance, security and compliance reports in an administration. | CIP network |
| 3. | The compliance process is preferably connected to an information security management system. | CIP network |
| Assurance | 4. | The CSP has a third party carry out an annual investigation (audit) on the design and control of the contracted cloud services. | CIP network |
| 5. | In the assessment, the third party involves both the cloud environment and the administration. | CIP network |
| Junction | 6. | The CSP ensures that the results from the annual assurance report (Third Party Communication (TPM)), the results of the periodic service reports and the results from the continuous compliance with the cloud security policy are aligned. | CIP network |

# C.04 Technical vulnerability management

### Object definition

Concerns a conservation process for the investigation and resolution of technical vulnerabilities.

### Object explanation

Collecting and managing security vulnerabilities and issues in cloud services. With regard to the services of the CSC, transparently communicating vulnerabilities of the measures taken (or to be taken) for IT and organization. The CSC wishes to be informed in a transparent manner of the vulnerabilities and issues related to the security of the cloud services.

By performing technical assessments on the ICT components, existing vulnerabilities become visible and can be displayed in a report. With this report, the CSP can consider which vulnerabilities are relevant and need to be fixed and which risks with regard to these vulnerabilities can be accepted.

The frequency of carrying out technical assessments should be determined with the current risk profile for the cloud service and action should be taken if implemented measures do not meet the requirements and/or expectations set or if shortcomings are identified.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Preventing the exploitation of technical vulnerabilities by unauthorized persons. | | |
| Risk | A technical vulnerability is not detected or not detected in time. | | |
| Control | Information on **technical vulnerabilities** of used information systems should be obtained in a timely manner; exposure to such vulnerabilities should be **evaluated** and appropriate measures taken to address the risk associated with them. | | BIO 2019: 12.6.1 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Technical vulnerabilities | 1. | The CSP makes information available to the CSC on the management of the technical vulnerabilities that may affect the cloud services. | ISO 27017 2015: 12.6.1 |
| 2. | The CSP has defined and established the roles and responsibilities related to managing technical vulnerabilities, including coordinating, monitoring, assessing risks and mitigating vulnerabilities. | ISO 27002 2017: 12.6.1a |
|  | 3. | If the probability of abuse and the expected damage are both high (NCSC classification vulnerability warnings), patches are installed as soon as possible, but no later than within a week. In the meantime, mitigating measures are taken on the basis of an explicit risk assessment. | BIO 2019: 12.6.1 |
|  | 4. | The timeframe within which to respond to announcements of potentially relevant vulnerabilities has been defined. | ISO 27002 2017: 12.6.1c |
| 5. | Periodically, penetration tests on ICT components are carried out to identify weaknesses. | SoGP 2018: TM1.1.7 |
|  | 6. | Technical weaknesses can be remedied by performing patch management in a timely manner, which includes:   * identifying, registering and acquiring patches; * the decision-making around the use of patches; * testing patches; * performing patches; * registering implemented patches. | SoGP 2018: TM1.1.9 |
| Evaluated | 7. | Evaluations of technical vulnerabilities are recorded and reported. | CIP network |
| 8. | The evaluation reports contain suggestions for improvement and are communicated with managers/owners of ICT components in which vulnerabilities and weaknesses have been found. | NCSC 2015: C.03.04 |

# C.05 Security Monitoring Reporting

### Object definition

Includes the continuous monitoring of security events and the reporting of the detected deviation from the agreed security level.

### Object explanation

For cloud services, security monitoring is understood to mean the reviewing, analysis, signalling and timely reporting of weaknesses, insecure interfaces and unauthorized access attempts, in order to prevent abuse and to take actions with the severity of the signalling.

The monitoring function is reserved for the responsible officer(s) and also takes place with registered data (logging).

The log data should be analysed regularly and the results of these analyses should be reported (alerting). The CSP must also regularly report on whether and the extent to which deviations have been detected at the agreed security level.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Record events (performance of the information security of the cloud environment), collect evidence and inform data subjects thereof. | | |
| Risk | Abuse of the performance of information security of the cloud environment. | | |
| Control | The performance of the information security of the cloud environment should be **monitored** regularly  **and** this should be **reported** to various stakeholders in a timely manner. | | ISO 27002 2017:12.4  SoGP 2018: SI2.1 |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Monitored and reported | 1. | Guidelines and agreements for monitoring and reporting on information security of the cloud environment have been established and are being applied. | SoGP 2018: S12.1.1 |
| 2. | Monitoring and reporting on information security are related to:   * formulated strategic and business goals; * risks that may affect the achievement of the strategic goals; * security incidents, such as cybersecurity attacks. | SoGP 2018: SI2.1.2 |
| 3. | The monitoring of information security and reports takes place with:   * collecting information from internal and external sources; * the insight gained through collected information from the combination of Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs). | SoGP 2018: SI2.1.5 |
| 4. | Information security reports are analyzed in conjunction with reports from other management disciplines (compliance and assurance management and vulnerability management). | SoGP 2018: S12.6 |
| 5. | Demonstrably, follow-up is given to improvement proposals from analysis reports. | CIP network |
| 6. | The security plans shall be periodically updated and assigned to the responsible officials. | NCSC 2015: 07.11 |

# C.06 Management organisation cloud services

### Object definition

Concerns a targeted pooling of knowledge and skills between persons with tasks, responsibilities and powers for the functional and technical management of cloud services.

### Object explanation

In order to adequately control and manage cloud services, the CSP must have established a control organisation, in which the structure and responsibilities for management processes with adequate privileges are expressed and positioned at the appropriate level.

In the relationship between the control processes of the CSP and the CSC, the tasks and responsibilities between functional and technical management have also been agreed.

|  |  |  |  |
| --- | --- | --- | --- |
| Objective | Adequately controlling and managing cloud services. | | |
| Risk | The punchline services do not run as necessary. | |  |
| Control | The CSP has set up a management organisation in which the **process structure** and the **tasks, responsibilities and powers** of the **officers** concerned are defined. | | CIP network |
| **Conformity indicator, number and measure** | | | **Derived/derived from** |
| Process structure | 1. | The coherence of processes is recorded in a process structure. | NCSC 2015: B.06.07 |
| Tasks, responsibilities and powers | 2. | The CSP has described the tasks and responsibilities for the execution of the management(s) activities and has recorded the corresponding powers in an authorisation matrix. | CIP network |
| Officials | 3. | The most important officers (stakeholders) for the control organisation have been appointed and the mutual relationships have been made transparent with an organisational chart. | CIP network |

# Accountability

This appendix gives a brief account of the approach, the choices that have been made and the substantive objects that have been used in this BIO Theme elaboration. In order to arrive at a document that has broad support and offers added value to government organizations, the objects have been traced along:

1. CSC requirements
2. Threats/vulnerabilities
3. Baselines

Government organisations that now have specific standards frameworks for cloud services have been asked to open their frameworks to a wider public for re-use through this thematic elaboration.

## CSC requirements

In order to trace the specifically CSC-oriented points of attention, questions were asked to government organizations to arrive at a set of requirements and wishes. With the requirements and wishes, objects have been identified. Target organizations and cloud group sessions were asked some questions, such as:

* How can this theme development help the organization acquire cloud services?
* What should at least be worked out in the BIO Thema development cloud services?
* What requirements are set by government organizations when acquiring cloud services?
* From this theme elaboration, are connections necessary with functional requirements for cloud services and normative?

## Threats/vulnerabilities

To identify specific objects, it also focuses on the common threats and vulnerabilities that arise from the application of cloud services.

## Baselines

In addition, existing baselines were consulted, insofar as they are specific to cloud services. The specific objects, also based on the requirements and wishes of the CSC side and the threats, have been selected from the baselines and focused on for the cloud environment. Furthermore, a link has been made with the BIO and with the ISO 27017, which is specifically aimed at cloud services. Figure 11 gives an overview of the steps described.

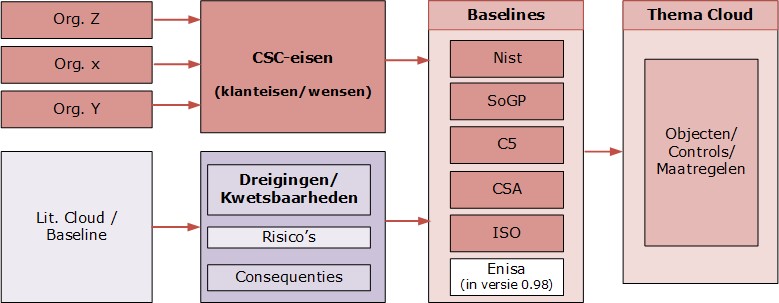


Figure 11: Trajectory of bio Thematic elaboration of Cloud services

# Explanation of objects in the policy domain

Below is an explanation of the policy area for each angle:

* Intention

An organization has formulated objectives when acquiring cloud services, such as: efficient business operations and a scalable and flexible service. To this end, it develops policy and strategy. Because this is developed with uncertain information, stakeholders have risk analysis(s) carried out. For carrying out risk analyses, a risk approach (method) to be used has been established (risk management).

* Function

In order to meet the objectives, the organization may decide to set functional requirements. They should describe the IT functionalities and related processes and security functions.

* Behavior

The IT functionalities are realized by actors (human resources) and IT objects (technical resources). Human resources refers to people who are subject to requirements, such as education, competence/skill. IT resources are 'Data' and IT objects (applications, servers and infrastructure).

* Structure

The deployment of the actors must be well organized by an organizational structure and the necessary IT objects an architecture.

Figure 12 shows threats/vulnerabilities of the mentioned policy objects.

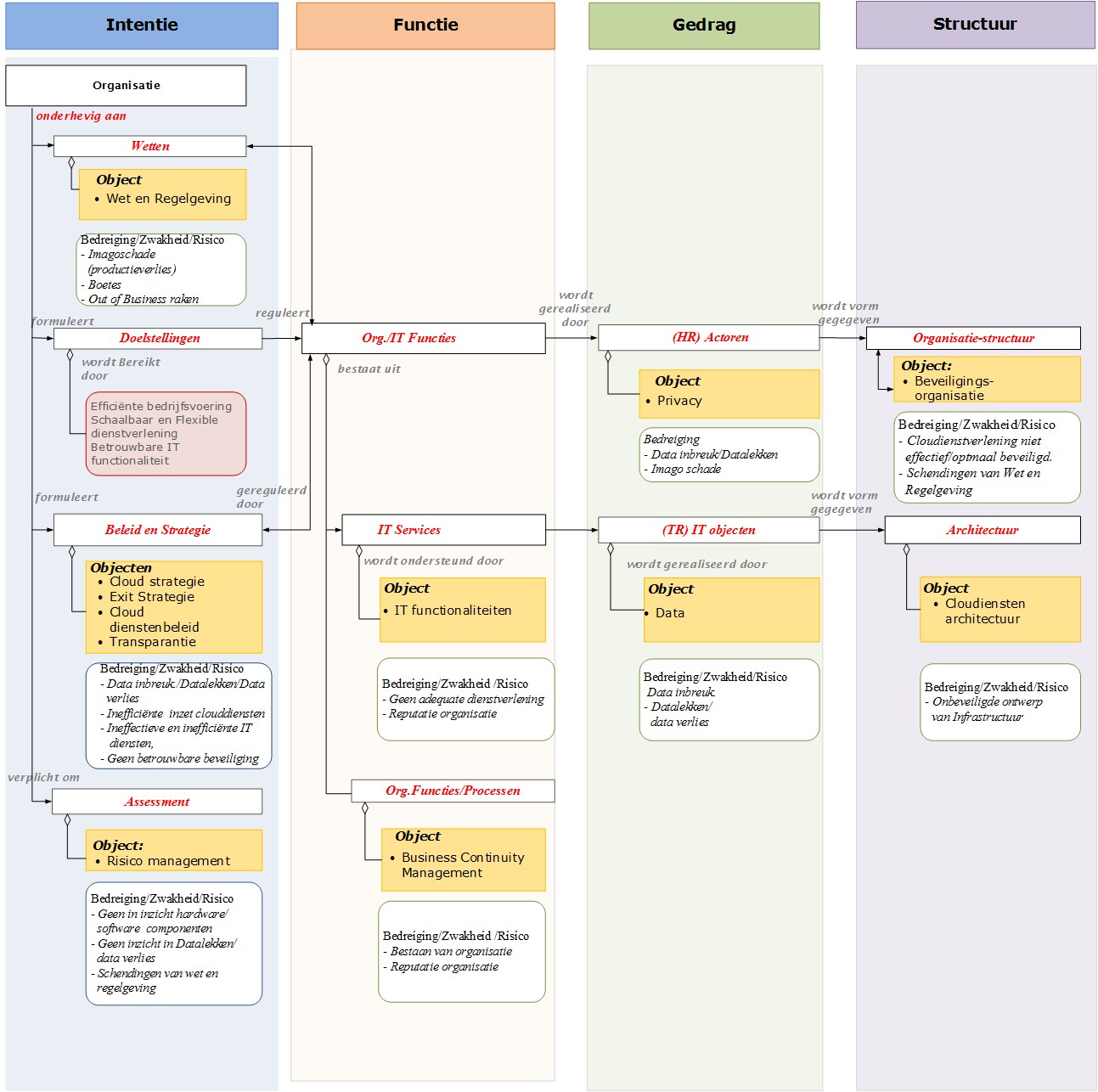


Figure 12: Threats/vulnerabilities of policy objects

## Threats/vulnerabilities cloud policy objects

Figure 13 shows the identified security objects for cloud services for the policy domain and thanks to the listed threats/vulnerabilities and risks. These threats/vulnerabilities and risks are not exhaustive and illustrate the way in which the writing group arrived at relevant policy objects: first a longlist and then a shortlist. The objects from the shortlist were then structured using the SIVA methodology. SIVA stands for Structure, Content, Form and Analysis Order. They are divided into the 3 domains: policy, implementation and control and 4 perspectives: intention, function, behavior and structure.

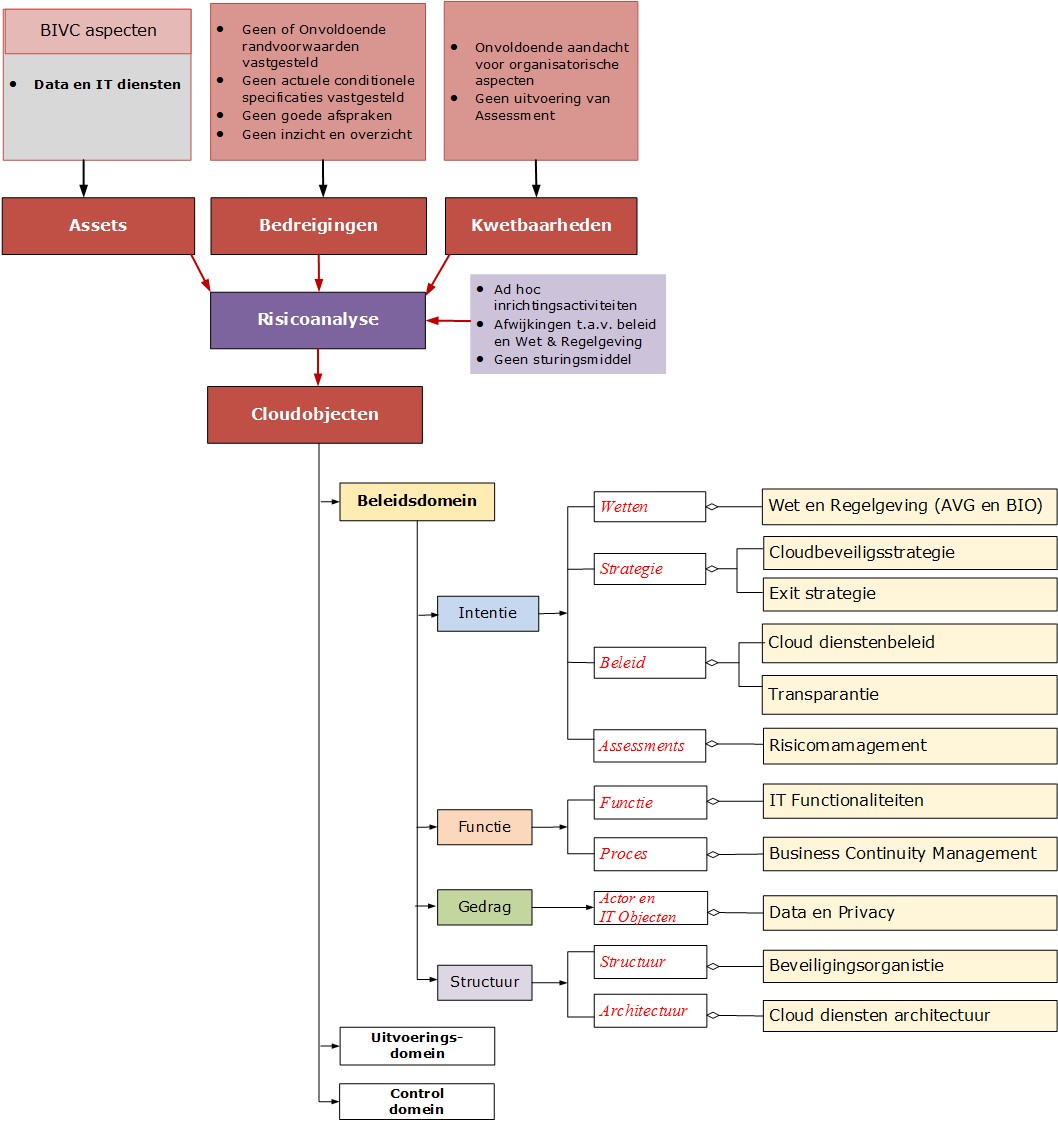


Figure 13: Policy objects structured with the SIVA methodology

 **Explanation of objects in the execution domain**

Below is an explanation of the implementation domain for each angle:

* Intention

In the implementation domain, the organization will, among other things, translate its policy into guidelines for carrying out a risk analysis and translate the implementation into procedures.

* Function

In this domain, organizational and technically oriented measures are taken for cloud services.

* Behavior

The cloud services have a number of specific elements, such as access and technically oriented components.

* Structure

The cloud services must provide a good overview through an architecture.

Figure 14 shows the threats/vulnerabilities of the mentioned execution objects.

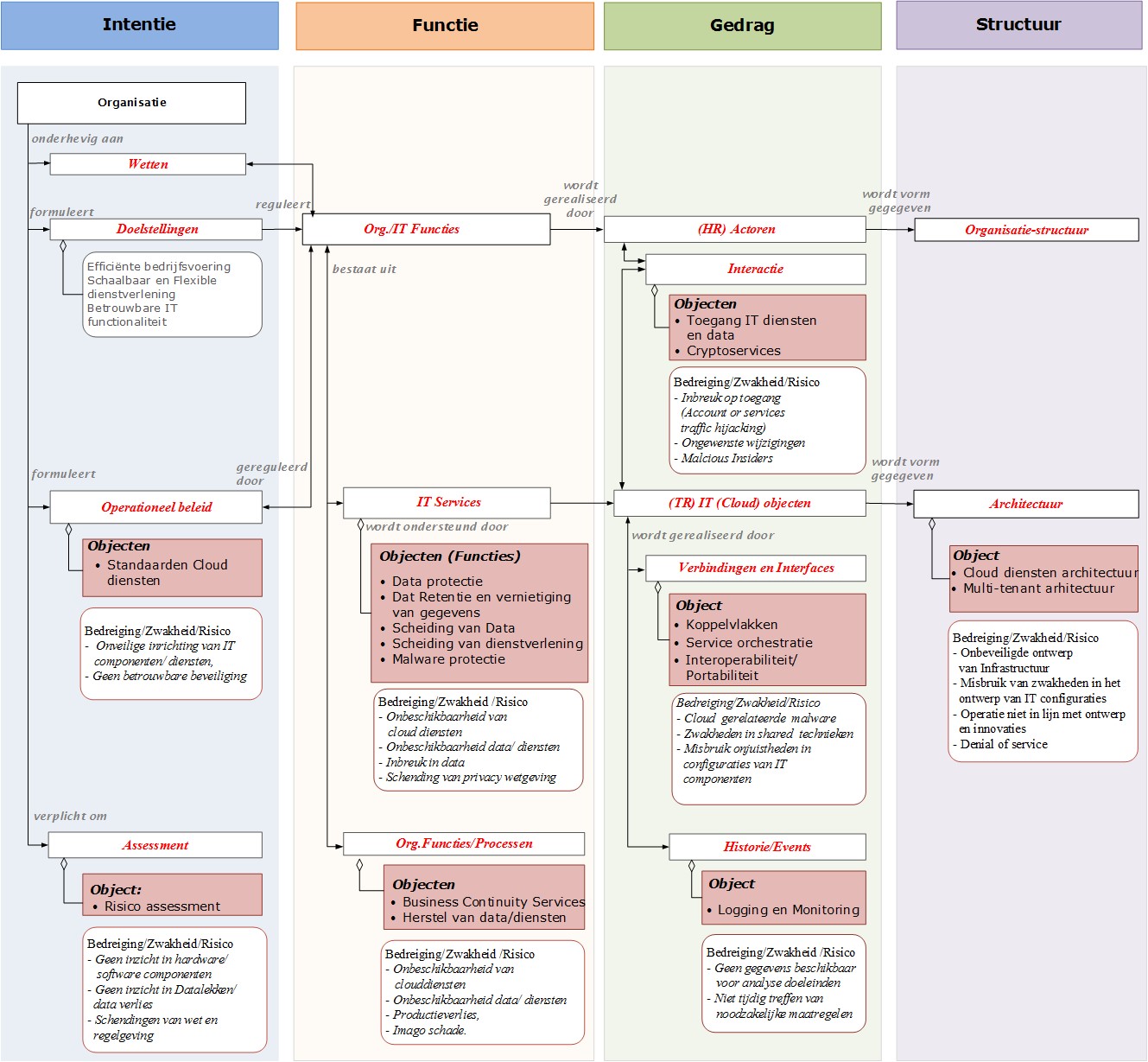


Figure 14: Threats/vulnerabilities of execution objects

## Threats/vulnerabilities cloud execution objects

The implementation domain has been analysed in the same way as mentioned in Appendix 2 Explanatory notes to objects in the policy domain. Here too, the listed threats/vulnerabilities and risks are not exhaustively named. Figure 15 shows the identified security objects for cloud services for the execution domain and thanks to the listed threats/vulnerabilities and risks.

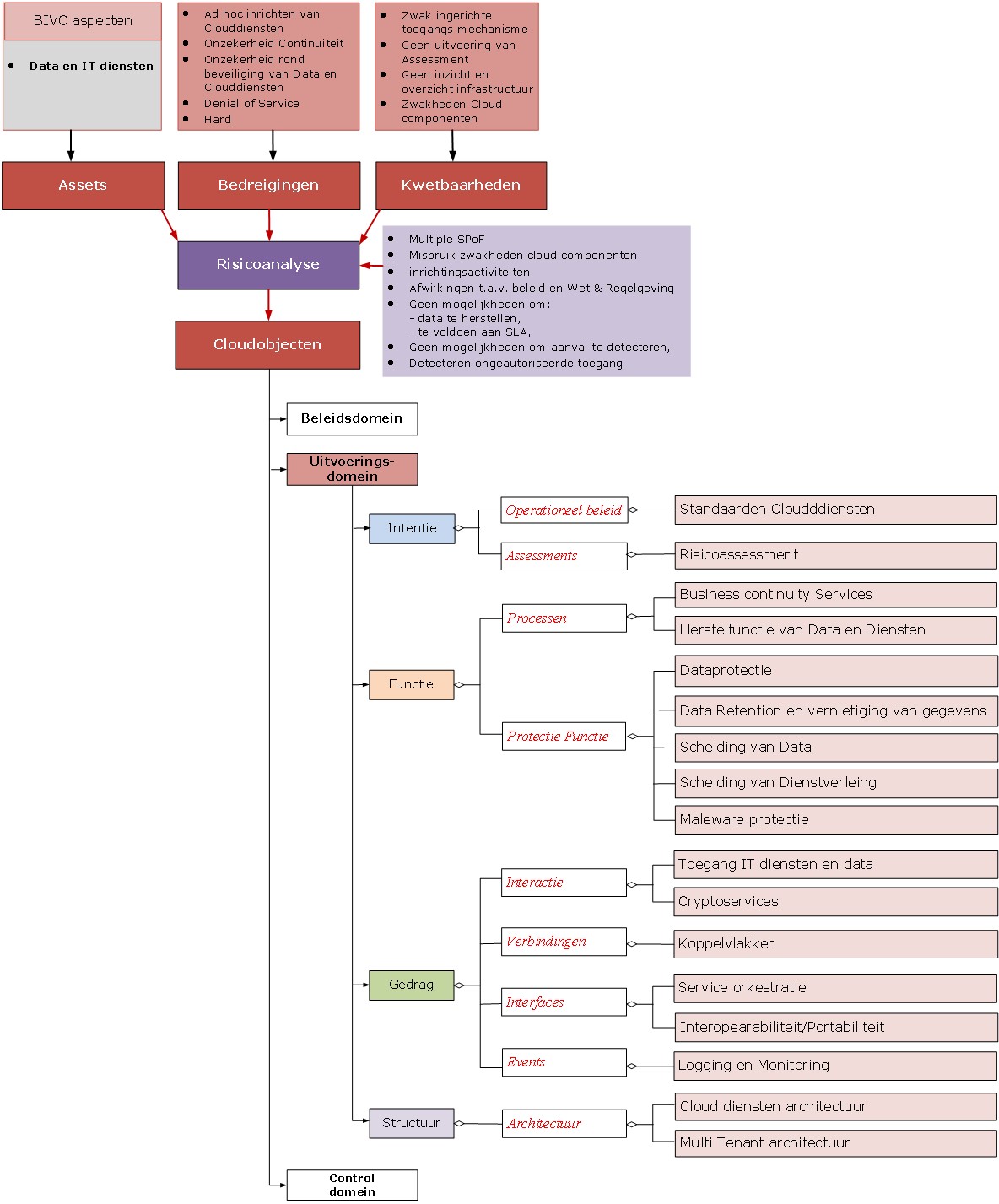


Figure 15: Execution objects structured with the SIVA methodology

 **Explanation of objects in the control domain**

Below is an explanation of the control domain for each angle:

* Intention

The organization has translated its policy for cloud services into a service management policy and evaluation guidelines for setting up, evaluating and monitoring the functioning and protection of the cloud services and carrying out activities for monitoring and reviewing the risks.

* Function

The organization has set up and implemented control processes for security controls and vulnerabilities of the cloud services.

* Behavior

The organization performs activities in its processes for monitoring cloud services and technical vulnerabilities.

* Structure

The organization has set up a control organization for the cloud services.

Figure 16 shows the threats/vulnerabilities of the mentioned control objects.

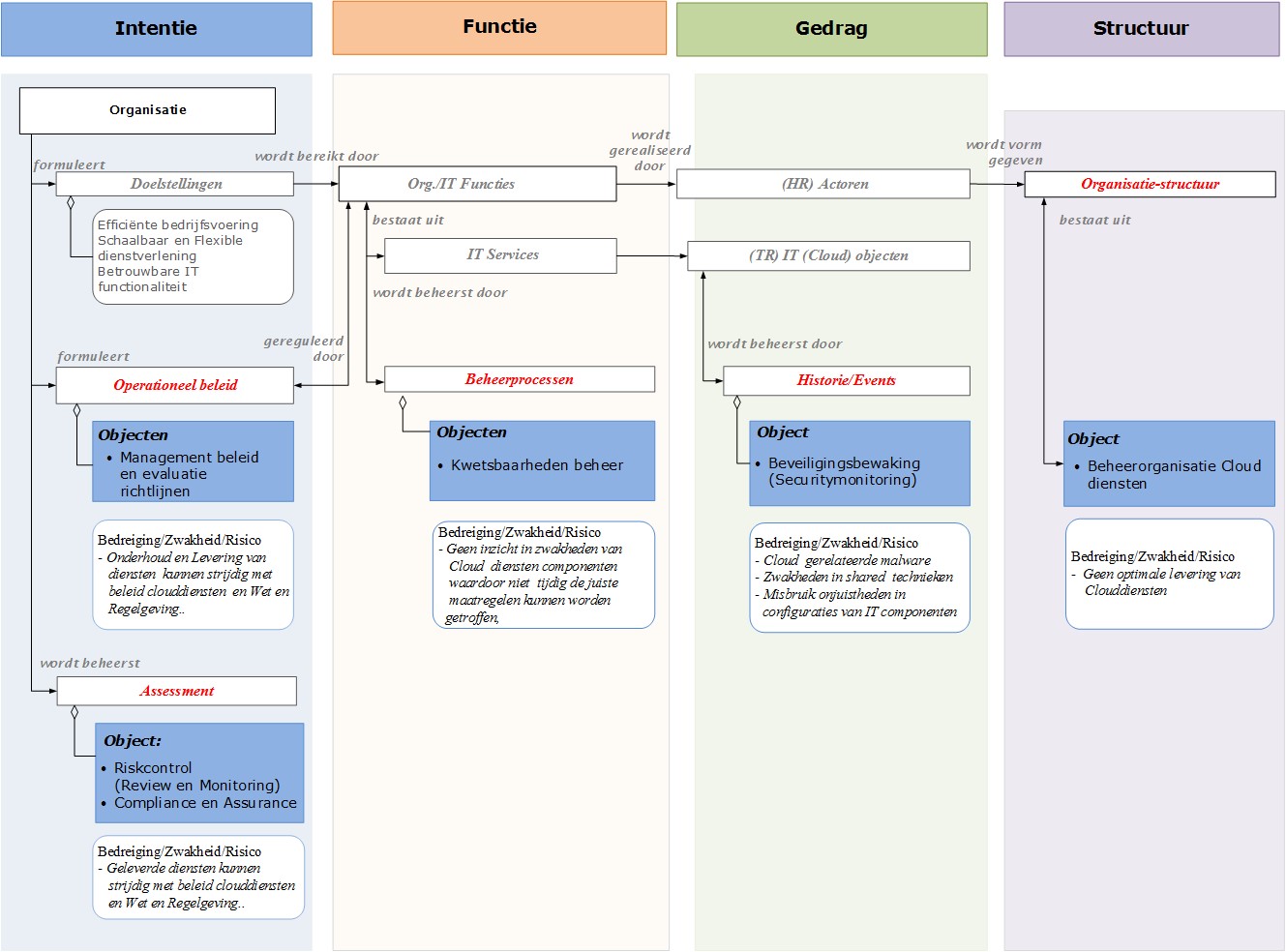


Figure 16: Threats/vulnerabilities of control objects

## Threats/vulnerabilities cloud control objects

The control domain has been analysed in the same way as stated in the Appendix 2 Explanation of objects in policy domain. Here too, the listed threats/vulnerabilities and risks are not exhaustively named. The relevant objects within the control domain are shown in Figure 17.

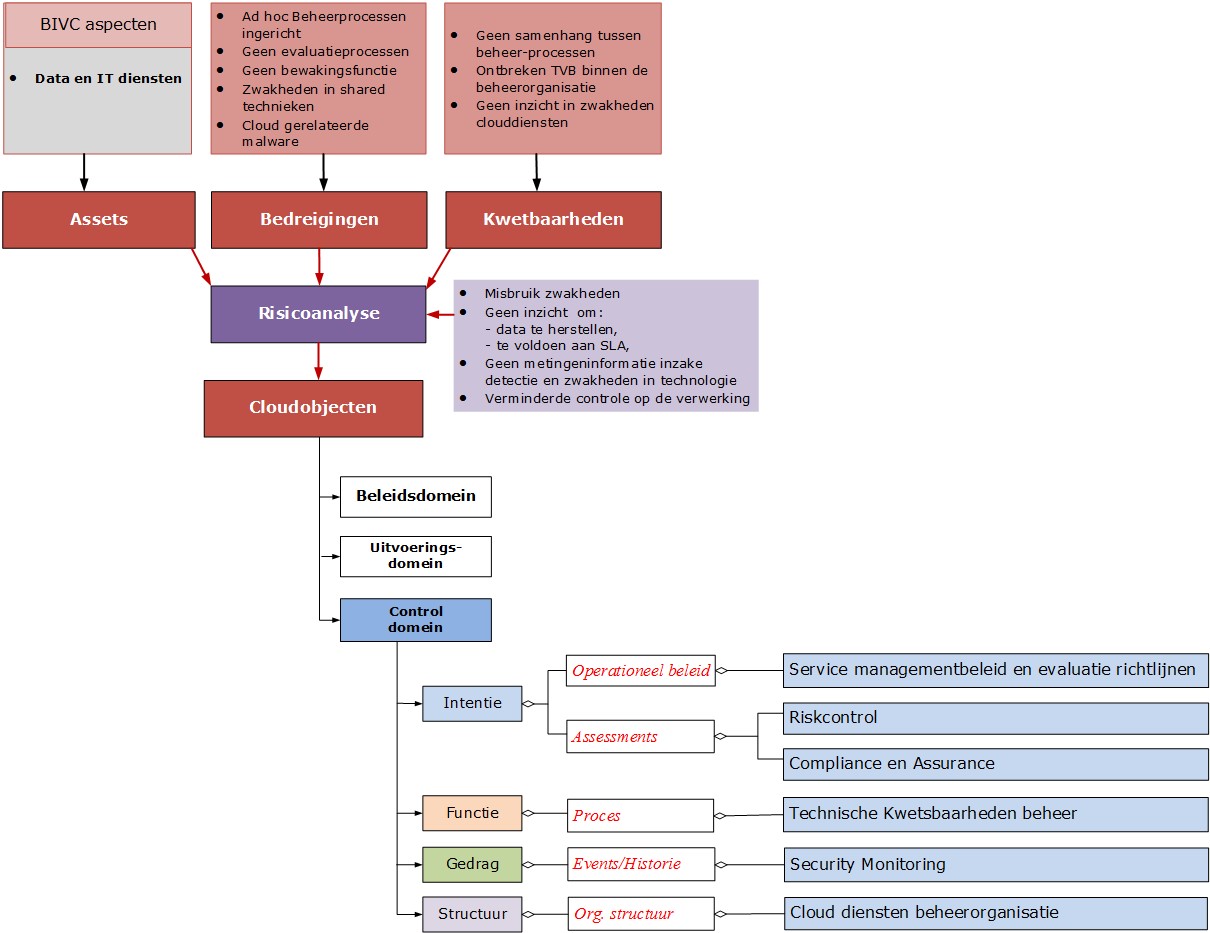


Figure 17: Control objects structured with the SIVA methodology

 **Decision tree for risk assessment ICT services**

The decision tree in Figure 18 supports the stakeholders for cloud services in making responsible decisions for placing data and/or business processes in the public cloud, private cloud, as outsourced IT or in their own data center 'on premise'. The decision tree has been worked out in relation to the risk assessment.

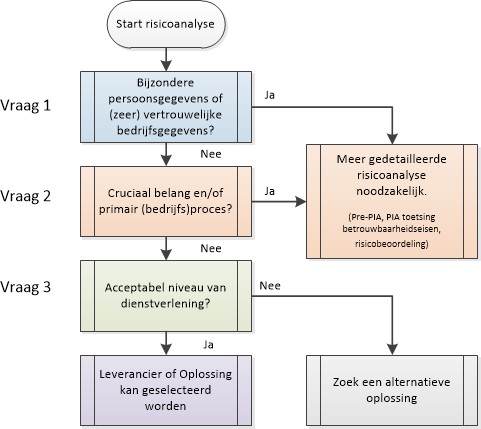


Figure 18: Decision tree for risk assessment

It is important to take the context of the government into account. Governments are expected to handle sensitive data of citizens and companies responsibly, but also with data of their own employees. For the question posed in step 1 about data , see Appendix 6 Summary of the AIVD position and policy outlook of the Ministry of the Interior and Kingdom Relations (BZK).

The decision tree is used as a self-assessment and tests successively for:

1. Dependency and vulnerability

Is it a primary business process with sensitive data of citizens and/or companies, where (special) personal data weighs extra heavily because of the GDPR, especially if it concerns the personal safety / privacy of your own employees?

1. Interests to be protected

Are these so-called crucial interests that are of primary importance for the survival of the organization, whereby the trust of the citizen and the company in the reliable government is at stake if that protection is insufficiently guaranteed?

1. Reliability of products and services

The reliability of the delivery of products and services is essential for the organization. The CSP plays a crucial role in this as the most important actor. Therefore, an appropriate service is required, whereby the character of the data/processes to be processed must be suitable for this.

Depending on the situational context, it will also concern company data that falls into one of the domains outlined in Figure 19 and that requires the appropriate measures.

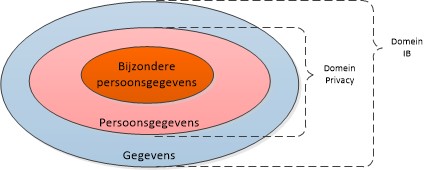


Figure 19: Schematic representation of types of data

## Dependency and vulnerability

Question 1: Does it concern personal data8 and/or (highly) confidential company data9?

Yes, a more detailed risk analysis10 is necessary (pre-DPIA, DPIA and/or risk assessment).

No, go to question 2.

## Interests to be protected

Question 2: Is it one of the following types of processes (is the character of the processes)?

1. By personal data, the GDPR means all information about an identified or identifiable natural person (the data subject) that can be identified directly or indirectly. For example, through name, identification number (BSN), location data or through elements that are characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

Directly identifiable: data that by its nature relates directly to a person, such as a person's name.

Indirectly identifiable: data that, by their nature, also determine the way in which the person concerned is assessed or treated in society.

Examples of indirect are the type of house or car of a person concerned, because this says something about the income and assets of the person concerned. Data that, in combination with other data, can lead to identifiability are also regarded as personal data.

1. Confidential company data, for example (still confidential) financial, technical or legal information, budgets, policy intentions, tenders and stock market-sensitive information. In short, all information that is not (yet) intended for third parties.
2. In the case of (a) privacy-sensitive data, the detailed risk analysis will consist of a so-called pre-DPIA (risk assessment with 9 questions), depending on the outcome followed by a formal DPIA; (b) in the case of confidential information, the classification will take place by checking the reliability requirements (is the desired level of availability, integrity and confidentiality).

Question 2a: Is it about the processing of data and/or financial flows in one or more processes of our organization that should not fall into the hands of crime, because that could seriously damage the trust that the citizen and the company place in the government as reliable?

Question 2b: Is it a primary process or processes of our organization, whereby if these processes are hindered or stopped at any time, in this example the damage to our organization will be great (both in financial sense and also in terms of image damage)?

Yes, a more detailed risk analysis is necessary (testing reliability requirements and, if necessary, agreeing on more and/or heavier security measures, including risk assessment).

No, go to question 3.

## Reliability of products and services

Question 3: Does the CSP provide an acceptable level of service?

Question 3a: Is the CSP of the application ISO 27001 certified?

Question 3b: If there is the storage of data at an external data center, is that data center ISO 27001 certified or otherwise certified (ISAE3402 'Assurance Reports on Controls at a Service Organization' of Service Organization Control (SOC) 2)?

Question 3c: Where is any (source) data of the province stored that is used when working with the application due to unwanted storage outside Europe?

Question 3d: Is the CSP prepared to carry out an external (independent) audit of compliance with laws and regulations?

If one of the 4 sub-questions from question 3 is answered negatively, an alternative solution must be sought for public cloud services, such as a private cloud environment, now or in the future delivered by the government, such as Rijkscloud, or IT outsourcing or on premise in its own data center.

 **Summary of the AIVD's position and policy outlook for the BZK**

In 2019, the General Intelligence and Security Service (AIVD) was asked for a position on the use of public cloud services for classified information or vital government processes, which require resistance to state actors. The Ministry of the Interior and Kingdom Relations (BZK) has also carried out a policy study. In its opinion, the AIVD makes no distinction between government services and other authorities.

Below are some quotes that reflect the core of the AIVD position, on which the policy outlook of BZK is also based.

## NBV position public cloud services (quotes from the AIVD letter dated 09/09/2019)

In the current situation, public cloud services do not offer verifiable and sufficient resistance to state actors because insufficient certainty can yet be obtained:

* that public sector data and processes are technically and procedurally adequately shielded against the cloud service provider, its subcontractors and its employees;
* whereas the cloud service provider can reliably prevent espionage and sabotage attacks by state actors;
* that the cloud service provider can reliably detect espionage and sabotage attacks by state actors and will respond adequately to them;
* that adequate control and supervision is possible on public cloud service providers.

In addition, public cloud services often use the internet, so that access and availability require extra care. In short, at the moment there is insufficient certainty that public cloud service providers can comply with vir-bi and bio. This NBV position is based on the current state of cloud technology, state cyber threats, national and international regulations and contract possibilities. Developments in this area are moving rapidly and it will be necessary to reconsider this position periodically, for example annually.

## Conclusion

In the current situation, therefore, the use of public cloud services is not suitable for classified national information (Dep.V to Stg.ZG), classified EU and NATO information and for vital government processes that require reliable resistance to state actors. The use of public cloud services is therefore also unsuitable for Dep.V classified information that requires reliable detection of state actors.

If it has been determined through risk analysis that no resistance to and no detection of state actors is necessary, then public cloud services can be used. (End of quotes from the AIVD letter.)

## Exploration of Cloud policy for Dutch government services (quotes from letter to CIO-Rijk, 16/09/2019)

= Concept for broad discussion=

This document contains an exploration for Cloud Policy of the Dutch National Service. The aim of this exploration is to give direction to the use and further development of cloud services by departments, and to formulate ambitions, taking into account insights from the AIVD for dealing with threats by Advanced Persistent Threats (APTs) such as state actors. The starting point is that cloud services must meet the conditions of general policy. These conditions are broadly described in the strategic i‐agenda for the Rijksdienst 2019 ‐2021.

## Considerations and policy intention

The cloud policy should clarify how private, hybrid and public cloud services can be used securely by government parties. Because the Baseline Information Security National Office (BIR) has now, formally, been transferred to the BIO, the remainder of this document talks about BIO‐BBN levels while the focus of this document (currently) concerns the National Service.

In this appendix, due to risk management, the possible policies have been elaborated around the application of BBN 1, 2 and 3 for various cloud implementation scenarios. The BIO determines on the basis of requirements for confidentiality. The distinction between three BBNs prevents too much administrative burden being created for simple systems without confidential information or without their own for high availability. While the BIO mainly focuses on confidentiality of data, in the Netherlands, driven by international developments, more attention is also asked for the availability of 'vital systems and processes'. In both applications, risk management with a proportional set of measures is a logical approach.

Risk management involves the insightful and systematic inventory, assessment and – by taking measures – making risks and opportunities manageable that threaten or promote the achievement of the objectives of the organization, in such a way that accountability can be given for the choices made.

## Principles

For all applications, that will have to be met with applicable frameworks.

The version of 1 October 2019 indicates that adjustments will be taken into account as soon as new insights give cause to do so. The aim is to revise these annually, or as much earlier as developments give cause to do so.

With the previous considerations and the input of safety experts, the following policy intentions have been established: For all levels (as outlined in the matrix) the condition applies: a coherent risk analysis has been carried out, in which requirements for vital and critical processes and sensitive data have been taken into account, and this has been followed up. The residual risks are either mitigated or accepted by the owner.

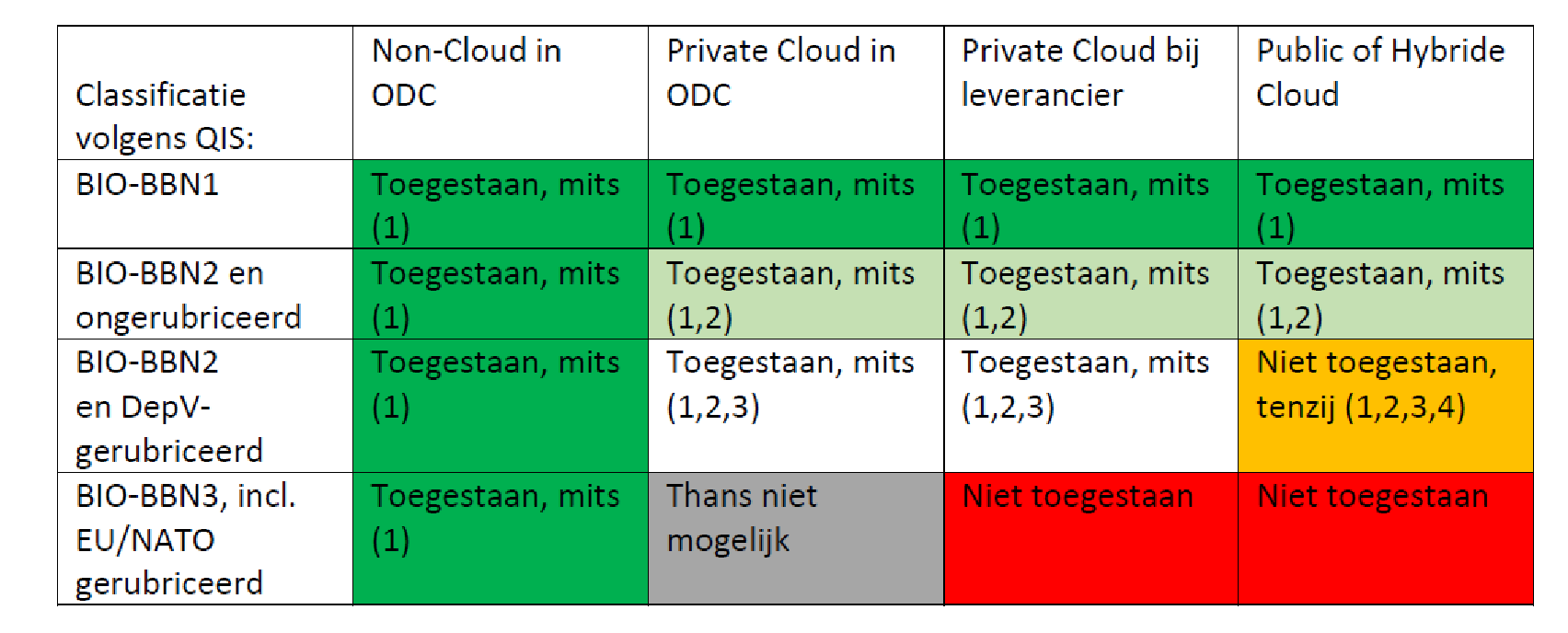


Figure 20: Intended Cloud Policy 1 October 2019 in matrix overview

Conclusion: One Cloud doesn't fit All.

Meaning of numbers 1, 2, 3 and 4 in the matrix:

1. The following are met:
   * A coherent risk analysis for vital and critical processes and sensitive data must have been carried out and the results thereof followed up.
   * The results have been recorded and (auditably) communicated.
   * The residual risks have been accepted by the system or process owner:
   * for departmental processes: with input from the CISO;
   * for interdepartmental processes: with input from the CISO-Rijk.
2. Appropriate facilities should be available to identify and intervene in activities of APTs such as state actors. This concerns a set of detection facilities and measures, which expert services (AIVD, MIVD or NCSC) have indicated are useful in relation to the risk that the department runs with the facility or process.
3. The processing of the (Dep.V) classified BIO‐BBN2 information has been approved in advance by the SG.
4. For the approval of the SG, the expert advice of the AIVD on Cloud services (see above) must be explicitly taken into account. It states (quote) 'the use of public cloud services is therefore also unsuitable for Dep.V classified information that requires reliable detection of state actors' (end of quotes).

1. Cloud computing is a model for quickly providing on-demand network access to a shared pool of configurable IT assets (such as networks, servers, storage, applications, and services) with a minimum of management effort or interaction with the provider (NIST: [https://csrc.nist.gov/publications/detail/sp/800-145/final)](https://csrc.nist.gov/publications/detail/sp/800-145/final). [↑](#footnote-ref-1)
2. The elaborations of the relevant topics are further referred to in this document as objects. [↑](#footnote-ref-2)
3. See [https://www.openkamer.org/kamervraag/2014Z09632/.](https://www.openkamer.org/kamervraag/2014Z09632/) [↑](#footnote-ref-3)
4. Points of attention for consequences has been taken over from Weolcan: [https://blog.weolcan.eu/wat-is-one-Cloud-Exitstrategy-precise-and-how-forage-you-it-from.](https://blog.weolcan.eu/wat-is-een-cloud-exit-strategie-precies-en-hoe-voer-je-het-uit) [↑](#footnote-ref-4)
5. Weolcan: [https://blog.weolcan.eu/wat-is-one-Cloud-Exit-strategy-precise-and-how-forage-you-it-from.](https://blog.weolcan.eu/wat-is-een-cloud-exit-strategie-precies-en-hoe-voer-je-het-uit) [↑](#footnote-ref-5)
6. A "Crypto Policy" object that includes policies about crypto services ap WTJV. [↑](#footnote-ref-6)