BIO Version 1

The Government Information Security Baseline (*Baseline Informatiebeveiliging Overheid* or BIO) is fully structured according to NEN-ISO/IEC 27001:2017, Appendix A and NEN-ISO/IEC 27002:2017.
The Standardisation Forum has included these standards in the 'comply or explain' list of mandatory standards for the public sector, in accordance with the comply or explain principle. This means that the government applies these standards unless there are explicitly stated reasons for not doing so.

The BIO describes the interpretation of the NEN-ISO/IEC 27001:2017 and NEN-ISO/IEC 27002:2017 standards for
the government. It strongly emphasises that BIO does not replace these standards.

In the BIO, specific government measures have the text colour green. NEN-ISO/IEC 27001:2017 and NEN-ISO/IEC 27002:2017 describe details for implementation (implementation guidelines) and requirements for process design (including the ISMS from NEN-ISO/IEC 27001:2017). Thus, those documents provide the details for the application, which are not described in the BIO and remain necessary for the proper implementation of the BIO.

Change history:

VERSION	DATE	COMMENTS
0.1	11-6-2017	Adjustments to BIR 2017 version 0.6
0.2	11-7-2017	Rewriting based on ISO 27001 approach (chapter 4), merge chapters 3 and 4, ISO 27001 approach in chapter 4, textual adjustment of controls (must/should)
0.3		Several comments processed
0.4	10-10-2017	Several comments from members processed, split baseline into 2 parts, analogous to the BIR2017
0.5	20-10-2017	Chapter 4 added in part 2 to secure ISMS as a control / measure
0.6	20-02-2018	Further tightening as a result of review comments, created separate addendum for specific government matters
0.7	02-05-2018	Adjustment as a result of comments from the Ministry of the Interior, 3 parts merged, alignment with the BIR2017 achieved, total revision of BIO, ISMS part lapsed as a result of comments
0.8	21-05-2018	Further adjustments as a result of comments and observations by municipalities, water authorities and provinces
0.9	25-05-2018	Further adjustments as a result of comments and distribution of draft to members of the Standards Working Group
1.0	01-06-2018	Latest changes and comments NCSC and BZK processed
1.01	11-10-2018	Changes from the community, comments Standardisation Forum and small typos fixed, copyright NEN added
1.02	01-11-2018	Designation NEN, year ISO changed from 2013 to 2017, no changes in content, the 2017 version came about as a result of a European decision.
1.03	13-03-2019	Adjusted passage on use of the NEN-ISO/IEC 27001:2017 and NEN-ISO/IEC 27002:2017 standards. Moved this passage and the change history from page 4 to page 2.
1.04	04-11-2019	Adjustments from BIO 1.03 to 1.04 due to maintenance round BIO 2019. Concerns correction of factual inaccuracies and division / adjustment / relocation of certain measures.

Preface

Information security is an important quality aspect of the government's information provision. Securing information, however, is not a one-time affair, but a process that always involves following a Plan-Do-Check-Act cycle.
Going through this process is a responsibility of the line management. To prevent information and information systems from being secured too lightly or too heavily, risk management is an important part of this process.

The first step in the security process is to make a risk assessment. This involves estimating the potential damage if information systems are (temporarily) unavailable, the information lacks integrity and/or this information falls into the wrong hands. It also assesses the threats from which the government needs to be protected. The assessment of potential damage and threats leads to security requirements to mitigate the risk. To cover these requirements, appropriate measures are taken or the (residual) risk is accepted.

The Government Information Security Baseline (BIO) helps line management take responsibility for information security. The complicated process of risk management is simplified with the BIO. In fact, the BIO defines standard basic security levels (*basisbeveiligingsniveaus* or BBNs) based on the generic damages and threats to the government with associated security requirements that must be met. For each business process, line management determines the BBN; the BIO offers a so-called BBN test for this purpose.

The BIO describes for each BBN which controls from the ISO 27002 (Code for Information Security) must be met. For all controls, it must be determined, based on an individual risk assessment, how the security objectives of the control can be met. Where applicable, some of the controls have been elaborated in mandatory, concrete government measures. Controls are assigned to roles, which makes it easier to distribute among responsible parties.
This also allows the service provider who has the expertise to determine which concrete measures to use to fill out the control.

Finally, accountability is required for risk assessment and effective implementation of controls. This accountability is part of the administrative accountability for the security of information systems. The manner and level of detail of accountability depends on the BBN. The higher the BBN, the more detail is required due to the higher potential impact. Service providers are accountable to their (shared) client and there is accountability to the chain partners with whom agreements about the security of information have been made. The client ensures that the services purchased are secured in accordance with the requirements set; the recipients of the services may rely on this and are informed by the client about exceptional situations.

The BIO thus provides the foundation for ensuring that the security of information (systems) of all operating units of government is improved. These business units can be confident that data sent to or received from other parts of government, in line with laws and regulations, is appropriately secured. Where compliance is not (yet) fully possible, the business units must make any risks transparent to their supply chain partners through an 'explain'.

The BIO is divided into two parts with the first part providing the background and the second part covering the actual framework to be implemented.

Table of contents

Part 1

Background BIO

1

Information security in government

1.1 Introduction

Information security is the process of determining the required security of information systems in terms of confidentiality, availability and integrity as well as implementing, maintaining and checking a coherent package of associated measures[1].

In this way, BIO aims to promote the security of information (systems) at all levels of government and administrative bodies of the government, so that all parts can trust that data exchanged between them, in line with laws and regulations, is appropriately secured. The goal is continuity in business processes by ensuring accurate and timely information. This means that the BIO also applies to control and measurement processes insofar as these are used within an administrative body.

In this way, BIO aims to promote the security of information (systems) at all levels of government and administrative bodies of the government, so that all parts can trust that data exchanged between them, in line with laws and regulations, is appropriately secured. The goal is continuity in business processes by ensuring accurate and timely information. This means that the BIO also applies to control and measurement processes insofar as these are used within an administrative body.

The BIO applies to government. In connection with this, the BIO applies to the following governing bodies:

- State Department
- Provinces
- Water Authorities
- Municipalities

In addition, it is recommended that the BIO be embedded in the terms of reference of other government organisations and organisations with which the government collaborates publicly-privately and private partnerships in which the government is the sole shareholder.

1.2 Information security frameworks and government starting points

The government applies risk management to achieve appropriate security of information and information systems within the context of business objectives. Risk management is the identification, assessment and – by taking measures – management of risks and opportunities that threaten or promote the achievement of the organisation's objectives, in such a way that the choices made can be justified[2].

1) Article 1(a) Regulations on Information Security Rijksdienst 2007, *Stcrt.* 2007, 122/11.

2) Article 5(2) BVR and Article 1(d) BVR.

The approach to risk management within the framework of BIO is that information security is handled cyclically and methodically on the basis of a PDCA cycle. The government layers choose the NEN/ISO 27001:2017[3] as the basis for this process-based design of risk management and the establishment of the PDCA cycle. For the central government, further specification is found in the general regulations for the security of information systems: the *Beveilingsvoorschrift Rijksdienst*[4] (BVR) (Security regulations for government agencies), the *Voorschrift Informatiebeveiliging Rijksdienst*[5] (VIR) (Regulations for government agency information security) and the *Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie*[6] (VIR-BI) (Regulations for government agency information security - Special information)

For BIO, the following applies (based on these documents of NEN/ISO 27001 and BVR, VIR and VIR-BI) in summary.

- A broad definition for an information system, namely "a coherent whole of data sets, and the persons, procedures, processes and software associated with them, as well as the storage, processing and communication facilities for the information system"[7].
- Line management is responsible for the security of information (systems).
- Information security is a cyclical process, following the Plan-Do-Check-Act cycle[8].
- This Plan-Do-Check-Act cycle makes line management responsible for taking measures based on risk management.
- The secretary/managing director of an organisation has ultimate responsibility[9] for such security and for the establishment and operation of the security organisation[10].
- Line management establishes the reliability requirements for its information systems based on an explicit risk assessment[11].
- Based on the reliability requirements, line management selects, implements and carries out the measures[12].

First and foremost, the BIO is a common framework of standards for the security of government information (systems). In addition, the BIO translates a number of standards into mandatory government measures:

- based on laws and regulations[13];
- because of the joint security of information chains;
- because they are fundamental to reliable or professional information provision.

The Government Information Security Baseline BIO is based on the ISO 27002 standard[14].

1.3 ISO 27002

The ISO 27002 'Code for Information Security' provides guidelines and principles for initiating, implementing, maintaining and improving information security within an organisation. This standard is a best practice to address information security risks related to confidentiality, integrity, and availability of information assets. The standard can be seen as a further specification of the ISO 27001 standard[15]. The ISO 27002 can serve as a practical guideline for designing security standards within an organisation and an effective method for achieving this security.

3) The NEN/ISO 31000 approach is seen as a good alternative to the 27001.
4) Beveiligingsvoorschrift Rijksdienst 2013, *Stcrt.* 2013, 15496.
5) Voorschrift Informatiebeveiliging Rijksdienst 2007, *Stcrt.* 2007, 122/11.
6) Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie 2013, *Stcrt.* 2013, 15497.
7) Article 1(b) VIR.
8) Article 4 VIR, ISO 6.1 and 9.1.
9) In some organisations, the person with ultimate responsibility is called the "chairman of the board" or "director" and the term "secretary/managing director" should be read as "chairman of the board" or "director".
10) Article 5(2) BVR and Article 4(1) BVR.
11) Article 4(a) and (b) VIR, ISO 27001 6.1 and 6.2.
12) Article 4(a) and (b) VIR, ISO 27001 6.1 and 6.2.
13) For further detail, see: Appendix 1: Laws and regulations.
14) NEN-ISO/IEC 27002:2017, (this is the 27002:2013 with consolidated correction sheets C1 and C2).
15) The NEN-ISO/IEC 27001 standard contains requirements with which the information security management system must comply. This is the standard used when auditing for certification. This standard specifies requirements for establishing, implementing, executing, controlling, assessing, maintaining and improving a documented Information Security Management System (ISMS) in the context of an organisation's overall operating risks.

The ISO consists of 114 controls; the term 'control' is translated in the ISO as a control measure[16]. BIO follows the structure of ISO 27002 and its controls. The controls have been adopted literally[17] in the BIO. This facilitates coordination with external partners or suppliers. In addition, the BIO fills in some of the provisions of the VIR on PDCA cycle and responsibilities in a generic way[18].

1.4 Review and adjustment

With the rapid development of technology, information security measure sets are rapidly becoming obsolete. The BIO is therefore written at an abstract level as much as possible where such changes and developments have the least possible impact on the measures.[19] The BIO describes the what and not the how. Nevertheless, changes may be necessary in the event of, for example, changes to underlying legislation and regulations, new or outdated guidelines or new threats and vulnerabilities.

This document is therefore regularly reviewed in its entirety and adjusted as necessary. In addition, specific consideration is given to whether changes and additions to the measures and (operational) guides are necessary or desirable in order to increase their practical applicability. Decisions about this are made through the existing information security forums and processed by the administrator of the BIO[20].

1.5 Standardisation Forum

The government follows the standards on the 'apply or explain' list of the Standardisation Forum[21] (hereinafter referred to as the Forum). The BIO is based on the NEN-ISO/IEC 27002:2017 and the BIO refers to the NEN-ISO/IEC 27001:2017, both standards are on the 'apply or explain' list[22] of the Forum. A number of technical measures from the BIO are also on the Forum's 'apply or explain' list or 'open standards' list[23]. Not all of these technical interpretations are elaborated in this BIO. The choice has been made to indicate only whether the measure is filled by a mandatory or open standard of the Forum. This makes the BIO less prone to maintenance.

16) The Dutch version of ISO 27002 speaks of control measures. However, there are also implementation measures. To make the distinction between those easier, the BIO applies the term 'controls'. The use of this term is consistent with information security practice.
17) Thus, unlike the various old baselines, the controls have not been textually modified.
18) Specifically, Article 4(a) and (b) of the VIR.
19) The ISO was also drafted from this principle.
20) To this end, a procedure has been agreed upon in the OBDO.
21) See also the website of the Standardisation Forum at https://www.forumstandaardisatie.nl
22) See also: https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht
23) See also: https://www.forumstandaardisatie.nl/open-standaarden/lijst/aanbevolen

Part 1 – BIO Background

2

Structure of the BIO

2.1 Structure of BBNs

In order to keep risk management manageable and efficient, BIO chooses a depth of risk management implementation that is proportional to the interests to be protected in combination with relevant threats. Therefore, the BIO distinguishes three basic security levels (BBNs). For BBN1, the emphasis is on 'what is the minimum expectation'? For BBN2, the focus is on protecting the most common categories of information according to the principle 'does the measure fall under good housekeeping; does this security demonstrate a trustworthy government?'. BBN3[24] applies to classified information Departmental Confidential or similarly confidential at other layers of government, requiring resistance to state actors or similar threats.

The choice of a BBN is made by the process owner and is based on risk management. The BIO is accompanied by a method of risk assessment called the BBN test[25]. Part 2 explains this method in more detail[26].

2.2 Controls

After the BBN test, line management goes through all applicable controls[27] from the BIO[28]. Based on a risk assessment, it is determined how to meet the stated security objectives of the controls. Implementation guidelines from ISO 27002, government measures, and/or operationalisations in guides can be used to meet these goals.

There is a hardship provision: in case a control *cannot* apply to a specific case, the control *is* not applicable. This applies, for example, to a control that pertains to an external link, while the relevant information system does not have an external link. The organisation does not have to answer for that.

2.3 Implementation guidelines

Each control is detailed in the ISO 27002 in implementation guidelines. When performing risk considerations, the implementation guidelines are very helpful. They help in choosing the required security measures. These guidelines should therefore be seen as examples of how the controls *can* be elaborated into measures; following these guidelines is not mandatory.

24) The additional requirements that apply from BBN3 onwards have not yet been detailed in this current version of the BIO.

25) The BBN test is not a full-fledged replacement for the Quickcan BIO or any other comprehensive risk analysis methodology.

The BBN test only ensures that the correct BBN can be easily selected and that it can be determined to what extent additional requirements are necessary.

26) Work will be done on a guide in which changes in levels for the aspects of availability, integrity and confidentiality will be indicated relative to the three BBN levels. Perhaps the controls and measures will be further specified according to the three different aspects.

27) The Dutch version of ISO 27002 speaks of control measures. However, there are also implementation measures. To make the distinction between them easier, the BIO uses the term 'controls'. The use of this term is consistent with information security practice.

28) With the exception of two controls (6.1.4 and 14.2.4), the BIO contains all the controls from the

These implementation guidelines are not included in the BIO; for this, reference is made to the ISO 27002.

2.4 Government measures

Some of the controls are elaborated into mandatory measures because they:

- result from *laws and regulations*[29]. Failure to do so would then violate these external laws and regulations;
- are so basic that they form the *foundation* of a reliable or professional information provision;
- are subject to security in a process chain or network; noncompliance by a single organisation is, on balance, *ineffective* for the entire chain. It constitutes a risk for all other partners in the chain and leads to additional measures and costs for them. For the chain as a whole, this is *inefficient*. For a *generic service*, a consideration analogous to the chain issue applies.

The BIO calls these mandatory measures 'government measures'. The government measures do not cover all of the security objectives of the control. As with the controls, there is a hardship clause here: in the event that a measure *cannot* apply to a specific case, the obligation lapses. This applies, for example, to a government measure that involves an external link, while the relevant information system does not have an external link.

References to relevant legislation and regulations have been added to a number of government measures. These references are either government-wide or specifically tailored to an area of interest (for example, the 'Code of Conduct for the Digital Work Environment') and are mandatory in nature.

2.5 Addendum

The BIO is written generically and is valid for all target groups. Some levels of government have specific laws and regulations that apply only within that layer of government.

In order to meet the needs of these levels of government and not to lose these specific laws and regulations, an addendum has been added to the BIO. In this addendum, these laws and regulations are linked to the control or measure to which they belong. The addendum has been added to the BIO in part 3.

2.6 Operationalisation in guides

To increase the practical applicability of the BIO, the BIO is supplemented with

guides. These are management recommendations that are not mandatory and are not essential to the operation of a system. A guide thus provides advice on how certain norms, standards, techniques or measures can be implemented or handled. A handout may be tailored more specifically to a layer of government (interdepartmental, municipality-wide, etc.) or to a particular area of concern.

This BIO includes references to good guides that are already available; guides may be added over time.

2.7 Roles

Generally, parts of the BIO are applied in different places in the organisation based on different responsibilities and relationships of authority. The BIO distinguishes three (main) roles: the secretary/managing director, the process owner, and the service provider. These roles are described below from the perspective of information security. There are, of course, more roles involved in information security, such as supervisor and employee, but the focus here is on the person responsible for implementing the control.

29) This concerns only the security requirements arising from laws and regulations. Other requirements are beyond the scope of the BIO.

Secretary/ managing director	As the person with final responsibility for security policy in the organisation, the secretary/managing director is responsible for implementing organisation-wide issues regarding information security[30]. In practice, this role may be performed by, for example, the CIO or a director of procurement[31].
Process owner	The process owner means the line manager responsible for the security of the relevant process/information system.
Service provider	This refers to the service provider (e.g. SSO) within the government or organisations in the market to which the secretary/managing director or process owner contracts or outsources (part of) the security task.

The BIO indicates which controls are applicable to which role. Because the government is a pluralist organisation, this allocation is indicative. The BIO does require that the controls and government measures associated with the roles be allocated internally, taking into account sufficient segregation of functions. Generally, the organisation of the information security function, including responsibilities, tasks and authorities, can be found in the organisation's information security policy.[32]

30) In some organisations, the person with final responsibility is called "secretary-general," "director," or "chairman of the board," and the term "secretary/managing director" should be read as "secretary-general," "director," or "chairman of the board."
31) In the case of the State, for example, this may include the security officer (BVA).
32) Article 3(b) VIR.

Part 1 – BIO Background

3

Basic security levels

As described in Section 2.1, the BIO distinguishes three basic security levels (BBNs). Each BBN consists of a number of controls, a number of mandatory government measures and an accountability and supervision regime. Each level builds on the previous level. In doing so, BBN2 complements the controls of BBN1. BBN2 also complements or replaces the government measures of BBN1 with measures of greater weight. The same is true for BBN3 in relation to BBN1 and BBN2.

If information is received from third parties, this received information will be treated in accordance with the instructions of the sender. If the sender does not provide a marking or classification, the information received is handled in accordance with the classification requirements of the receiving process.

3.1 BBN1

Information systems at BBN1 are systems for which for BBN2 is considered too stringent. It may be that higher availability and integrity requirements are still needed. BBN1 is what all government systems must meet as a minimum.

Controls and government measures stem from:
- laws and regulations;
- generally applicable security principles (fundamental controls and measures).

3.2 BBN2

For information systems within the government, BBN2 is the starting point. BBN2 is applicable if[33]:
- confidential information is processed;
- possible incidents lead to administrative commotion;
- the safety of other systems depends on the safety of one's own system.

The interest to be protected in BBN2 is maximum Departmentally Confidential (DepV), (as defined in the VIR-BI)/similarly confidential with other levels of government and privacy-sensitive information with a heightened level of confidentiality. Such information is common in government. It further covers commercially confidential information or policy-making information; thus, it is not limited to information classified as DepV/similarly confidential with other governmental agencies.

BBN2 information is pre-emptively protected against all threats with the exception of advanced threats, such as Advanced Persistent Threats (APTs), originating from state actors or professional criminals. For this, there is protection afterwards: it must be possible to detect them and to respond to them appropriately. Thus, for information systems where Departmentally Confidential information and similar confidentiality is processed at other levels of government and where resistance to the advanced threat of state actors or equivalent professional criminals is required, the BBN2 is not sufficient.

33) See the BBN test in Part 2 for more details.

The controls of BBN2 include the controls of BBN1. This also applies to the measures where some measures of BBN1 are weighted in the BBN2 variant. The choice to do so stems from:

- laws and regulations, particularly security requirements as a result of WBP/GDPR;
- connection requirements of generic/common services;
- dependencies in chains and networks;
- minimum requirements for efficient security of BBN3.

3.3 BBN3

BBN3 focuses on the protection of information classified as Departmentally Confidential and similarly confidential with other levels of government, while resisting the threat, such as Advanced Persistent Threats (APTs), posed by state actors and professional criminals. BBN3 applies if:

- loss of information has a major impact, the loss of which cannot be explained if it is not classified and protected at BBN3;
- information with a classification (other than BBN2) is provided by third parties;
- connection to an infrastructure BBN3 is required to be able to process information on that infrastructure (e.g., to avoid compromising classified information already on the infrastructure).

For reasons of efficiency, BBN3 aligns with relevant NATO regulations that also already take into account the provision of resistance to state actors[34]. This means that BBN3 consists of the controls and governmental measures from BBN2, supplemented by relevant requirements from the VIR-BI, relevant provisions from regulations from other layers of government and from the NATO Information Security Treaty[35]. Not all parts/measures are applicable for the national context and for NATO Restricted[36]. The elaboration of BBN3 will therefore specifically indicate which parts/measures of the NATO Treaty are specifically applicable.

34) For both EU and NATO classified information, the security regulations take into account providing resistance to state actors by default. For BIO, it was ultimately decided to align with NATO regulations because NATO requirements are more detailed than those of the EU and thus provide more assurance that actual resistance to state actors can be provided. For the record, the NATO treaty only has a direct effect on NATO classified information; BBN3 is Dutch information to which the NATO treaty does not directly apply;
the applicability of the NATO treaty for BBN3 is a choice that the government itself makes through this BIO.

35) CM(2002)49 with associated enclosures and directives.

36) There are passages that deal only with the protection of information classified NATO Confidential and above.

4

Accountability for the BIO

The secretary/managing director of an organisation is *ultimately responsible* for the integral security and the design and operation of the security organisation[37]. In this capacity, they are ultimately responsible for the implementation of all security frameworks in their organisation, including the proper application of the BIO.

Administrative accountability for the application of BIO is part of accountability for the security of information (systems). This is also where accountability is given to the chain partners with whom agreements on information security have been made.

4.1 Responsibility dependent on basic security level

The ISO 27001 and the VIR stipulate that line management establishes that the measures taken are demonstrably in line with the reliability requirements and that these measures are complied with[38]. The proportionality described earlier also applies when assigning the level at which responsibility for risk management is vested:

- For BBN1, the process owner is fully responsible for making (responsible) decisions. Only occasionally and upon request do they inform the CISO on the state of affairs regarding its BBN1 information systems.
- For BBN2, the process owner should submit the information system for consultation with the CISO before it is commissioned (preferably in the design/development phase)[39].
- For BBN3, prior permission must be granted by the secretary/managing director for the processing of special information (in accordance with the VIR-BI)[40]. For granting permission, mandating is possible to, for example, the CIO or CISO and, in the case of the national government, to the BVA.

Organisations may deviate from this for BBN1 and BBN2 in the information security policy[41].

4.2 Explains on government measures

Government measures that do not apply do not need to be named as an 'explain'.

The organisation should have a registration of government measures which are not or cannot be fully complied with yet. These are explains according to the 'comply or explain' principle. The resulting risks are also specified here.

Explains regarding government measures can create a difference in protection between parties when working together in chains, creating a risk for the processed (and

37) Article 4(1) BVR.
38) Article 4(b) VIR.
39) In the case of DepV information, in accordance with the VIR-BI, the BBN3 regime for accountability applies.
40) Article 3(b) VIR-BI.
41) Article 3(b) VIR.

shared) information. Parties with explains need to coordinate this with their (collaboration or chain) partners, so that together they take appropriate measures or temporary measures that mitigate or reduce the risk as long as the explains are not implemented in accordance with the BIO.

The following applies to government agencies: explains that affect the security of other parts of the government agencies are provided with a advice from the Security Accreditation Authority (SAA, covered by the Subcommittee on Information Security) and submitted by the ministry to the CIO Board.

4.3 Chain collaboration

Within the government and with other external parties, there is a great deal of collaboration in chains, and therefore, as indicated in Section 1.1, the common security of information chains also forms a basis for the concretisation of government measures.

A chain is a partnership between organisations that, in addition to their own goals, pursue one or more jointly chosen (or politically imposed) goals. These chain partners are independent, but are also dependent on each other when it comes to achieving the joint (chain) goals[42]. An information chain concerns the exchange of information within such a partnership.

In the context of chain collaboration, too, the responsibility for information security cannot be delegated.

If an organisation entrusts information to chain partners, this organisation remains responsible for ensuring that chain partners carefully protect the entrusted information. The organisation must therefore require or impose connection requirements on the supplying or purchasing party. In addition, the organisation must provide delivery guarantees to the receiving party. To do this, the organisation must have an understanding of which information systems and infrastructures it depends on, which depend on it, and how the governance of both of these is structured.

4.4 Service providers

The BIO does not distinguish between internal or external service providers when declaring controls and government measures applicable. Internal and external service providers are also treated equally in the way their services are accounted for. This means the following for all service providers.

- Periodically, all service providers are held accountable through a Statement of Compliance (or partial ICV; with applicable scope) to the client at the government.

- Service providers follow the security requirements set by government organisations or chain partners for the services of the service provider. For reasons of efficiency, a service provider may offer a standard security level, but this does not diminish the stated responsibility of government organisations.

- For services provided to a single organisation, the service provider is accountable to the commissioning organisation. The commissioning organisation includes accountability in its ICV. The commissioning organisation also oversees specific services.

- For services offered to multiple governments or governmental entities, the service provider establishes one accountability for the benefit of all customers. For the State, the CIO Board determines annually who will oversee the security of these services.

42) https://noraonline.nl/wiki/Ketensturing/De_wereld_van_ketens/Wat_is_een_keten%3F .

In addition to being accountable for their services, service providers are themselves bound as an organisation to information security rules. Here, however, there is a distinction between internal and external service providers:

- Internal service providers, as part of the government, are themselves directly bound by the BIO. As such, they are bound by the regular accountability and oversight procedures of the relevant levels of government. With the State, this includes oversight from the ADR, ARK and the BVA. The internal service provider is also bound to deliver an annual In Control Statement (*In Control Verklaring* or ICV). In it, the service provider declares that it is in compliance with the BIO (including government measures) for its own operations.

- External service providers are not part of the government and therefore are not themselves directly bound by the BIO or the delivery of an ICV. They do have to meet the client's requirements. Conditions for the purpose of information security should therefore be stipulated in the contract. In the BIO, Chapter 15 on supplier relationships includes controls and government measures to ensure proper assurance of information security in contracts.

It is possible for an (external) service provider to have a quality mark such as an ISO 27001 certificate or, for example, an ISAE 3402 statement. The value of such a seal or statement depends on its scope and depth. It usually says something about the process that is set up at the service provider. So while this does add value, has overlap with the BIO controls, and can be used as part of the Statement of Compliance, it does not fully encompass and capture the accountability for the government measures from the BIO. Additional agreements will always need to be made about the 'gap' between quality mark or directive and the BIO controls. Additional justification must be provided for this.

Part 2

BIO Framework

Introduction

The BIO Framework consists of a BBN test to determine the appropriate basic security level (BBN) and the tables of controls and measures. The BBN test is performed for each business process. The BBN determines which controls to go through next. For each control, it must be determined what measures are needed in addition to the mandatory government measures. For further explanation of the structure of the BIO and the BBNs, please refer to Part 1 of this BIO.

In the document, the controls are then structured as follows:

Control number in accordance with with ISO 27002	**BBN (1, 2 or 3)**	**Control text (ISO 27002)**	**Responsible party(ies)** Secretary/managing director Process owner Service provider
O-measure number	BBN (1, 2 or 3)	G-measure	
		Guide *(optional)*	

To indicate the difference between ISO 27002 controls and government measures, different colour markings have also been used:

- Blue are the ISO controls.
- Green are government measures (G-measure).

Where appropriate, reference is made to guides to elaborate the measures. These guides are not mandatory, do not have a number and are shown as a link.

The 'Responsible party(ies)' column indicates who is responsible for implementing the control: secretary/managing director (ultimately responsible for an organisation's operations), process owner and/or service provider.

BBN test

In going through this test, BBN2 is the starting point for all information systems.

Step 1: Is BBN2 sufficient?
Usually, BBN2 applies to a specific information system. However, BBN2 may not be sufficient. BBN2 is insufficient if:

- the information needs to be protected from state actors or similar threats;
- information is provided by third parties and they require BBN3 for the security of the relevant information;
- connection to an infrastructure BBN3 is required to be able to process information on that infrastructure (e.g., to avoid compromising classified information already on the infrastructure).

In each of these cases, BBN3 or higher (see VIR-BI in the case of the State) is applicable.

Step 2: Is BBN2 too stringent?
In BBN2 information systems, the unwanted or unintended disclosure of information can lead to BBN2 damage:

- Political damage to a director: director must be accountable to the (elected) controlling bodies, e.g. in response to accountability questions.
- repair diplomatic damage through official scaling up.
- Financial implications: can no longer be absorbed within the budget of the (implementing) organisation; no auditor's report issued.
- Loss of public respect; citizen complaints or significant loss of employee motivation.
- Binding designation of the Dutch Data Protection Authority in connection with violation of privacy.
- Direct damage to reputation, for example through negative publicity.

If such damages do not apply, then BBN1 applies.

Step 3: Determine additional requirements for availability and/or integrity
In the case of BBN1, does systems failure and/or information mutilation result in damage similar to BBN2 damage[43]? In that case, it can be considered to take (part) of the BIO controls and measures, which oversee availability or integrity at the level of BBN2. Accountability and monitoring are done according to BBN2.

In the case of BBN2 or BBN3, does systems failure and/or the mutilation of information result in greater damage than the BBN2 damage[44]? In that case, it is determined on the basis of an explicit risk assessment which controls require additional and/or more stringent measures. Accountability and monitoring are done according to BBN3.

43) See step 2.
44) See step 2.

Controls and government measures

For the sake of recognisability, it was decided to keep the numbering of the chapters and the controls in line with the numbering used in the ISO 27002.

5

Information security policies

5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1	**1**	**Policies for information security** A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.	Secretary/ Managing Director
5.1.1.1	1	An information security policy has been established by the organisation. This policy is established by the organisation's leadership and includes at least the following items: a. The strategic principles and preconditions that the organisation uses for information security and in particular the embedding in and alignment with the general security policy and the information provision policy. b. The organisation of the information security function, including responsibilities, tasks and powers. c. The assignment of responsibilities for chains of information systems to line managers. d. The common reliability requirements and standards applicable to the organisation. e. The frequency with which the information security policy is reviewed. f. The promotion of security awareness.	
		Guides: BIO-001-Informatiebeveiligingsbeleid	

5.1.2	1	**Review of the policies for information security** The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Secretary/ Managing Director
5.1.2.1	1	The information security policy is periodically assessed and, if necessary, adjusted in line with the (existing) governance and P&C cycles and external developments.	

6

Organisation of information security

6.1 Internal organisation

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation.

6.1.1	**1**	**Information security roles and responsibilities** All information security responsibilities shall be defined and allocated.	Secretary/managing director
6.1.1.1	1	The organisation's leadership has defined what the responsibilities and roles are in the area of information security within its organisation.	
6.1.1.2	1	Information security responsibilities and roles are based on relevant regulations and laws.	
6.1.1.3	1	The role and responsibilities of the Chief Information Security Officer (CISO) are defined in a CISO job profile.	
6.1.1.4	1	A CISO has been appointed in accordance with an established CISO job profile.	
		Guide: BIO-CISO-functieprofiel	
6.1.2	**1**	**Segregation of duties** Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	Process owner Service provider
6.1.2.1	1	Measures are in place that detect or prevent unintentional or unauthorised access to the organisation's assets.	
6.1.3	**2**	**Contact with authorities** Appropriate contacts with relevant authorities shall be maintained.	Secretary/managing director Process owner Service provider
6.1.3.1	2	The organisation has elaborated who is in contact with what (government) agencies and regulators regarding information security matters (permits/incidents/ calamities) and what requirements are relevant to these matters.	
6.1.3.2	2	The contact overview is updated annually.	
6.1.4	**-**	**Lapsed**	-
6.1.5	**2**	**Information security in project management** Information security shall be addressed in project management, regardless of the type of the project.	Process owner Service provider

6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

6.2.1	**1**	**Mobile device policy** A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Process owner Service provider
		Guide: BIO Mobile Device Management[45]	
6.2.1.1	2	Mobile devices are set up so that business information is not stored unknowingly ('zero footprint'). If zero footprint is not (yet) achievable, a mobile device (such as a laptop, tablet, and smartphone) offers the opportunity to protect access through an access security mechanism and, if confidential data is stored, encryption of that data. In the case of storage of confidential information, these mobile devices must allow for 'remote erasure'.	
6.2.1.2	2	At a minimum, the following aspects are implemented in the deployment of mobile devices: a. Awareness programmes address behavioural aspects of safe mobile work. b. The device is part of patch management and hardening. c. Mobile Device Management (MDM) or Mobile Application Management (MAM) solutions are used. d. Users sign a mobile work user agreement, declaring that they are aware of the dangers of mobile work and that they will do so safely. This statement relates to all mobile devices used by the employee for business purposes. e. Compliance with paragraphs (b), (c) and (d) shall be reviewed periodically.	
6.2.2	**2**	**Teleworking** A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Secretary/ managing director Service provider
		Guide: BIO Teleworking Policy	

45) MAM (Mobile Application Management) is also part of that.

7

Human resource security

	General guide: Human resources

7.1 Prior to employment

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

7.1.1	**1**	**Screening** Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Secretary/ managing director Process owner
7.1.1.1	1	Each organisation has an established screening policy. A Certificate of Good Conduct (VOG) may be requested upon commencement of employment and upon change of position.	
7.1.2	**1**	**Terms and conditions of employment** The contractual agreements with employees and contractors shall state their and the organisation's responsibilities for information security.	Secretary/ managing director Process owner
7.1.2.1	1	All employees (internal and external) are made aware of their responsibilities regarding information securities upon appointment or internal transfer. The regulations and instructions applicable to them with regard to information security are easily accessible.	

7.2 During employment

Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

7.2.1	**1**	**Management responsibilities** Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	Secretary/ managing director
7.2.1.1	1	There is affiliation with a whistleblower programme so that anyone can report security issues anonymously and safely.	

7.2.2	**1**	**Information security awareness, education and training** All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.	Secretary/ managing director Process owner
7.2.2.1	1	All employees have a responsibility to protect the organisation's information. Everyone knows the rules and requirements related to information security and, where relevant, the special requirements for classified environments.	
7.2.2.2	1	All employees and contractors using the information systems and services have successfully completed I-awareness training within three months of employment.	
		Guide: i-Awareness Government	
7.2.2.3	1	Management emphasises to its employees and contractors at the time of appointment and internal transfer and, for example, in work meetings or in personnel interviews, the importance of information security education and training and actively encourages them to follow it periodically.	
7.2.3	**1**	**Disciplinary process** There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Secretary/ managing director

7.3 Termination and change of employment

Objective: To protect the organisation's interests as part of the process of changing or terminating employment.

7.3.1	**1**	**Termination or change of employment responsibilities** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Secretary/ managing director Process owner

8

Asset management

8.1 Responsibility for assets

Objective: To identify organisational assets and define appropriate protection responsibilities.

8.1.1	**1**	**Inventory of assets** Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Process owner Service provider
		Guide: Coherence of management processes and information security	
8.1.2	**1**	**Ownership of assets** Assets maintained in the inventory shall be owned.	Process owner Service provider
8.1.3	**1**	**Acceptable use of assets** Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Secretary/ managing director Process owner
8.1.3.1	1	All employees are demonstrably made aware of the code of conduct for the use of the organisation's assets.	
8.1.3.2	1	The code of conduct for the use of the organisation's assets are laid down in the contract for external personnel in accordance with the house rules or code of conduct.	
8.1.4	**1**	**Return of assets** All employees and external party users shall return all of the organisational assets in their possession upon termination of their employment, contract or agreement.	Secretary

8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation.

8.2.1	**1**	**Information classification** Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Process owner
		Guide: BIO-Dataclassificatie	
8.2.1.1	1	The information in all information systems has been classified through explicit risk assessment, so that it is clear what protection is needed.	
8.2.2	**1**	**Labelling of information** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.	Process owner
8.2.3	**1**	**Handling of assets** Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.	Process owner Service provider

8.3 Media handling

Objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.

8.3.1	**1**	**Management of removable media** Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.	Process owner Service provider
		Guide: Mobile data carriers	
8.3.1.1	1	There is a deletion instruction that states that removable media that is reusable and leaves the organisation has its unnecessary content irretrievably removed (ISO 27002 – Implementation Guideline 8.3.1.a).	
8.3.2	**2**	**Disposal of media** Media shall be disposed of securely when no longer required, using formal procedures.	Service provider
		Guide: Disposal of ICT resources	
8.3.2.1	2	Media containing confidential information is stored in a location that is not accessible to unauthorised persons.	
8.3.2.2	2	Disposal is done in a safe way, for example by burning or shredding. Removal of data only is also possible by deleting the data before the media is used for another application in the organisation (ISO 27002 – Implementation Guideline 8.3.2.a).	
8.3.2.3	2	To erase all data on the medium, the data is irretrievably deleted, for example, by overwriting at least twice with fixed data and once with random data. It is verified that all data has been irretrievably deleted.	
8.3.3	2	**Physical media transfer** Media containing information shall be protected against unauthorised access, misuse or corruption during transportation.	Secretary/ managing director
8.3.3.1	2	There is an established procedure for the physical transport of media.	
8.3.3.2	2	The use of couriers or transporters for transportation of information classified at BBN2 or higher meets predefined reliability requirements.	

9

Access control

	General guide: Logical access control policy	

9.1 Business requirements of access control

Objective: To limit access to information and information processing facilities.

9.1.1	**1**	**Access control policy** An access control policy shall be established, documented and reviewed based on business and information security requirements.	Secretary
9.1.2	**1**	**Access to networks and network services** Users shall only be provided with access to the network and network services that they have been specifically authorised to use.	Service provider
		Guide: MDM	
9.1.2.1	1	Only authenticated devices can access a trusted zone.	
9.1.2.2	1	Users with their own or unauthenticated devices (Bring Your Own Device) will only be granted access to an untrusted zone.	

9.2 User access management

Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.

9.2.1	**1**	**User registration and de-registration** A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Process owner Service provider
9.2.1.1	1	There is a comprehensive formal registration and log-off procedure for managing user identifiers.	
9.2.1.2	1	The use of group accounts is not permitted unless justified and recorded by the process owner.	

9.2.2	**1**	**User access provisioning** A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Process owner Service provider
9.2.2.1	1	Access to information systems has been granted only after authorisation by an authorised officer.	
9.2.2.2	1	Based on a risk assessment, it has been determined where and in what way segregation of duties is applied and what access rights are given.	
9.2.2.3	2	There is an up-to-date mandate register or job profiles showing which individuals have authority to grant access rights.	
9.2.3	**1**	**Management of privileged access rights** The allocation and use of privileged access rights shall be restricted and controlled.	Process owner Service provider
9.2.3.1	2	The issued special authorities shall be reviewed at least quarterly.	
9.2.4	**1**	**Management of secret authentication information of user** The allocation of secret authentication information shall be controlled through a formal management process.	Service provider
9.2.5	**1**	**Review of user access rights** Asset owners shall review users' access rights at regular intervals.	Process owner Service provider
9.2.5.1	1	All issued access rights shall be reviewed at least once a year.	
9.2.5.2	1	Follow-up on findings is documented and treated as a security incident.	
9.2.5.3	2	All issued access rights shall be reviewed at least once every six months.	
9.2.6	**1**	**Removal or adjustment of access rights** The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Process owner Service provider

9.3 User responsibilities

Objective: To make users accountable for safeguarding their authentication information.

9.3.1	**1**	**Use of secret authentication information** Users shall be required to follow the organisation's practices in the use of secret authentication information.	Secretary/ managing director Service provider
9.3.1.1	2	Employees are supported in managing their passwords by providing a password vault.	

9.4 System and application access control

Objective: To prevent unauthorised access to systems and applications.

9.4.1	**1**	**Information access restriction** Access to information and application system functions shall be restricted in accordance with the access control policy.	Process owner Service provider
9.4.1.1	2	Measures are in place to ensure the physical and/or logical isolation of information of specific interest.	
9.4.1.2	2	Users can access and process only the information with specific interest that they need to perform their task.	
9.4.2	**1**	**Secure log-on procedures** Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Process owner Service provider
9.4.2.1	1	If access is granted from an untrusted zone to a trusted zone, this is done only on the basis of at least two-factor authentication.	
9.4.2.2	2	Granting access to the network to external suppliers is subject to prior risk assessment. The risk assessment determines the conditions under which suppliers are granted access. A record shows how the rights were granted.	

9.4.3	**1**	**Password management system** Password management systems shall be interactive and shall ensure quality passwords.	Service provider
9.4.3.1	1	If two-factor authentication is not used, the password length is at least 8 positions and complex in composition. With a password length of 20 positions or more, the complexity requirement is dropped. The number of failed login attempts is up to 10. The length of time an account is blocked after exceeding the number of times of incorrect login is recorded.	
9.4.3.2	2	In situations where two-factor authentication is not possible, the password is renewed at least every six months (see also 9.4.2.1).	
9.4.3.3	2	Password requirements should be enforced automatically.	
9.4.3.4	2	Initial passwords and passwords that have been reset have a maximum validity of one business day and must be changed upon first use.	
9.4.3.5	2	Passwords that comply with the password policy have a maximum validity period of one year. Where the policy is not applicable, a maximum validity period of six months applies.	

9.4.4	**1**	**Use of privileged utility programs** The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Service provider
9.4.4.1	1	Only authorised personnel have access to system resources.	
9.4.4.2	2	The use of system resources is logged. The logging is available for research for six months.	

9.4.5	**1**	**Access control to program source code** Access to program source code shall be restricted.	Process owner Service provider

10

Cryptography

	General guide: Encryption Policy

10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

10.1.1	**2**	**Policy on the use of cryptographic control measures** A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Secretary
10.1.1.1	2	The cryptography policy elaborates at least on the following topics: a. When cryptography is deployed. b. Who is responsible for implementation. c. Who is responsible for key management. d. What standards serve as the basis for cryptography and how the Forum's standards are applied. e. The way in which the level of protection is determined. f. When communicating between organisations, policies are set mutually.	
10.1.1.2	2	Cryptographic applications comply with appropriate standards.	
10.1.2	**1**	**Key management** A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Service provider
10.1.2.1	2	In case of PKIoverheid certificates: apply the PKIoverheid requirements regarding key management. In other situations: apply the standard ISO 11770 for cryptographic key management.	
10.1.2.2	2	There are (contractual) agreements on spare certificates from an alternative supplier if risk assessment shows that they are necessary.	

11

Physical and environmental security

	General guide: Access policy	

11.1 Secure areas

Objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.

11.1.1	**1**	**Physical security perimeter** Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Secretary/ managing director
11.1.1.1	1	Standards are used to set up secure areas.	
11.1.2	**1**	**Physical entry controls** Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Secretary/ managing director
11.1.2.1	2	In the event of concrete security risks, warnings are sent, in accordance with mutual agreements, to the relevant colleagues within the government security domain.	
		Guide: Protocol for the exchange of personal security information	
11.1.3	**1**	**Securing offices, rooms and facilities** Physical security for offices, rooms and facilities shall be designed and applied.	Process owner Service provider
11.1.3.1	1	Key management is set up based on a key plan.	
11.1.4	**1**	**Protecting against external and environmental threats** Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Process owner Service provider
11.1.4.1	1	The organisation has established which paper records and equipment are critical to the operation. Security measures have been taken against external threats based on an explicit risk assessment.	
11.1.4.2	1	Housing of IT equipment takes into account the probability of consequences of disasters caused by nature and human action.	

11.1.5	**2**	**Working in secure areas** Procedures for working in secure areas shall be designed and applied.	Process owner Service provider
11.1.6	**1**	**Delivery and loading areas** Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.	Service provider

11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.

11.2.1	**1**	**Equipment siting and protection** Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.	Service provider
11.2.2	**1**	**Supporting utilities** Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Service provider
11.2.3	**1**	**Cabling security** Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Service provider
11.2.4	**1**	**Equipment maintenance** Equipment shall be correctly maintained to ensure its continued availability and integrity.	Service provider
11.2.5	**1**	**Removal of assets** Equipment, information or software shall not be taken off-site without prior authorisation.	Service provider
11.2.6	**1**	**Security of equipment and assets off-premises** Security shall be applied to off-site assets taking into account the different risks of working outside the organisation's premises.	Service provider
11.2.7	**1**	**Secure disposal or reuse of equipment** All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Service provider
		See government measures of 8.3.2.	

11.2.8	**1**	**Unattended user equipment** Users shall ensure that unattended equipment has appropriate protection.	Process owner Service provider
11.2.9	**1**	**Clear desk and clear screen policy** A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Secretary/ managing director Service provider
11.2.9.1	2	An unmanned workstation is always locked.	
11.2.9.2	2	Information is automatically made inaccessible with, for example, a screen saver after an inactivity of no more than 15 minutes.	
11.2.9.3	2	Sessions on remote desktops are locked on the remote platform after a set period of time.	
11.2.9.4	2	Taking over sessions on remote workstations at another workstation is only possible through the same secure login procedure used to create the session. This may only be deviated from after an explicit risk assessment.	
11.2.9.5	2	When using a chip card token to access systems, when the token is removed, the access security lock is automatically activated.	
		Guide: Logical access control	

12

Operations security

12.1 Operational procedures and responsibilities

Objective: To ensure correct and secure operations of information processing facilities.

12.1.1	**1**	**Documented operating procedures** Operating procedures shall be documented and made available to all users who need them.	Process owner Service provider
12.1.2	**1**	**Change management** Changes to the organisation, business processes, information processing facilities and systems that affect information security shall be controlled.	Process owner Service provider
12.1.2.1	1	At a minimum, the change management procedure addresses: a. administering changes; b. risk assessment of potential impacts of the changes; c. approval process for changes.	
		Guide: Coherence of management processes and information security	
12.1.3	**1**	**Capacity management** The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Service provider
12.1.4	1	**Separation of development, testing and operational environments** Development, testing, and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment.	Process owner Service provider
12.1.4.1	2	No testing is done in the production environment. This can only be deviated from with the prior approval of the process owner and written record of this.	
12.1.4.2	2	Changes to the production environment are always tested before they are put into production. This may only be deviated from with prior approval by the process owner and written record of this.	

12.2 Protection from malware

Objective: To ensure that information and information processing facilities are protected against malware.

12.2.1	**1**	**Controls against malware** Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Secretary/ managing director Service provider
		Guide: Implementation of detection solutions Guide: Anti-malware policy	
12.2.1.1	1	File downloading is controlled and limited based on risk and need-of-use.	
12.2.1.2	1	Users are educated about the risks with respect to surfing behaviour and clicking on unknown links.	
12.2.1.3	1	The anti-malware software and associated recovery software used is current and supported by periodic updates.	
12.2.1.4	1	Computers and media are routinely scanned as a precaution. The scan performed should include: a. Scanning all files received over networks or via any form of storage medium for malware before use. b. Attachments and downloads before use.	
12.2.1.5	1	The malware scan is performed in various environments, such as mail servers, desktop computers, and upon access to the organisation's network.	

12.3 Backup

Objective: To protect against the loss of data.

12.3.1	**1**	**Information backup** Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Process owner Service provider
		Guide: Back-up and recovery	
12.3.1.1	1	A backup policy is in place that defines and establishes requirements for retention and protection.	
12.3.1.2	1	Based on an explicit risk assessment, the maximum allowable data loss and the maximum recovery time after an incident were determined.	
12.3.1.3	2	At a minimum, the backup policy contains the following requirements: a. Data loss is up to 28 hours. b. Recovery time in case of incidents is a maximum 16 working hours (two 8-hour days) in 85% of cases.	
12.3.1.4	2	The backup process provides for storage of the backup at one location, where an incident at one location cannot result in damage at another.	
12.3.1.5	2	The restore procedure is tested at least annually or after a major change to ensure proper operation if it must be performed in an emergency.	

12.4 Logging and monitoring

Objective: To record events and generate evidence.

12.4.1	**1**	**Event logging** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Process owner Service provider
		Guide: Logging policy	
		Guide: NCSC guide detection solutions	
12.4.1.1	1	A log line contains at least: a. the event; b. the necessary information to trace the incident to a natural person with a high degree of certainty; c. the device used; d. the result of the action; e. the date and time of the event.	
12.4.1.2	1	A log line never contains data that could lead to a security breach.	
12.4.1.3	2	The information processing environment is monitored by an SIEM and/or SOC through detection facilities, such as the National Detection Network (for central government organisations only). These are deployed on the basis of a risk assessment, based in part on the nature of the data and information systems to be protected, so that attacks can be detected.	
12.4.1.4	2	When new threats (attacks) are discovered via 12.4.1.3, they are mandatorily shared within the government within applicable legal frameworks, including with the NCSC (for central government organisations only) or through the sectoral CERT (for other government organisations), through (preferably automated) threat intelligence sharing mechanisms.	
12.4.1.5	2	The SIEM and/or SOC have clear rules about when an incident must be reported to the management responsible.	
12.4.2	**1**	**Protection of log information** Logging facilities and log information shall be protected against tampering and unauthorised access.	Service provider
12.4.2.1	1	There is a summary of log files that are generated.	
12.4.2.2	1	For the purpose of log analysis, the logging retention period is determined based on an explicit risk assessment. Within this period, the availability of the log information is ensured.	
12.4.2.3	2	There is an (independent) internal audit procedure that tests for the unchanged existence of log files at least semi-annually.	
12.4.2.4	2	Improper modification or deletion of log data or attempts to do so will be reported as a security incident as soon as possible through the information security incident procedure in accordance with Chapter 16.	
12.4.3	**1**	**Administrator and operator logs** System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Service provider
12.4.4	**1**	**Clock synchronisation** The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised to a single reference time source.	Service provider

12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

12.5.1	**1**	**Installation of software on operational systems** Procedures shall be implemented to control the installation of software on operational systems.	Service provider

12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

Management of technical vulnerabilities		Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Service provider
		Guide: Penetration tests	
12.6.1.1	1	If the probability of abuse and the expected damage are both high (NCSC vulnerability alert classification), patches are installed as soon as possible, but no later than within a week. In the meantime, mitigating measures are taken based on an explicit risk assessment.	
12.6.2	**1**	**Restrictions on software installation** Rules governing the installation of software by users shall be established and implemented.	Service provider
12.6.2.1	2	Users cannot install anything themselves on their work environment, other than what is offered or allowed through the ICT vendor (whitelist).	

12.7 Information systems audit considerations

Objective: To minimise the impact of audit activities on operational systems.

12.7.1	**1**	**Information systems audit controls** Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Process owner Service provider

13

Communications security

13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

13.1.1	**1**	**Network controls** Networks shall be managed and controlled to protect information in systems and applications.	Service provider
13.1.2	**1**	**Security of network services** Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Service provider
13.1.2.1	2	The data traffic entering or leaving the organisation is monitored / analysed for malicious elements using detection facilities (as described in the guideline for implementation of detection solutions), such as the National Detection Network (for central government organisations only) or GDI, which are deployed based on a risk assessment, partly based on the nature of the data and information systems to be protected.	
		Guide: NCSC guide detection solutions	
13.1.2.2	2	When new threats are discovered via 13.1.2.1, they are mandatorily shared within the government, including with the NCSC (for central government organisations only) or the sectoral CERT, preferably by automated mechanisms (threat intelligence sharing), taking into account the applicable legal frameworks.	
13.1.2.3	2	Wireless connections such as Wi-Fi and wired connections outside the controlled area will use encryption means for which the NBV has issued a positive deployment recommendation.	
13.1.2.4	1	In interconnection points with remote or untrusted zones, measures are in place to identify and respond to possible attacks that negatively affect the availability of the information supply (e.g. DDoS attacks, Distributed Denial of Service attacks).	
13.1.3	**1**	**Segregation in networks** Groups of information services, users and information systems shall be segregated on networks.	Service provider
13.1.3.1	2	All separated groups have a defined security level.	

13.2 Information transfer

Objective: To maintain the security of information transferred within an organisation and with any external entity.

13.2.1	**1**	**Information transfer policies and procedure** Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Secretary/ managing director
13.2.2	**1**	**Agreements on information transfer** Agreements shall address the secure transfer of business information between the organisation and external parties.	Process owner Service provider
13.2.3	**1**	**Electronic messaging** Information involved in electronic messaging shall be appropriately protected.	Service provider
13.2.3.1	1	For the security of electronic (e-mail) messages, the established open standards against phishing and eavesdropping apply to the 'comply or explain' list of the Forum. For securing website traffic, the open standards against eavesdropping on the Forum's 'apply or explain' list apply.	
13.2.3.2	2	For secure message exchange with basic registration systems, in accordance with the 'apply or explain' list of the Forum, the current version of Digikoppeling is used.	
13.2.3.3	2	Use PKIoverheid certificates for web and mail traffic of sensitive data. Sensitive data includes digital documents within the government from which users can derive rights.	
13.2.3.4	2	To provide assurance of the integrity of the electronic message, electronic signatures use the AdES Baseline Profile standard.	
13.2.4	**1**	**Confidentiality or non-disclosure agreements** Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed and documented.	Secretary/ managing director Process owner Service provider

14

System acquisition, development and maintenance

14.1 Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

14.1.1	**1**	**Information security requirements analysis and specification** The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Process owner
14.1.1.1	1	For new information systems and for changes to existing information systems, an explicit risk assessment must be performed for the purpose of determining security requirements, based on the BIO.	
		Guide: Risk analysis method	
		Guide: Risk management ISO 27005	
14.1.2	**1**	**Securing application services on public networks** Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.	Service provider
		See government measure 13.2.3.3.	
14.1.3	**1**	**Protecting applications services transactions** Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.	Service provider
		See government measure 13.2.3.3.	

14.2 Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

14.2.1	**1**	**Secure development policy** Rules for the development of software and systems shall be established and applied to developments within the organisation.	Secretary/managing director Process owner
14.2.1.1	1	The common principles around 'security by design' are the starting point for the development of software and systems.	
		Guide: Grip on Secure Software Development (SSD).	
14.2.2	**1**	**System change control procedures** Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Process owner Service provider
		Guide: Change management process	
14.2.2.1	1	Change management takes place based on a generally accepted management framework.	
14.2.3	**2**	**Technical review of applications after operating platform changes** When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organisational operations or security.	Service provider
6.1.4	**-**	**Lapsed**	-
14.2.5	**1**	**Secure system engineering principles** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Service provider
14.2.5.1	1	See government measure 14.2.1.1	
14.2.6	**1**	**Secure development environment** Organisations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Service provider
14.2.6.1	1	System development environments are appropriately secured based on an explicit risk assessment	

14.2.7	**1**	**Outsourced development** The organisation shall supervise and monitor the activity of outsourced system development.	Process owner
14.2.7.1	1	A prerequisite for outsourcing processes is an explicit risk assessment. The necessary security measures that follow from this are imposed on the supplier.	
14.2.8	**1**	**System security testing** Testing of security functionality shall be carried out during development.	Service provider
14.2.9	**1**	**System acceptance testing** Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Process owner Service provider
14.2.9.1	1	Structured testing methodologies are used for acceptance testing of systems. The tests are preferably automated.	
14.2.9.2	1	A report is made of the test results.	

14.3 Test data

Objective: To ensure the protection of data used for testing.

14.3.1	**2**	**Protection of test data** Test data shall be selected carefully, protected and controlled.	Process owner Service provider

15

Supplier relationships

15.1 Information security in supplier relationships

Objective: To ensure protection of the organisation's assets that is accessible by suppliers.

15.1.1	**1**	**Information security policy for supplier relationships** ion security requirements for mitigating the risks associated with supplier's access to the organisation's assets shall be agreed with the supplier and documented.	Secretary/ managing director Process owner
15.1.1.1	1	In calls for tenders where information (supply) plays a role, requirements with regard to information security (availability, integrity and confidentiality) are specified. These requirements are based on an explicit risk assessment.	
15.1.1.2	2	Based on an explicit risk assessment, the control measures related to supplier access to business information are determined.	
15.1.1.3	2	With all suppliers who process personal data as processors for or on behalf of the organisation, processing agreements are concluded in which all legally required agreements are established.	
		Guide: Whitepaper Cloud computing	
		Guide: Cloud computing	
		Guide: Processor agreements (government), Model processor agreement municipalities (municipalities)	

15.1.2	**1**	**Addressing security within supplier agreements** All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information.	Process owner Service provider
15.1.2.1	1	The security requirements from the request for proposal are explicitly included in the (procurement) contracts where information plays a role.	
15.1.2.2	1	Procurement contracts explicitly include performance indicators and associated accountability reports.	
15.1.2.3	1	In situations where contract terms are imposed by suppliers, a risk assessment was used prior to signing the contract to clarify the consequences of this for the organisation. It is made explicit which consequences are accepted and which must be mitigated upon entering into the agreement.	
15.1.2.4	1	To ensure confidentiality or secrecy, standard procurement terms and conditions are used in IT procurement.	
15.1.2.5	2	Before entering into a contract, a risk assessment determines whether dependence on a supplier is manageable. An explicit elaboration of the exit strategy is a fixed part of the contract.	
15.1.2.6	2	Procurement contracts explicitly include the possibility of an external audit that can be used to test the reliability of the service provided. An audit is not required if the contractor demonstrates through certification that the desired reliability of the service is assured.	
		Guide: Model for a processor agreement	
15.1.3	**1**	**Information and communication technology supply chain** Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Process owner Service provider
15.1.3.1	2	Suppliers must disclose their supply chain and be transparent about the measures they have taken to extend the requirements imposed on them to their suppliers.	
		Guide: Procurement terms and information security requirements	
		Guide: Change management process	

15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

		15.2.1 1 Monitoring and review of supplier services Organisations shall regularly monitor, review and audit supplier service delivery.	Process owner
15.2.1.1	2	Vendor performance with regard to information security is assessed annually against predetermined performance indicators, as included in the contract.	
		Guide: Change management process	
		Guide: Contract management	
15.2.2	**2**	**Managing changes to supplier services** Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Process owner

16

Information security incident management

16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.1	**1**	**Responsibilities and procedures** Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Secretary/ managing director Process owner
		Guide: Coherence of management processes and information security	
		Guide: Implementation of detection solutions	
16.1.2	**1**	**Reporting information security events** Information security events shall be reported through appropriate management channels as quickly as possible.	Secretary/ managing director Process owner Service provider
16.1.2.1	1	There is a hotline where security incidents can be reported.	
16.1.2.2	1	There is a reporting procedure in place that describes the roles and responsibilities of the hotline.	
16.1.2.3	1	All employees and contractors are demonstrably aware of the reporting procedure for incidents.	
16.1.2.4	1	Incidents will be reported internally as soon as possible, but always within 24 hours.	
16.1.2.5	1	The process owner is responsible for resolving security incidents.	
16.1.2.6	1	The follow-up of incidents is reported to the person responsible on a monthly basis.	
16.1.2.7	1	Information taken from the Coordinated Vulnerability Disclosure (CVD) procedure is part of incident reporting[46].	
		Guide: Contract management	

46) Previously, Coordinated Vulnerability Disclosure (CVD) was called responsible disclosure.

16.1.3	1	**Reporting information security weaknesses** Employees and contractors using the organisation's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Process owner Service provider
		See government measure 16.1.2.4	
16.1.3.1	1	A Coordinated Vulnerability Disclosure (CVD) procedure has been published and implemented[47].	
		Guide: Responsible Disclosure	
16.1.4	**1**	**Assessment of and decision on information security events** Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Process owner Service provider
16.1.4.1	2	Information security incidents that have resulted in a suspected or possibly deliberate breach of the availability, confidentiality or integrity of information-processing systems should be reported as quickly as possible (within 72 hours), whether or not automated, to the NCSC (for central government organisations only) or the sectoral CERT.	
16.1.5	**1**	**Response to information security incidents** Information security incidents shall be responded to in accordance with the documented procedures.	Process owner Service provider
		Guide: Incident management and response policy	
16.1.6	**2**	**Learning from information security incidents** Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Secretary/ managing director Process owner Service provider
16.1.6.1	2	Security incidents are analysed for the purpose of learning and preventing future security incidents.	
16.1.6.2	2	Security incident analyses are shared with relevant partners to prevent recurrence and future incidents.	
		Guide: Implementation of detection solutions	
16.1.7	**2**	**Collection of evidence** The organisation shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Secretary/ managing director Process owner Service provider
16.1.7.1	2	In case of a (suspected) information security incident, the retention period of the logged incident information at least three years.	

47) Previously, Coordinated Vulnerability Disclosure (CVD) was called responsible disclosure.

17

Information security aspects of business continuity management

17.1 Information security continuity

Objective: Information security continuity shall be embedded in the organisation's business continuity management systems.

		General guide: Business continuity management	
17.1.1	**1**	**Planning information security continuity** The organisation shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Secretary/ managing director Process owner
		Guide: Coherence of management processes and information security	
17.1.2	**1**	**Implementing information security continuity** The organisation shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Process owner Service provider
17.1.3	**1**	**Verify, review and evaluate information security continuity** The organisation shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Process owner Service provider
17.1.3.1	2	Continuity plans are tested annually for validity and usability.	
17.1.3.2	2	By performing an explicit risk assessment, the business-critical process elements and their associated reliability requirements are identified.	
17.1.3.3	2	Service of the business-critical components is restored within a week at the latest in the event of an emergency.	

17.2 Redundancies

Objective: To ensure availability of information processing facilities.

17.2.1	**1**	**Availability of information processing facilities** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Service provider

18

Compliance

18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.1.1	**1**	**Identification of applicable legislation and contractual requirements** All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organisation.	Secretary/ managing director Process owner Service provider
18.1.2	**1**	**Intellectual property rights** Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Secretary/ managing director Process owner Service provider
18.1.3	**2**	**Protection of records** Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislatory, regulatory, contractual and business requirements.	Process owner Service provider
18.1.3.1	2	The process owner has provided insight into the retention period for each type of information.	
18.1.4	**1**	**Privacy and protection of personally identifiable information** Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Secretary/ managing director Process owner Service provider
18.1.4.1	1	In accordance with the GDPR, every organisation has a Data Protection Officer (FG) with sufficient mandate to perform his/her function.	
18.1.4.2	2	Organisations regularly monitor compliance with the privacy rules and information processing and procedures within their area of responsibility on the basis of the relevant policy rules, standards and other security requirements.	
		See government measure 14.2.6.1	
18.1.5	1	**Regulation of cryptographic controls** Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Secretary/ managing director
18.1.5.1	1	Cryptographic control measures must explicitly align with standards on the Forum's 'comply or explain' list.	
		See government measure 10.1.1.1	

18.2 Information security reviews

Objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.

18.2.1	**1**	**Independent review of information security** The organisation's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Secretary/ managing director Process owner Service provider
18.2.1.1	2	There is an information security management system (ISMS) which demonstrably covers the entire PlaniDo-Check-Act cycle in a structured manner.	
		Guide: ISMS	
18.2.1.2	2	There is an established audit plan in which choices are made annually for which systems perform what type of security audits.	
18.2.2	**1**	**Compliance with security policies and standards** Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Secretary/ managing director Process owner Service provider
18.2.2.1	1	Information security is reported in the P&C cycle, resulting in an annual In Control Statement (ICV) to be issued for information security. If sufficiently recognisable, the ICV for information security be part of regular, generic accountability.	
18.2.3	**1**	**Technical compliance review** Information systems shall be regularly reviewed for compliance with the organisation's information security policies and standards.	Process owner Service provider
18.2.3.1	2	Information systems are audited annually for technical compliance with security standards and risks to actual security. This can be done, for example, by (automated) vulnerability analyses or penetration tests.	
		Guide: Penetration tests	

Annex 1: Laws and regulations

To make the BIO feasible in practice, many government measures include references to existing laws and regulations. The advantage of these references is that whoever starts working with BIO is made aware that there are already existing laws and regulations in which (security) requirements have been laid down. Moreover, this also positions these references in the framework of the ISO 27002 classification. A conscious decision was made to make references rather than reformulate to avoid misinterpretation.
For the laws and regulations mentioned, the BIO only included certain security aspects. It is not the intention of the BIO to fully cover the mentioned laws and regulations.

The government measures include references to the following laws and regulations:

- Ades baseline profile standard
- General Civil Service Regulations (ARAR)
- General governmental terms and conditions for IT agreements (ARBIT 2016)
- GDPR (replaces the WBP and came into effect on 25 May 2018);
- 2013 Security Regulations (BVR 2013), *Government Gazette.* 2013, 15496
- CM(2002)49
- Conduct rules for the digital work environment (1 July 2016; SGO decision)
- The 2015 NkBR (Standards Framework for Securing State Offices)
- Internal whistleblower policy
- ITIL, ASL or BiSL framework
- National Access Policy Framework
- NCSC classification
- 'apply or explain' list of the Standardisation Forum.
- Program of Requirements PKI Government
- Responsible disclosure procedure
- Regulations for government agency information security (VIR2007), *Government Gazette.* 2007, 122/11
- Regulations for government agency information security - Special Information (VIR-BI 2013)
- Security Screening Act (WVO)
- Archives Act
- Work and Income Implementation Structure Act (SUWI Act)
- Basic Registration of Persons Act (BRP Act)
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)

The BIO focuses only on the information security aspect. It is possible that the laws and regulations listed above have a broader effect than just information security. Introducing the BIO does not always fully cover these laws and regulations.

Annex 2: Basic security levels

The basic security levels are elaborated along the lines of availability, integrity and confidentiality. The BBN test helps with choosing the most appropriate level. The availability levels are based on the prevailing availability levels used by major internal service providers. The confidentiality levels are aligned with the damage scenarios that apply to the Interests to be Protected. The breakdown is as follows:

BBN1: availability = Low	integrity = Low	confidentiality = Low
BBN2: availability = Medium	integrity = Medium	confidentiality = Medium
BBN3: availability = Medium	integrity = Medium	confidentiality = High

BBN1	
Availability = Low	The information system is allowed to be down occasionally for up to two weeks (also in peak periods) and this has little or no impact on citizens/users. Outages can result in limited damage, such as: • financial implications; to be absorbed within the established space within the (implementing) organisation's budget; still does not lead to the failure to obtain an audit opinion; • limited loss of management control; • irritation and discomfort among citizens ventilated in the media; • internal negative publicity (reputation damage). These impacts are quantified as follows: • Office automation and organisation-specific systems have an availability of at least 98% on a monthly basis during opening hours, even during peak periods. • Maximum data loss 28 hours. • Maximum recovery time in case of incidents is within 40 working hours (five 8-hour working days) in 85% of cases.
Integrity = Low	No special measures are necessary to ensure the accuracy, timeliness and completeness of information[48]. The loss of integrity may result in limited damage, such as: • financial implications; to be absorbed within the established space within the (implementing) organisation's budget; still does not lead to the failure to obtain an audit opinion; • limited loss of management control; • irritation and discomfort among citizens ventilated in the media; • internal negative publicity (reputation damage).
Confidentiality = Low	Knowledge of information by unauthorised persons (outsiders) is not desirable, but does not result in damage of any magnitude. This is unclassified information. The public disclosure of this information may result in: • financial implications; to be absorbed within the (implementing) organisation's budget; • irritation and discomfort among citizens ventilated in the media; • internal negative publicity (reputation damage).

48) VIR definition.

BBN2	
Availability = Medium	The information system is allowed limited short-term downtime for up to one week (including peak periods) and this has tangible impacts on citizens/users. Outages can result in limited damage, such as: • political damage to a director: director must answer to accountability questions; • repair diplomatic damage through official scaling up; • financial implications: can no longer be absorbed within the established space within the (implementing) organisation's budget; no audit opinion obtained; • significant loss of management control; • loss of public respect; citizen complaints; • organisation-wide negative publicity (reputation damage) or significant loss of employee motivation. The availability quantified is as follows: • Office automation and organisation-specific systems have an availability of at least 98% on a monthly basis during opening hours, even during peak periods. • Maximum data loss 24 hours. • Maximum recovery time in case of incidents is within 16 working hours (two 8-hour days).
Integrity = Medium	Appropriate measures are necessary to ensure accuracy, timeliness and completeness (VIR definition). The loss of integrity may result in substantial damage, such as: • political damage to a director: director must answer to accountability questions; • repair diplomatic damage through official scaling up; • financial implications: can no longer be absorbed within the established space within the (implementing) organisation's budget; no audit opinion obtained; • significant loss of management control; • loss of public respect; citizen complaints; • organisation-wide negative publicity (reputation damage) or significant loss of employee motivation.
Confidentiality = Medium	Protection of data and other interests to be protected in government processes, where confidentiality, among other things, is relevant as it concerns sensitive information. The public disclosure of the data may result in: • political damage to a director: director must answer to accountability questions; • repair diplomatic damage through official scaling up; • financial implications: can no longer be absorbed within the (implementing) organisation's budget; no audit opinion obtained; • loss of public respect; citizen complaints or significant loss of employee motivation; • binding designation of the Dutch Data Protection Authority in connection with violation of privacy; • direct damage to reputation, for example through negative publicity.

BBN3	
Availability = Medium	The information system is allowed limited short-term downtime for up to one week (including peak periods) and this has tangible impacts on citizens/users. Outages can result in limited damage, such as: • political damage to a director: director must answer to accountability questions; • repair diplomatic damage through official scaling up; • financial implications: can no longer be absorbed within the established space within the (implementing) organisation's budget; no audit opinion obtained; • significant loss of management control; • loss of public respect; citizen complaints; • organisation-wide negative publicity (reputation damage) or significant loss of employee motivation. The availability quantified is as follows: • Office automation and organisation-specific systems have an availability of at least 98% on a monthly basis during opening hours, even during peak periods. • Maximum data loss 24 hours. • Maximum recovery time in case of incidents is within 16 working hours (two 8-hour days).
Integrity = Medium	Appropriate measures are necessary to ensure accuracy, timeliness and completeness (VIR definition). The loss of integrity may result in substantial damage, such as: • political damage to a director: director must answer to accountability questions; • repair diplomatic damage through official scaling up; • financial implications: can no longer be absorbed within the established space within the (implementing) organisation's budget; no audit opinion obtained; • significant loss of management control; • loss of public respect; citizen complaints; • organisation-wide negative publicity (reputation damage) or significant loss of employee motivation.
Confidentiality = High	Loss of information has a major impact, which cannot be explained if it is not classified and protected at the BBN3 level; • information with a classification (other than BBN2) is provided by third parties; • connection to an infrastructure requires BBN3 (e.g., to avoid compromising classified information already on the infrastructure) in order to be able to process information on that infrastructure; • resistance to state actors is necessary.

Part 3

BIO Addendum

Addendum Introduction

This addendum lists all requirements that are specific and mandatory for a particular layer of government. Because the central government has a number of specific documents such as the VIR, VIR-BI, which do not apply to other levels of government, they are expressly included in this addendum. In addition, texts have been included that could not be properly handled in the first two volumes, and this is mainly due to the role of the NCSC for the national government and the presence of a number of sectoral CERTs at the other levels of government.

The addendum is complementary to the texts and standards in Parts 1 and 2.

5. Information security policies

5.1 Management direction for information security

Measure	Organisation	BBN	Directive	Responsible party(ies)
5.1.1.1	Government	1	Directive:VIR, article 3	Secretary/ managing director
5.1.2.1	Government	1	Directive: VIR, Article 3(e)	Secretary/ managing director
5.1.2.1	Government	1	The information security policy shall be reviewed at least once every three years, or in the event of significant changes due to reorganisation or change in the division of responsibilities, and adjusted as necessary.	Secretary/ managing director

6. Organisation of information security

6.1 Internal organisation

6.1.1.2	Government	1	Directive: VIR, VIR-BI, BVR	Secretary/ managing director
6.1.3.3	Government	1	The organisation provides contact details to the NCSC for the purpose of following up on incidents, vulnerabilities, and threats.	Secretary/ managing director/ Service provider
6.1.3.3	Municipality Water Authority	1	The organisation provides contact details to the sectoral CERT for the purpose of following up on incidents, vulnerabilities, and threats.	Secretary/ managing director/ Service provider

7. Human resource security

7.1 Prior to employment

7.1.1	Government	1	Directive: VIR-BI	Secretary/ managing director Process owner
7.1.1.1	Government	1	Upon commencement of employment, all employees (internal and external) submit a Certificate of Good Conduct (VOG) issued specifically for the position.	

7.2 During employment

7.2.1	Government	1	Directive internal whistleblower policy	Secretary/ managing director

8. Asset management

8.1 Responsibility for assets

8.1	Government	1	Directive: Code of conduct for the digital work environment	Secretary/ managing director Process owner

8.3 Media handling

8.3.1	Government	2	VIR-BI: approved products NBV	Process owner Service provider
8.3.1.2	Government	2	The manner in which confidential or higher classified information is stored meets the requirements of the NBV.	Process owner Service provider

11. Physical and environmental security

11.1 Secure areas

11.1.1.1	Government	The following is used to set up secure areas: a. the National Access Policy Framework (2010); b. the Standards Framework for Securing State Offices (NkBR 2015); c. the Security Regulations for the State (BVR 2013).	Secretary/ managing director
11.1.3.1	Government	Guide: NkBR 5.4	Process owner Service provider

14. System acquisition, development and maintenance

14.1 Security requirements of information systems

14.1.1.1	Government	1	Guide:	VIR	Process owner

15. Supplier relationships

15.1 Information security in supplier relationships

15.1.2	Government	1	VIR-BI	Process owner Service provider
15.1.2	Government	1	ARBIT	Process owner Service provider
15.1.2	Municipality	1	GIBIT	Process owner Service provider

16 Information security incident management

16.1 Management of information security incidents and improvements

16.1.4.1	2	Information security incidents that have resulted in a suspected or possibly deliberate breach of the availability, confidentiality or integrity of information-processing systems should be reported as quickly as possible (within 72 hours), whether or not automated, to the NCSC by or on behalf of the department security contact (DSC, operational contact person for the NCSC) or the chief Information Security Officer (CISO).