Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

RWS INFORMATIE

Information Security: TSP

Information Security: Tender Specification Process for IS contracts

Date:	14 September 2021
Status:	Final

Credits

Published by:	Security Centre, Rijkswaterstaat
Information:	Marco Rijkschroeff / Turabi Yildirim / Sahar Habib
Telephone:	
Fax:	
Prepared by:	Security Centre, Rijkswaterstaat
Layout:	
Date:	14 September 2019
Status:	Final
Version number:	1.75

Contents

1 Information security of process requirements in IS procurement contracts 6
1.2 Organising information security 6
1.3 Safe staff 7
1.4 Managing business assets 8
1.5 Access security 8
1.6 Cryptography 9
1.7 Physical and environmental security 9
1.8 Security of operations 9
1.9 Communications security 10
1.10 Acquisition, development and maintenance of equipment and software 11
1.11 Supplier relations 12
1.12 Managing information security incidents 12
1.13 Information security aspects of business continuity management 13
1.14 Compliance 13
Appendix A: Sources in contract texts 15
Appendix B: Numbering of contract requirements 17

1 Information security of process requirements in IS procurement contracts

NOTE: This document is an annex with the process requirements listed in the adopted master document 'Information Security in Standard RWS IS Contract Requirements'.

References to external documents are described as {n} or IBR-m and can be found in Appendix A. Terms beginning with a capital letter are proper nouns and refer to specific meanings in the ARBIT and ARVODI contract texts. Other terms correspond to the definitions mentioned in the Dutch version of NEN/IEC ISO 27000. For all other terms, reference is made to their general meaning as found in the leading Dutch dictionary 'Van Dale Groot woordenboek van de Nederlandse taal'. Background information on the numbering of requirements used can be found in Appendix B.

1.1 Information security policy

5.1.1	The Contractor demonstrates for the agreed Performance that the Client's TSP and TSR requirements for cyber security are an integral part of the scope of certifying the Contractor in accordance with the most recent version of the NEN-ISO/IEC 27001, under which the interfaces between the Client and the Contractor are also detailed, and that the Contractor remains certified for at least the term of the Agreement. Alternatively, the Contractor may choose to flesh out the Client's TSP and TSR requirements for cyber security with control measures and integrate them into its own Information Security Management System (ISMS). The principle of 'comply or explain' applies to all TSP and TSR requirements for cyber security.
5.1.SC-01a	The Contractor must secure the part of its information service required for the registrations and files requested by the Client and required for processing the information and documents classified by the Client in such a way that they are protected against loss, unauthorised access and unauthorised alteration.
5.1.SC-01a Melvin's proposal in email of 15/8	The Contractor must secure the part of its information service required for the registrations and files requested by the Client and required for processing the information and documents classified by the Client in such a way that they are protected against loss, unauthorised access and unauthorised alteration.
5.1.SC-01b	If the Client does not refer to specific security guidelines in the measures to be implemented, the Contractor must adhere to the guidelines from the most recent version of the NEN-ISO/IEC 27002 standard.
5.1.SC-01b Melvin's proposal in email of 15/8	If the Client does not refer to specific security guidelines in the measures to be implemented, the Contractor must adhere to the guidelines from the most recent version of the NEN-ISO/IEC 27002 standard.

1.2 Organising information security

6.1.1	The Contractor must demonstrably assign the responsibilities, duties, and powers for at least all processes mentioned in the Agreement to the appropriate positions within the project organisation and the organisation at large.
6.1.2	The Contractor must have a policy for segregation of duties (if reasonably possible) for assigning operational, controlling and management tasks involved in the Performance, and demonstrably must have operationally embedded this in processes that also detect or prevent unauthorised access to business assets.

6.1.2 Melvin's proposal in email of 15/8
The Contractor must have a policy for segregation of duties (if reasonably possible) for assigning operational, controlling and management tasks involved in the Performance, and demonstrably must have operationally embedded this in processes that also detect or prevent unauthorised access to business assets.

6.1.5
The Contractor must have an operationally embedded project management process for the Performance that demonstrably integrates information security.

6.2.1
The Contractor must have a demonstrable operationally embedded process for securing and encrypting data on mobile devices involved in the Performance, taking into account the IBR-1 guideline: *Data Classification Policy* {10}, the current security status of the encryption methods used {1} and the GISB Guide: Mobile Device Management {9}.

6.2.2
Remote access to all information systems in the Client's network involved in the Performance is permitted solely through a specially equipped Third Party Access service {2} of the Client.

6.2.2 Melvin's proposal in email of 15/8
Remote access to all information systems in the Client's network involved in the Performance is permitted solely through a specially equipped Third Party Access service {2} of the Client.

1.3 Safe staff

7.1.1
The Contractor must have a demonstrable operationally embedded process for screening of the Personnel who perform work:

1. relating to developing or revising design drawings and/or documents;
2. for the purpose of developing, testing, managing, installing, configuring and/or operating software or equipment;
3. in operating or technical areas;
4. on cables and pipes;
5. on security and safety documentation and instructions,

in relation to the Performance at least by means of a relevant Certificate of Good Conduct. A screening for this purpose must always have been done within the past five years during the contract period. Pending the screening request, the person concerned may make a self-declaration, which will suffice for a maximum of six weeks from their start date at the Performance. This period cannot be extended.

7.1.1 Melvin's proposal in email of 15/8
The Contractor must have a demonstrable operationally embedded process for screening of the Personnel who perform work:

- relating to developing or revising design drawings and/or documents;
- for the purpose of developing, testing, managing, installing, configuring and/or operating software or equipment;
- in operating or technical areas;
- on cables and pipes;
- on security and safety documentation and instructions,
- in relation to the Performance at least by means of a relevant Certificate of Good Conduct. A screening for this purpose must always have been done within the past five years during the contract period. Pending the screening request, the person concerned may make a self-declaration, which will suffice for a maximum of six weeks from their start date at the Performance. This period cannot be extended.

7.2.2a
The Contractor must have given a demonstrable operational assurance that Personnel have received education and training in security awareness appropriate to the nature of the work to be performed, as well as annual refresher training, which at least also addresses personal responsibility and the Client's specific security frameworks.

7.2.2a Melvin's proposal in
The Contractor must have given a demonstrable operational assurance that Personnel have received education and training in security awareness appropriate to the nature of the work to be performed, as

email of 15/8	well as annual refresher training, which at least also addresses personal responsibility and the Client's specific security frameworks.
7.2.2b	The Contractor must have given a demonstrable operational assurance that Personnel responsible for testing information systems involved in the Performance have updated and specialised knowledge, experience and training in relation to testing its security.
7.2.2b	The Contractor must have given a demonstrable operational assurance that Personnel responsible for testing information systems involved in the Performance have updated and specialised knowledge, experience and training in relation to testing its security.
7.3.1	The Contractor must have a demonstrable operationally embedded process for defining the responsibilities and duties relating to information security for the Performance and must communicate to Personnel that: 1. these remain in force after the termination or change of their employment; 2. these must be implemented.

1.4 Managing business assets

8.1.1a	The Contractor must have given a demonstrable operational assurance that an inventory of all information systems involved in the Performance has been drawn up in a Configuration Management Database (CMDB), such that it can be used effectively for an effective Configuration Management (CM) ITIL process and that this CMDB will be kept up to date.
8.1.1b	At the Client's request, the Contractor must transfer the data listed in the Configuration Management Database (CMDB) for all information systems involved in the Performance.
8.1.SC-12	The Contractor must use all means of access provided by the Client (including tokens and passes to objects, data, information systems and Industrial Automation) solely for the purpose and under the conditions for which they have been provided. The security measures must also not be circumvented.
8.1.SC-12 Melvin's proposal in email of 15/8	The Contractor must use all means of access provided by the Client (including tokens and passes to objects, data, information systems and Industrial Automation) solely for the purpose and under the conditions for which they have been provided. The security measures must also not be circumvented.
8.2.1	The Contractor must have given a demonstrable operational assurance that all information involved in the Performance is classified in accordance with IBR-1 guideline: *Data classification policy* {10} and that the associated security measures are observed.
8.3.x	The Contractor must have operationally embedded processes for the safe removal of media, transport of media, management of removable media and the irretrievable removal of unnecessary contents of reusable media involved in the Performance, in accordance with IBR-1 guideline: *Data classification policy* {10} and GISB Guide: Guide on the safe removal of ICT assets {8}.

1.5 Access security

9.1.1	The Contractor must ensure an operationally embedded procedure for providing physical or logical access to information processing facilities, including the issue and withdrawal of accounts and authorisations, and an updated registration of this.
9.1.SC-02	If the Client or a third party is responsible for providing physical or logical access to information processing facilities, the Contractor must comply with the access procedure used by the Client or a third party.
9.1.SC-02 Melvin's proposal in	If the Client or a third party is responsible for providing physical or logical access to information processing facilities, the Contractor must comply with the access procedure used by the Client or a third party.

email of 15/8

9.1.SC-03 Melvin's proposal in email of 15/8

If the Client or a third party is responsible for providing physical or logical access to information processing facilities, the Contractor must comply with the access procedure used by the Client or a third party.
If the Contractor or third party is responsible for managing and storing passwords of information processing facilities or devices required for such information processing (such as cameras, sensors, etc.), the Contractor must transfer all admin and other passwords that it has set or created to the Client at the end of the contract.

9.2.x At least every six months, the Contractor must review and update the Personnel's physical and logical access rights to information processing facilities through an operationally embedded and formal process and cooperate in the periodic review and clean-up of the Client's end-user accounts and rights.

9.3.1 The Contractor must require Personnel to comply with the IBR-3 guideline: *Password Use Policy* {10} when using authentication credentials relating to the Performance.

9.4.4 The Contractor must have a demonstrable operationally embedded process for controlling the use of system tools, capable of circumventing control measures for information systems involved in the Performance. Its use must be logged.

9.4.5 The Contractor must have given a demonstrable operational assurance that only specifically authorised Personnel have access to the Source Code of the information systems involved in the Performance.

1.6 Cryptography

10.1.x If the Contractor is contractually or legally required to use cryptography to protect information involved in the Performance, it must have policies and operationally embedded processes for the use of these cryptographic control measures, including the use, protection and service life of the associated cryptographic keys throughout their lifecycle in accordance with appropriate standards (e.g. Public Key Infrastructure [*PKI Overheid*] or ISO 11770).

1.7 Physical and environmental security

11.1.1 The Contractor must have defined and operate physical security zones to protect areas containing sensitive or essential information and information processing facilities relating to the Performance.

11.1.5 The Contractor must have demonstrably operationally embedded procedures for working in secure areas, as referred to in requirement TSP 11.1.1.

11.2.7 The Contractor must have a demonstrable operationally embedded process for destroying data on media when disposing of or replacing information systems or parts of them containing this media and involved in the Performance, in accordance with GISB Guide: Guide on the safe removal of ICT assets {8}.

11.2.8 The Contractor must have demonstrable operationally embedded procedures for protecting unattended information systems involved in the Performance.

11.2.8 Melvin's proposal in email of 15/8

The Contractor must have demonstrable operationally embedded procedures for protecting unattended information systems involved in the Performance.

1.8 Security of operations

12.1.1 The Contractor must have and make available demonstrable operationally embedded operating procedures to the Personnel and, if applicable, the Client's employees, required for the Performance.

12.2.1 The Contractor must have demonstrable operationally embedded processes for protection against malware on information systems involved in the Performance, focusing on at least prevention, detection, communication and recovery.

12.2.1 Melvin's proposal in email of 15/8	The Contractor must have demonstrable operationally embedded processes for protection against malware on information systems involved in the Performance, focusing on at least prevention, detection, communication and recovery.
12.2.SC-17	During maintenance and when connecting peripheral equipment to the Client's ICT, the Contractor must comply with the IBR-8 guideline: *Guideline for safely connecting management and maintenance equipment to RWS's ICT systems* {10} and GISB Guide: Mobile Device Management {9} for protection against malware.
12.2.SC-17 Melvin's proposal in email of 15/8	During maintenance and when connecting peripheral equipment to the Client's ICT, the Contractor must comply with the IBR-8 guideline: Guideline for safely connecting management and maintenance equipment to RWS's ICT systems {10} and GISB Guide: Mobile Device Management {9} for protection against malware.
12.3.1a	The Contractor must have a demonstrable operationally embedded process for making at least daily backups of all information and software in use for the Performance.
12.3.1b	The Contractor must test the recovery process that forms part of the backup process of all information and software in use for the Performance at least once a year and communicate the outcome to the Client.
12.4.1	The Contractor must have a demonstrable operationally embedded process for sufficient periodic assessments of log files of the information systems involved in the Performance. For this purpose, the interval between two assessments may never exceed one month.
12.4.3	The Contractor must have a demonstrable operationally embedded process for sufficient periodic assessments of log files of the information systems involved in the Performance. The interval between two assessments may never exceed one month.
12.4.CC-21	Unless a different retention period has been agreed with the Client, the Contractor must keep log files of the information systems involved in the Performance available for at least three months (and at least three years in the case of a suspected incident), and hand over these log files to the Client for inspection on request.
12.6.1	For the purpose of information security, the Contractor must conduct a risk analysis and assessment in accordance with NEN-ISO/IEC 27005, or its equivalent, at least once a year and implement appropriate measures.
12.6.1 Melvin's proposal in email of 15/8	For the purpose of information security, the Contractor must conduct a risk analysis and assessment in accordance with NEN-ISO/IEC 27005, or its equivalent, at least once a year and implement appropriate measures.
12.6.SC-16	The Contractor must check the information systems involved in the Performance for vulnerabilities using common testing methodologies and in accordance with the GISB Guide: Penetration testing {12} and patch the information systems in coordination with the Client and after its approval.
12.6.SC-16 Melvin's proposal in email of 15/8	The Contractor must check the information systems involved in the Performance for vulnerabilities using common testing methodologies and in accordance with the GISB Guide: Penetration testing {12} and patch the information systems in coordination with the Client and after its approval in accordance with the Patch Management Framework {16}.

1.9 Communications security

13.1.1	To protect information in information systems, the Contractor must have demonstrable operationally embedded processes for managing and controlling networks involved in the Performance, focusing on at least the following aspects: - Management of network security - Technical vulnerability management - Identification and authentication

- Network audit logging and monitoring
- Intrusion detection and prevention
- Protection against malicious code
- Cryptographic-based services
- Business continuity management.

13.1.SC-15 The Contractor must ensure that the number of data network links is limited to the functionally necessary ones only, that each link has an appropriate form of security and does not pose unacceptable risks. A risk analysis and assessment has been made for each link.

13.1.2 The Contractor must have included security mechanisms, service levels and management requirements for all services involved in the Performance in a Service Level Agreement (SLA) with the Client, focusing on at least the security aspects of availability, incident reporting, implementation of changes and escalation.

13.1.SC-18 At the Client's request, the Contractor must provide an up-to-date summary of all data network links with their associated security measures.

13.1.SC-18 Melvin's proposal in email of 15/8 At the Client's request, the Contractor must provide an up-to-date summary of all data network links with their associated security measures.

13.2.1 The Contractor must have demonstrable operationally embedded policies, procedures and control measures to protect the transport of information involved in the Performance, which passes through all types of communication facilities.

1.10 Acquisition, development and maintenance of equipment and software

14.1.1 The Contractor must make security an integral part of the development and maintenance process for information systems throughout their life cycle. This must be done on the basis of an explicit risk assessment for the purpose of establishing security requirements in accordance with the GISB Guide: Risk Analysis Methodology {11} and the Guide: Risk Management ISO-27005 {13}. In the case of software, at least the measures mentioned in the CIP document Grip on SSD - Security requirements for web and other applications {3} must be implemented for this purpose.

14.1.SC-24 The Contractor must make security an integral part of the development and maintenance process for mobile applications throughout their life cycle. For this purpose, at least the measures mentioned in the document 'Guide on Mobile App Development and Management for the Central Government {4} must be implemented.

14.2.x The Contractor must have demonstrable operationally embedded information security in the processes that form part of the development life cycle of information systems involved in the Performance, implementing at least the process requirements from the IBR-4 guideline: *Guidelines on security during development* {10}. In the case of software, at least the process requirements from the CIP document Grip on SSD - Security requirements for web and other applications {3} must be implemented for this purpose.

14.2.x Melvin's proposal in email of 15/8 The Contractor must have demonstrable operationally embedded information security in the processes that form part of the development life cycle of information systems involved in the Performance, implementing at least the process requirements from the IBR-4 guideline: Guidelines on security during development {10}. In the case of software, at least the process requirements from the CIP document Grip on SSD - Security requirements for web and other applications {3} must be implemented for this purpose.

14.2.SC-05 The Contractor guarantees the operation of information systems (at least until their End of Life (EOL) as specified by the Supplier) that are part of the Performance, on/with products or software that are not at their EOL and with an up-to-date patch level. Alternatively, it offers a free upgrade to make this possible.

14.2.SC-05 Melvin's proposal in email of 15/8	The Contractor guarantees the operation of information systems (at least until their End of Life (EOL) as specified by the Supplier) that are part of the Performance, on/with products or software that are not at their EOL and with an up-to-date patch level {16}. Alternatively, it offers a free upgrade to make this possible.
14.2.SC-06a	For information systems involved in the Performance, the Contractor must, within 60 days of becoming aware of vulnerabilities in the case of software and within six months in the case of equipment, release adaptations or patches free of charge (at least until the End of Life (EOL) of this information system as specified by the Supplier) for the purpose of remedying these vulnerabilities.
14.2.SC-06a	For information systems involved in the Performance, the Contractor must, within 60 days of becoming aware of vulnerabilities in the case of software and within six months in the case of equipment, release adaptations or patches {16} free of charge (at least until the End of Life (EOL) of this information system as specified by the Supplier) for the purpose of remedying these vulnerabilities.
14.2.SC-06b	The Contractor must have an operationally embedded process for periodically implementing security patches or software updates to keep the information systems up to date.
14.3.1	The Contractor must in a demonstrably careful manner choose, protect, control and destroy test data involved in the Performance after use.

1.11 Supplier relations

15.1.3	If subcontractors are used in rendering the Performance, the Contractor must ensure that the Client's security requirements are adhered to by those involved when procuring services or products from companies.
15.1.3 Melvin's proposal in email of 15/8	If subcontractors are used in rendering the Performance, the Contractor must ensure that the Client's security requirements are adhered to by those involved when procuring services or products from companies.
15.1.SC-25	If subcontractors are used in rendering the Performance, and procuring services or products may result in the vendor lock-in of a subcontractor and/or compromise national security, the Contractor must first submit this to the Client for approval.
15.1.SC-25 Melvin's proposal in email of 15/8	If subcontractors are used in rendering the Performance, and procuring services or products may result in the vendor lock-in of a subcontractor and/or compromise national security, the Contractor must first submit this to the Client for approval.
15.2.1	The Client has the right to conduct audit(s) to review the design, existence and/or operation of the requirements specified in the contract between the Client and the Contractor. The Contractor must cooperate voluntarily in this audit.
15.2.1 Melvin's proposal in email of 15/8	The Client has the right to conduct audit(s) to review the design, existence and/or operation of the requirements specified in the contract between the Client and the Contractor. The Contractor must cooperate voluntarily in this audit.

1.12 Managing information security incidents

16.1.x	The Contractor must have an operationally embedded process for registering, reporting and handling information security incidents that is consistent with the Client's incident management process, implementing at least the requirements from the IBR-5 guideline: *Guideline for Information Security Incidents* {10}. These information security incidents must be reported to the Client at least every month.
16.1.SC-19	The Contractor must have an operationally embedded process for the registration and response to security incident and/or event reports from the Client's Security Operations Centre.
16.1.SC-19 Melvin's	The Contractor must have an operationally embedded process for the registration and response to security incident and/or event reports from the Client's Security Operations Centre.

proposal in email of 15/8

1.13 Information security aspects of business continuity management

17.1.2 The Contractor must have a demonstrable continuity plan for maintaining the Performance in adverse situations in accordance with the GISB General Guide to Continuity Management {14}, in which the continuity of information security is also ensured.

17.1.3 The Contractor must demonstrably verify and update the continuity plan for the Performance at least once a year to ensure that it remains sound and effective. The continuity plan can be based on the GISB General Guide to Continuity Management {14}.

1.14 Compliance

18.1.3 The Contractor must have demonstrable operationally embedded procedures to protect against loss, destruction, falsification, unauthorised access and unauthorised release of registrations on information systems involved in the Performance, in accordance with legal, regulatory, contractual and business requirements.

18.1.SC-20 The Contractor must implement measures to secure documents such as offers, contracts, network diagrams, risk analysis calculations, vulnerability scans, penetration test reports, accounts and passwords against espionage in the broadest sense.

18.1.CC-09 The Client's data or software, or the metadata generated by them, located on the Contractor's information systems is and will remain the Client's property at all times. If the Client has provided data to the Contractor, the Personnel may use it only for the purpose for which it has been provided.

18.1.CC-09 Melvin's proposal in email of 15/8 The Client's data or software, or the metadata generated by them, located on the Contractor's information systems is and will remain the Client's property at all times. If the Client has provided data to the Contractor, the Personnel may use it only for the purpose for which it has been provided.

18.1.CC-10 The Contractor must have demonstrable operationally embedded processes for destroying the Client's data or software on the Contractor's equipment and all backup media following the termination of the contract between the two parties.

18.1.CC-12 If the Client's data is located on the Contractor's information systems, the Contractor must assist in transferring this information to the new supplier or back to the Client following the termination of the contract between the two parties.

18.1.CC-14 If the Client's data or software is located on the Contractor's information systems, the Contractor must indicate where these information systems are located. If they are located outside the EU, this must only be in countries offering an adequate level of data protection. The European Commission determines which countries meet this criterion[1].

18.1.SC-23 When using certificates for RWS's public web services or for authenticating servers with cooperation partners, the Contractor must use Public Key Infrastructure [*PKI Overheid*] certificates that must be requested from the Client. In other cases, the appropriate standards must be applied in accordance with the NCSC guideline: ICT Security Guidelines for Transport Layer Security {1}.

18.2.1 At least once a year, the Contractor must conduct an audit of the design, existence and operation of the information security measures mentioned in the contract with the Client, and report to the Client (as part of the Information Security Plan IV) on the findings and intended improvement measures.

18.2.2 The Contractor must have demonstrable operationally embedded processes for periodically assessing compliance with policies, standards and other requirements relating to security among the Personnel involved in the Performance.

18.2.3 The Contractor must have demonstrable operationally embedded processes for periodically assessing compliance with technical policies, standards and other requirements relating to the security of the

[1] Currently, these countries are Norway, Iceland, certain Channel Islands, Argentina, Canada, Switzerland and the US (with restrictions).

information systems involved in the Performance. Compliance can be demonstrated with automated or other vulnerability assessments or penetration tests; see the GISB Guide: Penetration testing {12} for this purpose.

18.2.SC-09 The Contractor must develop an Information Security Plan detailing the control measures implemented and update the Information Security Plan annually following periodic assessments of the design, existence and operation of the control measures. The Client provides the template for the Information Security Plan IV {15}.

18.2.SC-10 The Contractor must prepare the Information Security Plan in coordination with the Client.

18.2.SC-21 The Contractor must specifically coordinate deviations from the security requirements for processes and information systems involved in the Performance with the Client. The Contractor must record these deviations as an 'explain' in the Information Security Plan IV and also describe any residual risk.

18.2.SC-22 In accordance with the arrangements made with the Client regarding any 'explains', the Contractor must implement the 'explains' improvement plan and periodically report on its status to the Client.

18.2.SC-08 The Contractor must comply with information security arrangements and procedures that describe the purpose, method and frequency of contact about information security at strategic, tactical and operational levels.

18.2.SC-09 Melvin's proposal in email of 15/8 The Contractor must develop an Information Security Plan detailing the control measures implemented and update the Information Security Plan annually following periodic assessments of the design, existence and operation of the control measures. The Client provides the template for the Information Security Plan IV {15}.

Appendix A: Sources in contract texts

Sources are mentioned in the contract texts, as follows.

Number	Source
{1}	National Cyber Security Centre (NCSC), *ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)* (ICT Security Guidelines for Transport Layer Security (TLS)), URL: https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
{2}	Rijkswaterstaat IRN, *Afspraken en Procedures Netwerkdienstverlening: Netwerktoegang voor Derden* (Network Service Arrangements and Procedures: Third Party Network Access), RWS Intranet URL: http://vpr.intranet.rws.nl/ProjectDirectory/Infosite_Netwerkdienstverlening/Lists/Veel%20gestelde%20vragen/DispForm.aspx?ID=49
{3}	Centre for Information Security and Privacy (CIP), *Grip op SSD - Beveiligingseisen voor (web)applicaties* (Grip on SSD – Security Requirements for web and other applications) URL: https://www.cip-overheid.nl/media/1500/20200720-ssd-normen-v30.pdf
{4}	Central government: *Handreiking Mobiele App Ontwikkeling en Beheer voor de Rijksoverheid* (Guide on Mobile App Development and Management for the Central Government) URL: https://www.noraonline.nl/wiki/Mobility
{5}	Rijkswaterstaat IRN, *RWS IV Aansluitvoorwaarden/RIVA* (RWS IV Connection Conditions/RIVA), URL: Classification RWS Company Confidential: https://werkwijzer.cf-prod.intranet.rws.nl/index.html Classification of RWS Information: https://www.rijkswaterstaat.nl/zakelijk/zakendoen-met-rijkswaterstaat/werkwijzen/werkwijze-in-iv/index.aspx
{6}	Rijkswaterstaat IRN, *Aansluitvoorwaarden NNV Rijkswaterstaat* (Connection Conditions for Rijkswaterstaat's national fibre optic infrastructure). http://vpr.intranet.rws.nl/ProjectDirectory/Infosite_Netwerkdienstverlening/Algemeen_klanten/PDC%20en%20DAP/Forms/AllItems.aspx
{7}	Open Web Application Security Project (OWASP), 'OWASP Top 10' https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
{8}	*BIO Handreiking Veilige afvoer van ICT-middelen* (GISB Guide: the safe removal of ICT assets) https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/04/201902-Handreiking-Veilige-afvoer-van-ICT-middelen-v2.0.pdf
{9}	*BIO Handreiking Mobile Device Management* (GISB Guide: Mobile Device Managementhttps://www.informatiebeveiligingsdienst.nl/product/mobile-device-management/
{10}	*Richtlijnen informatiebeveiliging bij RWS IV-contracteisen v1.0* (Information security guidelines for RWS IV contract requirements v1.0)
{11}	*BIO Handreiking Risicoanalysemethode* (GISB Guide: Risk analysis method) https://www.informatiebeveiligingsdienst.nl/product/handreiking-diepgaande-risicoanalyse-methode-gemeenten/

{12}	BIO Handreiking Penetratietesten (GISB Guide: Penetration testing) https://www.informatiebeveiligingsdienst.nl/product/handreiking-penetratietesten-v1-0/
{13}	*Handreiking Risicomanagement ISO-27005* (Guide for Risk Management ISO-27005)
{14}	*BIO Algemene handreiking continuïteitsbeheer* (GISB General Guide to Continuity Management) https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/07/201903-Model-Continu%C3%AFteitsplan_v2.0.docx
{15}	Template for the Information Security Plan IV
IBR-1	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Beleid voor gegevensclassificatie* (Data classification policy)
IBR-2	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Beleid voor logische toegangsbeveiliging* (Logical access security policy)
IBR-3	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Beleid voor wachtwoordgebruik* (Password use policy)
IBR-4	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Richtlijnen voor beveiligen bij ontwikkelen* (Guidelines on security during development)
IBR-5	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Richtlijnen voor informatiebeveiligingsincidenten* (Guidelines for information security incidents)
IBR-6	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Richtlijnen voor fysieke beveiliging* (Guidelines for physical security)
IBR-7	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Richtlijnen voor logging* (Guidelines for logging)
IBR-8	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Richtlijnen voor het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT systemen van RWS* (Guidelines for safely connecting management and maintenance equipment to RWS's ICT systems)

Appendix B: Numbering of contract requirements

The numbering of the contract requirements refers to the corresponding three-point standards in the NEN document ISO/IEC 27002:2013: *IT Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging* (IT Security Techniques – Practical guideline with information security control measures) and is primarily for internal RWS use. Because this proved to be practical, deviations from this numbering have occurred in some cases. The following deviations apply:

1. In some cases, a requirement has been split into two parts; in that case, an ‘a’ and a ‘b’ have been added after the three-point standard to distinguish between them
2. In some cases, the three-point standards under one two-point standard have merged into one contract requirement. In this case, the third digit in the three-point standard notation is replaced by an ‘x’.
3. Requirements from the CIP document *Cloud computing - Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)* (Cloud computing- An operational product based on the Civil Service Information Security Baseline (CSISB)) for which no corresponding requirement exists within ISO/IEC 27002 have been added to a corresponding two-point standard, with the third ‘digit’ in the three-point notation ‘CC-n’, where ‘n’ corresponds to the number of the standard from the CIP document.
4. Requirements from the RWS Security Centre itself for which no corresponding requirement exists within ISO/IEC 27002 have been added to a corresponding two-point standard, with the third ‘digit’ in the three-point notation ‘SC-n’, where ‘n’ corresponds to the number on the list of SC requirements.

Page 17 of 17