



CIO Platform Nederland

Het CIO Netwerk van Nederland voor CIO's en ICT eindverantwoordelijken in grote organisaties

*Information Security*



**CIO Platform Netherlands**

**Information Security Checklist**

*Published by the CIO Interest Group*

*Including explanatory notes on use on the backside*

CIO Platform Netherlands  
June 2010

1	<b>Intellectual property</b>	<p>The parties involved accept that the intellectual property rights relating to all software or other materials such as analyses, designs, documentation, reports, tenders and any preparatory material provided by or on behalf of one party to the other under the agreement will remain with the party who has provided them.</p> <p>See also e.g. <i>NEN-ISO/IEC 27002:2007 sub-section 6.2.3 (t)</i></p>
2	<b>Confidentiality</b>	<p>The parties involved are willing to conclude a confidentiality agreement which determines the way in which information relating to the service or the product will be handled/processed as well as the sanctions which can be applied if such an agreement is violated. On request both parties will be provided with an explanation regarding the way in which the other party complies with this stipulation.</p> <p>See also e.g. <i>NEN-ISO/IEC 27002:2007 sub-section 6.1.5</i></p>
3	<b>Facilities</b>	<p>The supplier is obliged to use the resources agreed on with the customer such as hardware, software, methods, techniques and design environment.</p> <p>See also e.g. <i>NEN-ISO/IEC 27002:2007 sub-section 7.1.3</i></p>
4	<b>In-house rules and regulations</b>	<p>The supplier guarantees that the staff employed by him to carry out the order, will undertake to comply with and conduct themselves in accordance with the in-house rules and regulations which apply at the customer's premises.</p> <p>The customer will provide the supplier with a copy of these for appraisal beforehand if required.</p>
5	<b>Policy</b>	<p>The supplier is able to demonstrate that the staff employed by him to carry out the order hold the correct training certificates required in order to provide the service or product specified in the agreement correctly.</p> <p>The supplier is able to demonstrate that a careful screening process is operated for the staff employed to carry out the order.</p> <p>The supplier guarantees that the staff employed by him to carry out the order will undertake to comply with and conduct themselves in accordance with the information security policy operated at the customer's premises. The customer will provide the supplier with a copy of this for appraisal beforehand if required.</p> <p>See also e.g. <i>NEN-ISO/IEC 27002:2007 sub-section 6.2.3 (a)</i></p>

6	<b>Subcontracting</b>	<p>The supplier guarantees that the use of subcontractors and relationships with these are in accordance with the stipulations in this checklist.</p> <p>The supplier is willing to provide the customer with an explanation regarding the way in which these stipulations are complied with beforehand.</p> <p>See also e.g. <i>NEN-ISO/IEC 27002:2007 sub-section 6.2.3 (u)</i></p>
7	<b>Auditing</b>	<p>The supplier consents to allow the customer to check on the process and the results of the agreement or to arrange for them to be checked by means of an (external) information security audit. Arrangements will then be made between the parties as to when, by which parties, at whose expense (including distribution) and at what cost the audit will be carried out.</p> <p>See also e.g. <i>NEN-ISO/IEC 27002:2007 sub-section 6.2.3 (n, o)</i></p>
8	<b>Access</b>	<p>The supplier guarantees that with regard to the order, the rules operated by the customer for physical and logical access (Identity &amp; Access Management) and remote access will be followed and complied with in full.</p> <p>The customer will provide the supplier with a copy of these for appraisal beforehand if required.</p> <p>See also e.g. <i>NEN-ISO/IEC 27002:2007 sections 9 and 11</i></p>
9	<b>Risk analysis</b>	<p>The supplier consents to allow the customer to carry out a risk analysis at the start of the provision of service at the customer's expense if the customer considers it necessary.</p> <p>See also e.g. <i>NEN-ISO/IEC 27002:2007 sub-section 6.2.1 (q)</i></p>
10	<b>Reporting</b>	<p>The supplier has implemented a process within which information security incidents and risks relating to the order are reported and dealt with effectively.</p> <p>The supplier is willing to allow this process to be inspected if required.</p> <p>See also e.g. <i>NEN-ISO/IEC 27002:2007 sub-section 6.2.3 (g, j and p), 13.1.1 and 13.1.2</i></p>

**Explanatory notes on use can be found on the reverse**

## **Explanatory notes on the use of the selection criteria relating to the 'Information Security Checklist'**

The aim is to improve the quality of information security in the Netherlands.

The checklist is intended to promote good commissioning practice in respect of information security-related aspects of products and services.

By using this checklist, potential contractors (suppliers) will be able to show to what extent they comply with the points included in the checklist.

Arrangements regarding compliance with information security for the order will be made between customer and supplier when agreeing on the order.

The CIG of the CIO Platform Netherlands has drawn up a checklist for (information) security-related aspects to be used for the purpose of assessing potential suppliers of IT products and/or services. It was discussed with and made known to (the members of) the ICT Office.

Members of the CIO Platform Netherlands are advised to use this checklist, as part of their own policy, during the initial phase of the selection process for suppliers of products and/or services.

Based on the standard for information security, ISO 27002, criteria are specified for which the supplier is requested to provide an insight into how he complies with information security. For a more detailed explanation of the criteria, reference to this standard is made for each subject.

In a follow-up process, if necessary and desired the CIO Information Security Interest Group of the CIO Platform will formulate this checklist in more detail/depth. This will, of course, be communicated in good time.

Information which are exchanged in connection with this checklist will be treated as strictly confidential by the parties involved.

On behalf of the Information Security Steering Committee,  
**The Information Security Steering Committee**