BSA | The Software Alliance

COUNTRY: **NETHERLANDS**

The Netherlands has a sophisticated and mature legal and policy framework for cybersecurity, which includes the National Cyber Security Strategy 2. Adopted in 2013, it is the second such strategy, as the country's cybersecurity framework is renewed every two years.

The Netherlands also has a National Cyber Security Centre, an expanded computer emergency response team, dealing with all cybersecurity related procedures and practices in a centralised manner. The centre also actively participates in the work of the Information Sharing and Analysis Centres (ISACs) for sectors involved with critical infrastructure.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The National Cyber Security Strategy 2 (NCSS2) <english.nctv.nl/images/national-cyber-security-strategy-2_tcm92-520278.pdf> was adopted by the Dutch government in 2013. The strategy contains a comprehensive appraisal of the cyber threats faced by the Netherlands and the best practices to address them. The "action programme" section of the strategy contains clear objectives and action items, each mapped to a broad expected delivery date. The strategy is the second of the Netherlands's cybersecurity strategies, the original National Cyber Security Strategy <www.ncsc.nl/binaries/en/organisation/about-the-ncsc/background/1/National+Cyber+Security+Strategy.pdf> being released in 2011. The second strategy is a revision based on the progress resulting from the first strategy, and the different priority areas that have emerged in the intervening years.
2.	What year was the national cybersecurity strategy adopted?	2013	A previous strategy was released in 2011.
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The policy letter Protecting Critical Infrastructure 2005 and the Third Progress Letter on National Security 2010 provide an assessment of the quality of the protection of Dutch critical infrastructure.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	◑	There is no legislation in place in the Netherlands that requires the establishment of a written information security plan. Information security is covered largely by the Government Decision on Information Security — Special Information 2013 <wetten.overheid.nl/BWBR0033507> as well as guidelines issued by the National Cyber Security Centre (NCSC.NL). <www.ncsc.nl>
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The Government Decision on Information Security — Special Information 2013 <wetten.overheid.nl/BWBR0033507> requires information important to the state, its ministries or its allies to be classified. The information is classified by a four-tiered classification system, as set out in the decision. The classification levels are assigned according to the level of risk involved in disclosing the classified information.
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	The Government Decision on Information Security — Special Information 2013 <wetten.overheid.nl/BWBR0033507> maps various security practices to assigned classification levels. These levels are set out in Article 2 of the decision and are assigned according to the level of risk involved in disclosing the classified information.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	◑	The Government Decision on Information Security — Special Information 2013 <wetten.overheid.nl/BWBR0033507> requires each information system to go through periodic audits, however, they are not set to occur within a mandatory timeframe. The Cyber Security Assessment Netherlands (CSAN) <english.nctv.nl/publications-products/Cyber_Security_Assessment_Netherlands> is a government cybersecurity report published annually, however it is not an audit of cybersecurity practices and procedures.

COUNTRY: NETHERLANDS

QUESTION	RESPONSE	EXPLANATORY TEXT
8. Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✓	The Cyber Security Assessment Netherlands (CSAN) is published annually. It contains a general cyber risk-assessment for the Netherlands, supported by incident data and a detailed analysis of detected cyber threats. The CSAN is available publicly in both Dutch and English. <english.nctv.nl/publications-products/Cyber_Security_Assessment_Netherlands>
9. Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✗	There is no legislation or policy in place in the Netherlands that requires each agency to have a chief information officer or chief security officer. The Government Decision on Information Security — Special Information 2013 <wetten.overheid.nl/BWBR0033507>, which details the duties and responsibilities of the security officer (Beveiligingsambtenaar), requires that security officers, when assigned, are assigned on a ministerial level. It does not, however, require each ministry to be assigned an officer.
10. Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✗	There is no legislation or policy in place in the Netherlands that requires mandatory reporting of cybersecurity incidents.
11. Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✓	Both the policy letter Protecting Critical Infrastructure 2005 and the Third Progress Letter on National Security 2010 include appropriate definitions for "critical infrastructure protection".
12. Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✓	The Netherlands recognises international certification schemes for information security — and only has local accreditation requirements for organisations handling some specific Government classified material.
OPERATIONAL ENTITIES		
1. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✓	The National Cyber Security Centre (NCSC.NL) <www.ncsc.nl> was established in 2012 and incorporated the CERT function of the superseded GOVCERT.NL. NCSC.NL is responsible for the coordination of incident response measures for the Dutch government institutions, as well as entities engaged with critical infrastructure.
2. What year was the computer emergency response team (CERT) established?	2012	
3. Is there a national competent authority for network and information security (NIS)?	◐	Network and information security is covered by the Ministry of Security and Justice. <www.government.nl/ministries/venj> There is no committed government agency for all network and information security. The National Cyber Security Centre (NCSC.NL) <www.ncsc.nl> is tasked with cybersecurity issues in particular.
4. Is there an incident reporting platform for collecting cybersecurity incident data?	✓	The National Cyber Security Centre (NCSC.NL) <www.ncsc.nl> is tasked with managing the reporting of cybersecurity incidents. The National Cyber Security Centre provides a multi-channel reporting structure to log cybersecurity incidents.
5. Are national cybersecurity exercises conducted?	✓	The Netherlands conducted three national cybersecurity exercises in the period 2007-2014. It has also participated in multi-national cybersecurity exercises organised by NATO.
6. Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✓	The National Cyber Security Centre (NCSC.NL) <www.ncsc.nl> is responsible for maintaining a national detection response network for the government sector and entities engaged with critical infrastructure. The exact structure of this network and procedures engaged with in the event of a cybersecurity incident are not publicly available.

COUNTRY: NETHERLANDS

	QUESTION	RESPONSE	EXPLANATORY TEXT
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✔	The National Cyber Security Centre (NCSC.NL) <www.ncsc.nl> is tasked with liaising with the private sector in carrying out its duties. In addition to the NCSC.NL, the Netherlands hosts two major public-private partnerships relevant to cybersecurity: • ECP <ecp.nl> is a public-private platform for promoting the use of information and communications technology in the Netherlands. • The National Continuity Forum (NCO-T) is a public-private partnership between the government and suppliers of telecommunication networks. In addition, the Netherlands has signed a memorandum of understanding on cybersecurity with Luxembourg and the Belgium, which includes cooperation and expertise-sharing on the development of public-private partnerships.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✔	The Hague Security Delta <www.thehaguesecuritydelta.com> is a security cluster of Dutch companies and other relevant institutions that deal directly with cybersecurity.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	–	The Netherlands already has a public-private partnership dedicated to cybersecurity.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✔	The National Cyber Security Centre (NCSC-NL) <www.ncsc.nl> participates in Information Sharing and Analysis Centres (ISACs) with holders of critical infrastructure on a sectoral basis.
2.	Have sector-specific security priorities been defined?	✖	Sector-specific security priorities have not been defined.
3.	Have any sector-specific cybersecurity risk assessments been conducted?	✖	Sector-specific cybersecurity risk assessments have not been conducted, however the National Cyber Security Strategy (NCSS2) 2013 <english.nctv.nl/images/national-cyber-security-strategy-2_tcm92-520278.pdf> proposes that risk analyses and security requirements for critical infrastructure sectors be carried out in cooperation with the National Cyber Security Centre (NCSC-NL). <www.ncsc.nl>
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	The National Cyber Security Strategy (NCSS2) 2013 <english.nctv.nl/images/national-cyber-security-strategy-2_tcm92-520278.pdf> includes a strong commitment to cybersecurity education, built around the establishment of a task force on cybersecurity education. The objective of the task force is to: "enlarge the pool of cyber security experts and enhance users' proficiency with cyber security, the business community and the government join forces to improve the quality and breadth of ICT education at all academic levels (primary, secondary and professional education)".