COUNTRY: CZECH REPUBLIC

The Cyber Security Strategy of the Czech Republic for the period 2011-2015 was published in 2011. The strategy provides general cybersecurity principles and clearly stated goals. On 1 January 2015, the Act on Cyber Security came into force. This law includes comprehensive provisions on most aspects of cybersecurity and is complemented by several important regulations.

The country has also established a national computer emergency response team CERT), CSIRT.CZ, as well as a CERT dedicated to government agencies: GOVCERT.CZ.

The National Cyber Security Centre was launched on 1 January 2015 to promote public-private partnerships. Furthermore, the Czech Republic is conducting a sector-based security risk assessment in cooperation with the academic and private sectors. The project is the first such assessment that addresses cybersecurity.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The Cyber Security Strategy of the Czech Republic for the Period 2011-2015 <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CzechRepublic_Cyber_Security_Strategy.pdf> was adopted in 2011. The strategy provides general cybersecurity principles and clearly stated goals. On 1 January 2015, the Law No. 181/2014 (The Act on Cyber Security) came into force. <https://www.govcert.cz/download/nodeid-1143/> The law includes comprehensive provisions on most aspects of cybersecurity, and is complemented by several important regulations.
2.	What year was the national cybersecurity strategy adopted?	2011	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The new Act on Cyber Security that came into force on 1 January 2015 includes provisions for the development of a critical information infrastructure plan in the Czech Republic. <https://www.govcert.cz/download/nodeid-1143/> The details of the infrastructure to be protected are set out in the following regulations: • Regulation No. 317/2014 Coll. on the Determination of Important Information Systems and their Determination Criteria; and • Decision of the Government No 315/2014 Coll. which amends the Decision of the Government No. 432/2010 Coll. on the Criteria for the Determination of the Elements of the Critical Infrastructure. <https://www.govcert.cz/en/legislation/legislation/>
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✔	The Act on Cyber Security 2014 <https://www.govcert.cz/download/nodeid-1143/> requires the National Security Authority (NBU) <www.nbu.cz> to manage the field of cybersecurity for the Czech Republic, which includes the monitoring and reporting of the implementation of the act and the operational status of the duties required by the act. It also requires organisations to prepare written security plans. The required content for these plans is set out in Regulation No. 316/2014 Coll. on Security Measures, Cyber Security Incidents and Reactive Measures (Cyber Security Regulation). <https://www.govcert.cz/en/legislation/legislation/>
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	Act 412 on the Protection of Classified Information 2005 <www.nbu.cz/download/nodeid-1814> requires data, of which disclosure may damage the interests of the Czech Republic or may be disadvantageous to the Czech Republic or its partners in carrying out its international obligations, to be classified. The four-tiered level of classification is outlined in Section 4 of the act. The 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?	✔	Act 412 on the Protection of Classified Information 2005 <www.nbu.cz/download/nodeid-1814> of the Czech Republic maps security practices, including requirements for the storage of and access to classified information, to the classification level of the data involved. The classification levels themselves are assigned according to the level of risk involved in disclosing the information.

COUNTRY: CZECH REPUBLIC

QUESTION	RESPONSE	EXPLANATORY TEXT
7. Is there legislation/policy that requires (at least) an annual cybersecurity audit?	◑	There is no legislation or policy in place in the Czech Republic that requires an annual cybersecurity audit. Article 15 of the Cyber Security Strategy of the Czech Republic for the Period 2011-2015 <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CzechRepublic_Cyber_Security_Strategy.pdf> states the need for legally binding rules that regulate cybersecurity standards — and this specifically includes "periodical" compliance audits. Pursuant to this article, the Act on Cyber Security 2014 <www.govcert.cz/download/nodeid-591> requires an information systems audit as a security measure. Audits, however, are not required to be carried out within a specific timeframe. Section 98 of Act 127 on Electronic Communications and on Amendments to Some Related Acts 2005 <portal.gov.cz/app/zakony/download?idBiblio=59921&nr=127~2F2005~20Sb.&ft=pdf> compels the Czech Telecommunications Office (CTU) to provide European Union Agency for Network and Information Security (ENISA) with an annual report covering the responses from the CTU to breaches to the security and integrity of the Czech network. Furthermore, Section 97 equips the CTU with the right to order an independent safety audit, however it is not compelled to do so.
8. Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✓	The Cyber Security Strategy of the Czech Republic for the Period 2011-2015 <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CzechRepublic_Cyber_Security_Strategy.pdf> states that support of current efforts towards cybersecurity — from the public, private, and military sectors — is an essential principle of the strategy. Pursuant to the strategy, the Act on Cyber Security 2014 <www.govcert.cz/download/nodeid-591> legislates the use of Information Security Management System (ISMS) as a security measure. The ISMS includes monitoring and testing of the efficiency of cybersecurity-related processes. The act does not require the findings that come from the monitoring and testing to be collated or publicly published.
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 Czech Republic that requires each agency to have a chief information officer or chief security officer.
10. Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✓	The Act on Cyber Security 2014 <https://www.govcert.cz/download/nodeid-1143/> requires persons to report cybersecurity incidents in their network, critical infrastructure system or other important information system to the national CERT and the national security authority.
11. Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✓	The Act on Cyber Security 2014 <https://www.govcert.cz/download/nodeid-1143/> includes an appropriate definition for "critical information infrastructure".
12. Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	◑	The Cyber Security Strategy of the Czech Republic for the Period 2011-2015 <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CzechRepublic_Cyber_Security_Strategy.pdf> includes a recommendation that the Czech Republic should "join effective and promising initiatives advocating the development of international legal standards dealing with cyber and information security issues", along with some other positive references to international standards. In practice, these steps are yet to be implemented.
OPERATIONAL ENTITIES		
1. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✓	CSIRT.CZ <www.csirt.cz> was established in 2011. It is responsible for coordinating security and incident response measures across all Czech networks. It is classified by the Act on Cyber Security 2014 <https://www.govcert.cz/download/nodeid-1143/> as the National CERT. GovCERT <www.govcert.cz> has jurisdiction over the public administration and critical information infrastructure. It is classified by the Act on Cyber Security 2014 <https://www.govcert.cz/download/nodeid-1143/> as the Governmental CERT.
2. What year was the computer emergency response team (CERT) established?	2011	

COUNTRY: CZECH REPUBLIC

QUESTION	RESPONSE	EXPLANATORY TEXT
3. Is there a national competent authority for network and information security (NIS)?	✓	The National Security Authority (NBU) <www.nbu.cz> manages the National Cyber Security Centre as per the Decision of the Government of the Czech Republic n. 781. The operation of the National Cyber Security Centre is undertaken with the close cooperation of GovCERT and CSIRT.CZ, which the Act on Cyber Security 2014 <https://www.govcert.cz/download/nodeid-1143/> and the Security Strategy of the Czech Republic <www.army.cz/images/id_8001_9000/8503/Czech_Security_Strategy_2011.pdf> regard as the government coordination centre for immediate response to computer incidents. Relevant bodies include the NBU, as well as the Czech Telecommunications Office (CTU), which is compelled by Act 127 on Electronic Communications and on Amendments to Some Related Acts 2005 <portal.gov.cz/app/zakony/download?idBiblio=59921&nr=127~2F2005~20Sb.&ft=pdf> to comply with all legislation regarding the protection and security of the data within its networks.
4. Is there an incident reporting platform for collecting cybersecurity incident data?	✓	CSIRT.CZ <www.csirt.cz> is tasked with managing the reporting of cybersecurity incidents. There is an email-based reporting structure to log cybersecurity incidents. CSIRT.CZ periodically publish statistics on the number of incidents logged and the status of their resolution. The Act on Cyber Security 2014 <https://www.govcert.cz/download/nodeid-1143/> requires the National Security Authority <www.nbu.cz> to keep a record of cybersecurity incidents.
5. Are national cybersecurity exercises conducted?	◑	The Czech Republic has participated in multi-national exercises organised by the European Union.
6. Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✓	Chapter Three of the Act on Cyber Security 2014 <https://www.govcert.cz/download/nodeid-1143/> outlines the incident management structure in the event of a state of cyber emergency. The comprehensive procedure includes specific responsibilities for the National Security Authority <www.nbu.cz>, including informing the Prime Minister. The Cyber Security Strategy of the Czech Republic for the Period 2011-2015 <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CzechRepublic_Cyber_Security_Strategy.pdf> outlines an intent for the Czech Republic to implement and update plans designed to deal with cybersecurity incidents. Moreover, the Security Strategy of the Czech Republic makes reference to a national and international early warning system in which CSIRT.CZ is involved. The processes of the system are not elaborated upon.
PUBLIC-PRIVATE PARTNERSHIPS		
1. Is there a defined public-private partnership for cybersecurity?	✗	The Czech Republic does not have a defined public-private partnership for cybersecurity. The National Cyber Security Centre (operated by the National Security Authority (NBU) <www.nbu.cz>) will become fully operational in 2015 and is expected to have a working group that includes representatives from the private sector.
2. Is industry organised (i.e. business or industry cybersecurity councils)?	✗	There is no significant industry-led platform for cybersecurity in the Czech Republic.
3. Are new public-private partnerships in planning or underway (if so, which focus area)?	◑	While there are no specific public-private partnerships being planned in the Czech Republic, the need to cooperate with the private sector in order to strengthen cybersecurity is a key principle of the Cyber Security Strategy of the Czech Republic for the Period 2011-2015.
SECTOR-SPECIFIC CYBERSECURITY PLANS		
1. Is there a joint public-private sector plan that addresses cybersecurity?	✗	The Czech Republic does not have sector-specific joint public-private plans in place.
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?	✓	The four-year environmental security risk assessment project EnviSec <www.envisec.cz> is being conducted in the Czech Republic. It covers, in part, the security of and access to environmental data sources.

COUNTRY: CZECH REPUBLIC

	QUESTION	RESPONSE	EXPLANATORY TEXT
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	The Czech Republic Cybersecurity Strategy 2001-2015 <www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF> includes several commitments to implementing cybersecurity education, including: • Increasing the cyber and information security awareness of citizens by disseminating relevant information in cooperation with the media; • Including cybersecurity in education programmes of public servants and promoting education in the private sector; • Cooperating with the private sector in the implementation of training programmes focusing on cyber and information security; and • Integrating cyber and information security in relevant methodologies at all levels of education.