COUNTRY: **GERMANY**

Germany has a comprehensive cybersecurity strategy, adopted in 2011 and complemented by a strong cybersecurity legal framework. The existence of the Federal Office for Information Security (BSI), in charge of managing computer and communication security for the German government, is a clear demonstration that cybersecurity is elevated to a high government level.

Germany also has a network of computer emergency response teams (CERTs), with the national CERT, CERT-BUND, working closely with both state-level and non-governmental CERTs.

Furthermore, the country has well-developed public-private partnerships, such as the Alliance for Cyber-Security and the UP KRITIS partnership, and its national policies and legal framework reflect this focus on cooperation.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The Cyber Security Strategy for Germany <www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.html> was adopted in 2011. It is a comprehensive strategy that includes guiding principles, clear goals, and an implementation plan.
2.	What year was the national cybersecurity strategy adopted?	2011	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The National Strategy for Critical Infrastructure Protection (CIP Strategy) <www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf> was adopted by the German Government in 2009. Critical infrastructure protection, as it relates to cybersecurity, is also addressed in the Cyber Security Strategy for Germany. <www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.html>
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or policy in place in Germany that requires the establishment of a written information security plan. Recommendations issued by the Federal Office for Information Security (BSI) <www.bsi.bund.de>, such as those of cloud computing providers, partly cover information security.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	Section 93-95 of the German Criminal Code <www.gesetze-im-internet.de/englisch_stgb> is related to the definition of national security secrets. Additionally, the Safety Assessment Act 1994 <www.gesetze-im-internet.de/bundesrecht/s_g/gesamt.pdf> requires data deemed in need of secrecy to protect the public interest be classified. Paragraph 4 of the act outlines a four-tiered system of classification levels. 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?	✔	The Regulation of the Ministry of the Interior for the Material and Organisational Protection of Classified Information (Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen) 2006, pursuant to the Safety Assessment Act 1994 <www.gesetze-im-internet.de/bundesrecht/s_g/gesamt.pdf>, maps various security practices to assigned classification levels. These levels are set out in Paragraph 4 of the act 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?	Draft	The draft Act to Increase the Security of Information Technology <www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?__blob=publicationFile> would require the Federal Office for Information Security (BSI) <www.bsi.bund.de> to conduct security audits of entities engaged with critical infrastructure once every two years.

COUNTRY: GERMANY

	QUESTION	RESPONSE	EXPLANATORY TEXT
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	Draft	The draft Act to Increase the Security of Information Technology <www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?__blob=publicationFile> would require the Federal Office for Information Security (BSI) <www.bsi.bund.de> to, in cooperation with federal authorities, analyse the potential for cyber threats to entities engaged with critical infrastructure and to continually update the government with regard to the security situation of entities engaged with critical infrastructure.
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 Germany 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 the Federal Office of Information Security 2009 <www.bmi.bund.de/SharedDocs/Downloads/EN/Gesetzestexte/bsi_act.html> requires federal authorities to report cybersecurity incidents to the Federal Office of Information Security upon detection. There is a draft amendment to the act <www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.html>, which proposes the strengthening of mandatory reporting requirements covering telecommunication service providers and entities engaged with critical infrastructure.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The National Strategy for Critical Infrastructure Protection (CIP Strategy) <www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf> includes appropriate definitions for "critical infrastructure" and "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?	✔	Germany recognises international security certifications, and although some local security guidelines have been developed, they do not require additional local certification or accreditation. For example, refer to the Cloud-fahrplan für die öffentliche verwaltung — a guideline published by the Fraunhofer Institute (FOKUS) as a road map to help federal institutions migrate IT services to Cloud. <www.oeffentliche-it.de/documents/18/21941/Cloud-Fahrplan+oeffentliche+Verwaltung>
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT-Bund <www.cert-bund.de> was established in 2012 and is responsible for warning systems and coordinating incident response measures for German federal government authorities. It works closely with German CERT alliances and state-level CERTs to provide wider coverage.
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)?	✔	The Federal Office for Information Security (BSI) <www.bsi.bund.de> acts as Germany's national competent authority for network and information security. The National Cyberdefence Centre, which reports to BSI, is the agency primarily responsible for cybersecurity.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	Operated by the Federal Office for Information Security (BSI) <www.bsi.bund.de>, CERT-Bund <www.cert-bund.de> is tasked with collecting information about cybersecurity incidents. They engage proactively by monitoring their constituency for cybersecurity incidents, as well as providing an online reporting structure to log cybersecurity incidents. The National Cyber Response Centre, which reports to BSI, provides a platform for cross-agency cooperation on cybersecurity. The Digital Agenda 2014-17 <www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2014/digital-agenda.html> states that the incident response capacities of the centre will be strengthened.
5.	Are national cybersecurity exercises conducted?	✔	Germany conducted three national cybersecurity exercises between 2010 and 2012. Germany also participated in multi-national exercises organised by the European Union and NATO.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	There is no national incident management structure in place in Germany for responding to cybersecurity incidents. The Act to Strengthen Federal Information Security 2009 <www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/BSI/bsiges2009_pdf.html> gives the Federal Office for Information Security the authority to act as the national authority for information security. The act does not outline a general incident management structure, nor specific practices related to cybersecurity.

COUNTRY: GERMANY

	QUESTION	RESPONSE	EXPLANATORY TEXT
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✔	UP KRITIS <www.bsi.bund.de/DE/Themen/KritischeInfrastrukturen/Umsetzungsplan/umsetzungsplan_node> is a public-private partnership between operators of critical infrastructure and the relevant public authorities. One of the explicit goals of the UP KRITIS is the "joint assessment and evaluation of cyber security". The Alliance for Cyber-Security <www.allianz-fuer-cybersicherheit.de> is an initiative of the German federal government in which key information technology stakeholders, both public and private, exchange information and establish and expand a knowledge database in order to strengthen cybersecurity in Germany.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✔	The Cyber-Security Council Germany <www.cybersicherheitsrat.de> is an independent cybersecurity association comprised of members from private entities engaged with critical infrastructure.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	✔	The National Cyber Security Council is to be established pursuant to the recommendations of the Cyber Security Strategy for Germany. <www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.html> This body would comprise of representatives from multiple federal ministries and selected representatives from the business community. Its purpose is to provide an interdisciplinary platform to coordinate the development of preventative tools and interdisciplinary cybersecurity approaches.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Germany 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?	✖	Sector-specific risk assessments have not been released.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	◑	The Cyber Security Strategy for Germany 2011 <www.germany.info/Vertretung/usa/en/06__Foreign__Policy__State/02__Foreign__Policy/05__KeyPoints/CyberSecurity-key.html> is unusually silent on the issue of cybersecurity education. However, a number of individual cybersecurity education campaigns operate in Germany, including: • Watch Your Web <www.watchyourweb.de> and • KlickSafe. <www.klicksafe.de>