COUNTRY: **DENMARK**

Denmark does not have a national cybersecurity strategy or a law dedicated to this subject. Denmark recently passed a law that establishes the Centre for Cyber Security, which both takes control of and supersedes its current government computer emergency response team (CERT). The scope and powers of the new centre are still to be confirmed.

The Danish private sector has established a formal framework for cooperation on cybersecurity issues through the Council for Digital Security.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✖	Denmark does not have a national cybersecurity strategy in place. The European Union Agency for Network and Information Security website <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategy-denmark> indicates that a cybersecurity strategy for Denmark is being prepared and is expected to be implemented by the end of 2014. The Danish Defence Agreement 2013-2017 <www.fmn.dk/eng/allabout/Pages/DanishDefenceAgreement2013-2017.aspx> outlines the measures the Ministry of Defence intends to take with regard to cybersecurity. This includes the establishment of the Centre for Cybersecurity under the Ministry of Defence and the establishment of a Computer Network Operations (CNO) function, in order to execute defensive and offensive military-led cyber operations.
2.	What year was the national cybersecurity strategy adopted?	–	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✖	Denmark has published official guidelines stating that compliance with international security standards will be required for government procurement relating to critical infrastructure and other ICT services. Refer to: Cloud computing and the legal framework (Guidance on legislative requirement and the contractual environment related to cloud computing), published by the Agency for Digitisation in August 2012. <digitaliser.dk/resource/2368677>
4.	Is there legislation/policy that requires the establishment of a written information security plan?	◑	The responsibility for information security, and associated operations, is shared among ministries and are not guided by a single plan. The Decree Establishing a Framework for Information Security and Preparedness <www.retsinformation.dk/Forms/R0710.aspx?id=136848>, pursuant to Act 169 on Electronic Communication Networks and Services, requires the National IT and Telecom Agency to develop specific rules affecting public electronic communications networks in order to establish a framework for information security and data protection. The Ministry of Defence, particularly through the Danish Defence Intelligence Service's Centre of Cybersecurity, plays a significant role in information security oversight and this role is addressed in the Danish Defence Agreement 2013-2017. <www.fmn.dk/eng/allabout/Documents/TheDanishDefenceAgrement2013-2017english-version.pdf>
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	Denmark classifies sensitive data according to a four-tiered classification system, as set out in the Danish Criminal Statutes. There is, however, no legal requirement for the classification of data according to a specific inventory of systems.

COUNTRY: DENMARK

	QUESTION	RESPONSE	EXPLANATORY TEXT
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	The Decree on Information Security and Preparedness for Electronic Communication Networks and Services <www.retsinformation.dk/Forms/R0710.aspx?id=136848>, pursuant to Act 169 on Electronic Communication Networks and Services, requires network and service providers to identify, select, and prioritise information security processes for networks — on the basis of the risk and consequences in the event of a breach of the network. There are access requirements for public information in the Law on Public Administration <www.ft.dk/RIpdf/samling/20121/lovforslag/L144/20121_L144_som_vedtaget.pdf>, but these are not mapped to risk levels. There are also limitations and security processes set out in the Law on the Danish Cybersecurity Centre <www.ft.dk/RIpdf/samling/20131/lovforslag/L192/20131_L192_som_vedtaget.pdf> for handling with personal data.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	There is no legislation or policy in place in Denmark that requires at least an annual audit. The duties of the Centre for Cybersecurity, as set out in the Act 192 on the Danish Centre for Cybersecurity <www.ft.dk/RIpdf/samling/20131/lovforslag/L192/20131_L192_som_vedtaget.pdf>, involve a monitoring of cybersecurity compliance. However, an annual audit is not specifically required.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✖	The responsibility for information security, and associated operations, is shared among ministries and are not guided by a single plan. The Decree Establishing a Framework for Information Security and Preparedness <www.retsinformation.dk/Forms/R0710.aspx?id=136848>, pursuant to Act 169 on Electronic Communication Networks and Services, requires the National IT and Telecom Agency to develop specific rules affecting public electronic communications networks in order to establish a framework for information security and data protection. The Ministry of Defence, particularly through the Danish Defence Intelligence Service's Centre of Cybersecurity, plays a significant role in information security oversight and this role is addressed in the Danish Defence Agreement 2013-2017. <www.fmn.dk/eng/allabout/Documents/TheDanishDefenceAgrement2013-2017english-version.pdf>
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 Denmark 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?	✖	There is no legislation or policy in place in Denmark that requires mandatory reporting of cybersecurity incidents.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The Danish Security and Intelligence Service (PET) <www.pet.dk> provides an appropriate definition of "critical infrastructure".
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	Denmark has published official guidelines stating that compliance with international security standards will be required for government procurement relating to critical infrastructure and other ICT services. Refer to: Cloud computing and the legal framework — Guidance on legislative requirement and the contractual environment related to cloud computing, published by the Agency for Digitisation. <digitaliser.dk/resource/2368677>
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	GovCERT <www.cert.dk> was established in 2009. It is responsible for the coordination of security and incident response measures for Danish government institutions and entities engaged with critical infrastructures. Since July 2014, GovCERT has operated under the Centre for Cybersecurity <fe-ddis.dk/CFCS>, which has a broader scope and wider capabilities.
2.	What year was the computer emergency response team (CERT) established?	2009	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The Centre for Cybersecurity <fe-ddis.dk/CFCS> operates as the national competent authority for network and information security in Denmark. It administrates GovCERT and acts as a central government repository of incident and cybersecurity data.

COUNTRY: DENMARK

	QUESTION	RESPONSE	EXPLANATORY TEXT
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	GovCERT <www.cert.dk> is tasked with managing the reporting of cybersecurity incidents within its constituency. The Centre for Cybersecurity <fe-ddis.dk/CFCS>, under which GovCERT operates, carries out activities to proactively investigate suspected cybersecurity incidents. The centre also publishes a "picture" of the current cybersecurity situation from the Danish perspective, which includes comparisons of national and international of cybersecurity incident statistics.
5.	Are national cybersecurity exercises conducted?	✔	Denmark has a commitment to conduct the national cybersecurity exercise Krisestyringsoevelser <brs.dk/beredskab/idk/krisestyringsoevelser/Pages/Krisestyringsoevelser.aspx> every two years. The Centre for Cybersecurity took part in cybersecurity exercises organised by the European Union in 2014.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	◑	The Centre for Cybersecurity <fe-ddis.dk/CFCS> and GovCERT <www.cert.dk> both have legal requirements to cooperate closely with government departments in the event of a cybersecurity incident, however Denmark does not have a clear incident management structure in place.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✖	There is no defined public-private partnership for cybersecurity in Denmark.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✔	The Council for Digital Security <www.digitalsikkerhed.dk> is a security and privacy advocacy group comprised of 20 private sector and academic organisations. Furthermore, Dansk IT <dit.dk>, a representative body for information technology professionals in Denmark, engages with cybersecurity in the course of its operations.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	✖	There are no new public-private partnerships being planned in Denmark.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Denmark 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, as of August 2014.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✖	Denmark is preparing a national cybersecurity strategy and this may contain some education commitments.