BSA The Software Alliance

COUNTRY: **LUXEMBOURG**

Luxembourg has a fairly limited cybersecurity strategy, published in 2013, which contains some key guiding principles but has little detail on their implementation. The country's legal framework for supporting cybersecurity is also yet to be fully developed. The need to encourage public-private cooperation is a principle mentioned in the cybersecurity strategy, but no formal cooperation is known.

Luxembourg has two computer emergency response teams (CERTs). CIRCL is a response coordinating body that covers all organisations operating in Luxembourg, while GOVCERT.LU is dedicated to public authorities. CASES, a government information security agency, engages in awareness raising activities and the promotion of best practices.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✓	The National Strategy on Cyber Security <mediacom.public.lu/cybersecurity/Strat__gieCybersecurity_122011.pdf> was adopted by the Luxembourg government in 2013. The strategy contains high-level statements of intent — organised around five "pillars" of cybersecurity, including: critical infrastructure; the legal framework; national and international cooperation; awareness and education; and mandatory standards.
2.	What year was the national cybersecurity strategy adopted?	2013	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✗	As of August 2014, the High Commissioner for National Protection <www.hcpn.public.lu/plans_nationaux/infcritique> is developing a critical infrastructure plan.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✗	There is no legislation or policy in place in Luxembourg that requires the establishment of a written information security plan.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	◑	Luxembourg classifies sensitive information against a four-tiered classification system, however there is no legislation or policy requiring the classification of particular data.
6.	Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?	✗	There is no legislation or policy in place in Luxembourg that requires security practices or requirements to be mapped to risk levels.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	◑	The Centre for State Information Technologies (CTIE) <www.ctie.public.lu> is responsible for organising security audits related to information technology, as stated in the Grand-Ducal Regulation of 7 May 2009. <www.legilux.public.lu/leg/a/archives/2009/0099/a099.pdf#page=2> However, audits are not required to be conducted annually and CTIE's jurisdiction does not comprehensively cover all government information systems.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✗	There is no legislation or policy in place in Luxembourg that requires a public report on cybersecurity capacity for the government.
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 Luxembourg 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 Luxembourg that requires mandatory reporting of cybersecurity incidents.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✓	The High Commissioner for National Protection <www.hcpn.public.lu> has published an appropriate definition for "critical infrastructure".

COUNTRY: LUXEMBOURG

	QUESTION	RESPONSE	EXPLANATORY TEXT
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	◑	The Luxembourg National Strategy on Cyber Security 2013 <mediacom.public.lu/cybersecurity/Strat__gieCybersecurity_122011.pdf> includes a recommendation to "establish mandatory standards", but provides no other details. The strategy contains a broad commitment to international cooperation.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✓	The Computer Incident Response Centre Luxembourg (CIRCL) <circl.lu> was established in 2008. It is responsible for coordinating incident response measures for its constituency, which covers all entities and organisations located in, or operating from, Luxembourg. In addition to CIRCL, GOVCERT.LU <www.govcert.lu> was established in 2011. It is responsible for coordinating incident response measures for Luxembourg state authorities and entities engaged with critical infrastructure.
2.	What year was the computer emergency response team (CERT) established?	2011	
3.	Is there a national competent authority for network and information security (NIS)?	◑	The Cyber World Awareness & Security Enhancement Services (CASES) <www.cases.lu> is an initiative of the Luxembourg government that provides extensive, high-quality information on best practices in information security for businesses and individuals. It does not act as a broader government authority for network and information security.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✓	The Computer Incident Response Centre Luxembourg (CIRCL) <circl.lu> is tasked with managing the reporting of cybersecurity incidents within its constituency. CIRCL provides an online reporting structure to log cybersecurity incidents. GOVCERT.LU <www.govcert.lu> is tasked with the management of cybersecurity incident data for incidents affecting government networks or entities engaged with critical infrastructure. They provide an online, form-based reporting platform to log incidents.
5.	Are national cybersecurity exercises conducted?	◑	Luxembourg participated in the multi-national cybersecurity exercise Cyber Coalition 2013 organised by NATO.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	◑	The Computer Incident Response Centre Luxembourg (CIRCL) <circl.lu> is responsible for cyber threat detection, however, scant details are available on a full national incident management structure.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✖	There is no defined public-private partnership for cybersecurity in Luxembourg.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✖	There is no significant industry-led platform for cybersecurity in Luxembourg.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	◑	The need to encourage coordination between the public and private sectors is addressed in the National Strategy on Cyber Security. <mediacom.public.lu/cybersecurity/Strat__gieCybersecurity_122011.pdf> In addition, Luxembourg has signed a memorandum of understanding on cybersecurity with Belgium and the Netherlands, which includes cooperation and expertise-sharing on the development of public-private partnerships. On the other hand, there is no evidence of specific public-private partnerships being planned.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Luxembourg 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.

COUNTRY: LUXEMBOURG

	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?	✓	Luxembourg has a comprehensive cybersecurity education program in place, built around the key publication — Information Security Guide for Use in School and at Home (2010, revised 2013) — and a series of accompanying online materials hosted at the BEE-Secure site. <www.bee-secure.lu>