COUNTRY: **LATVIA**

The Latvian cybersecurity strategy, published in 2014, contains a clear set of concrete objectives matched with specific implementation dates. It also has a strong legal framework for supporting cybersecurity, an important pillar of which is the Law on Security of Information Technology adopted in 2010. This law sets out the roles and responsibilities of the country's national computer emergency response team, CERT.LV.

While the cybersecurity strategy provides for the establishment of formalised public-private partnerships for cybersecurity, no such platforms yet exist.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The Latvian Cybersecurity Strategy 2014-2018 and its amendments <likumi.lv/doc.php?id=267527> came into effect in June 2014. It is composed of simple goals and objectives set to quarterly implementation deadlines. These objectives are based around five conceptual aspects of cybersecurity: governance and resources; justice and mitigation; preparedness and capacity; public awareness, education and research; and international cooperation.
2.	What year was the national cybersecurity strategy adopted?	2014	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✖	A discrete critical infrastructure protection strategy or plan does not exist. Measures concerning the protection of critical infrastructure are addressed, in part, in the Law on the Security of Information Technology 2010. <www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.doc>
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or policy in place in Latvia 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?	✔	The Law on State Secrets 1997 <www.knab.gov.lv/uploads/eng/on_official_secrets.pdf> requires all data that is listed by Cabinet as a state secret, or disclosure of which may cause harm to the security, economic, or political interests of the state to be classified. Information is classified according to a three-tiered classification system. 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 Law on State Secrets 1997 <www.knab.gov.lv/uploads/eng/on_official_secrets.pdf> maps various security practices to assigned classification levels. Section 3 sets out these levels, which are assigned according to the level of risk involved in disclosing the classified information. The Law on the Security of Information Technology 2010 <www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.doc> enforces security requirements for data deemed to be personal data, in accordance with the risks involved in processing such data. The law does not further map security requirements to specific risk levels.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✔	The Law on the Security of Information Technology 2010 <www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.doc> requires appointed security officers to carry out an examination of the security of information technologies on at least a yearly basis. The law also requires officers to organise the elimination of any deficiencies detected.
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 Latvia that requires a public report on cybersecurity capacity for the government. The Law on the Security of Information Technology 2010 <www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.doc> requires the Security Incidents Response Institution to maintain "in a publicly accessible way" recommendations regarding the prevention of current risks or information technologies.

COUNTRY: LATVIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✔	The Law on the Security of Information Technology 2010 <www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.doc> requires the head of each state and local government authority to appoint a person responsible for the management of information security within that particular authority. The appointed individuals have their specific duties outlined in the law.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✔	The Law on the Security of Information Technology 2010 <www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.doc> requires any state or local government authority, or owner or lawful possessor of critical information technology infrastructure, subject to a cybersecurity incident to report that the occurrence of the incident without delay.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	Section 3 of the Law on the Security of Information Technology 2010 <www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.doc> includes an appropriate definition for "critical infrastructure" and an explanation of the defence 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?	◑	The Latvian Cybersecurity Strategy 2014-2018 <likumi.lv/doc.php?id=267527> is silent on standards and certification requirements for procurement, but it does contain a strong general commitment to international cooperation in the cybersecurity field.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT.LV <cert.lv> was established in 2006, initially under the name LATNET CERT, and incorporated under its current name in 2012. It is responsible for coordinating security and incident response measures across all Latvian networks. It is overseen by the Ministry of Transport and operated by University of Latvia's Institute of Mathematics and Computer Science.
2.	What year was the computer emergency response team (CERT) established?	2006	
3.	Is there a national competent authority for network and information security (NIS)?	✔	CERT.LV <cert.lv> acts as the national competent authority for network and information security in Latvia. It was granted this responsibility as it acts as the Information Technology Security Incident Prevention Institution referred to by the Law on the Security of Information Technology 2010. <www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.doc>
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT.LV <cert.lv> is tasked with managing the reporting of cybersecurity incidents. It provides an email-based reporting structure to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	✔	Latvia conducted a national cybersecurity exercise in 2011. Latvia has also participated in multi-national cyber exercises organised by NATO.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	Section 6 of the Law on the Security of Information Technology 2010 <www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.doc> outlines the sequences of actions that are to be taken in the event of an information technology security incident. These include procedures on informing relevant ministers and, if required, the notification and involvement of European Union representatives. The National IT Safety Council, comprised of the relevant ministers, is the responsible entity within the Latvian government for responding to information technology security concerns.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✖	There is no defined public-private partnership for cybersecurity in Latvia.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✖	There is no significant industry-led platform for cybersecurity in Latvia.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	◑	The establishment of a public-private partnership to support cybersecurity research is a required action of the Latvian Cybersecurity Strategy 2014-2018. <www.mk.gov.lv/lv/mk/tap/?pid=40267912>

COUNTRY: LATVIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Latvia 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 Latvian Cybersecurity Strategy 2014- 2018 <likumi.lv/doc.php?id=267527> includes five priority areas. The third priority is "Public awareness, education and research". There is a detailed timeline for specific education initiatives over the period 2014-2020.