COUNTRY: **ITALY**

Italy updated its security laws in 2007 and adopted cybersecurity plans in 2013 and 2014, resulting in a strong legal framework supporting cybersecurity. The Italian cybersecurity strategy also calls out public-private partnerships as the intended direction for cybersecurity, but no formalised cooperation yet exists.

CERT-PA was established in 2014. It is responsible for cybersecurity warning systems and the coordination of incident response measures for Italian government institutions.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The National Strategic Framework for Cyberspace Security and the National Plan for Cyberspace Protection and ICT Security <www.sicurezzanazionale.gov.it/sisr.nsf/english/italian-national-cyber-strategy.html> were adopted by prime-ministerial decree in January 2014. They comprise a comprehensive strategy that provides an assessment of Italy's cybersecurity capacity and outlines the roles and responsibilities of relevant ministries and agencies. They work in conjunction with the Italian Digital Agenda, a government-led initiative to invest in digital development.
2.	What year was the national cybersecurity strategy adopted?	2014	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	Italy has published multiple guidelines that address critical infrastructure protection, including • Network Security of Critical Infrastructures; • Network Security: From Risk Analysis to Protection Strategies; and • Guideline on Managing Local Emergencies. The Italian Digital Agenda has a working group that address infrastructure and security specifically as it related to cybersecurity and critical information infrastructure protection.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or policy in place in Italy 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?	✔	As part of a reorganisation of Italy's security services, Law No. 124/2007 <www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html> established the Department of Information Security (DIS) <www.serviziinformazionesicurezza.gov.it>, which acts on the advice of the Prime Minister. DIS is tasked with classifying information deemed a state secret and does so according to a four-tiered classification system. Levels of the classification system 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?	✔	Law No. 124/2007 <www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html> established the Department of Information Security (DIS) <www.serviziinformazionesicurezza.gov.it>, which dictates the security requirements for handling classified information according to the classification level given to the information. These classification levels 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?	✖	Section 38 of Law No. 124/2007 <www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html> requires the government to send to parliament a written annual report on its security intelligence policy and achievements in the past year — with a document on cyber defence and security attached. An audit of compliance is not required and the exact procedures to be followed in compiling the stated report are not detailed in the law.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✔	Section 38 of Law No. 124/2007 <www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html> requires the government to send to parliament a written annual report on its security intelligence policy and achievements in the past year — with a document on cyber defence and security attached. The tabling of such a report in parliament allows it to be publicly accessible.

COUNTRY: ITALY

	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)?	✖	There is no legislation or policy in place in Italy 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 Italy that requires mandatory reporting of cybersecurity incidents.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The National Strategic Framework for Cyberspace Security <sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf> provides an appropriate definition for "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?	✔	The National Strategic Framework for Cyberspace Security 2014 <www.sicurezzanazionale.gov.it/sisr.nsf/english/italian-national-cyber-strategy.html> contains a clear commitment to adopt international standards. It states that Italy will update security standards to conform to international requirements.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT-PA <www.agid.gov.it/infrastrutture-sicurezza/cert-pa> was established in 2014, as an expansion of the tasks performed by the superseded CERT-SPC. It is responsible for cybersecurity warning systems and the coordination of incident response measures for Italian government institutions.
2.	What year was the computer emergency response team (CERT) established?	2014	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The Cybersecurity Unit is a body established by the Decree of the Council of Ministers 24 January 2013 in order to support the Prime Minister in all activities concerning crisis response management, including developing and promoting necessary procedures for inter-ministerial coordination, dissemination of cyber alerts, and information sharing with public and private stakeholders. The Political Strategic Committee (CoPS) is a permanent body tasked with the political and strategic guidance of crises. It is chaired by the Prime Minister and composed of ministers from relevant ministries. The Inter-ministerial Unit for Situation and Planning (NISP) is a monitoring and crisis-prevention body, which supports CoPS in its duties.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT-PA <www.agid.gov.it/infrastrutture-sicurezza/cert-pa> is tasked with the management of incident reporting for cybersecurity incidents occurring within its government-based constituency.
5.	Are national cybersecurity exercises conducted?	✔	Italy conducted the cybersecurity exercise Cyber Italy in 2011 and 2012. Italy also participated in multi-national cybersecurity exercises organised by NATO.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	The Cybersecurity Unit, which acts under the instruction of the Prime Minister, is responsible for activating the non-permanent Inter-ministerial Situation and Planning Unit (Cyber Crisis Unit) in the event of a cybersecurity incident that is considered relevant to national security, or is of such magnitude as to require inter-ministerial coordination.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	◑	CERT-PA <www.agid.gov.it/infrastrutture-sicurezza/cert-pa> is required to facilitate public-private information sharing to aid information exchanges and the coordination of cybersecurity incident prevention measures.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	◑	While there is no industry-led dedicated cybersecurity platform in Italy, the Italian Association of Critical Infrastructures' Experts (AIIC) <www.infrastrutturecritiche.it/aiic-en> is a non-profit association composed of academic representatives, network providers and entities engaged with critical infrastructure. AIIC works to provide an inter-disciplinary approach to developing critical infrastructure strategies, methodologies and technologies. ANITEC <www.associazioneanitec.it>, a representative body for information technology companies in Italy, engages with cybersecurity in the course of its operations.

COUNTRY: ITALY

	QUESTION	RESPONSE	EXPLANATORY TEXT
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	◑	The National Strategic Framework for Cyberspace Security <sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf> describes public-private partnerships as playing a central role in the future direction of cybersecurity in Italy. It highlights the intention of the Italian government to work closely with the private sector by sharing information and collaborating in the area of crisis management planning.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Italy 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 National Strategic Framework for Cyberspace Security 2014 <sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf> includes a comprehensive commitment to cybersecurity education, including an "Operational Guideline on Training and Education" and a nine-point action plan.