COUNTRY: **AUSTRIA**

The Austrian Cyber Security Strategy was adopted in 2013. It is part of a broader ICT security initiative of the Austrian government, as set out in the National ICT Security Strategy 2012. The Strategy is an extensive plan that maps targeted cybersecurity objectives into organised fields of action.

Austria has an established computer emergency response team, CERT.at, with a broad and well-defined scope. There are also several public-private partnerships related to cybersecurity operating in the country, such as the Centre for Secure Information Technology Austria (A-SIT) and Kuratorium Sicheres Österreich.

The Austrian Trust Circles provide formal structures for sector-specific information exchanges related to the critical information infrastructure of various sectors. These platforms are tasked with developing sector-specific risk management plans. The Austrian Trust Circles are an initiative of CERT.at and the Austrian Federal Chancellery.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The Austrian Cyber Security Strategy <www.bka.gv.at/DocView.axd?CobId=50999> was adopted in 2013. It is part of a broader ICT security initiative of the Austrian government, as set out in the National ICT Security Strategy 2012. <www.oesterreich.gv.at/DocView.axd?CobId=48411> The Austrian Cyber Security Strategy is an extensive plan that maps targeted cybersecurity objectives into organised fields of action.
2.	What year was the national cybersecurity strategy adopted?	2013	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The Austrian Programme for Critical Infrastructure Protection Masterplan <www.kiras.at/uploads/media/MRV_APCIP_Beilage_Masterplan_FINAL.pdf> was adopted in 2008. Measures concerning the protection of critical infrastructure are also addressed in the National ICT Security Strategy of Austria 2012 <www.oesterreich.gv.at/DocView.axd?CobId=48411> and the Austrian Security Strategy 2013. <www.bka.gv.at/DocView.axd?CobId=52251>
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	As of August 2014, there is no legislation or other formal requirement for the development of written information security plans. The Austrian Cyber Security Strategy <www.bka.gv.at/DocView.axd?CobId=50999> recommends a review of legislation and policy, but this review is not yet complete.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	Information gathered by government in an official capacity is assigned a classification level in accordance with the classification system outlined in the Information Security Act 2002. <www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20001740/InfoSiG%2c%20Fassung%20vom%2017.06.2014.pdf> The classification system itself is four-tiered, and is based on 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 Information Security Ordinance 2003 <www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR30003326/NOR30003326.pdf> maps security practices to assigned classification levels. These levels are set out in the Information Security Act 2002 <www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20001740/InfoSiG%2c%20Fassung%20vom%2017.06.2014.pdf> 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?	✔	The Information Security Ordinance 2003 <www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR30003326/NOR30003326.pdf> requires the information security officer appointed to each ministry to perform a yearly review of the information security arrangements in their ministry. There is not a specific focus on cybersecurity.

COUNTRY: AUSTRIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	◑	Section 5 of Austria's Cyber Security Strategy <http://www.bmi.gv.at/cms/BMI_Service/cycer_security/130415_strategie_cybersicherheit_en_web.pdf> calls for the establishment of a platform that would periodically prepare an incident-related cybersecurity outlook — however, as of August 2014, no such report has been published. In addition, the Information Security Ordinance 2003 <www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR30003326/NOR30003326.pdf> requires the information security officer appointed to each ministry to perform a yearly review of the information security arrangements in their ministry, however they relate specifically to level of compliance with regard to federal information security laws and regulation, and are not an assessment of the cybersecurity capacity level of the ministry. Furthermore, there is no requirement for these reports to be made publicly available.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	It does not appear to be mandatory for each agency to appoint a CIO. However, an Office of the Chief Cybersecurity Officer has been recommended for the whole Austrian Government as a "central contact for public cyber security matters" (National ICT Security Strategy of Austria 2012. <www.oesterreich.gv.at/DocView.axd?CobId=48411>)
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	As of August 2014 there is no mandatory requirement for reporting cybersecurity incidents. Cooperation and communication is expected between all parties, but there is no formal legislation or other requirement to report incidents. The Austrian Cyber Security Strategy <www.bka.gv.at/DocView.axd?CobId=50999> recommends a review of legislation and policy, but this review is not yet complete.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	A definition for "critical infrastructure", as it relates to "critical infrastructure protection", exists in Annex 3 of Austria's Cyber Security Strategy. <www.bmi.gv.at/cms/BMI_Service/cycer_security/130415_strategie_cybersicherheit_en_web.pdf>
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	The Austrian Cyber Security Strategy 2013 <www.bka.gv.at/DocView.axd?CobId=50999> discusses standards briefly, and defers to the broader National ICT Security Strategy 2012 <www.oesterreich.gv.at/DocView.axd?CobId=48411> for more details on structures for standards, certification and quality assessment, which states: "Austria plans to establish a certification body for cybersecurity products and cybersecurity assessors. A centralised body will be established which will be responsible for coordinating the publication of quality standards for cybersecurity in Austria and of minimum requirements for conducting reviews of cyber security quality standards." In practice this approach will likely be based on an extension of the Austrian Information Security Manual. The strategy notes that the manual "complies with international requirements, its structure and content facilitate the implementation of the ISO/IEC 27000 series of standards", and "the internationally recognised manual makes an important contribution to ensuring a minimum level of protection, and is updated on a regular basis".
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT.at <www.cert.at> was established in 2008. It is responsible for coordinating security and incident response measures on a national level. GovCERT Austria <www.govcert.at> has jurisdiction over government institutions and critical information infrastructure. It is supported by CERT.at.
2.	What year was the computer emergency response team (CERT) established?	2008	
3.	Is there a national competent authority for network and information security (NIS)?	◑	Austria's Cyber Security Strategy <www.bka.gv.at/DocView.axd?CobId=50999> calls for the establishment of the Cyber Crisis Management, a body consisting of state representatives and representatives of entities associated with critical infrastructure. This body is responsible for internal and external cybersecurity, and is involved in the preparation of crisis management and continuity plans.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT.at <www.cert.at> is tasked with collecting information about cybersecurity incidents. They engage proactively by monitoring their constituency for cybersecurity incidents, as well as having in place a reporting structure to log cybersecurity incidents.

COUNTRY: AUSTRIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
5.	Are national cybersecurity exercises conducted?	✔	Austria carried out the cybersecurity exercise Cyber Planspiel <www.onlinesicherheit.gv.at/nationale_sicherheitsinitiativen/it_notfall_und_krisenuebungen/71384.html> in 2012. Austria also participated as a non-member country in a multi-national cybersecurity exercise organised by NATO in 2013. Austria's Cyber Security Strategy <www.bka.gv.at/DocView.axd?CobId=50999> states that regular cyber exercises will be held to test cyber crisis and continuity plans.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	Austria's Cyber Security Strategy <www.bka.gv.at/DocView.axd?CobId=50999> requires the Federal Ministry of the Interior (with assistance from the Federal Ministry of Defence and Sports) to coordinate tasks performed in relation to incident management in the framework of the Operational Coordination Structure. These coordination tasks will be transferred to the Federal Ministry of Defence and Sports in the event of a cyber defence incident.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership (PPP) for cybersecurity?	✔	Austria has many established public-private partnership initiatives that concern cybersecurity. The Centre for Secure Information Technology Austria (A-SIT) <www.a-sit.at> and Kuratorium Sicheres Österreich <www.kuratorium-sicheres-oesterreich.at> are recognised in Austria's Cyber Security Strategy <www.bka.gv.at/DocView.axd?CobId=50999> for their role in this regard.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✔	SBA Research <www.sba-research.org> is an information security research centre funded by partners from both the academic and business sectors. Cyber Security Austria <www.cybersecurityaustria.at> is an independent not-for-profit association that runs industry-targeted educational programs and releases publications with the objective of strengthening cybersecurity in Austria.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	✔	The Austrian Cyber Security Strategy <www.bka.gv.at/DocView.axd?CobId=50999> requires the establishment of the Austrian Cyber Security Platform — a public-private partnership that will facilitate a permanent on-going dialogue between all cybersecurity representatives from government, the private sector, and academia. It will work in parallel to existing public-private partnerships. As of August 2014, there has been no significant progress towards its establishment.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✔	The Austrian Trust Circles <www.austriantrustcircle.at> provide a formal framework for the exchange of information related to the critical information infrastructure of various sectors. They are recognised in Section 5 of the Austrian Cyber Security Strategy <www.bka.gv.at/DocView.axd?CobId=50999> as "sector-specific information platforms" and are tasked with developing sector-specific risk management plans. The Austrian Trust Circles are an initiative of CERT.at and the Austrian Federal Chancellery.
2.	Have sector-specific security priorities been defined?	✖	Austria carried out the cybersecurity exercise "Cyber Planspiel" <https://www.onlinesicherheit.gv.at/nationale_sicherheitsinitiativen/it_notfall_und_krisenuebungen/71384.html> in 2012. Austria also participated as a non-member country in a multi-national cybersecurity exercise organised by NATO in 2013. Austria's Cyber Security Strategy <www.bka.gv.at/DocView.axd?CobId=50999> states that regular cyber exercises should be held to test cyber crisis and continuity plans.
3.	Have any sector-specific cybersecurity risk assessments been conducted?	✖	Sector-specific risk management plans have been proposed, but none have yet been completed.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	Austria's Cyber Security Strategy <www.bka.gv.at/DocView.axd?CobId=50999> calls for the establishment of the Cyber Crisis Management, a body consisting of state representatives and representatives of entities associated with critical infrastructure. This body is responsible for internal and external cybersecurity, and is involved in the preparation of crisis management and continuity plans.