BSA The Software Alliance

COUNTRY: **UNITED KINGDOM**

The United Kingdom has a comprehensive cybersecurity strategy, which was released in 2011. It is complemented by a strong cybersecurity legal framework and two computer emergency response teams (CERTs). CERT-UK mainly supports operators of critical infrastructure while GovCertUK supports government agencies. Other relevant bodies include the National Security Council and the Office of Cyber Security and Information Assurance.

The United Kingdom also has a well-developed system of public-private partnerships in which the private sector actively participates. This collaborative approach also is strongly supported by its cybersecurity strategy. The Centre for the Protection of National Infrastructure (CPNI), for example, organises sector-specific information exchanges, covering 14 sectors.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World <www.gov.uk/government/publications/cyber-security-strategy> was adopted in 2011. The strategy includes a strong statement of principles and an assessment of cybersecurity threats faced by the UK. The implementation plan contained within the strategy is based around key targeted objectives.
2.	What year was the national cybersecurity strategy adopted?	2011	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The Centre for the Protection of National Infrastructure (CPNI) <cpni.gov.uk> is tasked with the protection of the United Kingdom's critical infrastructure. The central document of the CPNI is the Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards <www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf>, which was adopted in 2010.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	◑	There is no legislation or policy in place in the United Kingdom that requires the establishment of a written information security plan. The Communications Electronic Security Group (CESG) <cesg.gov.uk>, the information security arm of the UK's Government Communications Headquarters (GCHQ) intelligence agency, has published guidelines for public organisations related to information security.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The Government Security Classifications Policy <www.gov.uk/government/publications/government-security-classifications>, which came into force in 2014, details a three-tiered system of classification for information that is required by domestic laws, including the Official Secrets Act 1989 <www.legislation.gov.uk/ukpga/1989/6>, to be classified. The three classification levels are assigned according to the sensitivity of the information and the risk level involved in disclosing the information.
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	The Government Security Classifications Policy <https://www.gov.uk/government/publications/government-security-classifications> details a three-tiered classification system. The classification levels are assigned with consideration of the level risk involved in disclosing the information. The policy then maps specific security requirements according to classification level.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	There is no legislation or policy in place in the United Kingdom that requires an annual cybersecurity audit. The UK Cyber Security Strategy <www.gov.uk/government/publications/cyber-security-strategy> acknowledges the ease and benefits of continuous monitoring of data with relation to digitisation, however, a specific auditing process and the frequency with which it should be carried out is not detailed.
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 the United Kingdom that requires a public report on cybersecurity capacity for the government. The UK Cyber Security Strategy <www.gov.uk/government/publications/cyber-security-strategy> includes an assessment of the UK's cybersecurity capacity as of 2011.

COUNTRY: UNITED KINGDOM

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 the United Kingdom 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 the United Kingdom that requires mandatory reporting of cybersecurity incidents, however, voluntary guidelines issued by both CERT-UK <www.cert.gov.uk> and GovCertUK <www.govcertuk.gov.uk> recommend the reporting of all incidents.
11. Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The Centre for the Protection of National Infrastructure (CPNI) <cpni.gov.uk> provides an appropriate definition for "critical infrastructure protection" in its policy documents — including the Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. <www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf>
12. Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	◑	The UK generally recognises international certification schemes, although some additional voluntary guidance on security standards is provided by the UK's National Technical Authority on Information Assurance. In June 2014 the government issued a new cybersecurity standard known as the Cyber Essentials Scheme. <www.gov.uk/government/publications/cyber-essentials-scheme-overview> From 1 October 2014, the UK government will require all suppliers bidding for certain sensitive and personal information handling contracts to be certified against the Cyber Essentials Scheme. The scheme includes some overlaps with, but also some differences to, international standards.
OPERATIONAL ENTITIES		
1. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT-UK <www.cert.gov.uk> was established in 2014. It is responsible for promoting cyber security situational awareness and for national cybersecurity incident management including providing support for entities engaged with national critical infrastructure. CERT-UK works closely with GovCertUK <www.govcertuk.gov.uk>, which is responsible for coordinating security and incident response measures for UK 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 National Security Council <www.gov.uk/government/organisations/national-security/groups/national-security-council> and the Office of Cyber Security and Information Assurance <www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance> act in conjunction to cover network and information security for the United Kingdom. The CESG <cesg.gov.uk> is the information security arm of the UK's GCHQ intelligence agency. It advises public organisations in helping them to maintain network integrity and strengthen cybersecurity.
4. Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT-UK <www.cert.gov.uk> is tasked with incident reporting and collecting information about cybersecurity incidents. It provides an online reporting structure to log cybersecurity incidents.
5. Are national cybersecurity exercises conducted?	✔	The United Kingdom conducted the cybersecurity exercise White Noise in 2009. The UK 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?	✔	CERT-UK <www.cert.gov.uk> acts according to the Cyber Security National Incident Management policy, which includes reporting and notification requirements.
PUBLIC-PRIVATE PARTNERSHIPS		
1. Is there a defined public-private partnership for cybersecurity?	✔	Cyber-Security Information Sharing Partnership (CISP) <cisp.org.uk> is a joint initiative of the United Kingdom government and industry to share information and collaborate on the issue of cyber threats. It follows the objectives and goals set out in the UK Cyber Security Strategy. <www.gov.uk/government/publications/cyber-security-strategy>

COUNTRY: UNITED KINGDOM

	QUESTION	RESPONSE	EXPLANATORY TEXT
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✓	There are multiple industry-organised and industry-engaged associations in the United Kingdom that provide a platform for cooperation and collaboration on cybersecurity, including: • The Information Technology Telecommunications and Electronics Association (techUK) <www.techuk.org>, a representative organisation of information technology and communication companies in the UK, hosts both a dedicated cybersecurity group as well as a general security and resilience group. • The Information Assurance Advisory Council (IAAC) <www.iaac.org.uk> is a not-for-profit research organisation comprised of representatives from the public, private, and academic sectors in order to promote a cross-sector approach to information assurance. • The UK Council for Electronic Business (UKCeB) <www.ukceb.oeg> is a representative organisation whose members come from the information technology and defence sectors. UKCeB sponsors a security and information assurance working group.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	–	The United Kingdom already has a public-private partnership dedicated to cybersecurity in place.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✓	The Centre for the Protection of National Infrastructure (CPNI) <www.cpni.gov.uk> organises public-private information exchanges around the fourteen different sectors involved with national infrastructure. The Network Security Information Exchange (NSIE) is the information exchange that engages directly with the cybersecurity sector.
2.	Have sector-specific security priorities been defined?	◑	The UK Cyber Security Strategy 2011 <www.gov.uk/government/publications/cyber-security-strategy> provides a sector based approach, particularly in addressing training and knowledge-sharing in sectors where small and medium-sized businesses operate. Security priorities have not been defined by sector.
3.	Have any sector-specific cybersecurity risk assessments been conducted?	✗	While the UK Cyber Security Strategy 2011 <www.gov.uk/government/publications/cyber-security-strategy> advocates both a sector-oriented and risk-based approach, sector-specific cybersecurity risk assessments have not yet been conducted.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✓	The UK Cyber Security Strategy 2011 <www.gov.uk/government/publications/cyber-security-strategy> includes a plan to "look at the best ways to improve cybersecurity education at all levels so that people are better equipped to use cyberspace safely". There is also a commitment to "building a culture that understands the risks and enables people to use cyberspace and improving cybersecurity skills at all levels". In practice the UK has developed some of the most advanced cybersecurity education initiatives in the region, including the Get Safe Online program. <www.getsafeonline.org>