METHODOLOGY AND CRITERIA
FOR THE CYBERSECURITY REPORTS

The cybersecurity maturity has been assessed against 25 criteria across five themes. Each of the criteria are given a "Yes," "No," "Partial," or "Not Applicable" status.

	THEME AND CRITERIA	✔ YES	✖ NO	◑ PARTIAL	NOT APPLICABLE (–)
	LEGAL FOUNDATIONS				
1.	Is there a national cybersecurity strategy in place?	YES: There is an adopted and publicly available cybersecurity strategy.	NO: There is no adopted and publicly available cybersecurity strategy. There may or may not be an adopted strategy or policy that addresses cyber or information security in part.	PARTIAL: Partial has not be used as an option for this criteria.	
2.	What year was the national cybersecurity strategy adopted?	Year (4 digits)			
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	YES: There is an adopted and publicly available critical infrastructure protection strategy in place.	NO: There is no adopted critical infrastructure protection strategy in place, and there is no legislation or policy that meaningfully addresses critical infrastructure protection in part.	PARTIAL: There is no adopted critical infrastructure protection strategy in place, however there is legislation or policy in place that meaningfully addresses critical infrastructure protection in part.	
4.	Is there legislation/policy that requires the establishment of a written information security plan?	YES: There is legislation or policy that has been adopted by the national government which requires the establishment of a written information plan.	NO: There is no legislation or policy that has been adopted by the national government which requires the establishment of a written information plan, nor has there been a written information plan otherwise adopted.	PARTIAL: There is no legislation or policy that has been adopted by the national government which requires the establishment of a written information plan. However, a publicly available written information plan has been adopted.	
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	YES: There is legislation or policy that has been adopted by the national government, or there is a clear and publicly available standard used by the national government, which requires that data be classified according to a clearly defined system.	NO: There is no legislation or policy adopted by the national government which requires that data be classified according to a clearly defined system, nor does legislation or policy exist that has general information classification practices, or targeted data classification practices that are only applied to a specific type of data.	PARTIAL: There is no legislation or policy adopted by the national government which requires that data be classified according to a clearly defined system. However, legislation or policy does exist that has general information classification practices, or has targeted data classification practices that are only applied to a specific type of data.	

METHODOLOGY AND CRITERIA FOR THE CYBERSECURITY REPORTS

	THEME AND CRITERIA	✔ YES	✖ NO	◑ PARTIAL	NOT APPLICABLE (–)
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	YES: There is legislation or policy that has been adopted by the national government that prescribes specific security practices for sensitive information and maps these security practices to risk levels.	NO: There is no legislation or policy that has been adopted by the national government that prescribes specific security practices for sensitive information and maps these security practices to risk levels.	PARTIAL: There is legislation or policy that has been adopted by the national government that prescribes specific security practices for sensitive information, but it does not map these security practices to risk levels.	
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	YES: There is legislation or policy that has been adopted by the national government that specifies a cybersecurity or information security audit procedure, and requires it be conducted on at least a yearly basis.	NO: There is no legislation or policy that has been adopted by the national government that specifies a cybersecurity or information security audit procedure. There may or may not be related reporting or surveying procedures.	PARTIAL: There is legislation or policy that has been adopted by the national government that specifies a cybersecurity or information security audit procedure, but does not require it be conducted on at least a yearly basis.	
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	YES: There is legislation or policy that has been adopted by the national government that requires a public report on cybersecurity capacity for the government.	NO: There is no legislation or policy that has been adopted by the national government that requires a public report on cybersecurity capacity for the government; nor is there legislation or policy that has been adopted by the national government that, in prescribing the responsibilities of an agency or individual, addresses a reporting or monitoring procedure for cybersecurity or information security that would address cybersecurity capacity.	PARTIAL: There is legislation or policy that has been adopted by the national government that, in prescribing the responsibilities of an agency or individual, describes a reporting or monitoring procedure for cybersecurity or information security that would address cybersecurity capacity to a limited extent, but does not require the establishment of a dedicated cybersecurity capacity report for the government.	
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	YES: There is legislation or policy that has been adopted by the national government that requires each agency to have a chief information officer or chief security officer.	NO: There is no legislation or policy that has been adopted by the national government that requires each agency to have a chief information officer or chief security officer. There may or may not be chief information officers or chief security officers otherwise appointed by the government.	PARTIAL: Partial has not be used as an option for this question.	
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	YES: There is legislation or policy that has been adopted by the national government that requires the mandatory reporting of cybersecurity incidents to the relevant authority.	NO: There is no legislation or policy that has been adopted by the national government that requires the mandatory reporting of cybersecurity incidents to the relevant authority.	PARTIAL: There is legislation or policy that has been adopted by the national government that requires the mandatory reporting of cybersecurity incidents in certain circumstances, or else requires particular agencies, entities, or individuals to participate in routine incident analysis processes.	

METHODOLOGY AND CRITERIA FOR THE CYBERSECURITY REPORTS

	THEME AND CRITERIA	✔ YES	✖ NO	◑ PARTIAL	NOT APPLICABLE (–)
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	YES: There is legislation or policy that has been adopted by the national government that includes an appropriate definition for "critical infrastructure protection" or else includes an appropriate definition for "critical infrastructure" in the context of critical infrastructure protection.	NO: There is no legislation or policy that has been adopted by the national government that includes an appropriate definition for "critical infrastructure protection," nor does legislation or policy include an appropriate definition for "critical infrastructure" in the context of critical infrastructure protection.	PARTIAL: Partial has not been used as an option for this criteria.	
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	YES: There is a formal commitment to use international standards and recognise international accreditation and certification schemes.	NO: Local standards or accreditation and certification schemes are in place instead of (or in addition to) international schemes.		Not applicable (–): No standards, certification or accreditation requirements are currently in place.
	OPERATIONAL ENTITIES				
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	YES: There is a functioning computer emergency response team which is recognised by the national government as the national computer emergency response team, or else there is a functioning computer emergency response team which represents, or has represented, their country in international computer emergency response team associations and at related events.	NO: There is no functioning computer emergency response team which is recognised by the national government as the national computer emergency response team, nor is there a functioning computer emergency response team which represents, or has represented, their country in international computer emergency response team associations and at related events.	PARTIAL: There is a computer emergency response team that satisfies the criteria for "Yes" – however, the functioning status or representative authority is unclear.	
2.	What year was the computer emergency response team (CERT) established?	Year (4 digits)			
3.	Is there a national competent authority for network and information security (NIS)?	YES: There is a government entity, or set of entities, responsible for the management and implementation of network and information security practices.	NO: There is no government entity, nor a set of entities, responsible for the management and implementation of network and information security practices.	PARTIAL: There is a government entity, or set of entities, with limited responsibility for the management and implementation of network and information security practices for the country in question; or else there is a government entity, or set of entities with responsibility for network and information security practices within a limited jurisdiction; or else in legislation or policy adopted by the national government there is a clear proposal to develop such an entity as described in the criterion for "Yes".	

METHODOLOGY AND CRITERIA FOR THE CYBERSECURITY REPORTS

	THEME AND CRITERIA	✔ YES	✖ NO	◑ PARTIAL	NOT APPLICABLE (–)
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	YES: There is active platform through which individuals or agencies can report cybersecurity incidents to the relevant government body. This platform may or may not restrict reporting to registered parties.	NO: There is no platform through which individuals or agencies can report cybersecurity incidents to the relevant government body.	PARTIAL: Partial has not been used as an option for this question.	
5.	Are national cybersecurity exercises conducted?	YES: The national government has conducted a dedicated cybersecurity exercise. The country in question may or may not have participated in a multinational exercise.	NO: The national government has not conducted a dedicated cybersecurity exercise, nor has the country in question participated in a multinational cybersecurity exercise.	PARTIAL: The national government has not conducted a dedicated cybersecurity exercise, but the country in question has participated in a multinational cybersecurity exercise.	
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	YES: A clear hierarchy and management structure to respond to cybersecurity incidents, which includes relevant authorities, agencies and stakeholders, has been published in legislation, policy or similar.	NO: No clear hierarchy and management structure to respond to cybersecurity incidents, which includes relevant authorities, agencies and stakeholders, has been published in legislation, policy or similar. Nor do particular relevant agencies have certain reporting requirements in the case of a cybersecurity incident	PARTIAL: No clear hierarchy and management structure to respond to cybersecurity incidents, which includes relevant authorities, agencies and stakeholders, has been published in legislation, policy or similar. However, particular relevant agencies have certain reporting requirements in the case of a cybersecurity incident.	
	PUBLIC-PRIVATE PARTNERSHIPS				
1.	Is there a defined public-private partnership (PPP) for cybersecurity?	YES: There is a clear, publicly acknowledged, public-private partnership that is dedicated to cybersecurity; or else there is a clear, publicly acknowledged, public-private partnership that covers cybersecurity as part of a wider network and information security focus.	NO: There is no clear, publicly acknowledged, public-private partnership that is dedicated to cybersecurity; nor is there a clear, publicly acknowledged, public-private partnership that covers cybersecurity as part of a wider network and information security focus; nor are there relevant government entities who liaise with the private sector as part of their duties.	PARTIAL: There is no clear, publicly acknowledged, public-private partnership that is dedicated to cybersecurity; nor is there a clear, publicly acknowledged, public-private partnership that covers cybersecurity as part of a wider network and information security focus. However, there are relevant government entities that liaise with the private sector as part of their duties.	
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	YES: There is an industry-led entity or association that is dedicated to cybersecurity.	NO: There is no industry-led entity or association that is dedicated to cybersecurity, nor is there an industry-led body that represents the wider information and communication technology industry or information security industry.	PARTIAL: There is no industry-led entity or association that is dedicated to cybersecurity, however there is an industry-led body that represents the wider information and communication technology industry or information security industry.	

METHODOLOGY AND CRITERIA FOR THE CYBERSECURITY REPORTS

	THEME AND CRITERIA	✔ YES	✖ NO	◑ PARTIAL	NOT APPLICABLE (–)
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	YES: There is no cybersecurity dedicated public-private partnership operating, however there is a clear commitment, in public available legislation or policy, to establish a cybersecurity dedicated public-private partnership.	NO: There is no cybersecurity dedicated public-private partnership operating, and there is no clear commitment, in public available legislation or policy, to establish a cybersecurity dedicated public-private partnership.	PARTIAL: There is no cybersecurity dedicated public-private partnership operating, however there is a commitment, in public available legislation or policy, for government agencies to establish closer links with the private sector.	Not Applicable (–): There is already a cybersecurity dedicated public-private partnership operating.
	SECTOR-SPECIFIC CYBERSECURITY PLANS				
1.	Is there a joint public-private sector plan that addresses cybersecurity?	YES: There is policy or legislation, adopted by the national government, which includes a plan that provides a sector-based approach to cybersecurity or information security; or else there is legislation or policy, adopted by the national government, which includes a plan that provides a sector-based approach to policy planning that includes a platform for cybersecurity or information security.	NO: There is no policy or legislation, adopted by the national government, which includes a plan that provides a sector-based approach to cybersecurity or information security and there is no legislation or policy, adopted by the national government, which includes a plan that provides a sector-based approach to policy planning that includes a platform for cybersecurity or information security.	PARTIAL: There is no policy or legislation, adopted by the national government, which includes a plan that provides a sector-based approach to cybersecurity or information security and there is no legislation or policy, adopted by the national government, which includes a plan that provides a sector-based approach to policy planning that includes a platform for cybersecurity or information security. However, there is policy or legislation that provides a sector-based approach to cybersecurity or information security for one particular sector, or a limited number of sectors.	
2.	Have sector-specific security priorities been defined?	YES: There is policy, legislation, or other relevant government publications that defines security priorities for specific sectors.	NO: There is no policy, legislation, or other relevant government publications that defines security priorities for specific sectors.	PARTIAL: There is policy, legislation, or other relevant government publications that defines security priorities for specific sectors. However, as part of a sector based approach, the government has defined the security priorities for those participating in public private sector platforms.	
3.	Have any sector-specific cybersecurity risk assessments been conducted?	YES: Any number of sector-specific cybersecurity risk assessments have been conducted.	NO: No sector-specific cybersecurity risk assessments have been conducted.		
	EDUCATION				
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	YES: An education strategy has been implemented or a commitment to implementation is available.	NO: There is no education strategy or commitment in place.	PARTIAL: Some education initiatives are in place, but a formal strategy is missing. Or education is in place, but is not targeting young people.	

	THEME AND CRITERIA	✔ YES	✖ NO	◑ PARTIAL	NOT APPLICABLE (–)
	ADDITIONAL CYBERLAW INDICATORS				
1.	Are cybersecurity services able to operate free from laws that discriminate based on the nationality of the vendor?	YES: There are no local requirements (especially on procurement rules) relating to the nationality of the vendor.	NO: Local requirements include references to the nationality of vendors.	PARTIAL: Some limited requirements may be in place on specific sectors that relate to the nationality of the vendor, but they are likely to only have a limited impact on cybersecurity services.	
2.	Are cybersecurity services able to operate free from laws or policies that mandate the use of specific technologies?	YES: There are no mandatory technology requirements in place.	NO: Mandatory technology requirements are in place usually in relation to the mandatory use of open source technologies).		
3.	Are cybersecurity services able to operate free from additional local testing requirements that go beyond international testing requirements?	YES: International testing is accepted.	NO: Local testing is required.		
4.	Are cybersecurity services able to operate free from laws or policies that mandate the submission of source code or other proprietary information?	YES: There are no requirements in law or policy (or procurement rules) for the submission of source code.	NO: Source code needs to be submitted in some circumstances.		
5.	Are cybersecurity services able to operate free from laws or policies that require service providers to locate their servers inside the subject country?	YES: There are no legal or policy requirements relating to the location of servers.	NO: According to local law and policy, servers must be located within the country in order to provide services there.	PARTIAL: There may be some specific sectors or circumstances where the location of the server has an impact on the provision of services.	
6.	Are cybersecurity services able to operate free from unnecessary restrictions on cross border data flows (such as registration requirements)?	YES: There are no unnecessary or unreasonable restrictions in place on the transfer of data. Examples of unnecessary restrictions include registration requirements, blanket prohibitions and requirements for prior regulatory approval.	NO: Some general rules can be in place to ensure an appropriate level of protection for data that is being transferred abroad, however these must not be unnecessary or unreasonable.	PARTIAL: Some restrictions may apply in specific sectors, but their overall impact on cybersecurity is limited.	