COUNTRY: **INDONESIA**

Legal Foundations: Indonesia is in the early stages of developing a national cybersecurity strategy. The legal framework for cybersecurity in Indonesia is weak. There is no clear classified security law or policy, and security practices are spread across different legislation. There are no specific cybersecurity provisions in place.

Operational Entities: ID.SIRTII/CC, the national CERT, seems to be in the early phases of operation. ID.CERT is a non-government CERT, but has been operating for longer.

Public-Private Partnerships: There is no dedicated cybersecurity public private partnership in Indonesia, so the CERT acts as the main liaison body for the private sector. Industry representative associations exist, but none are dedicated to cybersecurity in particular.

Sector-Specific Cybersecurity Plans: Indonesia lacks any joint public-private sector plan to address cybersecurity.

Education: Indonesia lacks a cybersecurity education strategy.

Additional Cyberlaw Indicators: Indonesia subjects cybersecurity service providers to a range of burdensome laws and policies, including discriminatory procurement preferences, local testing requirements, and limits on data flows.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✖	Indonesia is in the early stages of developing a national cybersecurity strategy.
2.	What year was the national cybersecurity strategy adopted?	–	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✖	There is no critical infrastructure protection plan in place in Indonesia.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	◑	There is no legislation or policy in place in Indonesia that requires the establishment of a written information security plan. As of May 2015, information security in Indonesia is addressed primarily by the Telecommunications Act 1999 and the Information and Electronic Transaction Act 2008. Certain requirements are reflected in the adoption by Indonesia of standard ISO 27001:2009 on the Information Security Management System.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	Information in Indonesia is classified against a four-tiered classification system, however the criteria for the classification systems is not publicly available.
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	◑	Certain security practices are detailed in the Telecommunications Act 1999 and the Information and Electronic Transaction Act 2008 — however, these are general practices and are not mapped to risk levels.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	◑	There is no legislation or policy in place in Indonesia that requires (at least) an annual cybersecurity audit. The Information Security Coordination Team, a group working under the Ministry of Communication and Information Technology <www.kominfo.go.id>, is responsible for the development, implementation, and monitoring of information security procedures, however it is not required to conduct auditing processes according to a specific timeframe. ID.SIRTII <www.idsirtii.or.id>, the Indonesian national CERT, issues near-annual reports on the cyber incident data it collects, however these are not required by law.

COUNTRY: INDONESIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✖	There is no legislation/policy in place in Indonesia that requires a public report on cybersecurity capacity for the government. The Information Security Coordination Team and the Directorate of Information Security, both organized under the Ministry of Communication and Information Technology <www.kominfo.go.id>, are responsible for providing reporting on and evaluating the field of information technology. However they are not required by law to publish a public report on cybersecurity capacity.
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 Indonesia 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 Indonesia that requires mandatory reporting of cybersecurity incidents.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✖	There is no legislation or policy in place in Indonesia that includes 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?	✖	Procurement of ICT services in Indonesia is heavily restricted and subject to local registration certification. Indonesia applies local standards and is developing a local certification scheme for ICT services that fall within the scope of Regulation No. 82 of 2012 on the Operation of Electronic Systems and Transactions. This will include some cybersecurity services.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	ID.SIRTII/CC <www.idsirtii.or.id> was established in 2007. It is responsible for coordinating incident response procedures for networks utilized by organizations and users in Indonesia. ID.CERT <www.cert.or.id> is a non-government CERT that plays a significant role in coordinating incident response measures in Indonesia.
2.	What year was the computer emergency response team (CERT) established?	2007	
3.	Is there a national competent authority for network and information security (NIS)?	✔	There are three agencies in Indonesia that act in coordination to fulfill the duties of a national competent authority for network and information security: • Desk on Information Resilience and Cyber Security (DK2ICN), organized under the Coordinating Ministry for Political, Legal and Security Affairs; • The Information Security Coordination Team coordinates and develops policy and technical guidelines on the implementation of information security measures; • The Directorate of Information Security formulates norms, standards, and procedures in the field of information security; and • ID.SIRTII <www.idsirtii.or.id> is responsible for coordinating incident response procedures and provides training and advice to network stakeholders. The latter three agencies are organized under the Ministry of Communication and Information Technology. Also of significance is the National ICT Council (DeTIKNas), a government coordinating committee dedicated to promoting Indonesia's information and communications sector. DeTIKNas is chaired by the President of Indonesia and has a membership composed of relevant ministers and senior members of the public service.
4.	Is there an incident-reporting platform for collecting cybersecurity incident data?	✔	ID.SIRTII <www.idsirtii.or.id> is tasked with collecting information about cybersecurity incidents. It has an email-based reporting structure to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	✖	Indonesia has not conducted a national cybersecurity exercise.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	There is no clear incident management reporting structure for responding to cybersecurity incidents in place in Indonesia. The ID.SIRTII <www.idsirtii.or.id> is the agency responsible for incident management and it is located within the Ministry for Communications and Information Technology <www.kominfo.go.id>.

COUNTRY: INDONESIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership (PPP) for cybersecurity?	◑	While Indonesia does not have a defined public-private partnership for cybersecurity, ID.SIRTII <www.idsirtii.or.id>, in conjunction with its functions as Indonesia's national CERT, engages directly with private-sector and academic stakeholders in order to develop and implement information security practices.
2.	Is industry organized (i.e., business or industry cybersecurity councils)?	◑	There is no industry-led association in Indonesia that is dedicated to cybersecurity. There are industry bodies that are active in the wider field of information technology: • MASTEL <www.mastel.or.id> is a non-profit organization composed of companies and professionals from the information and communications technology sector; and • The Indonesian Internet Service Providers Association (APJII) <www.apjii.or.id> is a representative body for Indonesian internet service providers. Both MASTEL and APJII engage with cybersecurity issues on behalf of their members.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	✖	As of May 2015, there are no documented new public-private partnerships being planned in Indonesia.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	There is no joint public-private sector plan in Indonesia that addresses cybersecurity.
2.	Have sector-specific security priorities been defined?	✖	Sector-specific security priorities have not been publicly defined, nor has there been a proposal to define sector-specific security priorities in legislation or policy, as of May 2015.
3.	Have any sector cybersecurity risk assessments been conducted?	✖	Sector cybersecurity risk assessments have not been conducted in Indonesia.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✖	Indonesia does not have a cybersecurity education or awareness raising strategy in place.
	ADDITIONAL CYBERLAW INDICATORS		
1.	Are cybersecurity services able to operate free from laws that discriminate based on the nationality of the vendor?	✖	In 2012, Indonesia became an observer to the WTO plurilateral Agreement on Government Procurement, but they are not yet a full member. There are many instances where government procurement includes a preference for domestic suppliers. For example, Regulation No. 82 of 2012 on the Operation of Electronic Systems and Transactions imposes requirements for providers to establish data centers in Indonesia and hire Indonesian staff for some roles. Also, Presidential Regulation 54/2010 <www.setneg.go.id//index.php?option=com_perundangan&id=2593&task=detail&catid=6&Itemid=42&tahun=2010> requires procuring entities to maximize local content in procurement, use foreign components only when necessary, and designate foreign contractors as sub-contractors to local companies. Presidential Regulation 2/2009 <www.setneg.go.id//index.php?option=com_perundangan&id=2250&task=detail&catid=6&Itemid=42&tahun=2009> requires all state administrations to "optimize" the use of local services and give price preferences for domestic providers.
2.	Are cybersecurity services able to operate free from laws or policies that mandate the use of specific technologies?	✔	There are no mandatory technology requirements in place in Indonesia.
3.	Are cybersecurity services able to operate free from additional local testing requirements that go beyond international testing requirements?	✖	The Regulation No. 82 of 2012 on the Operation of Electronic Systems and Transactions <flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html> includes a complex system of certification and testing, based on three levels of certificates: Electronic Systems Capability Certificate, Electronic Systems Certificates and Reliability Certificates. There is some potential for testing for Reliability Certificates to be provided by international providers, but the majority of the rules envisage local testing. As of May 2015 many of the detailed requirements have not yet been published.

COUNTRY: INDONESIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
4.	Are cybersecurity services able to operate free from laws or policies that mandate the submission of source code or other proprietary information?	✖	Regulation No. 82 of 2012 on the Operation of Electronic Systems and Transactions <flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html> requires providers to register with a government agency and to provide source code (or to place source code in escrow) for certain types of applications in Indonesia.
5.	Are cybersecurity services able to operate free from laws or policies that require service providers to locate their servers inside the subject country?	✖	The Law on Information and Electronic Transactions 2008 includes some very broad requirements relating to the organization of data systems. A regulation under the Act (Regulation No. 82 of 2012 on the Operation of Electronic Systems and Transactions <flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html>) provides more detailed requirements. Article 17 (2) requires operators to place their data centers in Indonesia.
6.	Are cybersecurity services able to operate free from unnecessary restrictions on cross-border data flows (such as registration requirements)?	◑	There are no specific registration requirements or other unnecessary restrictions on cross-border data flows in Indonesia, apart from the local server requirements in Regulation No. 82 of 2012 on the Operation of Electronic Systems and Transactions <flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html> (discussed in the criteria above).