Global Cyber Security Capacity Centre

Cyber Security Capability Maturity Model (CMM) - Pilot

Global Cyber Security Capacity Centre

University of Oxford

12/15/2014

Table of Contents

Introduction

The goal of the Global Cyber Security Capacity Centre is to increase the scale and effectiveness of effective cyber security capacity building, both within the UK and internationally. The Centre will make this knowledge available to governments, communities and organisations to underpin increasing their cyber capacity in ways appropriate to ensuring a cyber space which can continue to grow and innovate in support of well-being, human rights and prosperity for all.

We currently consider cyber security capacity as being comprised of five dimensions:

1. devising cyber policy and strategy
2. encouraging responsible cyber culture within society
3. building cyber skills into the workforce and leadership
4. creating effective legal and regulatory frameworks
5. controlling risks through organization, standards and technology

Cyber Security Capability Maturity Model

In each dimension there are multiple factors which characterise what it means to possess cyber security capacity; countries, regions and organisations will have varying degrees of capacity in each factor and consequently across each and all dimensions. Indeed, we advocate that it is possible to identify a range of levels of capacity capability that might be attained. Our objective is to identify these levels in a cyber security capability maturity model (CMM) – whereby the lowest level would imply a non-existent or limited level of capacity, and the highest level both a strategic approach and an ability to optimise against environmental considerations (operational, threat, socio-technical and political).

We decided to apply the following definitions to the five levels of maturity in the Capability Maturity Model:

- Start-up: At this level either nothing exists, or it is very embryonic in nature. It could also include initial discussions about cyber capacity building, but no concrete actions have been taken. It also includes a lack of observed evidence in this particular indicator.
- Formative: Some features of the indicators have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined - or simply "new". However, evidence of this activity can be clearly evidenced.
- Established: The elements of the sub-factor are in place, and working. There is not, however, well-thought out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the *relative* investment in the various elements of the sub-factor. But the indicators is functional and defined.

- Strategic: Choices have been made about which parts of the indicator are important, and which are less important for the particular organization/nation. Of course, we would all like everything to be as important as everything else, but with finite resources, choices must be made. The strategic level reflects the fact that these choices have been made. They should have been made contingent on the nation/organization's particular circumstances.
- Dynamic: At the Dynamic level, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances: for example, the technology of the threat environment, global conflict, a significant change in one area of concern (e.g. Cybercrime or privacy). Dynamic organizations have developed methods for changing strategies in stride, in a "sense-and-respond" way. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this level.

Such a model allows an entity to self-assess its current cyber security capacity. In each case, understanding the requirements to achieve higher levels of capacity should directly indicate areas requiring further investment, and the data required to evidence such capacity levels. This means that the CMM could also be used to build business cases for investment and expected performance enhancements. Necessarily there are relationships that exist between the factors both within and between dimensions.

This work is part of a process. We invite you to feed into the enhancement of the CMM, so that it not only contains the most relevant and applicable material, but also reflects the international operational environment. Please contact Lara Pace (lara.pace@oxfordmartin.ox.ac.uk) if you have any questions on how best to engage with the Capacity Centre.

Dimension 1: Cyber Security Policy and Strategy

D1-1: National Cyber Security Strategy					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Strategy Development	Little or no evidence exists of a cyber security national strategy, although some cyber component may be the responsibility of one or more departments of government. This will have been developed without broad, cross-governmental consultation. Cyber security strategy development may acknowledge societal values, traditions, and legal principles but will not be the result of wide consultation with stakeholders. Advice may have been sought from international partners.	An outline national cyber security strategy has been articulated built on a foundation of government consultation. Some relevant departments have contributed. Processes for strategy formation and renewal have been initiated. Consultation processes will have been established for key stakeholder groups, including international partners.	A national cyber security strategy has been established. Agreement has been reached on the content of, and responsibility for a specific mandate to consult across public and private sectors and civic society. Consultation processes will have been followed and observations fed back to the identified strategy 'owners'. Data and historic trends are used to predict, identify and plan. An understanding of national cyber security risks and threats drives capacity building at a national level. Metrics and measurement processes are established.	Representation of the overarching national cyber strategy can be made with authority and confidence by multiple stakeholders across government. Wider stakeholders feel they understand how their interests are represented, and are confident of the processes by which they can influence strategy. Strategy review and renewal processes are confirmed. Regular scenario and real-time cyber exercises that provide a concurrent picture of national cyber resilience are conducted. Metrics and measurement processes are implemented and inform decision making. Cyber security strategic plans, aligned with national strategic plans, drive capacity building and investments in security.	Continual revision and refinement of cyber security strategy is conducted responsively to adapt to changing socio-political, threat and technology environments. Promotion of trust and confidence building measures (TCBMs) is undertaken to ensure the continued inclusion and contribution of all stakeholders including the private sector and international partners. Wide and continuous societal participation in cyber security issues.
Organisation	No overarching national cyber security programme can be discerned. Budgets, if	A coordinated cyber programme has been designed and disseminated.	The single cyber programme has a designated departmental owner or	Evidence of considered resource allocation across government departments	A singular national cyber security posture exists with the ability to reassign tasks

D1-1: National Cyber Security Strategy					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
	they exist, reside in disparate public offices rather than being governed by a central cyber programme co-ordination.	However, budgets may still be distributed with inter-departmental co-operation still necessary if the goals of the single programme are to be achieved.	coordinating body with a consolidated budget. The programme is now defined, with goals, milestones, and metrics to measure progress. Clear roles and responsibilities for cyber security functions within government have been agreed.	involved in cyber security risk assessment and management in accordance with the strategy.	and budgets dynamically according to changing risk assessment. Iterative application of metrics and resulting refinements to operations and strategy, across the breadth of government are involved in cyber security risk assessment and management. A national body is appointed to disseminate and receive feedback on the strategy from wider society.
Content	Various national strategies may exist with a reference to cyber security, but if so, the content is generic, not necessarily aligned with national goals, and does not provide actionable directives.	Content includes links established between cyber security and national risk priorities, but these are generally ad-hoc and lacking in detail.	The content of the national cyber security strategy is established. It is linked explicitly to national risks, priorities and objectives. Content at a minimum should seek to raise public awareness, mitigate cyber-crime, establish incident response capability and protect critical national infrastructure. Critical national security cyber infrastructure has been identified.	National cyber security strategy content is updated with metrics and measurements to help leaders evaluate the success of the various cyber security objectives and guide resource investment.	The content of the strategy is reappraised and modified in response to the cyber security environment. New content relating to cyber security objectives is regularly incorporated in the strategic plan. Additionally, content of the national cyber strategy should seek to lead, promote and encourage international cooperation to ensure a secure, resilient and trusted cyberspace.

D1-2: Incident Response					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Identification of Incidents	No catalogue of the existence or nature of national level incidents has been developed.	Certain cyber events/threats have been categorised and recorded as national-level incidents/challenges.	A central registry of national-level incidents is functional.	Regular, systematic updates to the national-level incident registry are made and prioritised. Some capacity exists for focusing analytical resources for incident response.	Capacity for adapting focus on incident identification and analysis is dynamic in response to environmental changes.
Organisation	Little or no organisation for national incident response exists. Response, if any, is reactive and ad-hoc.	Private sector organisations key to national cyber security have been identified and contacted, but no formal co-ordination and information sharing mechanisms exist between public and private sectors. A central body has been designated to collect emergency threat information but a specific mandate for a national cyber response agency is yet to be agreed.	A routine, co-ordinated relationship exists between the public and private sectors for national-level incident responses. The scope of such co-ordination is largely limited to the established incident registry. Tools and procedures for combating national-level incidents are still largely reactive. Emergency response capacity is clearly identified and distributed, with framework funding.	Distinct and formal security roles and responsibilities have been established embracing government, critical infrastructure, enterprise, and individual systems. The objectives of the organisation responsible for incident response are aligned with those of the national cyber defence centre, if one exists. Resources allocated to emergency response are adequate to the cyber security threat environment.	An early warning capacity is incorporated into the mission of the emergency response organisation, which seeks to shape and manage the threat landscape before responding to specific threats/challenges. Tools for early detection, identification, prevention, response and mitigation of zero-day vulnerabilities are embedded in emergency response organisation(s).
Coordination	Responsibility may have been allocated informally to an acknowledged member of staff within each agency/ministry incident response organisation.	At a national-level official agency/ministry leads for incidents have been designated and publicised. However, channels of communication between	Co-ordinated national incident response is established and published, with clear processes, roles and responsibilities defined	Sub-national/sectorial incident-response organisations are established. The primary coordination channels necessary for incident	Incident response has the ability to alter coordination mechanisms based on the threat environment.

D1-2: Incident Response					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
		these leads remain ad hoc/inconsistent.	and lines of communication prepared for times of crisis.	response are established and resources are allocated proportionately. This coordination mechanism is recognised and understood by all stakeholders involved. Technical capabilities now go beyond coordinating response and include focusing strategic resources in coordinating incident analysis and support, and threat intelligence services.	Multi-level national coordination between all levels and sectors is central to incident response. Coordination exists between regional and international incident response organisations.

D1-3: Critical National Infrastructure (CNI) Protection					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Identification	Some understanding of critical assets and vulnerabilities is understood, but no formal categorisation of assets and vulnerabilities has been produced.	A list of generic CNI assets has been created.	A detailed audit of critical assets is performed on a regular basis. Dissemination of critical asset audit lists are discussed with relevant stakeholders.	CNI risks have been prioritised according to vulnerability and impact, which guides strategic investment. Vulnerability/asset management processes are in place in order that incremental security improvements can be made. A distinction has been drawn between critical assets and essential services for day-to-day activity.	Priority listing of CNI assets is regularly re-appraised to capture changes in the threat environment. The impact of cyber security risk on the business operations of owners of critical assets, including direct and opportunity costs, impact on revenue, and hindrance to innovation, are understood and incorporated into future planning.
Organisation	There is little to no interaction between government ministries and	A mechanism is established for regular vulnerability disclosure between the	Defined reporting requirements between CNI asset owners and the public	There is a clear understanding as to those elements of CNI cyber	There is constant effort to balance the requirements of national cyber security with

D1-3: Critical National Infrastructure (CNI) Protection					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
	owners of critical assets. No formal collaboration mechanism exists.	public and private sector, but the scope of reporting requirements has not been specified.	sector are sufficient to address national security needs.	security which are managed centrally, and those which are managed locally.	the needs of the owners of critical infrastructure and assets.
Response Planning	Response planning to an attack on critical assets may have been broadly discussed, but no formal plan exists.	Protection of critical assets includes basic level cyber security awareness and data security policies, but no protection processes or procedures have been agreed.	Information and operation protection procedures and processes have been established, supported by adequate technical security solutions Risk management procedures are used to create a response plan able to produce a repeatable course of action in the event of an incident. Communication links are proven, analysis and harm mitigation measures are undertaken, and exercises are conducted to prepare for an event.	Assessment of the breadth and severity of harm incurred by critical assets is regularly conducted and response planning is geared on that assessment. Improvements in response mechanisms are routinely considered in order to prevent a stagnant or hesitant response.	Continuous security monitoring reveals whether protective measures continue to be effective and, if not, what technologies, policies or processes should be reviewed.
Coordination	Informal procedures for dialogue between the public and private sector may be developed, but lack protocols for information sharing and are generally on an ad hoc and unstructured basis.	Dialogue has occurred to determine the criteria by which industries/bodies are deemed critical to national cyber infrastructure. An informal community of CNI industries has been established with the intent of sharing threat information.	Formal internal and external CNI communication strategies have been defined and are consistent across sectors. An external communication strategy has been developed and endorsed by central government. The government's policy perspective, decision-making process and machinery for managing and	A public awareness campaign to facilitate the CNI communication strategy is established with a point of contact for this information. Cyber security requirements and vulnerabilities in CNI supply systems have been clearly identified and are managed. A vulnerability review process has been implemented, which ensures that resources	Trust has been established between the government and CNIs with respect to data security and exchange of threat information. Information is fed into the strategic decision making process. Cyber security risk management is part of the organizational culture and actively reflects the network operating environment.

D1-3: Critical National Infrastructure (CNI) Protection					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
			ensuring cyber security are all agreed and consolidated. A clear point of contact for internal and external CNI cooperation is established. Where there are privately operated elements of the CNI, government bodies invited as observers. Dialogue between tactical (technical and security) and strategic (senior management) levels regarding cyber risk practices takes place on a regular basis.	dedicated to coordinating management of supply system vulnerabilities remain sufficient.	C-level board members are able to make informed risk management decisions based on reliable intelligence communicated effectively.
Risk Management	Threat awareness by CNI operators exists minimally, if at all. Basic risk management skills and understanding may be incorporated into business practices, but cyber security is subsumed into IT and data protection risk and is not recognised more broadly.	Some awareness and training has been provided so that incident management can run efficiently. Authorised access, both physical and remote, has been controlled, and some training has been provided to employees about the management of access privileges. CNI industry has basic capabilities to detect, identify, protect, respond and recover from cyber threats. But such capabilities	Minimum security measures and guidelines for CNI cyber best practice have been established. Incident response procedure has been defined and all necessary entities participate actively. Information shared between government and CNI uses language and assumptions readily understood by the community. Insider threat detection is accounted for in CNI cyber security risk management.	Cyber security is firmly embedded into general risk management practice. Security measures are developed to ensure business continuity of CNI in the context of the prevailing risk environment. Resources have been allocated to ensure the timeliness and effectiveness of incident response. These resources are allocated in proportion to the assessed potential impact of an incident.	Audit practices to assess network and system dependencies and vulnerabilities (i.e. unmitigated dependencies) are implemented on a regular basis and inform continuous reassessment of the risk portfolio for CNI. Continual self-assessment and self-regulation is encouraged and established. Procedures to optimize the legal framework concerning CNI by amending existing legislation or enacting new legal regulations are in place as needed.

D1-3: Critical National Infrastructure (CNI) Protection					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
		are uncoordinated and vary in quality.	Comprehensive legislation on critical infrastructures (substantive/procedural law) and regulatory procedures have been implemented, providing a legal basis for CNI network, operator-side and user-side security. The implementation of CNI standards is monitored and reviewed.	Regular participation in national cyber exercises in order to evaluate cyber readiness, protection and emergency response.	

D1-4: Crisis Management					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Planning	It may be generally understood that crisis management is necessary for national security. Exercise design and planning authority may have been allocated in principle (either directly or via consultants), but planning has not been thoroughly outlined or is conducted last minute. Monitors, if they exist, are internal and may lack adequate training.	A preliminary needs assessment of measures that require testing has been undertaken with consideration of a simple exercise scenario, with limited size and geographic scope. Appropriate resources have been allocated to the exercise. The exercise is conducted internally within organisations or ministries, without broader	A realistic high level scenario informs a plan to test information flows and decision-making comprehensively. New information is injected into the exercise at key points. External monitors are utilised, or professional training is provided for internal monitors.	Planning process includes the engagement of participants, an outline of their role in the exercise, and the articulation of benefits and incentives for participation. Trust is developed well in advance via the recruitment and pre-exercise briefing process and through guaranteed confidentiality control. Specific, Measurable, Attainable, Relevant, and Time-Bound (SMART) objectives and performance	The exercise programme is wide in its geographic scope and participation, as well as in its political/technical complexity. The exercise addresses international challenges and produces scalable results for policy development and strategic decision making. Outside observers participate and contribute to the process. A media policy and public relations plan is promoted to an appropriate degree, without

D1-4: Crisis Management					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
		cooperation or coordination. Key stakeholders and other subject matter experts, such as think tanks, academics, civil leaders and consultants are included in the planning process.		key indicators (PKI) are set in the planning stage and seek to inform decisions in crisis management.	divulging sensitive information.
Evaluation	No evaluation of crisis management protocols and procedures has been conducted or has only been considered in principle. Results from exercises do not inform overall crisis management.	General awareness of crisis management techniques and goals exist to inform a crisis management exercise. The exercise is evaluated and commentary is provided by participants on an ad hoc basis, but does not feed into decision making.	Stakeholders are included in the evaluation process. Measurable indicators of success are gathered, including questionnaires, repeated testing, follow-ups, and lessons learned. Findings are collated, analysed and fed into the decision-making process. Findings are evaluated against national/international crisis management best practice.	SMART and PKI produce structured, measurable results that will inform useful recommendations for policy makers and stakeholders. Tailored, sector-specific reports are prepared for each stakeholder, while ensuring sensitive information is secured. Crisis management evaluation results inform cost/benefit calculations in national strategy implementation and budgetary allocations.	An evaluation of the crisis management exercise is provided for the international community, so that lessons learned can contribute toward a global understanding of crisis management. Crisis management is embedded in risk analysis, review and management.

D1-5: Cyber Defence Consideration					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Strategy	National security policy and defence strategy may be published and may contain a digital or information security component.	Specific threats to national security in cyberspace have been identified, such as external threat actors (both state and non-state), insider threats, supply systems vulnerabilities, and threats to military operational capacity, but a coherent response strategy does not yet exist.	National cyber defence policy/White Paper exists and outlines the military's position in its response to different types and levels of cyber-attacks (for example, cyber enabled conflict producing a conventional, kinetic effect and offensive cyber-attacks aimed to disrupt infrastructure including emergency response).	National cyber defence complies with relevant international law and is consistent with national and international rules of engagement in cyberspace. Resources dedicated toward engaging in international cyber defence forums are allocated based on national strategic objectives.	The evolving threat landscape in cyber security is captured through repeated review in order to ensure that cyber defence ways and means continue to meet national security objectives. Rules of engagement are clearly defined and the military doctrine that applies to cyberspace is fully developed and takes note of significant shifts in the cyber security environment
Organisation	Informal management of cyber defence may be distributed among the armed forces and/or government organisations, with occasional reference to signals intelligence. There is no clear command structure for cyber security in the defence apparatus.	Cyber operations units are incorporated into the different branches of the armed forces, but no central command and control structure exists.	There is a defined organisation within the Defence ministry responsible for conflict using cyber means.	Highly specialised expertise with advanced strategic cyber capabilities and full situational awareness are integrated into the national defence strategic posture.	Defence ministry contributes to the debate in developing a common international understanding of the point at which a cyber-attack might trigger a cross-domain response.
Coordination	The national defence apparatus contains no (or limited) capacity for cyber resilience (intended to reduce vulnerabilities to national security interests).	Cyber defence capability requirements are agreed between the public and private sector in order to minimise the threat to national security incurred by both sectors.	The need for coordination in the event of exfiltration of digital information by malicious actors is recognized and prepared for. Defence organisations and critical infrastructure providers have established a mechanism to report threat intelligence.	Some analytical capacity exists to support the coordination of and resource allocation for national cyber defence; possibly including a cyber-defence research centre.	The entity in charge of cyber defence coordinates strategic integration regarding cyber events between government, military and critical infrastructure including budgets and identifies clear roles and responsibilities. This process then feeds into the re-evaluation of the

D1-5: Cyber Defence Consideration					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
					national security posture of the nation.

D1-6: Digital Redundancy					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Planning	Digital redundancy measures may be considered, but not in a systematic, comprehensive fashion.	Stakeholders convene to identify gaps and overlaps in emergency response asset communications and authority links. Emergency response asset priorities and standard operating procedures are established in the event of a communications disruption along any node in the emergency response network.	Emergency response assets are hardwired into a national emergency communication network. Appropriate resources are allocated to hardware integration, technology stress testing, personnel training and crisis simulations drills.	Outreach and education of redundant communications protocols is undertaken for key stakeholders and is tailored to their unique roles and responsibilities.	Stakeholders contribute to international efforts on redundancy communication planning.
Organisation	Current emergency response assets have been identified, but lack any level of integration.	Emergency response assets are mapped and identified, possibly including details of their location and their designated operators.	Communication is distributed across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities.	Emergency response assets practice interoperability and function effectively under compromised communications scenarios. The results of these scenarios then inform strategic investment in future emergency response assets.	Optimised efficiency is in place to mediate extended outages of systems. National-level assets can act to assist neighbours in the event of an international-level crisis or incident. Emergency response interoperability mapping and drills are proposed, scheduled, and undertaken on an annual basis.

Dimension 2: Cyber culture and society

D2-1: Cyber Security Mind-set					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Government	There is an absence or minimal recognition of a cyber security mind-set within government agencies.	Leading agencies have begun to place priority on cyber security, such as by identifying risks and threats.	Cyber security best practices are widely known across government at all levels.	Most agencies across all levels of government have ingrained a proactive cyber security mind-set which ensures a foundation of cyber security in all levels of strategic planning.	The security mind-set has been routinised and become a habit. The cyber security mind-set serves as a foundation for ministries' personal approaches to their responsibilities and is evidenced as global best practice.
Private Sector	Business and industry have no or little recognition of the need for prioritizing a cyber security mind-set.	Leading firms have begun to place priority on a cyber security mind-set by identifying high-risk practices.	Cyber security mind-set has been engrained across business and industry.	All the organisations, including SMEs across most industries have fostered and routinised a proactive cyber security mind-set which ensures a foundation of cyber security in all levels of strategic planning.	The cyber security mind-set serves as a foundation for personal approaches within the private sector regarding their responsibilities and is evidenced as global best practice.
Experts	No or little discussion has been initiated among cyber security experts towards building a common understanding of what constitutes a cyber security mind-set.	An identifiable group of experts has begun to debate and promote a common cyber security mind-set within their community with a responsibility to support and protect users.	Developing consensus among experts on the appropriate mind-set for cyber security experts, which has begun to gather support within the community.	A common mind-set for cyber security experts has been fostered and proactively shape strategic behaviour.	Cyber security experts demonstrate an ingrained cyber security mind-set, contributing towards an environment that consistently produces solutions to potential new and emerging risks and threats.

D2-1: Cyber Security Mind-set					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Society[at-large]	Society is unaware of cyber threats in general and is therefore unable to take concrete cyber security measures. Society is aware of cyber threats in general, but do not take any proactive steps to improve their cyber security.	A cyber security mind-set is proliferated, but inconsistently, throughout society. Programmes and materials have been made available to train and improve digital security practices.	Societal consciousness of the secure use of online systems has been developed. A growing proportion of users have the skills to manage their privacy online, and protect themselves from intrusion, interference, or unwanted access of information by others.	Growing numbers of users have routinised a cyber security mind-set, employing secure practice as a matter of habit, without undue distraction focusing on security issues. Most users have the information, confidence and practical tools to protect themselves online, while support and resources are provided to vulnerable members of society.	Users demonstrate a cyber security mind-set: habitually employing more secure practices in their everyday use of online networks. Cyber security skill-set of a country's population is advanced so that threats facing society can be effectively addressed by users.

D2-2: Cyber security Awareness					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Awareness raising	The need for awareness of cyber security threats and vulnerability across the general public and private sector is not recognised, or is only the initial stages of discussion.	Awareness-raising campaigns established with defined targets, but is ad-hoc, not necessarily covering all groups, and not closely linked to cyber security strategy. Training courses, seminars and online resources are available for target demographics, but no coordination or measurement efforts have been conducted.	A national program for raising cyber security awareness which addresses a wide range of demographics and issues exists led by a national champion, with clear understanding of how campaigns and products will be utilised based on consultation with stakeholders. Single online portal linking to appropriate information exists and is well known.	Metrics for effectiveness are established for selected awareness campaigns and evidence of application and learnings are fed into future campaigns. Exercises and monitoring activities have been undertaken to measure levels of awareness. Market in awareness raising offerings are tracked and measured, interventions based on evidenced gaps or failures.	Contribution of metrics toward national strategy renewal processes and the redistribution of resources based on performance have been established. Awareness raising mechanisms are reconfigured in response to performance evidenced by monitoring - quickly and where necessary, which results in the redistribution of planned budgets and future investments.

D2-2: Cyber security Awareness					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
			Evidence of multi-stakeholder engagement in delivery of services and products can be found in order to enhance awareness of cyber security risks.	The program is supported by specific processes created to enable re-use of campaign materials and resources, involving clear methods for obtaining a measure of suitability and quality. Campaigns contribute toward and draw from international awareness raising initiatives.	Awareness campaign planning gives explicit consideration to the movement of people, so that campaigns continue to impact the entire society. The stakeholder community (in the widest sense) is able to feed requirements into the intervention-planning process, and there is evidence of personalisation of awareness raising materials to target groups.

D2-3: Confidence and trust on the Internet					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Trust in use of online services	The use of online services is characterised by lack of trust or blind trust. Trust in online services is a or no concern and no coordinated actions are established by operators of internet infrastructure.	Operators of the infrastructure are considering measures that address concerns regarding trust in online services but have not established them. Provision of services and development of internet infrastructures across all sectors are being under research. Support for take-up by users as well as freedom of access to communication	Measures needed to provide more secure online services have been implemented. A national coordinated program to promote trust in online services has been established. Infrastructure and services are developed, and provision of public access facilities and reduction of costs to access are defined.	Measures of effectiveness, including consideration of secondary impacts, of the national program to promoting trust are collected and inform resource allocation. Measures assessing trust in online services include individual's sense of control over providing personal data online. User-consent policies are in place, which are designed to	Through the iterative application and assessment of quantitative and qualitative metrics in online infrastructure and service development, trust in online service is improved. Individuals assess the risk in using online services and continuously adjust their behaviour based on this assessment.

D2-3: Confidence and trust on the Internet					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
		technologies by citizens or social groups is being considered.		provide constraints on the collection, use or disclosure of sensitive personal information.	
Trust in e-government	Government offers no e-services or has begun to offer e-services online but has not publicly promoted the necessary secure environment. Obstacles to access, including restrictions imposed by governmental policy or economic conditions such as lack of infrastructure are a concern.	Government continues to increase e-service provision, but also recognises the need for the application of security measures to promote trust in these services. Undesirable online practices are being discussed between government and regulatory authorities, political and interest groups, and human rights advocates.	Breaches in e-services have been identified and acknowledged, and disclosed in an ad-hoc manner by government. The public sector coordinates actions to avoid attacks using personal information, which cause lack of trust by consumers. Data sharing in the use of e-government services is enabled, and efforts to protect personal information from unauthorised disclosure is in place. High level Internet crimes against e-government services are prioritised in order to mitigate occurrences. Compliance to Internet and web standards that prevent or protect the anonymity of users is promoted.	Disclosure of information is the default: public authorities are obliged to publish certain information about their activities (based on common understanding of strategic need), and members of the public are entitled to request information from public authorities. Privacy by default as a tool for transparency is promoted. User-generated content processes are employed to provide feedback on ineffective material. Processes are employed for gathering user-generated feedback in order to guide strategic decision-making regarding management of of online content.	E-government services are continuously improved in order to promote a transparent/open and secure system that people trust. Impact assessments on privacy protection in e-government provisions are consistently taking place and feed back into strategic planning.
Trust in e-commerce	E-commerce services are not offered or offered in a non-secure environment,	E-commerce services are being provided to a limited extend but are still not fully organised.	E-commerce services are fully established in a secure environment.	Stakeholders recognise the need of building user trust in order to ensure business continuity. Resources are	E-commerce services are fully organised and continuously improved in order to promote a

D2-3: Confidence and trust on the Internet					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
	leading to lack of trust by users. There is a lack of secure and reliable payment systems and policy for the handling of personal information. Users are unfamiliar with e-commerce and do not have adequate knowledge about how personal information is handled.	Stakeholders recognise the need for e-commerce services provision and have begun discussion of investments in this area. Users are informed of the utility of security solutions and secure and reliable payment systems.	Security solutions are being updated and reliable payment systems have been made available. Multiple stakeholders invest in e-commerce. Stakeholders create privacy policies that seek to establish limitations around personal information sharing. Users have developed trust in internet vendors based on secure experiences in e-commerce services. Terms and conditions of the use of e-commerce services is easily accessible.	allocated based on trust perceptions. Users feel confident that personal information provided to e-commerce services will remain secure and that users can maintain control of the distribution of this information. Stakeholders make strategic decisions to confirm user's trust in e-commerce through enhanced service functionality and the provision of feedback mechanisms.	transparent, trustworthy and secure system. Impact assessments on privacy protection in e-commerce provisions consistently take place and feed back into strategic planning. Terms and conditions provided by e-commerce services are clear and comprehensible to all users. Feedback on user experience in the use of e-commerce services is integrated into service provision in order to enhance the trust between consumers and producers.

D2-4: Privacy online					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Privacy Standards	Government discussions of privacy issues may have begun and include multiple stakeholders, but no privacy standards are in place.	Laws and policies promoting access to government and other public information are being considered.	All relevant actors from the private sector and civil society are actively driving change in practices, laws, and regulations that impinge on privacy. Government is considering adoption of human rights legislation with a focus on privacy.	Stakeholders comply with regionally and internationally recognised standards for human rights, particularly regarding privacy but implementation of these standards is not pervasive. Compliance with such standards provides strategic guidance for investment in privacy protection.	Domestic actors, policies and practices actively shape positive international perceptions of privacy and are central to informing multi-stakeholder decisions. Compliance to privacy components of the Universal Declaration of Human Rights is demonstrated, and research is conducted that considers the optimal application of human rights (and particularly privacy) to cyber security.
Normative and behavioural perspectives on freedom of expression online	Discussions within government regarding free expression online are not taking place or are at an initial level but there is not adherence to standards. Associated actors and strategies that affect freedom of expression as well as legal and regulatory choices are identified.	Freedom of expression and freedom of information are only limited by a country's laws, especially those on privacy. But also they are affected by legal, technical and regulatory issues tied to cultural political and economic contexts. Freedom of citizens or social groups to have access to communication is being considered. Individuals place a high value on an open Internet in which they are free to express their views and accept the rights of others to express their views, even	All relevant actors from the private sector and civil society are actively driving change in practices, laws, and regulations that impinge on free expression. Identification of the diversity of associated actors and strategies that affect freedom of expression as well as legal and regulatory choices are being defined. Access-Freedom of connection: infrastructure and services are developed, media literacy and skills are developed, provision of	Stakeholders comply with regionally and internationally recognised standards for human rights, particularly regarding freedom of expression online but implementation of these standards is not pervasive. Compliance with such standards provides strategic guidance for investment in promoting free expression online. Broadband internet and freedom of information are recognised as fundamental human rights.	Compliance to free expression components of the Universal Declaration of Human Rights is demonstrated, and research is conducted that considers the optimal application of human rights (and particularly freedom of expression) to cyber security. Freedom of expression is reconciled with an obligation to exercise it responsibly, in a manner that promotes a secure and prosperous society.

D2-4: Privacy online					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
		if they disagree, as long as they remain within the bounds of acceptability.	public access facilities, and reduction of costs to access are set.		
Employee Privacy	Minimal or no discussion among private sector leaders regarding privacy issues in the workplace exists.	Privacy in the workplace is recognised as an important component of cyber security and is beginning to be institutionalised in employee programs.	Employers maintain privacy policies that provide a minimum level of privacy for employees.	Employees are sensitised to their privacy rights within the organisation and individual privacy obligations are understood based on strategic planning. Compliance to human rights relevant best practices on privacy in the workplace is achieved.	Privacy impact assessments are regularly conducted and feed into policy revision.

Dimension 3 - Cyber security education, training and skills

D3-1: National availability of cyber education and training					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Cyber Education	Some educational offerings may exist but no recognised requisite body of knowledge. No accreditation in cyber security education exists.	Marketplace for cyber security education and training exists and evidence of take-up. Professionals' initiatives are directed towards increasing attractiveness of cyber security careers and relevance to wider leadership roles. Access to educators is available in cyber security specifically for cyber security specialists.	Some education in cyber security at the national and institutional levels exists, ranging from primary to post-graduate levels, including vocational education. Programmes exist for education of individuals in addition to tailored professional offerings. Access to educators is available in cyber security for a wide variety of professions.	Educational offerings are weighted and focused based on an understanding of current risks and skills requirements. Metrics are developed to ensure that educational investments meet the needs of the cyber security environment.	Integration and synergy across educational elements exists. Prevailing cyber security requirements are considered in the re-development of any general curricula. Research and development is a leading consideration in cyber security education. Content in education programmes aligns with practical cyber security problems and business challenges.
Training	Little or no training in cyber security exists.	Training in information security exists, but is ad-hoc and uncoordinated. Professional bodies offer awareness raising programmes for continuing professional development based on international best practices. Training courses, seminars and online resources may be	Stakeholders invest in cyber security training which extends beyond IT roles into company boards and across full range of employees. The needs of society are well understood and a body of knowledge requirements is documented. The modes and procedures of training are assessed for	A range of high quality cyber security training courses is available. The quality of these courses is internationally recognised. The connection of training and educational programmes to national and institutional cyber security strategy priorities is clear.	Public and private sector training exists collaboratively, is constantly adapting and seeks to build skillsets drawn from both sectors.

D3-1: National availability of cyber education and training					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
		available for targeted demographics, but measures of effectiveness do not exist.	effectiveness and some requirements are established.		

D3-2: National Development of cyber security education					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
National development of cyber security education	Few or no professional instructors exists in cyber security. No programme exists to train teachers in cyber security. Links to capture national education and skills priorities may be considered. A network of national contact points for governmental, regulatory bodies, critical industries and education institutions may be established to improve coordination of actions. A national budget focused in cyber security may be developed.	Exploratory training programmes for cyber security instructors have been set up. A small cadre of professional instructors exit, but with limited resources. An office exists for responsibility of development and delivery of the national strategy in cyber education and manages the budget. Budget lines for training and research are identified. Stakeholders across government identified (donors, investors) and regular communication lines	Specific actions (public-private sector) extending knowledge, enhancing skills and expanding capability on cyber security are clearly evidenced. Broad consultation across government, private sector, academic and civil society stakeholders informs national education and skills priorities, as well the strategy to follow up. International partners and community (universities, schools, academics, etc.) consulted to benefit from lessons learnt. Government funded centres of excellence in cyber security, accessibility to cyber education and skills,	Government budget and spending on cyber security training and education is increased based on the return on investment. Governmental initiatives directed towards increasing attractiveness of cyber security careers are promoted, informed by a gap-analysis of skills. The levels of cooperation and collaboration across three key stakeholders (government, private sector & academia) focused on cyber security training & education is enhanced.	Availability of accredited high quality university and further education degrees and courses on cyber security exist. Cyber security education programmes maintain a balance between preserving core components of the curriculum and promoting adaptive processes that respond to rapid changes in the cyber security environment. International cyber centres of excellence are established through twinning programmes led by world class institutions.

D3-2: National Development of cyber security education					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
	The justification of how budget helps to manage education and research either does not exist or is only just being discussed.	are established to ensure repeatability. Funding dedicated to national research at universities for basic and applied research exists.	alignment of education with real-world problems and funding dedicated to national research exist.		

D3-3: Corporate training & educational initiatives within companies					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Training in cyber security	Cyber security training programs are not performed. There are few trained IT personnel designated to support cyber security issues as they occur. Skillset may exist but is not strategically located and tools are limited pool to a pool of authorized users.	There is no knowledge transfer from trained cyber security employees. Because of limited training, there is only informal use of existing tools, models, or templates for the organization's cyber security planning, with no automated data integration.	Knowledge transfer from trained cyber security employees exists on an ad hoc basis. Job creation initiatives for cyber security are established and encourage employers to train staff. Structured cyber security training programs exist that specify precise roles and responsibilities. Some data systems, tools, and models are available with limited trained personnel to operate; technical training is still required.	There is a sufficiently established cadre of skilled employees trained in the organization's cyber security issues, processes, planning and analytics. The cyber security skills development programme is integrated, optimized and automated. Levels of professionalism in information assurance and cyber security are more evident across the public and private sector.	Cyber security knowledge exchange to promote skill development is continuous. Life cycle management of cyber security training is used to inform future training programmes. Data systems, tools, and models are used by a wide range of practitioners. Automated data integration is now possible due to advanced cyber security skillset.

D3-4: Corporate Governance, Knowledge and Standards					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Boardroom Understanding of Cybersecurity	Boards have little or no knowledge of cyber security issues. Fiduciary duty considerations are not discussed	Boards have some awareness of cybersecurity issues, but not how they might affect the organization, or what direct threats they might face.	Boards have an understanding of how companies are at risk in general, some of the primary methods of attack, and how their company deals with cyber issues (usually abdicated to the CIO). Event management is largely reactive. Some optional board education in cyber-security may take place.	Boards know what their strategic assets are, have put specific measures in place to protect them, and know the mechanism by which they are protected. The boardroom can allocate specific funding and people to the various elements of cyber risk, contingent on their company's own, prevailing situation. Corporate contingency plans are in place to address various cyber-based attacks and their aftermath. Some mandatory board education in cyber-security takes place. The board has a clear sense of cyber fiduciary duties.	Boards are able to change cyber-security strategy quickly and appropriately. New threats are considered at every board meeting, and funding and attention reallocated to address those threats. Board is looked to as a source of knowledge in corporate cybersecurity governance. Boards' governance is cyber risk based and improves governance specifically in this area.

Dimension 4 - Legal and regulatory frameworks

D4-1: Cyber security legal frameworks					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Legislative framework for ICT Security	Legislation relating to ICT security does not exist yet or is in the process of being developed. Efforts to draw attention to the need to create a legal framework on cyber security have been made and may include the need of a gap analysis.	Experienced partners may have been consulted to support the country's efforts in establishing a comprehensive policy and legal and regulatory frameworks, bringing together multiple stakeholders across sectors involved in ICT. Key priorities for creating cyber security legal frameworks have been identified, potentially in a model framework, but not yet established.	Comprehensive ICT legislative and regulatory frameworks addressing cyber security has been implemented. Legislation protecting the rights of individuals and organizations in the digital environment has been adopted.	The country has reviewed existing laws and regulatory mechanisms, identified where gaps and overlaps exist, and prioritized what areas need improvement. Legal, regulatory and technological measures and resources that will ensure the integrity, confidentiality, availability and the overall security of digital information and ICT are reviewed and improved periodically.	Procedures to optimize the protection of the ICT sector by amending existing legislation or enacting new legal regulations are in place, supported by regular research. Mechanisms for improving the harmonization of ICT legal frameworks with national cyber security-related ICT policies, international laws, standards and best practices exist and constantly evolve. Participation in the development of bilateral, regional and international cyber security cooperation agreements and treaties focused on ICT is a priority, and have been signed and ratified by multiple parties. Efforts are in place to exceed minimal baselines specified in these treaties.
Privacy, data protection & other human rights	Privacy and data protection legislation does not exist yet or is in the process of being developed.	Partial legislation exists regarding privacy, data protection and freedom of online expression.	Comprehensive data protection legislation and regulatory procedures have been implemented.	International and regional trends and best practices inform the assessment of domestic legal frameworks	In order to meet dynamic changes in the application of technology to privacy, data protection and human rights, procedures are in

D4-1: Cyber security legal frameworks					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
	Domestic law doesn't recognize fundamental human and civil rights in connection with cyber-specific/related offences.		Domestic law recognizes fundamental human and civil rights in connection with cyber-specific offences. Domestic law specifies the individual's right to privacy during the collection, use and disclosure of personal information by law enforcement agencies.	and associated resource planning. A comprehensive structure within the criminal justice system as a whole is in place to combat cybercrime while respecting human rights. The country is engaged and works with international organizations on privacy and data protection. Legal mechanisms are in place that enable strategic decisions to be made that determine the timeframe in which personal data is no longer required for the investigation and must be deleted.	place to amend and update legal frameworks as needed. The country has ratified or acceded to international treaty and other agreements and efforts are in place to exceed minimal baselines specified in these treaties. The state is also an active contributor in the global discourse on human rights in cyberspace.
Substantive cybercrime law	Specific substantive criminal law for cybercrime does not exist or general criminal law exists and is applied ad-hoc to cybercrime.	Partial legislation exists in substantive cybercrime law that applies some aspects of cybercrime to legal and regulatory frameworks. Specific substantive criminal law for cybercrime is being discussed among lawmakers, but the development of the law has not yet commenced.	Comprehensive legislation that criminalizes a variety of cybercrime acts has been adopted.	The state has signed relevant regional or international instruments on cybercrime and allocated resources according to national priorities.	Legislation is regularly reviewed and updated to account for the dynamic environment of cyber security. The state has ratified regional or international instruments on cybercrime, and consistently seeks to implement these measures into domestic law. Efforts are in place to exceed

D4-1: Cyber security legal frameworks					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
					minimal baselines specified in these instruments. The state is also an active contributor in the global discourse on international cybercrime treaties.
Procedural cybercrime law	Specific procedural criminal law for cybercrime does not exist or general criminal law exists and is applied ad-hoc to cybercrime.	Partial legislation exists in procedural cybercrime law that applies some aspects of cyber security to legal and regulatory frameworks. Procedural criminal law for cybercrime is being discussed among lawmakers, but development of the law has not yet begun.	Comprehensive criminal law with procedural powers for investigation of cybercrime and evidentiary requirements to deter, respond to and prosecute cybercrime has been implemented. Best practices are applied by law enforcement in exercising procedural powers.	In the case of cross-border investigation, procedural law stipulates what actions need to be conducted under particular case characteristics, in order to successfully prosecute cybercrime.	Legislation is regularly reviewed and updated to account for dynamic environment of cyber security. The state has ratified regional or international instruments on cybercrime, and consistently seeks to implement these measures into domestic law. Efforts are in place to exceed minimal baselines specified in these instruments. The state is also an active contributor in the global discourse on international cybercrime treaties.

D4-2: Legal Investigation					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
	The institutional capacity of law enforcement authorities to prevent and combat computer crime does not exist. There is minimal interaction between government ministries and law enforcement authorities. No formal collaboration mechanism exists. No specialized officers and digital forensics experts exist, or consultation has begun to consider these capacities in specific departments/units/ entities. Digital chain of custody and evidence integrity management does not exist. There is no collaboration with other cyber security stakeholders to assess the underlying factors that facilitate criminal conduct in cyberspace are unknown. No or minimal forms of participation among international cooperation exists to prevent and combat cybercrime.	Some investigative measures are deployed by law enforcement officers in accordance with domestic law. Some specialized officers, digital forensics experts and equipment allows for the investigation of some complex cybercrimes, but action remains un-coordinated.	A comprehensive institutional capacity to investigate and manage cybercrime cases has been established. There are sufficient human, procedural, and technological resources available to ensure effective and efficient investigation of cybercrime cases. Full investigative measures provided for in domestic law are deployed by law enforcement officers. Digital chain of custody and evidence integrity is established including formal processes, roles and responsibilities. National standards for the training of law enforcement officers exist. Cybercrime law enforcement officers are enabled to attend criminal proceedings in person in order to testify and provide information on cybercrime and electronic evidence in court.	Resources dedicated to fully operational cybercrime units have been allocated based on strategic decision making. Cybercrime officers are certified as “specialised experts” in order to testify in court proceedings. Advanced investigative capabilities allow the investigation of complex crimes against computer systems, supported by regular testing and training of investigators. Law enforcement agencies have the resources to maintain the integrity of data to meet international evidential standards in cross-border investigation. Domestic law enforcement agencies are informally integrated with regional and international counterparts.	All law enforcement officers receive continuous training based on relative responsibilities and new, evolving threat landscapes. Law enforcement can utilise sophisticated digital forensic tools in order to adapt to the dynamic environment of cybercrime, and these technologies are consistently updated. Measurements, statistics and trends involving the investigation, charging and prosecution of criminals are constantly collected and analysed in order to support a comprehensive understanding of the online criminal environment and inform decision making. The institutional capacity of law enforcement is frequently reviewed and revised based on an assessment of effectiveness.

D4-2: Legal Investigation					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
			Formal collaboration mechanisms with other stakeholders have been established to identify and asses the underlying factors that facilitate criminal conduct in cyberspace. Formal mechanisms of international cooperation in order to prevent and combat cybercrime by facilitating their detection, investigation, and prosecution at both the domestic and international levels.		
Prosecution services	Prosecutors do not receive adequate training and resources to understand or review electronic evidence. There is minimal interaction between government ministries and prosecution services, with no formal mechanism for collaboration. There are no specialised cybercrime prosecutors, or consultation has begun to consider this capacity within the legal community. No or minimal forms of participation among	A limited number of specialised cybercrime prosecutors have the capacity to build a case based on digital information, but this capacity is largely ad-hoc and un-institutionalised.	A comprehensive institutional capacity to prosecute and handle cybercrime cases and cases involving electronic evidence is established. There are sufficient human, training and technological resources available to ensure effective prosecution of cybercrime cases, and cases involving electronic evidence. National standards for the training of prosecutors exist. Formal mechanisms of international cooperation in	There are institutional structures in place that allow for a clear distribution of tasks and obligations within the prosecution services at federal, regional and local levels, in accordance with the resources and requirements of the domestic legal system. There is a strategic relationship between law enforcement agencies and prosecution services which allows for rapid and	A cybercrime prosecution unit is established with the capacity to prosecute successfully complex cybercrimes in country and cross border. All prosecutors receive continuous training based on relative responsibilities and new, evolving threat landscapes. Prosecutors have the training necessary to understand and navigate the progressive and complex system of relationships

D4-2: Legal Investigation					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
	international cooperation exists to prevent and combat cybercrime.		order to prevent and combat cybercrime by facilitating their detection, investigation, and prosecution at both the domestic and international levels.	accurate judicial proceedings. Prosecutors are certified as "specialised experts" in order to testify in court proceedings. Measurements, statistics and trends involving the investigation, charging and prosecution of criminals is constantly collected and analysed in order to support a comprehensive understanding of the online criminal environment.	between cybercrimes, as well as other related crimes.
Courts	A separate court structure or specialized judges for cybercrime cases and cases involving electronic evidence does not exist. Consultation may have begun to consider this capacity in the judicial community. There is minimal interaction between government ministries and judicial services, with no formal mechanism for collaboration No or minimal forms of participation among international cooperation exists to prevent and combat cybercrime.	A limited number of specialised cybercrime judges have the capacity to preside over a case on cybercrime, but this capacity is largely ad-hoc and not systematic. Judges do not receive sufficient resources or cybercrime-related training to review and understand electronic evidence for conducting a case at trial.	There are sufficient human and technological resources available to ensure effective and efficient legal proceedings regarding cybercrime cases, and cases involving electronic evidence. Judges have the appropriate training in order to understand the investigative measures conducted by law enforcement in order to preside effectively over cybercrime cases. National standards for the training of judges and other judicial personnel exist.	The country has strategically considered implementing specialized judicial services/courts on cybercrime. There are institutional structures in place that allow for a clear distribution of tasks and obligations within the court system at federal, regional, and local levels, in accordance with the requirements of the domestic legal system. There is a strategic relationship between judicial personnel and law enforcement agencies and prosecution services in	Judiciary receive continuous training based on relative responsibilities and new, evolving threat landscapes. The judicial system is aware of constant changes in the cyber security environment and allocates resources where appropriate.

D4-2: Legal Investigation					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
			Formal mechanisms of international cooperation in order to prevent and combat cybercrime by facilitating their detection, investigation, and prosecution at both the domestic and international levels.	order to enhance rapid and accurate judicial proceedings. Judicial personnel are certified as "specialised experts" in court proceedings. Measurements, statistics and trends involving the investigation, charging and prosecution of criminals is constantly collected and analysed in order to support a comprehensive understanding of the online criminal environment.	

D4-3: Responsible Disclosure					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Responsible Disclosure	The need for a responsible disclosure policy in public and private sector organisations is not acknowledged.	Organisations develop the ability to receive and disseminate vulnerability information. A vulnerability disclosure framework is in place, which includes a disclosure deadline, scheduled resolution, and an acknowledgement report.	A vulnerability disclosure framework has been created. Setting a disclosure deadline of reporting serious vulnerabilities. Embarked provision deadlines are agreed for the report of resolution of the vulnerability.	An analysis of the technical details of the vulnerability is published and advisory information is disseminated according to individual roles and responsibilities. The large majority of products and services are updated within predetermined deadlines.	Responsible disclosure policies are continuously reviewed and updated based on the needs of all affected stakeholders. Responsible disclosure mechanisms are synchronised internationally, so that best practice in this area is created.

D4-3: Responsible Disclosure					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
		Software and service providers accept bug and vulnerability reports and address them. Software and service providers commit to refrain from legal action against a party disclosing information responsibly.	Ability to share technical details of the vulnerability with other stakeholders who can distribute the information more broadly	Responsible vulnerability disclosure process for all involved stakeholders (product vendors, customers, security vendors and public) is set.	All affected products and services are routinely updated within deadline. National and international processes are in place for review and reduction of deadlines.

Dimension 5: Standards, organisations, and technologies

D5-1: Adherence to standards					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Implementation of standards and minimal acceptable practices	No standards or practices have been identified for use in securing cyberspace data, information, technology or infrastructure. Or, initial identification of some appropriate standards and practices has been made, possibly some limited ad hoc implementation attempts, but no concerted endeavour to implement or change existing practice in a measurable way.	Information risk management standards have been identified for use and there have been some initial signs of promotion and take-up within government, public sectors and CNI organisations. There is some evidence of measurable Implementation and adoption of international standards and least acceptable practices. If they exist, then there is some measurable implementation of national standards and acceptable practices.	Nationally agreed baseline of cyber security related standards and least acceptable practices has been identified, and adopted widely across government, public sector and CNI organisations. Adoption and compliance is measured and reported. Some body within government exists to assess level of adoption across public and private sector. Government schemes exist to promote continued enhancements, and metrics are being applied to monitor take-up. Consideration is being given to how standards and practices can be used to address risk within supply chains within the CNI, by both government and the CNI organisations.	Choice of standards to be adopted is being made in the context of budgeting decisions, and resources are allocated according to risk assessments. Government and organisations promotes adoption of standards and practise according to assessment of national risks (economic and security) and budgetary choices. There is evidence of debate between government and other stakeholders as to how national and organisational resource decisions should align and drives standards and practice adoption. Evidence of contribution to international standards bodies exists and contributes to thought leadership and sharing of experience by organisations.	Continual process improvement is adopted and applied to both the choice of adopted standards and practices as well as to their implementation. Adoption of standards is fluid and non-compliance decisions are made in response to changing threat environments and resource drivers. Evidence of collaborative risk management exists in non-compliance decisions across sectors and CNI, which constantly adapts to the evolving cyber security landscape. Government is engaged in campaigns to promote dynamic approaches in use of standards and practices to support industry in both contributing to national security and in developing business opportunities. Evidence exists of mature debate in wider society on the dynamic use of

D5-1: Adherence to standards					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
					standards and practices based on continuous needs assessment.
Procurement	No evidence of use of cyber security related standards in guiding procurement processes – or some recognition of guidance being available but no effort to utilise it.	Evidence of use of cyber security standards in defining procurement practices exists	The implementation of standards in procurement practices meet international IT guidelines, standards and acceptable practices. Mature use of standards in procurement practices is evidenced through measurement and quality assessments of process effectiveness.	Critical aspects of procurement and supply such as prices and costs, quality, timescales and other value added activities are continuously improved, and procurement process improvements are made in the context of wider resourcing planning across the enterprise. Organisations are able to benchmark the skills of their procurement professionals against the competencies outlined in procurement standards and identify any skills and capability gaps. Internal stakeholders have a comprehensive understanding of E-sourcing or E-tendering systems and purchase-to-pay systems (P2P) in order to implement these tools in performing key tasks in procurement and supply.	Organisations have the ability to monitor use of standards in procurement processes and support deviations and non-compliance decisions in real-time through risk-based decision making. Best practices are included in procurement and compliance corporates quality assurance.
Software Development	There is no identification of software development standards relating to integrity and resilience for	Core activities and methodologies for software development processes focused on integrity and	Government has an established programme for promoting standards adoption in software	Security considerations are incorporated in all stages of development and processes.	Software development projects continuously assess the value of standards and reduce or enhance levels of

D5-1: Adherence to standards					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
	use in public and private sector deployments. Or there is some identification but only limited evidence of take-up.	resilience are being discussed within professional communities. Government promotion of relevant standards and concepts – although not necessarily resulting in widespread use. Evidence of organisations within the CNI and the public sector supplying or seeking to adopt standards in code development, and achieving some accreditations. Government have considered the promotion of cyber secure software development practices.	development – both for public and commercial systems. Government tracking compliance of standards. Evidence of CNI organisations requiring standards usage in their new developments. Evidence that high integrity systems and software development techniques are present within the educational and training offerings in country.	Core development activities including configuration and documentation management, security development and lifecycle planning have been adopted. Selection of standards and decisions to adopt are made as part of resource planning. Procurement of software developed according to required standards is considered based on an assessment of risk in investment decisions.	compliance according to risk-based decisions. Procurements of software for the public sector include on-going assessments of the value of standards in delivering software quality – throughout the lifetime of the contract (as opposed to simply initially at procurement stage). Requirements are built into contracts with suppliers.

D5-2: Cyber security coordinating organisations					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Command and Control Centre	A cyber security Command and Control Centre does not exist or is being considered at a national level.	Command and Control function is informally performed by national incident response capability or some other entity, with no formal coordination capability.	A Command and Control organization is identified and existing, but with no automated gathering, processing and analysis. Formal executive command and control on cyberspace exists as a national strategic matter	A Command and Control Centre with enhanced automation is established, providing basic national situation awareness. Selection of Command and Control Centre objectives is made as part of resource planning and strategic policy development.	A national cyberspace Command and Control Centre is fully developed, it receives and correlates information from incident response capability organisations, public/private organisations, LSPs, CII, defence and intelligence organisations, and is highly automated providing

D5-2: Cyber security coordinating organisations					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
					advanced situation awareness. Active situational awareness is coordinated with the national executive office. Threats and trends are analysed periodically, and findings feed into development and redevelopment of government policies and measures addressing cybercrime
Computer emergency Response Teams / CERTs	Incident response is not coordinated and is performed in an ad-hoc manner.	Existence and activity of some incident response team or personnel in the country, with identified roles and responsibilities Activity is concentrated on detecting and responding to organisational specific cyber incidents.	A national incident response capability is established and involves key stakeholders. Incident response capability's financial sustainability is considered and planned through the involvement of key stakeholders A vulnerability management plan is developed and implemented. Incidents are categorized consistent with response plans. Response and recovery plans are in place and managed. National vulnerability database assessment of impact on critical functions.	National incident response capability supports the establishment of sector-specific capabilities. Level of cooperation and collaboration with local, regional and international incident response teams with an objective of resource and information sharing. Assessment of the effectiveness of the CERT feeds into the resourcing of the CERT. Reporting of incidents occurring across sectors and response plans and corresponding recovery plans are tested.	National incident response capability is fully financially sustainable and politically supported, regardless of political transition. International cooperation aimed at shaping best practice among expert groups is consistently reviewed and approved.

D5-2: Cyber security coordinating organisations					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
			Information is shared consistent with response plans. Key stakeholders are aware of existing national CERTs and their responsibilities.	Forensics services are widely available for incident investigation and evaluation. Information sharing is voluntarily promoted among external stakeholders.	

D5-3: Cyber Security marketplace					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Cyber security Technologies	Few or no cyber security technologies are produced domestically, international offerings may be restricted or sold as a premium.	Security technology and processes in government and private sector are available and deployed. The domestic market may provide generic, non-specialised products; offerings are not market driven. Security considerations are now embedded in software and infrastructure.	Information technology control systems are created and managed. Domestic cyber security products are now being produced by local providers. Technologies are deployed in country to detect and record cyber-incidents, including sophisticated attacks. Advanced security technology and processes in sensitive enterprise networks are deployed to enable information exchange.	Cyber security technologies, including software, abide by secure coding guidelines, best practices and adhere to internationally accepted standards. Security technologies and processes across the government and private sectors are kept up-to-date, based on strategic risk assessment. This risk assessment also informs the application of market incentives toward prioritised products to mitigate identified risks. Domestic cyber security products are	Security features in software architecture are continuously updated as required. Security functions in software and computer system configurations are automated in the development and deployment of security solutions. National dependence on foreign technologies is increasingly mitigated through enhanced domestic capacity.

D5-3: Cyber Security marketplace					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
				exportedtoother nations and are considered superior products.	
Cyber Insurance	The need for a market in cyber insurance has not been identified through the assessment of financial risks for government and the private sector.	The need for a market in cybercrime insurance has been identified through the assessment of financial risks for public and private sector. Sharing of best practice in assessment and risk reduction, including the development and use of appropriate standards and varied products is now being discussed	Market for cyber insurance is established and encourages information sharing among participants; products suitable for SMEs are on offer.	Cyber insurance specifies a variety of coverages to mitigate consequential losses. These coverages are selected based on strategic planning needs and identified risk.	A vibrant, innovative and stable cyber insurance market exists and adapts to emerging risks. Planned risk reduction programmes are constantly reviewed and maintained. Insurance premiums are offered for consistent cyber-secure behaviour. Insurance products are aligned with dynamic applications of cyber security standards and practices.

D5-4: National Infrastructure Resilience					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Infrastructure Technology	Availability and affordability of reliable Internet services and infrastructure in the country, and adoption rates of those services are a concern but may not yet be established.	Technology and processes in government and private sectors are deployed, but not necessarily in a strategic manner. Government services, information and digital	Technology and processes deployed in the national infrastructure meet international IT guidelines, standards, and acceptable practices.	Rigorous security processes have been established across private and government sectors, especially for security risk management, threat assessment, incident	Acquisition of infrastructure technologies is affectively controlled, with flexibility incorporated according to changing market dynamics.

D5-4: National Infrastructure Resilience					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
	Technology to support e-commerce and business-to-business interactions is a concern but few or no coherent actions have been established.	content are provided online, but possibly to a limited extent. Cyber security processes are considered, but may not have been fully implemented.	Use of the Internet for communication between government and the population, between universities and the population, and within the population itself is integrated into everyday operating practice. Internet is used for business reliable e-commerce and electronic business interactions; authentication processes and measures are established	response and business continuity. Regular assessment of processes according to standards and guidelines are conducted together with assessment of national information infrastructure security, and drive investment in new technologies. Benefits to businesses from additional investment in technology with enhanced security are measured and assessed.	Costs for infrastructure technologies are continually assessed and minimised. Processes are fully automated, often incorporated into the technology itself, allowing IT to be aligned and managed according to the business needs.
National Resilience	Government has little or no control of its own technology infrastructure; networks and systems are outsourced, with potential adoption from unreliable third-party markets. There may be a dependence on other countries for cyber security technology.	National infrastructure is managed informally, with no documented processes, roles and responsibilities. There is regional support for cyber security technology and infrastructure in country.	National infrastructure is formally managed, with documented processes, roles and responsibilities, and limited redundancy. Regional support for cyber technologies is supplemented by a national programme for infrastructure development.	Risk-based management and best practices with formal vulnerability analysis is conducted. Assessments of national resilience for critical services are conducted to protect information systems and the operators of critical infrastructures.	There is affectively controlled acquisition of critical technologies with managed strategic planning and service continuity processes in place. High availability of critical technologies as part of the formal governance framework is mainstream. Scientific, technical, industrial and human capabilities are being systematically maintained, enhanced and perpetuated in order to maintain the

D5-4: National Infrastructure Resilience					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
					country's independent resilience

The Global Cyber Security Capacity Centre is funded by the United Kingdom Foreign and Commonwealth Office and hosted by the Oxford Martin School
Oxford Martin School, University of Oxford,
Old Indian Institute, 34 Broad Street, Oxford
OX1 3BD, United Kingdom

Tel: +44 (0)1865 287430 • Fax: +44 (0) 1865 287435
Email: cybercapacity@oxfordmartin.ox.ac.uk
Web: www.oxfordmartin.ox.ac.uk