CYBERSECURITY CAPACITY REVIEW

Republic of Iceland

November 2017

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

This review was conducted by the Global Cyber Security Capacity Centre, at the University of Oxford, at the request of the Ministry of Transport and Local Government in Iceland.

This report of the review is published by the Ministry of Transport and Local Government, Iceland, April 2018.

ISBN: 978-9935-494-00-9

CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: *Dr Maria Bada, Ms Carolin Weisser*

Reviewed by: *Professor Paul Cornish, Professor William Dutton, Professor Michael Goldsmith, Professor Basie von Solms*

Approved by: *Professor Michael Goldsmith*

LIST OF ABBREVIATIONS

(Icelandic names of Icelandic authorities and organisations are given in parenthesis)

APTA	Act on the Post and Telecom Administration
CA	Consumer Agency (Neytendastofa)
NATO CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CSC	Cyber Security Council (Netöryggisráð)
CEO	Chief Executive Officer
CERT-IS	Computer Emergency Response Team Iceland (Netöryggissveit Póst- og fjarskiptastofnunar, Netöryggissveitin)
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CMM	Cybersecurity Capacity Maturity Model
CNI	Critical National Infrastructure
CSIRT	Computer Security Incident Response Team
DoH	Directorate of Health (Embætti Landlæknis)
DPA	The Icelandic Data Protection Authority (Persónuvernd)
ECA	Electronic Communications Act
EEA	European Economic Area
ENISA	European Union Agency for Network and Information Security
EPC	European Patent Convention
EPO	European Patent Organisation
EU	European Union
FSA	Financial Supervisory Authority (Fjármálaeftirlitið)
GDPR	General Data Protection Regulation
GCSCC	Global Cyber Security Capacity Centre
ICRU	Iceland Crisis Response Unit (Íslenska friðargæslan)

ICT	Information and Communication Technologies
IDF	Iceland Defense Force (Varnarliðið á Íslandi)
ISP	Internet Service Provider
MoESC	Ministry of Education, Science and Culture (Mennta- og menningarmálaráðuneytið)
MFA	Ministry for Foreign Affairs (Utanríkisráðuneytið)
MoI	Ministry of the Interior (Innanríkisráðuneytið)
MoII	Ministry of Industries and Innovation (Atvinnuvega- og nýsköpunarráðuneytið)
MoJ	Ministry of Justice (Dómsmálaráðuneytið)
MoTLG	Ministry of Transport and Local Government (Samgöngu- og sveitarstjórnarráðuneytið)
MoU	Memorandum of Understanding
NCIP	National Commissioner of the Icelandic Police (Ríkislögreglustjóri)
NATO	North Atlantic Treaty Organisation
NCSS	National Cybersecurity Strategy
NIS Directive	The EU Network and Information Systems Security (NIS) Directive
OSCE	Organisation for Security and Cooperation in Europe
PTA	Post and Telecom Administration in Iceland (Póst- og fjarskiptastofnun)
RU	Reykjavík University (Háskólinn í Reykjavík)
SAFT	Safer Internet Centre Iceland
STPC	Science and Technology Policy Council (Vísinda- og tækniráð)
SMEs	Small and Medium Enterprises
UoI	University of Iceland (Háskóli Íslands)
WIPO	World Intellectual Property Organisation
WTO	World Trade Organization

EXECUTIVE SUMMARY

The Global Cyber Security Capacity Centre (GCSCC, or 'the Capacity Centre') has undertaken a review of the maturity of the cybersecurity capacity of the Republic of Iceland, hosted by Iceland's Ministry of Transport and Local Government (MoTLG). The objective of this review is to enable the government of Iceland to reassess its cybersecurity capacity in order to prioritise strategic investment in national cybersecurity.

Over the period 21–23 June 2017, stakeholders from the following sectors participated in a series of consultations with GCSCC staff: government departments and ministries, legislators and policy owners, criminal justice, law enforcement, academia, as well as the private and financial sectors.

The consultations were premised on the Capacity Centre's Cybersecurity Capacity Maturity Model for Nations (CMM)[1], which defines five dimensions of cybersecurity capacity:

- Policy and strategy
- Culture and society
- Education, training and skills
- Legal and regulatory frameworks
- Standards, organisations and technologies

Each dimension comprises a number of *factors* which, taken together, explain what it means to possess cybersecurity capacity. Factors are further subdivided into *aspects* and for each aspect there are *indicators*, setting out those conditions that define the level of *maturity* achieved in any given aspect. There are five *stages* of maturity, ranging from the *start-up* to the *dynamic*. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage is indicative of a strategic approach and the ability to adapt or change in response to environmental considerations. The five stages of the CMM are defined as follows:

- **Start-up:** At this stage either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence of cybersecurity capacity at this stage.
- **Formative:** Some aspects have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined – or simply new. However, evidence of this aspect can be clearly demonstrated.
- **Established:** The indicators of the aspect are in place, and functioning. However, there is not well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in this aspect. But the aspect is functional and defined.

[1] Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition

- **Strategic:** At this stage choices have been made about which indicators of this aspect are important, and which are less important for the particular organisation or state. The strategic stage reflects the fact that these choices have been made, conditional upon the state's or organisation's particular circumstances.
- **Dynamic:** At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technological sophistication of the threat environment, global conflict or a significant change in one area of concern (e.g. cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

Figure 1 below provides an overall representation of cybersecurity capacity in the Republic of Iceland and illustrates the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' is placed at the perimeter.

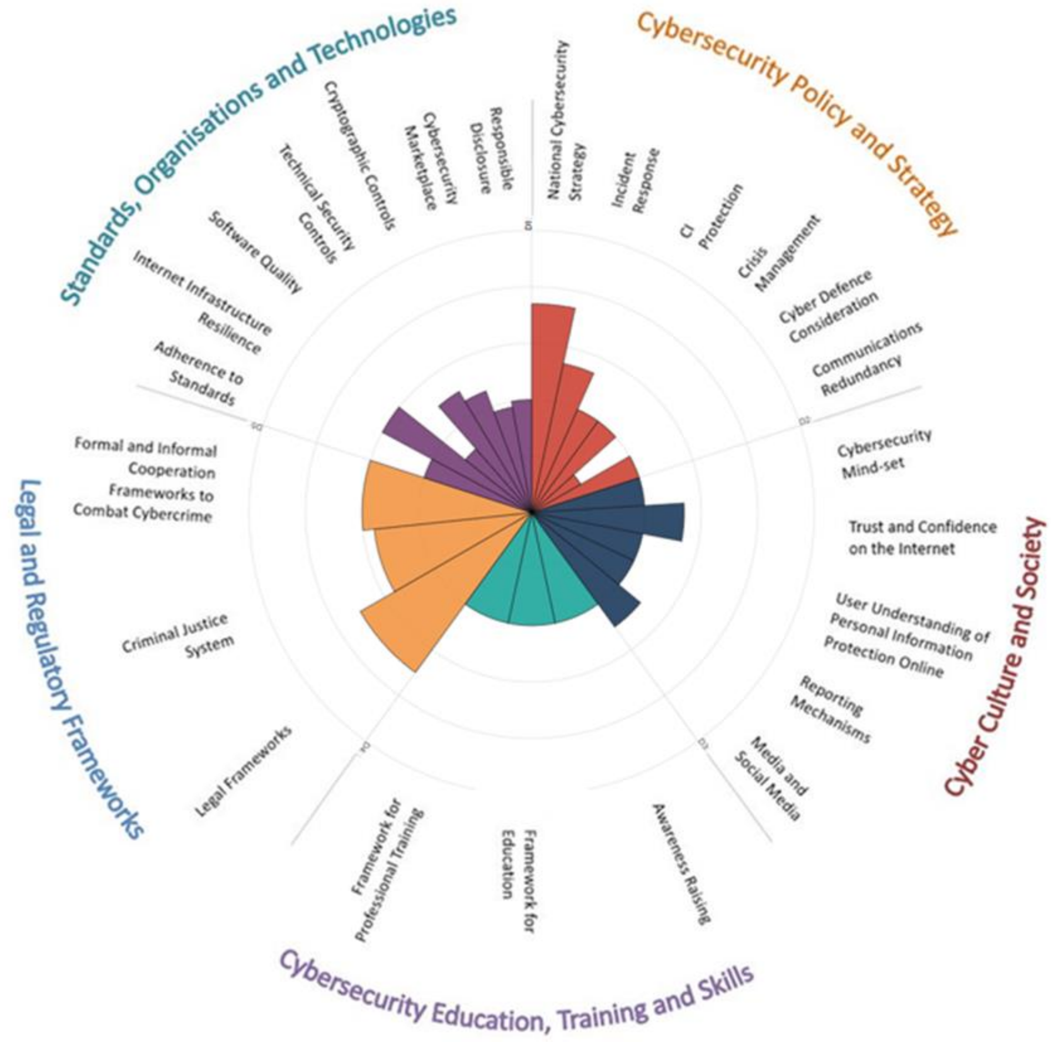

Figure 1: Overall representation of the cybersecurity capacity in the Republic of Iceland

Policy and Strategy

The *policy and strategy* dimension of cybersecurity capacity for Iceland was gauged to range from *start-up* to *established* stages of maturity.

The Republic of Iceland is at an established stage of maturity regarding the National Cybersecurity Strategy factor. Iceland has published the Icelandic National Cyber Security Strategy (NCSS) 2015-2026, approved by the Minister of the Interior in April 2015 together with a three year Plan of Action. The Ministry of the Interior (MoI) was divided into two new Ministries on 1 May 2017, the Ministry of Justice (MoJ) and the Ministry of Transport and Local Government (MoTLG). Since then MoTLG has been the designated coordinating body with a mandate to work towards the revision and the implementation of the National Cyber Security Strategy and the Action Plan and has started consulting across public and private sectors, and with civil society. The NCSS called for the appointment of a special Cyber Security Council (CSC) for government and public sector representatives and a Cyber Security Forum with representatives from private sectors in addition to the representatives in the CSC, in order to address collaboration on cybersecurity topics related to the implementation of the NCSS in Iceland.

Iceland's incident response capacity is at a *formative to established* stage of maturity. CERT-IS – Iceland's national CSIRT (Computer Security Incident Response Team) – has been established with specified roles and responsibilities with emphasis on the electronic communications market. In particular CERT-IS has the role of national point-of-contact, but does not at this time handle the Government CERT role. However, negotiations regarding this role are underway. CERT-IS has developed incident response processes, but these are and will not be publicly available. However, an incident response plan for Critical Information Infrastructure (CII) incidents has been published and distributed to members of the telecommunications sector. An overall central registry of national-level cybersecurity incidents is not yet operational. CERT-IS records incidents of all levels of severity that are reported to the group, but handling is prioritized by constituency, severity and impact. The registry of incidents is, however, not as of yet publicly accessible in any way. The National Commissioner of the Icelandic Police (NCIP) and CERT-IS aim to cooperate on creating a classification of national level incidents.

The members of CERT-IS receive training in an ad-hoc manner. Moreover, CERT-IS collaborates with Nordic countries (Denmark, Finland, Iceland, Norway and Sweden) through the Nordic National CERT Collaboration (NCC). A Nordic cybersecurity exercise took place in 2015 and assessed the quality of the incident response processes, procedures, interactions, and information-sharing mechanisms that exist under the NCC Agreement. Additionally, CERT-IS has good relations with the financial sector and aims to cooperate with a new collaborative forum, the Nordic Financial CERT.

The protection of critical infrastructure (CI) considerations are at a *formative* stage of maturity. A list of general CI assets has been created. The National Commissioner of the Icelandic Police (NCIP) is responsible for identifying these assets. However, the CI asset audit list is not disseminated to relevant stakeholders. Currently there is informal and ad-hoc threat and vulnerability disclosure among CI owners as well as between CI and the government, but the scope of reporting requirements has not been specified. CI owners have some capacity to detect, identify, respond to and recover from cyber threats, but such capabilities are uncoordinated and vary in quality.

No official national risk assessment plan has been developed as yet. The Civil Protection Act[2] is the official framework for all crisis situations, including cyber-incident or cyberattack. Simulations and training exercises have been conducted in order to better prepare for a cyber-crisis situation, however these exercises are not coordinated at the national level, with the active participation of all relevant stakeholders in all sectors.

Iceland's cyber defence considerations are at a *start-up* stage of maturity. Iceland's Cyber defence is mainly being considered in terms of national cyber resilience and the country is prioritising the protection of national CI assets as a priority action of the NCSS. Beyond that it is also part of Iceland's defence planning. The Ministry for Foreign Affairs is the central authority for defence and in charge of implementation of the Defence Act No 34/2008, due to the absence of a dedicated Ministry of Defence. In accordance with a Memorandum of Understanding (MoU) between the Ministry for Foreign Affairs and the Ministry of Interior - now Ministry of Justice, and due to the lack of a standing army, the Icelandic Coast Guard from July 2014 (ICG) is responsible for operational defence activities related to NATO including NATO Iceland Air Defence System, CRC, Host Nations Support and operation of the Keflavik Air Base. The Iceland Crisis Response Unit (ICRU) has been a separate entity within the MFA since 2001. Its main role is to contribute to multilateral organisations and to provide secondments of civilian experts to the field. Iceland has established contacts with the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) while material and resources prepared by the Centre, especially the Tallinn Manual, have already been utilised. In 2018, Norway will host NATO's high-visibility exercise Trident Juncture in which Iceland participates, as the defence of Iceland is an integral part of the exercise.

In the event of a communications disruption, mechanisms are in place to maintain the operational functionality of the national emergency communications network. Current emergency response assets have been identified. Within both the public and the private sectors, TETRA Systems for Mission Critical Communications are deployed. Furthermore, fibre optic lines and nodes are shared with the public network. The finance sector also conducts crisis response simulations regularly and emergency drills are tested frequently.

Culture and Society

During consultations, the national capacity regarding *cybersecurity culture and society* ranges from *formative* to *established* stages. The government has recognised the need to prioritise cybersecurity across its institutions, and the risks and threats in cybersecurity have influenced the processes and structures across government institutions but in particular leading agencies. Leading firms within the private sector have begun to place priority on a cybersecurity mind-set by identifying high-risk practices. Among society-at-large, a growing

[2] https://www.althingi.is/lagas/nuna/2008082.html (in Icelandic)
https://www.government.is/publications/legislation/lex/2017/12/21/Civil-Protection-Act-No.-82-2008/
(English translation)

number of users feel it is a priority for them to employ good cybersecurity practices. However, cultural aspects and the general level of trust, which is ingrained in the Icelandic culture, has inhibited users from thinking about privacy online and considering protection of their information online as their own personal responsibility.

Overall, the participating stakeholders accepted that most Internet users in Iceland trust in the security of the Internet, but this often approaches a "blind" trust that can place individuals and society at risk. However, strong trust has enabled the establishment of e-government services in Iceland. The Government continues to increase e-service provision and tax declarations are already being submitted electronically. In addition, e-commerce services are fully established by multiple stakeholders in a relatively secure environment.

Users and stakeholders within the public and private sectors have general knowledge about how personal information is handled online but (proactive) cybersecurity practices are often not used, either due to perceived inconvenience, or to the way people weigh up the trade-offs in service and protection of their personal information. Act No. 77/2000 on Privacy as regards to the Processing of Personal Data has been in force since 2000 and implements the provisions of Directive 95/46/EC. On grounds of Art. 11 and 12 of the Data Protection Act the Icelandic Data Protection Authority (DPA) has set forth Rules No. 299/2001 on the Security of Personal Data. Iceland is also in the process of implementing the EU General Data Protection Regulation (GDPR).

In Iceland, the public and private sectors provide some channels for reporting child abuse online, but these channels are not coordinated and are used in an ad-hoc manner. A hotline through Barnaheill - Save the Children Iceland - focuses on child abuse. Also, the Icelandic Red Cross runs the 1717 Helpline. Any incident, also cyber-related, can be reported via the police emergency number 112, while incidents such as child abuse are also referred to Europol and Interpol. Participants noted that communication links have not been established between the police and the private sector and CERT-IS lacks the resources to take up this role. Moreover, there is ad-hoc media coverage of cybersecurity, with limited information provided and limited reporting on specific issues that individuals face online, such as cyber-bullying. Also, discussions on social media about cybersecurity are not prominent.

Education, Training and Skills

Observations made during the consultations show that *cybersecurity education, training and skills* capacity in Iceland ranges from a *formative to an established stage of maturity*. Awareness-raising programmes, courses, seminars and online resources are available for target demographics from public, private, academia, and civil society sources. However, no national programme for cybersecurity awareness-raising, led by a designated organisation is currently established. The National Cybersecurity Strategy recognises the enhancement of general awareness of cybersecurity issues and this is one of the measures towards the implementation of the nation's Strategy. Executives are aware of general cybersecurity issues, but not necessarily aware of how these issues and threats might affect their particular organisation. Executives of some particular sectors, such as finance, telecommunications, Internet providers and cloud operators are aware of cybersecurity risks, and how their organisation deals with cybersecurity issues, but not of the broader strategic implications for government and society. However, apart from those in the financial sector there are no mandatory training courses or programmes.

In higher education, some courses exist in cybersecurity-related fields, such as information security, network security and cryptography, but cybersecurity-specific courses are not yet offered in Iceland. Some universities offer programmes in computer science and computer engineering at an undergraduate and postgraduate level with cybersecurity often being a module within these curricula.

The CSC has now established an informal agreement with the Department of Information Security and Communication Technology at NTNU, Norwegian University of Science and Technology, which is one of the most advanced in the field of information security in the Nordic countries. A part of this plan is to develop closer ties with UoI and RU, e.g. concerning graduate and undergraduate courses and also concerning events that can help to stimulate interest in cybersecurity and provide interesting challenges for students.

Research and development is an important consideration in education. The MoESC and the Ministry of Industries and Innovation (MoII) have the main responsibility for running the research and innovation scheme. However, it was not possible to identify whether specific programmes and research funds on cybersecurity or related fields are running currently.

At the national level, the need for training professionals in cybersecurity in Iceland has been documented. ICT professional certification with some security modules or components is available. Review participants mentioned that currently the Estonian Technology Fund, a state-run public institution that invests into young and growth-oriented technology companies, is dedicated to the provision of online courses because overall there is not enough expertise among educators to provide training in cybersecurity. Executive training courses for CEOs or chief financial executives are offered on an ad-hoc basis, including topics such as good governance practices related to cybersecurity and risk management.

Legal and regulatory frameworks

The *legal and regulatory frameworks* in Iceland range between *formative* and *established* stages of maturity. Iceland has implemented provisions relevant to cybersecurity comprehensively in its ICT legislative and regulatory frameworks. The Regulatory Framework of the European Union – through the country's EEA membership – applies in Iceland and has shaped many regulations and existing legislation to protect the rights of individuals and organisations in the digital environment. The *Electronic Communications Act (ECA) No. 81/2003*, the *Act on the Post and Telecom Administration (APTA) No. 69/2003*, and its *Amendment No. 62/2012* stipulate certain provisions regarding cybersecurity and critical information infrastructure. Additionally, the Icelandic Media Law requires providers to ensure that the transmission of service via electronic communications networks is secure (Article 45). *Act No. 30/2002 on Electronic Commerce and other Electronic Services* stipulates the liability of ISPs and establishes a system of takedown notices in certain cases for IP addresses or other online content that violates the law, in accordance with the Directive 2000/31/EC of the European Parliament.

Data protection legislation in Iceland has been implemented with the adoption of *Act No. 77/2000 on the Protection of Privacy as regards the Processing of Personal Data ("Data Protection Act")* which implements Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It includes general conditions for the collection of personal data and protection from misuse, and it promotes a practice of personal data processing in accordance with fundamental principles and rules regarding data protection and privacy.

Icelandic law recognizes fundamental human rights on the Internet, including privacy online, freedom of speech, freedom of information, and freedom of assembly and association. The country has also ratified or acceded to several international agreements, such as the *UN Universal Declaration of Human Rights*, the *Convention for the Protection of Human Rights and Fundamental Freedoms* of the Council of Europe, the *Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data* and those of the International Labour Organization and the Organization for Security and Co-operation in Europe.

Comprehensive legislation on the protection of children has been adopted and enforced according to Iceland's *Child Protection Act, No. 80/2002*. Iceland has ratified the UN Convention on the Rights of the Child and other relevant international conventions.

Substantive cybercrime legal provisions are contained in the general criminal law. In 2007 the country ratified the Council of Europe Convention on Cybercrime, also known as the 'Budapest Convention', whose recommendations are consistently implemented into domestic law. The General Penal Code No. 19 contains substantive cybercrime legal provision since its amendment in 2014. The government is working towards the implementation of the NIS Directive and the GDPR in 2018, therefore it is expected that existing gaps in legal and regulatory frameworks will be fulfilled.

Across the criminal justice system, capacities are at initial stages of development in Iceland. The police, headed by the National Commissioner of the Icelandic Police (NCIP), has only limited digital-forensics capacity and cases are investigated by the digital forensics unit of the Reykjavik Metropolitan Police. Two policemen in the Metropolitan Police are specifically assigned to investigate sexual violence against children on the internet. The country needs more skilled personnel as well as the procedural and technological resources to conduct investigations in a comprehensive way. Training for law-enforcement officers on cybercrime and digital evidence is ad-hoc or not specialised.

Formal mechanisms of international cooperation have been established in order to prevent and combat cybercrime. Iceland has established agreements with Interpol and Europol as well as agreements with neighbouring countries on cross-border information sharing. Moreover, informal relationships between government and criminal justice as well as between ISPs and law enforcement exist with clear communication channels resulting in the regular exchange of information on cybercrime cases. Some specialised cybercrime prosecutors have the capacity to build cases on electronic evidence, but this capacity is limited as training is largely ad-hoc, not institutionalised and informal.

According to participants, Iceland has fully acknowledged the need for formal and informal cooperation and has established mechanisms for international cooperation in order to prevent and combat cybercrime by facilitating its detection, investigation, and prosecution through established communication channels. The country cooperates with Interpol and Europol and other nations (e.g. Norway and the US) regarding cross-border information sharing and has signed Mutual Legal Assistance agreements which are successfully applied.

Standards, Organisations and Technologies

Iceland's capacity in *cybersecurity standards, organisations and technologies* was identified as ranging from *start-up* to *established* stages. The government and the private sector have adopted ICT security, procurement and software development standards and good practices, such as ISO. However, compliance to these standards is not mandatory. Iceland achieves leading scores in technological readiness and Internet access and broadband penetration is one of the highest internationally. Internet is used for e-commerce transactions. However, authentication processes are often weak, e.g. many websites only require simple authentication. There are legal requirements for operational security in articles 11-13 of the *Data Protection Act and Rules No 299/2001*; however, in a very broad sense. According to participants, telecommunication companies and other CNI have their own internal standards.

Software quality is a matter of concern. Priority is mostly given to the quality and performance of software. Additionally, monitoring and quality assessment is conducted in an ad-hoc manner only in few private institutions, so there is no evidence of the extent of software quality deficiencies.

All sectors in Iceland deploy up-to-date technical security controls, including patching and backups, but to very different levels. Companies have internal policies for updates and automated software updates are becoming more common. Cryptographic controls deployed meet international standards and guidelines exist for each sector accordingly. Although some state-of-the-art tools, such as SSL or TLS, are deployed routinely by web service providers to secure all communications between servers and web browsers, and EU legislation relating to data protection and e-signatures has been implemented (Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures) - or is being implemented respectively (GDPR) - participants pointed out a lack of understanding amongst the general public about the deployment of such controls. The implementation of the GDPR could provide more general understanding to the general public.

The domestic market in Iceland is small and only provides some specialised cybersecurity products, which are not demand-driven. Most organisations rely on products from international companies. Local suppliers of software and services such as penetration testing and auditing do consider cybersecurity. Cyber-insurance is offered by a domestic insurer who resells international products, but uptake is limited as the terms are often not suitable for local companies.

No vulnerability-disclosure framework is in place. Stakeholders mainly share technical details of vulnerabilities informally with other stakeholders, who can distribute the information more broadly; but this is not common. Currently, organisations have established their own processes and mechanisms to receive, disseminate and share information on vulnerabilities, and only some organisations are obliged to report to CERT-IS.

Additional Reflections

This was the 18th country review supported directly by the Global Cyber Security Capacity Centre at Oxford. It was intended to assist the Government of the Republic of Iceland to gain insights into the breadth and depth of the country's cybersecurity capacity. Iceland has commenced the process of developing different aspects of cybersecurity capacity across all dimensions, including through revising the National Cybersecurity Strategy and revisiting legal frameworks and regulation. The review suggests a number of specific steps by which Iceland's cybersecurity capacity might achieve greater levels of maturity.

INTRODUCTION

The Global Cyber Security Capacity Centre (GCSCC, or 'the Capacity Centre') has undertaken a review of the maturity of the cybersecurity capacity of the Republic of Iceland, hosted by the Ministry of Transport and Local Government. The objective of this review is to enable the government of Iceland to reassess its cybersecurity capacity in order to prioritise strategic investment in national cybersecurity.

Over the period 21–23 June 2017, stakeholders from the following departments of government, organisations and functional sectors participated in a three-day consultation with GCSCC staff to review Iceland's cybersecurity capacity:

- Public Sector Entities:
    - Ministry of Transport and Local Government
    - National Cybersecurity and Telecommunications Service under the Ministry of Transport and Local Government
    - Ministry of Agriculture
    - Ministry of Communications
    - Ministry of Education, Science and Culture
    - Ministry of Energy
    - Ministry of Environment / National Weather Service
    - Ministry of Finance
    - Ministry of Health
    - Ministry of Justice
    - Ministry for Foreign Affairs
    - Ministry of Industries and Innovation
    - Data Protection Authority
- Directorate of Health, Post and Telecommunications Administration
- Landspítali - National Hospital of Iceland
- Legislators/Policy owners/Public Prosecution
- CERT-IS
- Icelandic Coast Guard
- Finance sector
- Academia
- Private sector
- Internet registries

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were premised on the GCSCC Cybersecurity Capacity Maturity Model[3] for Nations (CMM) which is composed of five distinct dimensions of cybersecurity capacity. Each dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity therein. Table I below shows the five dimensions with their comprising factors:

DIMENSIONS	FACTORS
Dimension 1: Cybersecurity Policy and Strategy	D1.1 National Cybersecurity Strategy D1.2 Incident Response D1.3 Critical Infrastructure (CI) Protection D1.4 Crisis Management D1.5 Cyber Defence Consideration D1.6 Communications Redundancy
Dimension 2: Cyber Culture and Society	D2.1 Cybersecurity Mind-set D2.2 Trust and Confidence on the Internet D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Social Media
Dimension 3: Cybersecurity Education, Training and Skills	D3.1 Awareness-raising D3.2 Framework for Education D3.3 Framework for Professional Training
Dimension 4: Legal and Regulatory Frameworks	D4.1 Legal Frameworks D4.2 Criminal Justice System D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5: Standards, Organisations and Technologies	D5.1 Adherence to Standards D5.2 Internet Infrastructure Resilience D5.3 Software Quality Protection D5.4 Technical Security Controls D5.5 Cryptographic Controls D5.6 Cybersecurity Marketplace D5.7 Responsible Disclosure

[3] See Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition

STAGES OF CYBERSECURITY CAPACITY MATURITY

Factors are further subdivided into aspects and for each aspect there are indicators, setting out those conditions that define the level of maturity achieved in any given aspect. There are five stages of maturity, discussed below. The maturity scale ranges from the *start-up* stage, implying an elementary and ad-hoc approach to capacity, to the *dynamic* stage where a strategic approach has been articulated and where the relevant agencies and organisations have developed the ability to respond and adapt as environmental considerations demand. The five stages are as follows:

- **Start-up:** At this stage either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence of cybersecurity capacity at this stage.
- **Formative:** Some aspects have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined – or simply new. However, evidence of this aspect can be clearly demonstrated.
- **Established:** The indicators of the aspect are in place, and functioning. However, there is not well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in this aspect. But the aspect is functional and defined.
- **Strategic:** At this stage choices have been made about which indicators of this aspect are important, and which are less important for the particular organisation or state. The strategic stage reflects the fact that these choices have been made, conditional upon the state’s or organisation's particular circumstances.
- **Dynamic:** At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technological sophistication of the threat environment, global conflict or a significant change in one area of concern (e.g. cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

CYBERSECURITY CONTEXT IN ICELAND

Iceland has one of the highest take-ups of internet access in the world, with an Internet penetration rate of 98 percent in 2015[4]. This is the highest proportion of Internet users of all European countries; the average household internet penetration rate within the European Union was 81 percent in 2014[5]. With near ubiquitous access, Icelanders are frequent Internet users, with 95 percent of users connecting to the internet daily or almost daily, and 99 percent of users connecting every week in 2014[6]. Iceland also has one of the highest index rates of internet and social media usage (6.8) in the world, according to the World Economic Forum[7]. Specifically, 84 percent of the population use social networks, 95 percent read news online, 95 percent send or receive emails, 36 percent store electronic content online, and 66 percent use internet commerce[8].

Iceland is promoting free speech, while Internet and digital media play a vital role in Icelandic society. In 2010, the Icelandic parliament adopted a resolution Nr. 23/138 suggesting that Iceland should take a lead in protection of free speech and freedom of expression[9], but it has had limited follow-up. There was no change in the Internet freedom environment in 2016. The annual statistics database on telecommunication use in the Nordic and Baltic countries (2016)[10] show that Iceland is the only country where most of the fixed broadband connections are still via DSL technology. Something that will change until 2020 with the closing down of the PSTN network. During the GCSCC review, participants often referred to regulations, laws, activities, processes etc. which are either mandatory or recommended as a consequence of Iceland's membership of the European Economic Area (EEA), NATO and other organisations such as Interpol. As an EEA member state, Iceland is also part of the Digital Single Market strategy, the goal of which is both to develop the European Data Economy and to promote online platforms, protecting Europe's assets by tackling cybersecurity challenges[11]. This initiative includes the planned review of the EU Cybersecurity Strategy in September 2017 as well as additional measures addressing cybersecurity standards, certification and labelling to make connected users more cyber secure. These developments may have an impact on the action plan for the Icelandic National Cybersecurity Strategy.

[4] Freedom House: Freedom on the Net 2016. https://freedomhouse.org/report/freedom-net/2016/iceland

[5] International Telecommunication Union, "Percentage of individuals using the internet," 2015, 2013 & 2008, http://bit.ly/1cblxxY

[6] Statistics Iceland, "Statistical Yearbook of Iceland 2015," http://bit.ly/1QUsztW

[7] World Economic Forum, The Global Information Technology Report 2015, bit.ly/1yutYRc

[8] Statistics Iceland, "Statistical Yearbook of Iceland 2015," http://bit.ly/1QUsztW

[9] Þingsályktun um að Ísland skapi sér afgerandi lagalega sérstöðu varðandi vernd tjáningar og upplýsingafrelsis. http://www.althingi.is/altext/138/s/1392.html

[10] https://www.pfs.is/english/about-pta/news/news/2017/06/22/Nordic-and-Baltic-statistics-on-telecommunication-use-in-2016-Fast-increase-in-data-use-over-mobile/

[11] http://europa.eu/rapid/press-release_IP-17-1232_en.htm

REVIEW REPORT

OVERVIEW

This section provides an overall representation of cybersecurity capacity in Iceland. The graphic (Figure 1) shows the maturity estimates made in each dimension. The concentric gridlines radiating from the centre of the graphic correspond to the five-stage maturity scale, with 'start-up' the closest to the centre and 'dynamic' the furthest. The stages of maturity for each factor extend out from the middle as an individual bar, and each colour-coded dimension covers one fifth of the graphic.

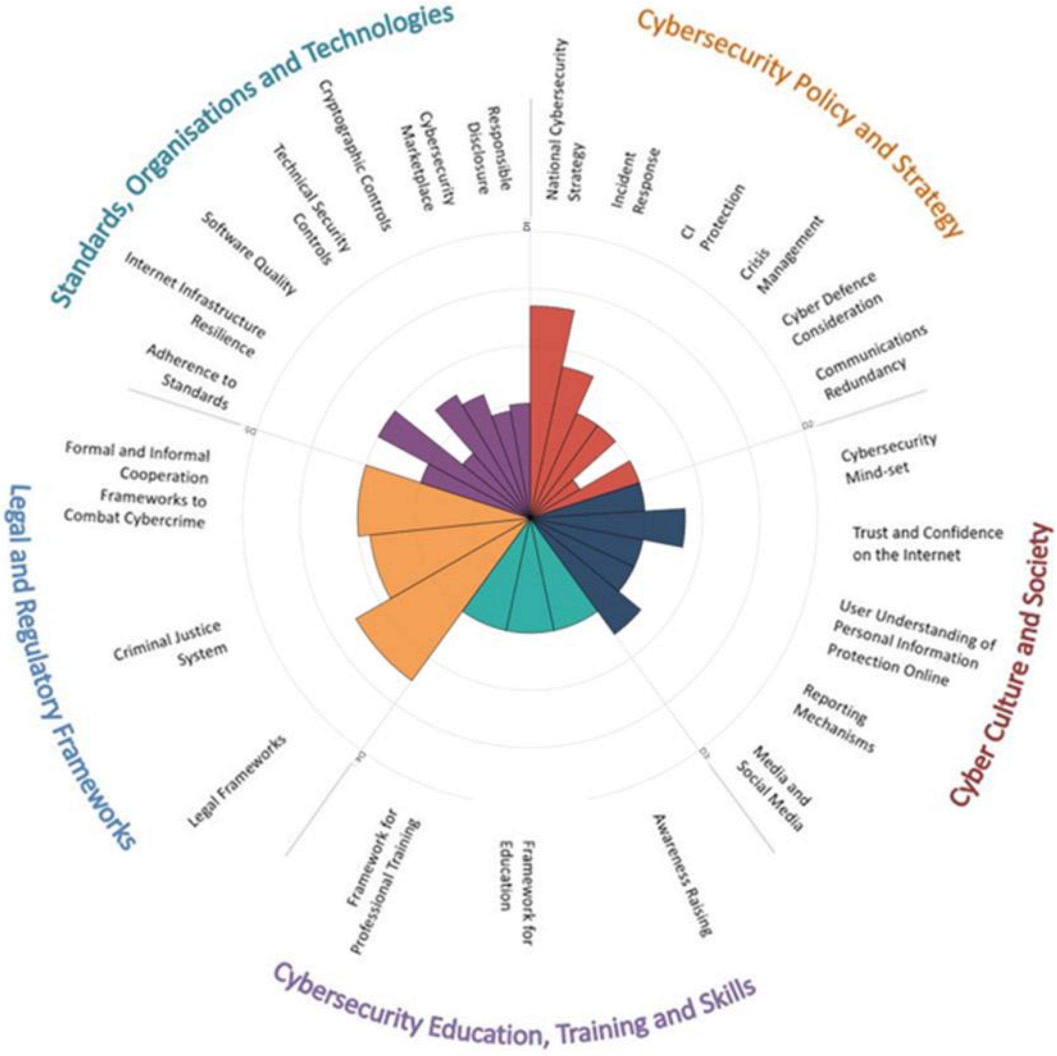

Figure 1: Overall representation of the cybersecurity capacity in the Republic of Iceland

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

Dimension 1 gauges the Icelandic capacity to develop and deliver cybersecurity policy and strategy and to enhance cybersecurity resilience through improvements in incident response, crisis management, redundancy, and critical infrastructure protection capacity. The Cybersecurity Policy and Strategy dimension also includes consideration of early warning, deterrence, defence and recovery. This dimension assesses the effectiveness of policy in advancing national cyber defence and resilience capacity, while facilitating the access to cyberspace increasingly vital for government, international business and society in general.

D1.1 NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to the coordination and direction of the government's cybersecurity agenda. A cybersecurity strategy makes it possible to prioritise cybersecurity as a critically important policy area, determines responsibilities and mandates of key cybersecurity government and non-governmental actors, and directs necessary and appropriate allocation of resources to emerging and existing cybersecurity issues and priorities.

Maturity Stage: **Established**

With the approval of the Ministry of the Interior (MoI), the Republic of Iceland's National Cybersecurity Strategy (NCSS) 2015-2026 was published in April 2015[12] together with a three year Plan of Action. A task force on cyber security had been set up in 2013 to provide recommendations and formulate the Strategy. Strategies of other Nordic and European countries were also examined alongside discussions with overseas peers.

The task force also discussed the threats and opportunities that have been identified and the experience gained from the plans of action already been put into practice in other Nordic and European countries.

[12] https://www.government.is/media/innanrikisraduneyti-media/media/frettir-2015/Icelandic_National_Cyber_Security_Summary_loka.pdf

Multi-stakeholder consultation processes have been followed and observations fed back to the identified strategy owners. A well-attended consultative meeting with stakeholders was held in 2014 including about representatives of some 60 institutions and enterprises.

The NCSS called for the appointment of a special Cyber Security Council (CSC) for government and public sector representatives and a Cyber Security Forum with representatives from private sectors in addition to the representatives in the CSC. The CSC takes responsibility for implementing the strategy while the Cyber Security Forum is charged with coordinating projects involving public and private stakeholders and creating the basis for collaboration on cybersecurity topics. The CSC will coordinate measures, particularly those involving government bodies. It will review the action plan at least once a year and make proposals on the prioritisation and funding of measures taken. The CSC is according to the NCSS to submit a report to the MoI every year on the implementation of the strategy.

The MoI was divided into two new ministries on 1 May 2017, the Ministry of Justice and the Ministry of Transport and Local Government (MoTLG)[13]. Since then the Ministry of Transport and Local Government (MoTLG) has been the designated coordinating body with a mandate to work towards the revision and the implementation of the National Cyber Security Strategy and the Action Plan and has started to consult across public and private sectors, and with civil society. The scope of responsibility of the MoTLG is as follows: air, land, and sea transport; electronic communications; information society issues; local government issues; regional development issues; and matters relating to Registers Iceland.

A review process (every 3-4 years) is implemented under the auspices of the Action Plan 2015-2018 to allow for new or revised measures, including for short periods of time.

The content of the NCSS is linked explicitly and directly to national assessments of risks, priorities and objectives, as well as business development. Direct and indirect links exist to many other official strategies and resolutions, e.g. the national strategy on civil protection public security, law enforcement and telecommunications; the strategy on national security; and the Icelandic State and Municipal Policy on the Information Society 2013-2016: “e-Power Expansion: - create, connect, participate“.

The NCSS addresses the need to protect critical infrastructure as well as respond to growing cybersecurity threats. It outlines Iceland’s cybersecurity vision out to 2026 and stipulates four main objectives: 1) increased capacity to prevent and respond to cybersecurity threats; 2) increased resilience; 3) improved legislation in line with international commitments; and 4) reliable law enforcement as regards cybersecurity.

The strategy covers all use of the Internet and Information Technology. The aims of the strategy are as follows: a) to enhance the security of individuals and groups in society by increasing cyber security; b) to promote the integrated functioning of important elements of the infrastructure of society by increasing the resilience of information systems to cope with hazards; and c) to establish closer collaboration and coordination on cybersecurity between Icelandic and international authorities.

[13] https://www.government.is/news/article/2017/05/01/Two-new-ministries-commence-operation/

As mentioned above, the strategy is intended to form the basis of collaboration and development in cybersecurity. The strategy itself will not amend the responsibilities and duties of those involved in cybersecurity even though proposals may be made for measures that may involve changes in these areas.

D1.2 INCIDENT RESPONSE

This factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, coordinate, and operationalize incident response.

Maturity Stage: Formative to Established

A National CSIRT (Computer Security Incident Response Team), CERT-IS[14] has been established with specified roles and responsibilities. CERT-IS has, according to law, the telecommunication sector as its primary constituency which includes certain critical information infrastructure (CII) entities. Other CII entities may sign contracts with CERT-IS. Other entities, outside the primary constituency, are served on best-effort terms.

The role of CERT-IS is to analyse cybersecurity threats and to give assistance to its primary constituency members using both proactive and reactive measures to prevent cybersecurity incidents and to minimize their impact. CERT-IS gives advice regarding threats and responses to its primary constituency members and publishes public warnings when needed.

According to the participants, each sector is responsible for handling conventional emergencies and preparing accordingly. The approach taken for cybersecurity is similar and an agreement with the national CERT-IS[15] has been made that cyber emergencies with national significance will be prioritised.

In the event of a cyber crisis the role of CERT-IS is to coordinate responses. As a National CSIRT, CERT-IS is the national point of contact in Iceland. The legal provisions for CERT-IS are stated in the Telecommunication Act no. 81/2003[16], art. 47a and regulation no. 475/2013[17] (see also D4.1).

No Government CERT exists yet. CERT-IS acts as a national CERT and in particular has the role of national point-of-contact, but does not at this time handle the Government CERT role. However, negotiations regarding this role are underway.

[14] https://www.cert.is/en/node/2.html
[15] https://www.cert.is/en/node/2.html
[16] http://www.althingi.is/lagas/nuna/2003081.html#G47A
[17] https://www.stjornartidindi.is/Advert.aspx?ID=f5282f2a-6827-4d98-9fc2-0afd611243d6

CERT-IS has developed incident response processes, but these are and will not be publicly available. However, an incident response plan for CI incident has been published and distributed to members of the telecommunications sector. Moreover, some participants referred to the lack of a catalogue of services provided by CERT-IS, but the position of CERT-IS as national CERT is that it should not provide a catalogue of services but a role defined by law. Defining the role of CERT-IS more precisely was a key element in ongoing service contract negotiations during the summer of 2017. Leads for incident response have been designated at the operational level, but national-level coordination has not yet been established. Distinct and formal security roles and responsibilities are not yet allocated across government, critical infrastructure, enterprise, and individual systems.

An overall central registry of national-level cybersecurity incidents is not yet operational. CERT-IS records incidents of all levels of severity that are reported to the group, but handling is prioritized by constituency, severity and impact. The registry of incidents is, however, not as of yet publicly accessible in any way. The National Commissioner of the Icelandic Police (NCIP) and CERT-IS are currently discussing an official classification scheme for CI incidents. Participants informed us that through the implementation of the EU NIS Directive, official classification will take place of national level incidents which expose vulnerabilities of national critical assets. The NCIP and CERT-IS aim to cooperate on creating a classification of national level incidents.

CERT-IS employees that work on incident handling and analysis receive mostly training in an ad-hoc manner, but baseline training requirements have been established. Budget restraints do limit the availability of training, but CERT-IS does take advantage of lower cost training opportunities that present themselves, for instance trough the Nordic National CERT Collaboration (NCC)[18]. Review participants indicated that human and financial resources allocated to incident response are not adequate to the cybersecurity threat environment and that incident response is still more reactive than anticipatory.

CERT-IS is not a member of FIRST yet, but preparation for FIRST and Trusted Introducer memberships is on the roadmap for 2018. Currently the service of CERT-IS is limited to the telecommunications sector but service contracts are being negotiated with the energy sector and planned with other sectors. In particular, CERT-IS has good relations with the financial sector and aims to cooperate with the planned Nordic Financial CERT.

Representatives from the finance sector indicated that an information-sharing platform (currently functioning by email) already exists for incidents-events experienced by banks. There was general agreement among different sector participants that the involvement of CERT-IS in this process would advance its capacity. CERT-IS notes that all opportunities for cooperation and information sharing are welcomed and one project in cooperation with a financial institution is currently under way.

Moreover, CERT-IS collaborates with the Nordic countries (Denmark, Finland, Iceland, Norway and Sweden) through the NCC cooperation. This includes technical cooperation and cybersecurity exercises to assess and strengthen cyber preparedness, examine incident response processes and enhance information sharing in the region. A Nordic cybersecurity

[18] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

exercise took place in 2015 and assessed the quality of the incident response processes, procedures, interactions, and information-sharing mechanisms that exist under the NCC Agreement.

The Data Protection Act as it is today does not require reporting of security breaches but the DPA still receives a few informal reports every year. Most knowledge of incidents concerning personal data is gathered through the media and individuals that are affected by such incidents.

Under the NCSS, the reporting of cybersecurity incidents is to be made obligatory as it is considered to be crucial for organisations that suffer a cyberattack. Review participants stated that the EU NIS Directive and the GDPR implementation will lead to the formalisation of a mechanism for incident reporting.

D1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

This factor studies the government's capacity to identify Critical Infrastructure (CI) and Critical Information Infrastructure (CII) assets and the risks associated with them, to engage in response planning and critical assets protection, to facilitate quality interaction with CI asset owners, and to enable comprehensive general risk management practice including response planning.

Maturity Stage: Formative

The protection of critical infrastructure from cyber-threats is a priority for the Icelandic authorities. The National Cybersecurity Strategy (NCSS) aims to promote the integrated functioning of important elements of the infrastructure of society by increasing the resilience of cyber systems to cope with hazards.

The Parliamentary Resolution on a National Security Policy for Iceland (no. 26/145)[19] speaks to Iceland's independence and sovereignty, territorial integrity, the safety of its citizens, and the protection of its governmental system and social infrastructure.

A list of general critical infrastructure (CI) assets has been created[20]. The National Commissioner of the Icelandic Police (NCIP) is responsible for identifying these assets. In the course of the CMM review it was mentioned that NCIP is currently in the process of developing a list of Critical Information Infrastructure (CII) assets as part of preparing the NIS Directive implementation.

[19] https://www.government.is/media/utanrikisraduneyti-media/media/Varnarmal/National-Security-Policy-ENS.pdf

[20] This has e.g. been published in the National Civil Protection Strategy (in Icelandic): https://www.stjornarradid.is/media/forsaetisraduneyti-media/media/frettir2/stefna-i-almannavarna-og-oryggismalum2015-2017.pdf

However, the CI asset audit lists is not disseminated to relevant stakeholders. Consequently, participants observed that formal internal and external CI communication strategies should be defined across sectors, with clear points of contact.

The scope of services by CERT-IS has been limited to the telecommunications sector, but it is currently being expanded to include other CI sectors as well. Currently, there is informal and ad hoc threat and vulnerability disclosure among CI owners as well as between CI and the government, but the scope of reporting requirements has not been specified. CERT-IS has not yet had the opportunity to coordinate information sharing between CI owners due to the lack of service contracts that limit the size and scope of its constituency. However, within the finance sector a specific timeframe for disclosure of incidents has been defined (as soon as possible but no later than 24h) (see D5.7).

Participants mentioned the Global Influenza Preparedness Plan[21] as an example of how the country could prepare for the organisation and coordination of responses to cyber incidents.

CI owners have the capacity to detect, identify, respond to and recover from cyber threats, but such capabilities are uncoordinated and vary in quality. Protection of CI assets includes basic level cybersecurity awareness and data security policies, but no protection processes have been agreed. Representatives from the finance sector mentioned that they have their own plans in the case of national level crisis. In addition, the Financial Supervisory Authority (FSA)[22] aims to safeguard the integrity and sound operation of the financial market and conducts periodic examinations of the operation of the stock exchanges[23].

The NCIP has developed a general response plan for responding to emergencies and it also has provisions for reacting to cyber-induced national level emergencies. CERT-IS has also developed an emergency plan for the telecommunication sector, which scope is at the present time mostly limited to defining the channels of communications and management process during a cyber crisis.

[21] http://www.landlaeknir.is/servlet/file/store93/item19632/Pandemic%20Influenza%20Preparedness%20Plan_March.06_.pdf
[22] https://en.fme.is
[23] https://en.fme.is/media/utgefid-efni/FME-arsskyrsla-2016-ENSKA-29072016.pdf

D1.4 CRISIS MANAGEMENT

This factor addresses crisis management planning, the conduct of specialised needs assessments, training exercises, and simulations that produce scalable results for policy development and strategic decision-making. Through qualitative and quantitative techniques, cybersecurity evaluation processes aim to produce structured and measurable results that would solicit recommendations for policymakers and other stakeholders and inform national strategy implementation as well as inform budgetary allocations

Maturity Stage: Formative

A preliminary cybersecurity needs assessment of measures and techniques that require testing has been undertaken. CERT-IS has conducted limited scope exercises for the telecommunications sector and such exercises are planned every other year. Key stakeholders and other subject matter experts, such as think tanks, academics, civil leaders and consultants are included in the planning process.

No official national risk assessment plan has been developed as yet. The Civil Protection Act[24] is the official framework for all crisis situations, including cyber-incidents and cyberattacks. Simulations and training exercises have been conducted in order to better prepare for a cyber-crisis situation, however these are not nationally coordinated exercises involving relevant stakeholders in all sectors.

CERT-IS plans to conduct exercises for each constituency sector every two years and exercises have already been conducted with the telecommunications sector. CERT-IS participates along with the constituency sectors in larger international exercises, such as the ones held by ENISA, and the Norwegian 'BlackScreen' exercise with the energy sector. Moreover, telecommunications companies participate in risk assessment exercises conducted by ENISA[25]. The finance sector also conducts exercises and crisis simulations. However, one of the sectors that is not participating in such simulations and cyber training activities is the health sector. This is expected to change since the Directorate of Health is now a member of the Cyber Security Council and will participate is future exercises.

[24] https://www.althingi.is/lagas/nuna/2008082.html (in Icelandic)
https://www.stjornarradid.is/publications/legislation/lex/2017/12/21/Civil-Protection-Act-No.-82-2008/ (English translation)

[25] https://www.enisa.europa.eu/topics/cyber-exercises

D1.5 CYBER DEFENCE CONSIDERATION

This factor reviews the government's capacity to design a cyber defence strategy and lead its implementation, including through a designated cyber defence organisation. It also reviews the level of coordination between various public and private sector actors in response to malicious attacks on strategic information systems and critical national infrastructure.

Maturity Stage: Start-up

Iceland's Cyber defence is mainly being considered in terms of national cyber resilience (see D1.3) and the country is prioritising the protection of national CI assets as a priority action of the NCSS. Beyond that it is also part of Iceland's defence planning. Following, we present the country's structure on defence related issues.

The Ministry for Foreign Affairs is the central authority for defence and in charge of implementation of the Defence Act No 34/2008[26], due to the absence of a dedicated Ministry of Defence. The Minister for Foreign Affairs formulates the defence policy within the framework of this Act and is responsible for the performance of a threat assessment regarding defence. The Minister is also responsible for the formulation and implementation of Iceland's Security and Defence Policy on the international arena and for representing the Government of Iceland in relations and cooperation with foreign states, military authorities and international security and defence organisations, including the North Atlantic Treaty Organisation. The Act does not apply to governmental matters that are civil in nature, such as policing and civil defence. Review participants noted that cybersecurity and defence is already being incorporated in national defence planning. This is now part of the formal agenda of national defence.

In accordance with a Memorandum of Understanding (MoU) between the Ministry for Foreign Affairs and the Ministry of Interior, now Ministry of Justice, and due to the lack of a standing army the Icelandic Coast Guard from July 2014 (ICG) is responsible for operational defence activities related to NATO, including NATO Iceland Air Defence System, CRC, Host Nations Support and operation of the Keflavik Air Base.

The Iceland Crisis Response Unit (ICRU)[27] has been a separate entity within the MFA since 2001. Its main role is to contribute to multilateral organisations and to provide secondments of civilian experts to the field.

The Iceland Defence Force (IDF) was a military command of the United States Armed Forces from 1951 to 2006. The IDF, created at the request of NATO, came into existence when the United States signed an agreement to provide for the defence of Iceland. The IDF also included civilian Icelanders and military members of other NATO nations.

[26] https://www.government.is/topics/foreign-affairs/national-security/
[27] https://www.government.is/topics/foreign-affairs/icru/

Iceland has established contacts with the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE)[28] while material and resources prepared by the Centre, especially the Tallinn Manual[29], have already been utilised. In 2018, Norway will host NATO's high-visibility exercise Trident Juncture[30] in which Iceland participates, as the defence of Iceland is an integral part of the exercise.

Iceland has excellent HAZMAT response to industrial accidents and has established a well-respected search and rescue (SAR) system, staffed by volunteers nationwide. In October 2016 the Government of Iceland signed the new MoU on cyber defence cooperation with NATO[31].

D1.6 COMMUNICATIONS REDUNDANCY

This factor reviews a government's capacity to identify redundancy within digital and non-digital data management and communications systems. Digital redundancy implies a cybersecurity framework in which duplication and failure of any component is safeguarded by frequent and effective backup. Most of these backups will use digital networks that are readily available but are also isolated from mainline systems. Redundancy in communications systems can be achieved by supporting a digital communications network with a radio communications network.

Maturity Stage: **Formative**

In the event of a communications disruption, mechanisms are in place to maintain the operational functionality of the national emergency communications network. Current emergency response assets have also been identified.

Stakeholders convene to identify gaps and overlaps in emergency response asset communications and authority links. Emergency response assets, priorities and standard operating procedures are mapped and identified in the event of a communications disruption at any node in the emergency response network.

Within both the public and the private sectors, TETRA Systems for Mission Critical Communications are deployed. In addition, fibre-optic nodes and cables are shared with the public network. An incident occurred involving the TETRA system in the past, which led to hardening the security of the system.

The finance sector also conducts crisis response simulations regularly and emergency drills are tested frequently.

[28] https://ccdcoe.org/about-us.html
[29] https://ccdcoe.org/tallinn-manual.html
[30] https://forsvaret.no/en/exercise-and-operations/exercises/nato-exercise-2018
[31] http://www.nicp.nato.int/iceland-signs-new-mou-on-cyber-defence-cooperation/index.html

RECOMMENDATIONS

The Global Cyber Security Capacity Centre offers the following recommendations for consideration by the Government of the Republic of Iceland. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the GCSCC Cybersecurity Capacity Maturity Model. Recommendations (R1.1 etc.) are grouped according to the respective factor.

NATIONAL CYBERSECURITY STRATEGY

R1.1 Ensure that the National Cybersecurity Strategy content includes, at a minimum: explicit links to national risks, priorities, objectives, and business development, raising public awareness, mitigating cybercrime, and protecting critical infrastructure from external and internal threats.

R1.2 Encourage the promotion and implementation of the National Cybersecurity Strategy by multiple stakeholders across government and other sectors.

R1.3 Administer a discrete cybersecurity budget line in order to allocate and manage resources.

R1.4 Conduct regular scenario and real-time cyber exercises that provide a concurrent picture of national cyber resilience.

R1.5 Collect and evaluate relevant metrics, monitoring processes and data in order to inform decision-making.

R1.6 Include in the NCSS provision for the protection of critical infrastructure from insider threats.

INCIDENT RESPONSE

R1.7 Develop an operational central registry of national level cybersecurity incidents and implement guidelines of the GDPR and the NIS.

R1.8 Improve incident identification and analysis in response and conduct regular, systematic updates to the national level incident registry.

R1.9 Ensure that the human and financial resources allocated to incident response are adequate to the cybersecurity threat environment by conducting regular scenario exercises designed to test human, organisational and financial capacities.

R1.10 Promote coordinated national incident response between public and private sectors, with lines of communication prepared for times of crisis.

R1.11 Develop a culture of risk assessment and management predictive methods to assess risk, its propagation and its aggregation for the national and CI domains.

R1.12 Establish mechanisms for regional and international cooperation for incident response between organisations to resolve incidents as they occur.

R1.13 Promote a platform for the reporting and sharing of incidents across sectors.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.14 Perform detailed audits of CI assets as it relates to cybersecurity on a regular basis and disseminate CI asset audit lists to relevant stakeholders.

R1.15 Implement regular audit practices to assess network and system dependencies to inform continuous reassessment of risk portfolio. Identify and establish specific auditing processes.

R1.16 Develop a strategy for strengthening formal coordination regarding Critical National Infrastructure (CNI) and information sharing between public and private sector.

R1.17 Establish a mechanism for regular vulnerability disclosure with defined scope for reporting incidents between CI asset owners and the government.

R1.18 Promote strategic engagement between government and CI.

R1.19 Define formal internal and external CI communication strategies across sectors, with clear points of contact.

R1.20 Optimize the legal framework concerning CNI by amending existing legislation or enacting new regulations as needed to encompass incident prevention, detection and response.

R1.21 Continue to invest in capability of Board Members and Senior Leaders of CI organisations to understand cyber-risk intelligence, in both private and public sectors, so that relevant individuals can lead in the face of crisis and take their part in risk management more generally.

R1.22 Use CI risk management procedures to create a national response plan including the participation of all vital entities.

CRISIS MANAGEMENT

R1.23 Prioritise crisis management exercises, especially at a local level, and communicate the value of these exercises to all sectors.

R1.24 Conduct compromised communications scenarios and exercises to test emergency response asset interoperability and effective functionality and incorporate the results of the exercises to inform strategic investment in future emergency response assets.

R1.25 Plan the exercises by engaging relevant participants, outlining their role in the exercise, and articulating the benefits and incentives for participation.

CYBER DEFENCE CONSIDERATION

R1.26 Review compliance of the National Security Strategy with international law and its consistency with national and international rules of engagement in cyberspace.

R1.27 Form a formal Research Cluster comprised by stakeholders from Government, Academia and Intelligence working on national cyber resilience. This Cluster will be working towards resilience on national CI (see D1.3).

R1.28 Initiate discussions regarding the membership to NATO CCDCOE and participation to exercises.

COMMUNICATIONS REDUNDANCY

R1.29 Undertake outreach to, and education of key stakeholders in the need for digital and communications redundancy.

R1.30 Test the interoperability and function of emergency response assets under compromised communications scenarios to inform strategic investment in future emergency response assets based on the results of these scenario exercises.

R1.31 Allocate resources to hardware integration, technology stress testing, personnel training and crisis simulations drills.

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

Forward-thinking cybersecurity strategies and policies entail a wide array of actors, including Internet users. All actors and Internet users need to understand the role they can play in safeguarding sensitive and personal data as they use digital media and resources. This dimension underscores the centrality of all users in achieving cybersecurity, but seeks to avoid conventional tendencies to blame users for the challenge of cybersecurity. Instead, cybersecurity experts need to build user-friendly operating systems and programs that can be incorporated in everyday practices online.

This dimension reviews elements of a responsible cybersecurity culture and society such as the understanding of cyber-related risks by all actors, developing a learned level of trust in Internet services, e-government and e-commerce services, and users' understanding of how to protect personal information online. This factor also entails the existence of mechanisms for accountability, such as channels for users to report threats to cybersecurity. In addition, this factor reviews the role of mass media and social media in helping to shape cybersecurity values, attitudes and behaviour.

D2.1 CYBERSECURITY MIND-SET

This factor evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society-at-large. A cybersecurity mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

Maturity Stage: Formative

The government has recognised the need to prioritise cybersecurity across its institutions, and the risks and threats have influenced the processes and structures across government institutions but in particular leading agencies.

According to review participants, increasing awareness-raising efforts concerning risks and threats exist, but there is a general lack of knowledge on the specific actions necessary. Training and education for public services on IT and cybersecurity is available, e.g. through the Information Society Project (see 3.3). However, this training programme is not mandatory for all employees. Another concern noted by participants is the fact that such programmes are neither coordinated nor long term, and therefore it is difficult for employees to retain the knowledge received.

Another general concern expressed in interviews was that employees within the public sector do not always follow specific online safety measures such as locking their computer, updating passwords, and not sharing passwords. For example, participants noted that mandatory password update was introduced last year within ministries, and that this has enhanced the understanding and cybersecurity awareness of employees. Moreover, physical penetration testing is now being introduced within some government institutions.

Leading firms within the private sector have begun to place priority on a cybersecurity mind-set by identifying high-risk practices. Programmes and materials have been made available to train and improve cybersecurity practices. For example, the finance sector is organising trainings for its employees. Also, the energy sector is participating in exercises with Norway in order to promote the understanding of risks to employees. However, participants noted that the private sector needs to ensure trust in their services by their customers, but that this is difficult when many Small and Medium Enterprises (SMEs) do not have sufficient resources to allocate more to cybersecurity.

Individuals across society-at-large inconsistently adopt a cybersecurity mind-set, but according to stakeholders, there is a shift towards a more proactive approach to cybersecurity. There was a general sense that a growing number of users feel it is a priority for them to employ good cybersecurity practices. However, cultural aspects and a generally high level of trust, which is ingrained in the Icelandic culture, can inhibit users from thinking about protecting their privacy online and making protection of their personal information online their own responsibility. Phishing attacks were an example used to better express this problem. Participants noted that phishing click rates are very high when the attacks are written in Icelandic, due to the fact that users trust these more than a phishing email in English. Users are not aware that they are part of a security chain and they need to share not only the benefits of the Internet but also responsibilities for a safe Internet.

D2.2 TRUST AND CONFIDENCE ON THE INTERNET

This factor reviews the level of user trust and confidence in the use of online services in general, and e-government and e-commerce services in particular.

Maturity Stage: Formative to Established

Overall, the participating stakeholders accepted that a limited proportion of Internet users critically assess what they see or receive online or consider that they have the ability to use the Internet and protect themselves online. Moreover, a limited proportion of users trust in the secure use of the Internet based on indicators of website legitimacy.

Operators of Internet infrastructure are developing measures to promote trust in online services but have yet to implement them.

As mentioned above Internet users in Iceland trust in the security of the Internet without basing that trust on website legitimacy. Their trust is too often an overly confident “blind” trust. People like the convenience of online services and either do not understand what secure browsing is, for instance, or they do not fully understand the risks that are associated with insecure Internet provision. Users do not necessarily lock their PCs and usually behave online much like they act in their everyday life, which is shaped by a general sense of trust that is characteristic of the Icelandic culture. Participants noted that identity theft is not considered a problem for the majority of users. According to the General Penal Code No. 19/1940 (see D4.1) identify theft is not criminalised unless it is used for unlawful purpose and practises.

E-government services have been firmly established in Iceland. The Government continues to increase e-service provision and tax declarations are already being submitted electronically. The government, along with other stakeholders and users, recognise the need for the application of security measures to establish trust in these services. However, participants noted that users trust in e-government services ‘’by default’’ as they do in other government services. The implementation of the EU General Data Protection Regulation (GDPR) and the NIS Directive will ensure security and data protection provisions for e-governance services. Thus, user trust in e-services is also expected to be strengthened among users.

Electronic certificates for authentication and two-factor authentication for document signing are being promoted and utilized broadly within the public sector.

E-commerce services are fully established by multiple stakeholders. Security solutions are updated and reliable payment systems have been made available. A growing proportion of users trust in the secure use of e-commerce services and the private sector promotes use of e-commerce services and trust in these services. Participants claimed that, generally, online-banking and other commercial services from local suppliers are being used; but that foreign services, such as Amazon, are used and trusted more.

D2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

This factor looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protection of personal information online, and whether they are sensitised to their privacy rights.

Maturity Stage: Formative

Iceland has adopted and enforced data protection legislation such as the Data Protection Act, No. 77/2000 which lays out general conditions for the collection of personal data and protection from misuse, and which promotes a practice of personal data processing in accordance with fundamental principles and rules regarding data protection and privacy. Based on the Act, the DPA has published rules No. 299/2001 on the Security of Personal Data. The rules explicitly ask for measures regarding higher risks to personal data when they are processed on the Internet (Article 4) as well as requiring all controllers to implement security measures in accordance with the risk involved in the processing of personal data along with measures to mitigate the risk. Iceland is also in the process of implementing the EU General Data Protection Regulation (GDPR). Moreover, the Regulation in the Protection of Information in the Public Communications Networks No 1221/2007 aims “to enhance consumer protection”.

Users and stakeholders within the public and private sectors have general knowledge about how personal information is handled online but (proactive) cybersecurity practices are rarely used, either due to perceived inconvenience or due to the way people weigh up the trade-offs in service and protection of their personal information.

Participants noted that social security numbers and personal information are widely used for authentication. However, users do yet not perceive that information as private. Once again, the discussion led to the cultural aspect and the everyday practices of the Icelandic society based on ‘implicit trust’.

D2.4 REPORTING MECHANISMS

This factor explores the existence of reporting mechanisms functioning as channels for users to report internet related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.

Maturity Stage: Formative

In Iceland, the public and private sectors provide some channels for reporting, child abuse online, but these channels are not coordinated and are used in an ad-hoc manner. Promotion of the existing reporting channels has not yet begun or is ad-hoc. As regards to channels for reporting identity theft, privacy and security breaches, and other incidents, such channels are almost non-existent. A system for reporting security breaches is being developed (autumn 2017).

A hotline through Barnaheill – Save the Children Iceland[32] focuses on child abuse. Its website also provides an online form to report illegal content. Barnaheill has operated a Hotline since November 2001. The Hotline has worked very closely with the police and with other Hotlines. The hotline is a member of the international organisation INHOPE, and participates actively in its development[33].

The National Commissioner of Icelandic Police (NCIP) is in charge of analysing reports and partners with Barnaheill in running the hotline. The police investigate leads and forward them to Barnaheill who uploads data to the IHRMS database – both will cooperate with other INHOPE hotlines. The police will also forward leads to Europol and Interpol.

The Icelandic Red Cross also runs the 1717 Helpline for people who need assistance because of grief, anxiety, distress, depression or suicidal thoughts. These can call the Red Cross helpline free of charge 24 hours a day. The phone line also has a crucial function during times of emergency.

Any incident, including cyber-related ones, can be reported via the police emergency number 112 or directly to police districts. Also, incidents such as child abuse are referred from the Police to Europol and Interpol.

Some participants noted that no formal communication links have been established between the police and CERT-IS on one hand and the private sector on the other hand. However, formal communication channels are present between the communications sector and CERT-IS based on the Electronic Communications Act[34]. According to CERT-IS it would be the most logical hub of communications in coordinating flow of information about incidents between

[32] www.barnaheill.is
[33] http://www.saft.is/wp-content/uploads/2013/10/SAFT_2013_annual_report_lowres.pdf
[34] http://www.althingi.is/lagas/nuna/2003081.html (in Icelandic), https://eng.innanrikisraduneyti.is/laws-and-regulations/english/electronic-communications/ (English translation)

law enforcement and CI owners. However, at present CERT-IS have neither the mandate nor the resources to do so for the entire CI sector.

D2.5 MEDIA AND SOCIAL MEDIA

This factor explores whether cybersecurity is a common subject across mainstream media, and an issue for broad discussion on social media. Moreover, this aspect speaks about the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Maturity Stage: Formative

There is ad-hoc media coverage of cybersecurity, with very limited information provided and reporting on specific issues that individuals face online, such as cyber-bullying. Overall, discussions on social media about cybersecurity are also limited.

Social media platforms such as YouTube, Facebook, Twitter, and international blog-hosting services are freely available and are used by a large part of the population[35]. The Media Commission[36] is an independent administrative committee under the Ministry of Education, Science and Culture (MoESC). According to the Media Law, it carries out a supervisory function [to ensure editorial independence of media] and attends to day-to-day administrative tasks in the fields covered by the law.

Review participants noted that due to potential reputational harm, incidents within the private sector are often not disclosed. According to the Crime & Safety Report (2017)[37], in 2013 Iceland suffered its first serious cyber-attack when a major telecommunication carrier was hacked, and detailed personal information on hundreds of Icelanders was released on the Internet. In 2015, the servers of several small, private institutions were attacked, and hackers aligned with ISIS targeted the computer network of a private missionary organisation. In November 2015 and in January 2016, in a demonstration against Iceland’s support of commercial whaling, the websites of the Icelandic government were attacked by the hacker collective *Anonymous*. Traditional media and social media reported about this attack, for example Iceland Review[38], Grapevine[39], the Hacker News[40]. These incidents raised the general public awareness. However, participants noted that journalists too do not necessarily understand cybersecurity issues and might misinform the public, and perhaps create fear.

[35] https://freedomhouse.org/report/freedom-net/2016/iceland
[36] http://fjolmidlanefnd.is/english/
[37] https://www.osac.gov/Pages/ContentReportDetails.aspx?cid=21376
[38] http://icelandreview.com/news/2015/11/30/increasingly-dangerous-internet-attacks-iceland
[39] https://grapevine.is/news/2015/12/09/vodafone-falls-prey-to-cyber-attack/
[40] http://thehackernews.com/2013/11/vodafone-iceland-hacked-and-exposed.html

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cyber Culture and Society*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the Republic of Iceland. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model. The recommendations are provided specifically for each factor.

CYBERSECURITY MIND-SET

R2.1 Enhance efforts at all levels of government, especially officials, and the private sector to employ cybersecurity good (proactive) practices. Design systems that enable users across society to embed secure practices more easily into their everyday use of the Internet and online services.

R2.2 Routinize cross-sectorial cooperation and information sharing among private and public sector organisations on cybersecurity risks and good practice.

R2.3 Identify vulnerable groups and high-risk behaviour across the public, in particular young people, to inform targeted, coordinated awareness campaigns, as recommended in R3.1.

TRUST AND CONFIDENCE ON THE INTERNET

R2.4 Establish ISP programmes to promote trust in their services based on measures of effectiveness of these programmes.

R2.5 Promote data protection by default and data protection by design as a tool for transparency in the provision of e-governance services (including e-health and e-police). Implement feedback mechanisms for use to ensure that the e-services are continuously improved and trust is strengthened among users.

R2.6 Employ processes for gathering user feedback within government agencies in order to ensure efficient management of online content.

R2.7 Ensure that the private sector applies security measures to establish trust in e-commerce services, including informing users of the utility of deployed security solutions.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.8 Promote the understanding of protection of personal information online among users and promote the development of their skills to manage their privacy online.

R2.9 Encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making.

R2.10 Promote the compliance to web standards that protect the anonymity of users.

R2.11 Promote data protection by default and by design as a tool for transparency.

R2.12 Develop user-consent policies designed to notify practices on the collection, use or disclosure of sensitive personal information.

R2.13 Establish reporting mechanisms for reporting online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents in accordance with GDPR, NIS directive.

R2.14 Encourage different stakeholders (public-private sector, Police, DPA, CERT-IS) to coordinate the reporting mechanisms and their roles and responsibilities, and to collaborate and share good practices to improve the mechanisms.

R2.15 Establish awareness programmes to promote the regular use of reporting mechanisms by public and private sectors, and their use as an investment in loss prevention and risk control.

R2.16 Establish awareness programmes to promote cyber security and data protection in the public sphere as well as within private entities that process a great amount of personal data on a daily basis, i.e. financial institutions, insurance, IT, marketing etc.

R2.17 Employ effectiveness metrics for all existing mechanisms and ensure that they contribute to their improvement.

MEDIA AND SOCIAL MEDIA

R2.18 Encourage media and social media providers to further extend the coverage beyond threat reporting and focus on informing the public about proactive and actionable cybersecurity measures, as well economic and social impacts.

R2.19 Encourage a frequent discussion about cybersecurity on social media.

R2.20 Ensure that the debate in social and mainstream media and the attitudes expressed inform policymaking.

DIMENSION 3
CYBERSECURITY EDUCATION, TRAINING AND SKILLS

This dimension reviews the availability of cybersecurity awareness-raising programmes for both the public and executives. Moreover, it evaluates the availability, quality, and uptake of educational and training offerings for various groups of government stakeholders, private sector, and the population as a whole.

D3.1 AWARENESS RAISING

This factor focuses on the prevalence and design of programmes to raise awareness of cybersecurity risks and threats as well as how to address them, both for the general public and for executive management.

Maturity Stage: **Formative**

Awareness-raising programmes, courses, seminars and online resources are available for target demographics from public, private, academic, and civil society sources, but no coordination or scaling efforts have been conducted. Awareness-raising programmes may be informed by international initiatives, but are not linked to the NCSS.

The main Aim No. 1 of the NCSS is Capacity Building, and it recognises that the public, enterprises and government should have the knowledge, skills and equipment needed to cope with cybersecurity threats. The enhancement of general awareness of cybersecurity issues is one of the measures towards the implementation of this aim.

Heimili og skóli (Home and School)[41], is the National Parent Association in Iceland and has been the National Awareness Node for Internet Safety in Iceland since 2004. The name created for the awareness-raising efforts is "Samfélag, fjölskylda og tækni" (Community,

[41] http://www.heimiliogskoli.is/

Family and Technology), with the acronym SAFT. The SAFT[42] empowers children and parents to enjoy the internet and new media in a safe and positive way. The emphasis is on awareness work on net-ethics, computer-game rating, source criticism, uses of mobile phones and data protection on the internet. The SAFT is co-financed by the European Union's Connecting Europe Facility. The project aims are to raise awareness about the safe and positive use of the Internet and new media among children, parents, teachers, policy makers, and the ICT industry in Iceland. Heimili og skóli is the overall coordinator for the Safer Internet Centre, coordinator for awareness actions and technical coordinator for awareness, hotline and helpline. Heimili og skóli is independent of government, political parties and religious organisations. Its members are parents' councils and organisations of all schools (elementary and upper level) and some individual parents[43].

Network and Information Security is one of the main tasks of the Post and Telecom Administration (PTA) and is an increasing part of its operations. The direct service from the PTA to the public with respect to cybersecurity is first and foremost the provision of information, where the Administration supports increased awareness of network and information security, among other things by maintaining an advisory website netöryggi.is[44]. Public and smaller companies can find practical information on how to enhance their own security on the Internet. The PTA cooperates with other domestic organisations that work on network and information security.

Iceland has established 7 February as Safer Internet Day[45], which aims to raise awareness about online safety issues and to promote safer and more responsible use of the internet and smartphones, especially among children and young people; but also to give parents additional knowledge about how to use the internet more safely and to protect children better. On 28 January the European Data Protection Day is being celebrated. The Icelandic DPA has on this occasion organized seminars and published guidelines on the use of social media.

The European Consumer Centres-net Iceland has on this occasion put together 'The Five Commandments for Safer Internet Use'[46]. This includes advice such as: 1) not posting photos of friends without their consent on Social Networks; 2) monitoring security settings on Facebook; 3) considering the consequences before illegally downloading music or movies; 4) checking the conditions of access and use of personal data before downloading a new app; 5) obtaining parent consent before paying with their credit card. In general, most of the existing efforts focus on protecting children. There are insufficient awareness-raising programmes targeting the general public and SMEs.

Because few major incidents have occurred in Iceland, the general public does not perceive cyber risks as being a national level. As seen above, cybersecurity awareness-raising efforts are in place, but no national level coordinated cybersecurity awareness programme covering different target groups has yet been developed.

[42] http://www.saft.is/
[43] http://www.saft.is/wp-content/uploads/2013/10/SAFT_2013_annual_report_lowres.pdf
[44] www.netöryggi.is
[45] http://www.eccisland.is/en/about-ecc-net/news/safe-internet-day-2017
[46] http://www.eccisland.is/sites/default/files/atoms/files/safe_internet_day_2017.pdf

D3.2 FRAMEWORK FOR EDUCATION

This factor addresses the importance of high quality cybersecurity education offerings and the existence of qualified educators. Moreover, this factor examines the need for enhancing cybersecurity education at the national and institutional level and the collaboration between government, and industry to ensure that the educational investments meet the needs of the cybersecurity environment across all sectors.

Maturity Stage: **Formative**

Some educational courses exist in cybersecurity-related fields, such as information security, network security and cryptography, but no cybersecurity-specific courses are yet offered in Iceland. It was noted during the consultations that the demand for cybersecurity education is evidenced through course enrolment and feedback within universities.

The need for enhancing cybersecurity education in schools and universities has been identified by leading government, industry, and academic stakeholders. Aim No. 1: Capacity building of the NCSS recognises that the public, enterprises and government should have the knowledge, skills and equipment needed to cope with cybersecurity threats. Some of the measures recognised and planned are to include: 1) cybersecurity education in all computer-related studies at all school levels, and 2) provide students with first degrees from Icelandic universities access to postgraduate studies in cybersecurity.

Several universities offer programmes in computer science and computer engineering at an undergraduate and postgraduate level while cybersecurity is often a module within the curriculum of these. However, there are no specialised degrees in cybersecurity. The University of Iceland (UoI)[47] offers undergraduate studies in Electrical and Computer Engineering as well as postgraduate studies in these fields. Reykjavík University (RU)[48] also offers undergraduate as well as postgraduate programmes in computer science, software engineering and applied computing.

At a postgraduate level, students often do projects related to cybersecurity. However, participants mentioned that in general there are not enough incentives for students to continue their studies and specialise in cybersecurity. It was also noted that the MoESC[49] needs to examine the fact that the model of three-year undergraduate studies does not allow enough time for specialization. These issues and the lack of promotion of cybersecurity or forensics as an attractive profession create a general lack of specialists in the field.

The CSC now has an informal agreement with the Department of Information Security and Communication Technology at NTNU, Norwegian University of Science and Technology, which is one of the most advanced in the field of information security in the Nordic

[47] http://english.hi.is
[48] https://en.ru.is
[49] https://www.government.is/ministries/ministry-of-education-science-and-culture/

countries[50]. Icelandic students can enrol on a similar basis as Norwegian students and take a degree in Master in Information Security, either full-time or part-time (e.g. along with work in Iceland). There are preliminary plans to have representatives from NTNU coming over Jan/Feb to introduce opportunities within cyber security to final year undergraduate students and with the aim of having some students applying by 1 March. A part of this plan is to develop closer ties with UoI and RU, e.g. concerning graduate and undergraduate courses and also concerning events that can help to stimulate interest in cybersecurity and provide interesting challenges for students.

No national budget focused on cybersecurity education has yet been established. Qualification programmes for cybersecurity educators are being explored, with a small cadre of existing professional educators.

In Iceland there is also a gender inequality in the cybersecurity field. The majority of experts working in computer science related posts and cybersecurity are men. Currently there are efforts to promote more women to join the field. The organisation of women within the School of Computing Science at Reykjavík University, /sys/tur ('systur' means sisters in Icelandic) was suggested as a channel for promoting cybersecurity as a profession among women.

Research and development is an important consideration in education. The MoESC and the Ministry of Industries and Innovation (MoII) have the main responsibility for running the research and innovation scheme. The MoESC supervises the affairs of the Science and Technology Policy Council (STPC) and the Scientific Committee, and co-ordinates the ministry's various projects in the fields of science, research and innovation and their integration with the formulation and implementation of education policy.

The Icelandic Centre for Research (RANNIS)[51] supports research, research studies, technical development and innovation in Iceland. RANNIS cooperates closely with the STPC and provides professional assistance regarding the preparation and implementation of science and technology policy in Iceland. However, it was not possible to identify any specific programmes and research funds on cybersecurity or related fields that are currently running.

[50] https://www.ntnu.edu/studies/mis

[51] https://en.rannis.is/

D3.3 FRAMEWORK FOR PROFESSIONAL TRAINING

This factor addresses the availability and provision of cybersecurity training programmes building a cadre of cybersecurity professionals. Moreover, this factor reviews the uptake of cybersecurity training and horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates into continuous skills development.

Maturity Stage: Formative

The need for training professionals in cybersecurity has been documented at the national level, and training programmes in cybersecurity are offered for public and private sector employees as well as for the general public.

ICT professional certification with some security modules or components is available. CISCO and other private companies also offer courses on ethical hacking and other relevant topics. Syndis[52] offers intensive hands-on training, teaching developers to spot and to exploit OWASP Top-10 issues by themselves, to develop a rigorous understanding and knowledge of the security issues and to avoid the problems in practice. Moreover, ad-hoc training courses, seminars and online resources are available for cybersecurity professionals from public or private sources. Seminars, tests and written guidelines have been provided to public organisations through the Information Society Project[53].

Review participants mentioned that currently the Estonian Technology Fund[54] is dedicated towards the provision of online courses, because overall there is not enough expertise among educators to provide training in cybersecurity.

Metrics evaluating take-up of ad-hoc training courses, seminars, online resources, and certification offerings exist, but are limited in scope.

Executive training courses for CEOs or chief financial executives are offered in an ad-hoc manner, including topics such as good governance practice related to cybersecurity and risk management.

During the consultations it was identified that overall no established cadre of cybersecurity-certified employees exists in Iceland. Currently, many experts are self-educated or gain their expertise on the job, and knowledge transfer from employees trained in cybersecurity to untrained employees is ad hoc.

[52] https://www.syndis.is/owasp-top-10-training

[53] https://www.stjornarradid.is/verkefni/upplysingasamfelagid/ (in Icelandic)

[54] https://rio.jrc.ec.europa.eu/en/organisations/estonian-development-fund
The Development Fund is a state-run public institution that invests into young and growth-oriented technology companies together with the private sector. The fund is aimed to invest into knowledge-intensive and high-technology Estonian companies that are in launching stage, offering management-related support to the relevant operators.

RECOMMENDATIONS

Following the information presented on the review of the maturity of *Cybersecurity Education, Training and Skills*, the following set of recommendations are provided to the Republic of Iceland. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

AWARENESS RAISING

R3.1 Develop a national cybersecurity awareness-raising programme with specified target groups, focusing on the most vulnerable users.

R3.2 Appoint a designated organisation (from any sector) to lead the cybersecurity awareness-raising programme.

R3.3 Engage relevant stakeholders from public and private sectors in the development and delivery of the awareness-raising programme as well as for the creation and utilisation of programmes and materials.

R3.4 Create a single online portal linking to appropriate cybersecurity information and disseminate the cybersecurity awareness programme via this platform.

R3.5 Enact evaluation measurements to study effectiveness of the awareness programmes at a level where they inform future campaigns taking into account gaps or failures.

R3.6 Promote awareness of risks and threats at lower levels of the government.

R3.7 Develop a dedicated awareness-raising programme for executive managers within the public and private sectors, particularly those in the financial, transport, health, CI and telecommunications sectors.

R3.8 Promote awareness regarding the protection of personal data online.

R3.9 Promote awareness raising efforts of cybersecurity crisis management at the executive level.

R3.10 Develop operational cyber security self-education websites.

FRAMEWORK FOR EDUCATION

R3.11 Create cybersecurity education programmes for instructors of cybersecurity to ensure that skilled staff is available to teach newly formed cybersecurity courses.

R3.12 Create accredited cybersecurity-specific degree courses at the university level, in addition to the other existing cybersecurity-related courses in the various Icelandic universities, in cooperation with other European/international universities.

R3.13 Promote efforts by Universities and other bodies to hold seminars/lectures on cybersecurity issues aimed at non-specialists, in cooperation with other European/international universities.

R3.14 Allocate additional resources to cybersecurity education for public universities, dedicated to national cybersecurity research and laboratories at universities.

R3.15 Establish cooperation agreements with European/International Universities in order students to enrol to programmes abroad.

R3.16 Provide more opportunities for individuals (such as students and experts) to gain experience, through internships and apprenticeships, in cooperation with other European/international universities, in order to enhance their expertise by combining education and practical training.

R3.17 Inform cybersecurity education priorities through broad consultation across government, private sector, academia and civil society, linked to the National Cybersecurity Strategy.

R3.18 Promote competitions and initiatives for students by government and/or industry in order to increase the attractiveness of cybersecurity careers.

R3.19 Ensure the sustainability of research programs.

R3.20 Develop effective metrics to ensure that educational and skill enhancement investments meet the needs of the cybersecurity environment.

FRAMEWORK FOR PROFESSIONAL TRAINING

R3.21 Establish more structured cybersecurity training programmes to develop skills towards building a cadre of cybersecurity-specific professionals.

R3.22 Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, legal training, tools, and models and operation of these tools.

R3.23 Train general IT staff on cybersecurity issues so that they can react to incidents as they occur.

R3.24 Ensure that affordable security professional certification is offered across sectors within the country.

R3.25 Develop a central platform for sharing training information for experts and create a national-level register of cybersecurity experts.

R3.26 Establish requirements for joint cybersecurity training for the public and private sector, and develop collaborative training platforms.

R3.27 Establish job creation initiatives for cybersecurity within organisations and encourage employers to train staff to become cybersecurity professionals.

R3.28 Begin to implement metrics evaluating take-up of ad-hoc training courses, seminars, online resources, and certification offerings.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

This dimension examines the government's capacity to design and enact national legislation directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, and other cybercrime-related issues. The capacity to enforce such laws is examined through law enforcement, prosecution, and court capacities. Moreover, this dimension observes issues such as formal and informal cooperation frameworks to combat cybercrime.

D4.1 LEGAL FRAMEWORKS

This factor addresses legislation and regulation frameworks related to cybersecurity, including: ICT security legislative frameworks; privacy; freedom of speech and other human rights online; data protection; child protection; consumer protection; intellectual property; and substantive and procedural cybercrime legislation.

Maturity Stage: **Established**

The Republic of Iceland has implemented provisions relating to cybersecurity comprehensively in its ICT legislative and regulatory frameworks. The Regulatory Framework of the European Union[55] – through the EEA membership – applies in the country and has shaped many regulations and existing legislation to protect the rights of individuals and organisations in the digital environment.

Relevant actors from private sector and civil-society stakeholders are generally involved in legislative processes and make their voices heard through the media or by contacting politicians directly[56]. According to review participants, the Ministry of Justice (MoJ), for instance, conducted a survey on the existing legislation to receive feedback from

[55] https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf

[56] https://www.althingi.is/pdf/Althingi2013_enska.pdf

stakeholders, and is currently preparing a report, in accordance with usual practice during legislative processes.[57]

The Electronic Communications Act (ECA) No. 81 from March 2003,[58] the *Act on the Post and Telecom Administration (APTA) No. 69, from March 2003*[59] and its *Amendment No. 62/2012*[60] provide the legal basis for the Post and Telecom Administration (PTA), an independent body under the MoTLG responsible for the administration of electronic communications and postal affairs. Both Acts stipulate certain provisions regarding cybersecurity and critical information infrastructure, and allow PTA to implement measures to maintain the integrity and security of public communications networks (ECA, Article 3). According to Article 6, the ECA also ensures the security of public networks from illegal access and the safety of the country's electronic communications with the outside world. Moreover, it requires those providing electronic communications services to take measures to ensure their security, to consult with operators and to inform subscribers in the case of a breach. Individuals who work in electronic communications are required to keep information confidential even after employment termination. Amendment No. 62 defines the role and responsibilities of CERT-IS (see D1.2) for the protection of critical information infrastructure (Article 8). Law enforcement only receives access to data where provisions of Article 70 of the Criminal Proceedings Act[61] apply.

The *Regulation on protection, functionality, and quality of IP communications services, No. 1223 from 2007*[62] applies to network and information security within the ECA and establishes the role of CERT-IS. It aims "to enhance consumer protection and strengthen the foundations of the information society by making increased requirements concerning the security of the electronic communications systems used by businesses and individuals." This includes security of IP traffic and email operations, as well as notification of customers, measures to limit the spread of security incidents, reporting mechanisms, and the supply of value-added services regarding security. Art. 42, paragr. 3 of the ECA stipulates that data should be retained for 6 months. This data can only be accessed following a judicial procedure, as per Art. 47, paragr. 7 of the ECA. Additionally, the *Icelandic Media Law*[63] requires providers to ensure that the transmission of service via electronic communications networks are secure (Article 45). *Act No. 30/2002 on Electronic Commerce and other Electronic Services* retains the liability of ISPs and establishes a system of takedown notices for IP addresses or other online content that violate the law, in accordance with the *Directive 2000/31/EC* of the European Parliament. According to a similar EU directive, *Act No 28/2001 on Electronic Signatures*[64] and *Regulation No. 780/2011*[65] define the legality of electronic signatures and their power to

[57] https://www.upr-info.org/sites/default/files/document/islande/session_26_-_octobre_2016/a_hrc_wg.6_33_isl_1_e_0.pdf

[58] https://www.stjornarradid.is/publications/legislation/lex/2018/01/16/Electronic-Communications-Act-No.-81-26-March-2003/

[59] https://www.stjornarradid.is/publications/legislation/lex/2018/01/04/Act-on-the-Post-and-Telecom-Administration-No.-69-24-March-2003/

[60] https://www.pfs.is/upload/files/Act%20no.62_2012.pdf

[61] https://www.government.is/publications/legislation/lex/2018/01/15/Law-on-Criminal-Procedure-No.-88-2008-Exerpts/

[62] https://www.pfs.is/upload/files/REGULATION_no.1223_IP%20communication.pdf

[63] http://fjolmidlanefnd.is/wp-content/uploads/2011/12/Log-um-fjolmidla_ensk-thyding_mai2015.pdf

[64] https://www.stjornarradid.is/publications/legislation/lex/2018/02/01/Merchants-and-Trade-Act-No-28-2001-on-electronic-signatures/

[65] http://www.neytendastofa.is/lisalib/getfile.aspx?itemid=2736

make legally binding agreements, and the requirements for certificates, signature-creation devices and certification service providers.

The first Data protection legislation in Iceland was adopted in 1981 and has been updated and enforced since then. The Data Protection Act No. 77/2000[66] includes general conditions for the collection of personal data and protection from misuse and it promotes a practice of personal data processing in accordance with fundamental principles and rules regarding data protection and privacy. It stipulates, inter alia, that data can only be obtained for specific purposes and only processed in a fair apposite and lawful manner. According to Articles 8 (general conditions) and 9 (sensitive data), data may only be processed if one of the criteria listed in the provisions is met, i.e. after the subject has given unambiguous and informed consent. When processing personal data controllers have a duty to inform the data subject, see Article 20 of the Data Protection Act. For example, the controller must provide the name and address of the controller, the purpose of the processing and other information, such as recipients or categories of the data and whether or not he is obliged to provide the data. The Act implements the *Directive 95/46/EC* of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [67] and safeguards the reliability and integrity of the personal data and its free flow within the EEA. As a member of the EEA Agreement Iceland is obliged to implement the GDPR into Icelandic law. The Ministry of Justice is responsible for the implementation. Most likely, the Minister of Justice will introduce before the parliament a new draft legislative bill, implementing the provisions of the GDPR, in 2018. The Data Protection Authority (DPA)[68], is an independent governmental body, which is responsible for monitoring data processing and the application of the *Data Protection Act*. It has also started to prepare for new duties laid upon it by the GDPR and at the same time offers guidance for businesses and other institutions. Additionally, *Rules No. 299/2001 on the Security of Personal Data*[69] explicitly provide measures regarding higher risks to personal data when it is processed on the Internet (Article 4). Moreover, the *Regulation on the Protection of Information in the Public Communications Networks no 1221/2007*[70] aims "*to enhance consumer protection and strengthen the foundations of the information society*" by defining the measures the PTA needs to undertake in order to guarantee the confidentiality, the availability and the integrity of information, and its lawful access. This includes business continuity plans, measures concerning employees, access controls and organisational and technological measures.

Several Icelandic laws recognize fundamental human rights on the Internet, including privacy online, freedom of speech, freedom of information, and freedom of assembly and association. The constitution[71] includes thirteen provisions regarding human rights, including the protection of freedom of expression (Article 73), privacy (Article 71), freedom of association (Articles 64 and 74) and assembly (Article 74), and has been updated according to

[66] https://www.personuvernd.is/information-in-english/greinar/nr/438
[67] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[68] https://www.personuvernd.is/information-in-english/greinar/nr/438
[69] https://www.personuvernd.is/information-in-english/greinar/nr/442
[70] https://www.pfs.is/library/Skrar/Innflutt/PDF/REGULATION_no.1221_Protection%20of%20information.pdf
[71] http://www.government.is/constitution/

the latest international developments.[72] Additionally, the *Media Act No 38/2011* [73] also requires media service providers to ensure human rights, such as freedom of expression and privacy in their activities (Article 26). The country's previous *Information Act No 50/1996* and the current *Information Act No. 140/2012*[74] provide a safeguard to the public's right to access information effectively and ensure the free flow of information. The country has also ratified or acceded to several international agreements, such as the *UN Universal Declaration of Human Rights*, the *Convention for the Protection of Human Rights and Fundamental Freedoms* of the Council of Europe**[75]**, and those of the International Labour Organization and the Organization for Security and Co-operation in Europe, such as the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No 108*[76]**.** The country is actively involved in the global discourse on human rights by submitting reports to international bodies, while also reviewing and adapting the recommendations to their legislation. The Icelandic Human Rights Centre (ICEHR)[77] is the national institution responsible for conducting research regarding human rights issues and for promoting and creating awareness about human rights. Freedom of Speech and Privacy legislations are also reviewed as part of the implementation of the Budapest Convention (see below).

Comprehensive legislation on the protection of children has been adopted and enforced according to Iceland's *Child Protection Act, No. 80/2002*. This legal and institutional framework is largely in line with the international human rights obligations in this field, e.g. ISPs have to filter out websites containing child abuse online if notified. Iceland has ratified the *UN Convention on the Rights of the Child* and other relevant international conventions and is applying them in the country[78]. However, review participants stated that there is no specific domestic law or provision in the online environment, speaking specifically to the protection of children online, nor directly to relevant criminal procedures.

The *Act No 62/2005 on the Consumer Agency and Consumer Spokesman*[79] safeguards consumers from business malpractice online and is enforced by the Consumer Agency (CA), a governmental agency under the auspices of MoII. The Act is complemented by the above-mentioned *Acts No. 30/2002 on Electronic Commerce and other Electronic Services* and *No. 28/2001 on Electronic Signatures.*[80] The latter fulfils the legal requirements of the European Parliament and Council *Directive 1999/93/EB*[81] to ensure that the certificates issued in Iceland are valid in the EEA. The CA is a founding member of the Forum of European Supervisory Authorities,[82] which "*support(s) the cooperation, information and assistance among the members and to facilitate the exchange of views and agreement on good practice*."

[72] https://www.upr-info.org/sites/default/files/document/islande/session_26_-_octobre_2016/a_hrc_wg.6_33_isl_1_e_0.pdf

[73] http://fjolmidlanefnd.is/wp-content/uploads/2011/12/Log-um-fjolmidla_ensk-thyding_mai2015.pdf

[74] https://www.government.is/publications/legislation/lex/2018/01/19/The-Information-Act-No.-140-2012/

[75] https://treaties.un.org/pages/showDetails.aspx?objid=080000028014a40b

[76] https://rm.coe.int/168008c2b8

[77] http://www.humanrights.is

[78] https://www.government.is/topics/social-welfare-and-families/

[79] www.neytendastofa.is/lisalib/getfile.aspx?itemid=1402

[80] https://www.stjornarradid.is/publications/legislation/lex/2018/02/01/Merchants-and-Trade-Act-No-28-2001-on-electronic-signatures/

[81] https://portal.etsi.org/esi/Documents/e-sign-directive.pdf

[82] http://www.fesa.eu/index.html

Iceland adheres to legislation addressing intellectual property of online products and services as other countries in EEA. *Copyright Act No. 126/2011*[83] comprises of provisions regarding intellectual property rights. The Icelandic Patent Office is the agency responsible for issues related to copyright and provides information and advice to individuals, companies and other institutions. The country is a member of major international bodies, such as the World Trade Organization (WTO), the World Intellectual Property Organisation (WIPO), the European Patent Organisation (EPO) and the Nordic Patent Institute. Moreover, Iceland adheres to key international agreements such as the Paris Convention for the Protection of Industrial Property, the Protocol Relating to the Madrid Agreement, the Patent Cooperation Treaty, The Geneva Act of the Hague Agreement Concerning the International Registration of Industrial Designs, and the European Patent Convention. Participants confirmed that cases of copyright violations have been prosecuted and sentenced.

There is no specific cybercrime law in Iceland. However, in 2007 the country ratified the Council of Europe Convention on Cybercrime, also known as the 'Budapest Convention', whose recommendations are consistently implemented into domestic law. For instance, *General Penal Code No. 19/1940*[84] (GPC) contains substantive cybercrime legal provision since its amendment in 1998, in addition to latter amendments to the GPC and the Act on Criminal Procedures which are related to the implementation of the Budapest Convention. The code prohibits e.g. unlawfully accessing other persons' data or its destruction or damage (Articles 257 and 228)[85], as well as "*unlawfully modifying, adding to of destroying computer software, or data or programs stored in machine-readable form, or taking other measures designed to influence the outcome of computer processing*" (Article 249a). However, as participants pointed out there are gaps in existing legislation. For instance, the act of breaking into a computer system may not be illegal in itself; only when damage occurs or the break-in is for financial gain, does it become a crime (see above). However, it should be noted that article 228 in the GPC stipulates that "a person who in an unlawful manner procures access to data or programs of others which are stored in a computerized form" can be fined or sentenced, to up to one year in prison. On the other hand, article 242 in the GPC stipulates that lawsuits on account of offences, against article 228 may only be brought by the injured party alone which limits the tools that the police and prosecutors have for investigation and prosecution in such cases. The penal code also bans the production, distribution, and possession of child pornography (Article 210), and illicit computer-related acts for personal or financial gain, such as fraud and forgery (Article 158). The *Act on Collection of Evidence Relating to Alleged Violations of Intellectual Property Rights, No. 53/2006*[86] contains comprehensive provisions for the investigation of cybercrime and evidentiary requirements, e.g. for electronic evidence (Article 4, 12), and cases have been brought to court. The *Act on Criminal Procedure No. 88/2008*[87] allows requesting electronic information from ISPs for the purpose of an investigation (Article 70).

[83] http://www.wipo.int/edocs/lexdocs/laws/is/is/is108is.pdf
[84] http://www.althingi.is/altext/stjt/2006.074.html
[85] http://www.parliament.am/library/Qreakan/islandia.pdf
[86] https://www.stjornarradid.is/publications/legislation/lex/2018/01/15/Act-on-Collection-of-Evidence-Relating-to-Alleged-Violations-of-Intellectual-Property-Rights-No.-53-2006/
[87] https://www.stjornarradid.is/publications/legislation/lex/2018/01/15/Law-on-Criminal-Procedure-No.-88-2008-Exerpts/

In spite of the shortcomings mentioned earlier, participants perceived the legislation in respect to cybersecurity as sufficient. However, the government still has to fulfil its commitment, expressed in the national ICT Security Policy from 2015, to update its legislation *"[to] reflect the international demands and obligations the country undertakes regarding cyber security and the protection of personal data*".[88] There are several gaps in existing legislation. Furthermore, the protection of infrastructure is limited to e-communications infrastructure and does not cover other CNI. With the NIS Directive to take effect in May 2018, several participants emphasized the need to address this lack of legislation protecting CNI, and criticized the slow process encountered in preparing its implementation. However, they anticipated its potential contribution towards closing the existing gaps in CNI protection in the very near future. Participants also expressed concerns about the state of preparedness of the private sector and of government institutions to implement the GDPR and the structures and processes it requires in the remaining months before it comes into effect from May 2018 onwards. From their perspective, efforts in the remaining time should focus on preparing the new legislation needed to implement the GDPR and putting it forth, but also foster the implementation across the private and public sectors.

D4.2 CRIMINAL JUSTICE SYSTEM

This factor studies the capacity of law enforcement to investigate cybercrime, and the prosecution's capacity to present cybercrime and electronic evidence cases. Finally, this factor addresses the court capacity to preside over cybercrime cases and those involving electronic evidence.

Maturity Stage: Formative

Across the criminal justice system, capacities are at initial stages of development in Iceland. The Police, headed by the National Commissioner of the Icelandic Police (NCIP), have only limited digital forensics capacity and cases are investigated by the digital forensics unit of the Reykjavik Metropolitan Police. Two policemen at the Metropolitan Police are also specifically assigned to investigate cases involving sexual violence against children on the internet. However, the country needs more skilled personnel as well as the procedural and technological resources to conduct investigations in a comprehensive way. Training for law enforcement officers on cybercrime and digital evidence is ad-hoc or not specialized. As a result, for instance, revenge porn is a recurring issue, because the lack of capacity hinders the police being able to tackle all cases. One way to mitigate these threats and resource gaps is regional and bilateral collaboration mechanisms, e.g. with the Norwegian police (see 4.3).

Some specialised cybercrime prosecutors have the capacity to build cases on electronic evidence, but this capacity is limited as training is largely ad-hoc, not institutionalised and informal. For instance, some prosecutors have participated in courses offered by the

[88] https://joinup.ec.europa.eu/community/epractice/news/iceland-boosts-ict-security-measures-shares-policy

International Association of Prosecutors[89], but the courses are not mandatory. A similar situation can be observed in courts. If judges receive training on cybercrime, digital evidence, or data protection, it is ad-hoc or not specialized and much of the training available is also not even known, for instance that by the Council of Europe[90]. On the other hand, a newly established Judicial Administration is preparing an overall analysis on the need for training of judges and other staff in order to build a training program. Both Judges and the Judicial Administration are aware of the importance of strengthening knowledge of digital processes and cybercrime. Furthermore, a provision in the new Act on Courts, going into effect on 1st January 2018, also strengthens the selection process of experts to the bench in order to create a substantial pool of these experts in all the major fields. In addition, it should be noted that risk analysis on data protection for judicial data has also been performed.

Participants confirmed that the cooperation with law enforcement is effective, even with the limited capacity as described, as those personnel who have the expertise are known and cases are automatically handed over.

While Iceland has not yet seen a large number of cybercrime cases brought before the courts, the limited levels of capacity in handling cybercrime cases could potentially lead to ineffective investigations, prosecutions and convictions, which would allow cybercriminals to remain unpunished and continue their criminal conduct. In addition to strengthening the legal framework, it is therefore important to elevate the capacities of the criminal justice system to successfully combat and prevent cybercrime.

D4.3 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

This factor addresses the existence and functioning of formal and informal mechanisms that enable cooperation between domestic actors and across borders to deter and combat cybercrime.

Maturity Stage: Established

Iceland has fully acknowledged the need for formal and informal cooperation and has established mechanisms of international cooperation in order to prevent and combat cybercrime by facilitating its detection, investigation, and prosecution, with established communication channels. The country cooperates with international organisation such as Interpol[91] and Europol,[92] and directly with governments, e.g. Norway and the US, regarding cross-border information sharing and has signed l Mutual Legal Assistance agreements which

[89] http://www.iap-association.org/
[90] http://www.coe.int/en/web/cybercrime/trainings
[91] https://www.interpol.int/Member-countries/Europe/Iceland
[92] https://www.europol.europa.eu/agreements/iceland

are successfully applied. The MoJ is the authority responsible for "*sending and answering requests for mutual assistance, the execution of such requests, or the transmission of them to the authorities competent for their execution*" as well as "*making or receipt of a request for extradition or provisional arrest*". The NCIP has the responsibility of being the 24/7 point of contact to provide immediate assistance for the purpose of cybercrime investigations or proceedings.[93] These tasks are then usually handed over to the digital forensics unit at the Reykjavik Metropolitan Police (see 4.1).

Cooperation between law enforcement and the private sector, in particular ISPs, is informal, as there are no legislative requirements for the exchange of information between domestic public and private sectors. Only telecommunications companies are required to report 'serious' incidents, to CERT-IS. However, there is no definition of what constitutes a serious incident. According to the participants, companies have often been hesitant to report incidents, though a shift towards more openness is being observed from companies which have begun to volunteer information. Between government and criminal justice actors, informal relationships have been established successfully, mostly based on personal connections, resulting in the exchange of information on cybercrime issues.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Legal and Regulatory Frameworks*, the following set of recommendations are provided to the Republic of Iceland. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC.

LEGAL FRAMEWORKS

R4.1 Continue to review existing legal and regulatory mechanisms for ICT security to identify where gaps and overlaps may exist and amend or enact new laws accordingly. Monitor the enforcement of the legislative frameworks and ensure that it informs resources allocation and legal reform. Put mechanisms in place for keeping ICT legal frameworks in harmony with national cybersecurity-related ICT policies, international law, standards and good practices.

R4.2 Ensure that international and regional trends and good practices inform the assessment and amendment of domestic legal frameworks protecting human rights online and associated resource planning. In order to meet dynamic changes in the application of technology to human rights, identify procedures to amend and update legal frameworks as needed.

[93] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=CZVDo71s&_coeconventions_WAR_coeconventionsportlet_enVigueur=false&_coeconventions_WAR_coeconventionsportlet_searchBy=state&_coeconventions_WAR_coeconventionsportlet_codePays=ICE&_coeconventions_WAR_coeconventionsportlet_codeNature=3

R4.3 Continue to actively contribute to the global discourse on human rights on the Internet. Foster research on human rights on the Internet and ensure that measures are in place to exceed minimal baselines specified in international agreements. Continue to actively contribute to the global discourse on human rights and move the focus on human rights on the Internet.

R4.4 Ensure that the GDPR and the Police Directive[94] on the processing of personal data is successfully implemented and legal mechanisms are in place that enable. Identify international and regional trends and good practices to inform the assessment and amendment of data-protection laws and associated resource planning.

R4.5 Improve national child protection online legislation to comply with regional and international law and standards.

R4.6 In order to meet dynamic changes in the application of technology to consumer protection, develop and implement procedures to amend and update legal frameworks as needed.

R4.7 Review the legislation on intellectual property online through consultation with key stakeholders and through public discourse to reflect changes in national priorities and the international ICT landscape.

R4.8 Develop and implement measures to exceed minimal baselines for substantive and procedural cybercrime frameworks specified in international treaties where appropriate, which includes procedures to amend those frameworks as needed.

R4.9 Ensure that in the case of cross-border investigation, procedural law stipulates what actions need to be conducted under particular case characteristics, in order to successfully investigate cybercrime.

CRIMINAL JUSTICE SYSTEM

R4.10 Invest in advanced investigative capabilities in order to allow the investigation of complex cybercrime cases, supported by regular testing and training of investigators.

R4.11 Allocate resources dedicated to fully operational cybercrime units based on strategic decision making in order to support investigations, especially at the local level.

[94] Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN .

R4.12 Enhance training and education of prosecutors and judges on cybercrime and data protection. Additional resources should be allocated for this purpose.

R4.13 Establish a formal mechanism to enable the exchange of information and good practices between prosecutors and judges to ensure efficient and effective prosecution of cybercrime cases.

R4.14 Collect and analyse statistics and trends regularly on cybercrime investigations, on cybercrime prosecutions and on cybercrime convictions.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

R4.15 Allocate resources to support the exchange of information between public and private sectors domestically and enhance legislative framework and communication mechanisms.

R4.16 Enhance established informal cooperation mechanisms between Internet Service Providers and PTA, DPA and law enforcement with clear communication channels.

DIMENSION 5
STANDARDS, ORGANISATIONS AND TECHNOLOGIES

This dimension addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

D5.1 ADHERENCE TO STANDARDS

This factor reviews government's capacity to design, adapt and implement cybersecurity standards and good practice, especially those related to procurement procedures and software development.

Maturity Stage: **Formative**

ICT security standards and good practices have been adopted by both the public and private sector and there is evidence of measurable implementation. Telecommunications companies must, according to the *ECA*, implement cybersecurity measures in their overall risk management; however, the Act does not specify which standards are mandatory across sectors. Many public organisations, including CNI, have introduced international standards such as the ISO 27000 family and are following relevant EU requirements. According to participants, the National Hospital and many of the municipalities have adhered to ISO 27001 for about ten years. Moreover, banks have to comply with the requirements of Fjármálaeftirlitið, the Financial Supervisory Authority (FSA)[95] and must have certification to the Payment Card Industry Data Security Standard (PCI-DSS). It was mentioned that it is often the requirement of corporate customers that financial organisations fulfil specific standards

[95] https://en.fme.is/

which are not a legal of regulatory requirement. This is also an observation regarding the private sector. Furthermore, all controllers processing personal data must adhere to the security provisions of the Data Protection Act, cf. Articles 11-13, and Rules No. 299/2001 on the Security of Personal Data. The rules especially refer to ISO/IEC 27001 as guidelines to follow when setting up an ISMS.

A different observation was made for the smaller health care institutions across the country and smaller and medium municipalities and enterprises in Iceland. Most of these organisations do not implement standards or do not seek certification due to limited human resources. It is common that those organisations use trusted domestic and international hosting companies that adhere to standards, wrongly assuming that they are no longer responsible for information security. On the other hand, PTA has observed that the majority of telecommunications companies follow ISO 27001 in order to fulfil compliancy requirements, although many abstain from certification due to its high costs. No measures to monitor compliance or metrics were known by the participants and there is no entity in the country which has the mandate to monitor the implementation of standards. Overall, participants expected significant changes due to the implementation of the GDPR which will both emphasise the responsibility of any organisation to adhere to certain standards and the need for monitoring. These developments will foster the implementation of standards in all sectors and will increase the awareness that adherence to standards is one crucial element to make an organisation cybersecure.

Regarding the standards related to procurement of software, similar conclusions can be drawn. There is no evidence for the adoption of and compliance to cybersecurity standards in procurement practices within the public and private sectors, nor measurement and assessments of process effectiveness. Organisations consider critical aspects of procurement such as prices and costs, quality, timescales and other value-added activities but often they are not aware of cybersecurity aspects or do not know which standards to adhere to in this regard. There is no unified process in the country to guide the identification of standards for procurement of software or hardware. Processes follow in general the requirements of the *Public Procurement Act, No. 120/2016*[96] which is aligned with the European regulation. Some larger public and private organisations follow ISO/IEC JTC 1/SC 32, ISO 29115[97], ISO 27001 and the Gartner Standards. However, the extent of the implementation of these depends on the sector and is ad-hoc. The Ríkiskaup, the government's public procurement office[98], for instance, has signed frame contracts with about seven hosting companies, which can be used by every public institution. Some large international companies follow their own procurement processes or base their decision on reputation of the product or supplier rather than actual standard adherence.

Focusing on standards in software development, there are no guidelines or protocols in place relating to cybersecurity. Although local companies and the professional communities in Iceland perceive security in software development as important, most participants agreed that it is not a priority, especially in smaller companies or in-house development offices, and

[96] https://www.stjornarradid.is/media/fjarmalaraduneyti-media/media/frettatengt2016/act-on-public-procurment-no.-120-2016.pdf
[97] https://www.iso.org/standard/45138.html
[98] https://www.rikiskaup.is/

may also be sacrificed because of the higher costs. The only exception is the financial sector that has to follow the requirements of the FSA. Participants expect that the implementation of the NIS directive and the GDPR will bring the issue of standard adherence to the attention of the other sectors as well.

D5.2 INTERNET INFRASTRUCTURE RESILIENCE

This factor addresses the existence of reliable Internet services and infrastructure in the country as well as rigorous security processes across private and public sectors. Also, this aspect reviews the control that the government might have over its Internet infrastructure and the extent to which networks and systems are outsourced.

Maturity Stage: Established

Iceland's Internet services and infrastructure have been established and are reliable. The technology and processes deployed for Internet infrastructure meet international IT guidelines, standards, and good practices. Iceland achieves leading scores in technological readiness[99] and Internet access and broadband penetration is one of the highest internationally[100]. Several submarine cables connect the country with the European and North American continent.

Internet is used for e-commerce and electronic business transactions (see D2.2). However, authentication processes are often weak, e.g. many websites only require simple authentication. There are also legal requirements for operational security; but telecommunication companies and other CNI often have their own internal standards or are only obliged that those are fit-for-purpose. Although national infrastructure is formally managed, including documented processes, roles and responsibilities, there is no regular assessment of those processes according to international standards and guidelines. An exception is again the financial sector which is regulated by the FSA.

[99] http://www3.weforum.org/docs/GCR2016-2017/05FullReport/TheGlobalCompetitivenessReport2016-2017_FINAL.pdf

[100] https://data.oecd.org/iceland.htm

D5.3 SOFTWARE QUALITY

This factor examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this factor reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the criticality of services.

Maturity Stage: Start-up to Formative

Software quality is a matter of concern and functional requirements in public and private sector are identified, but not necessarily in a strategic manner. Priority is mostly given to the quality and performance of software. As there is no inventory of software used in public and private sectors, nor is a catalogue of secure software, software is mostly selected because it is known or recommended. Additionally, monitoring and quality assessment is conducted in an ad-hoc manner only in few private institutions, so no evidence of software quality deficiencies is gathered. Policies and processes on software updates and maintenance are increasingly put in place, but primarily by international companies or enterprises that focus on the Internet or software development.

D5.4 TECHNICAL SECURITY CONTROLS

This factor reviews evidence regarding the deployment of technical security controls by users, public and private sectors and whether the technical cybersecurity control set is based on established cybersecurity frameworks.

Maturity Stage: Formative to Established

Up-to-date technical security controls, including patching and backups, are deployed in all sectors in Iceland but to very different levels. Companies have internal policies for updates and automated software updates are becoming more common. However, participants expressed doubts that these controls are tested on a regular basis. As many smaller companies and public sector organisations use hosting services and other suppliers they often are not aware of their remaining responsibility to be cyber secure.

Users have general understanding of the importance of, for instance, anti-malware software, but it is questionable whether this is translated into actual behaviour, such as regular updates. ISPs often offer such software and have established policies for technical security control deployment as part of their services. Technical cybersecurity control systems are deployed but not consistently based on established cybersecurity frameworks, such as the

SANS Top-20 cybersecurity controls. Physical security controls are increasingly deployed on various levels, for instance in ministries, to prevent unauthorised personnel from entering computing facilities.

D5.5 CRYPTOGRAPHIC CONTROLS

> *This factor reviews the deployment of cryptographic techniques in all sectors and users for protection of data at rest or in transit, and the extent to which these cryptographic controls meet international standards and guidelines and are kept up-to-date.*

Maturity Stage: Formative to Established

Across stakeholder groups there is a broad understanding of secure communication services, such as encrypted or signed email, and many institutions support these because of increased public pressure and notification through a popular Facebook group[101] where experts in Iceland discuss cybersecurity issues. However, international counterparts have pointed out that documents provided by Icelandic partners sometimes do not meet international standards. No guidelines in this regard for each sector exist – except for in financial institutions. Although some state-of-the-art tools, such as SSL or TLS, are routinely deployed by web service providers to secure all communications between servers and web browsers, and all EU laws have been implemented on data protection and e-signatures, participants pointed out a lack of infrastructure to manage encryption, as no such services are offered in Iceland.

D5.6 CYBERSECURITY MARKETPLACE

> *This factor addresses the availability and development of competitive cybersecurity technologies and insurance products.*

Maturity Stage: Start-up to Formative

The domestic market in Iceland is very small and only provides a few specialised cybersecurity products, which are not demand-driven. Most organisations rely on products from international companies. Local suppliers of software and services such as penetration testing and auditing do consider cybersecurity, as mentioned above (D5.3) but it is not a priority.

[101] https://www.facebook.com/search/top/?q=Net%C3%B6ryggi

Cyber-insurance is offered by a domestic insurer who resells international products, but uptake is limited as the terms are often not suitable for local companies.

D5.7 RESPONSIBLE DISCLOSURE

This factor explores the establishment of a responsible-disclosure framework for the receipt and dissemination of vulnerability information across sectors and, if there is sufficient capacity, to continuously review and update this framework.

Maturity Stage: Formative

Stakeholders mainly share technical details of vulnerabilities informally with other stakeholders, who can distribute the information more broadly; but this is not common and is mostly not done publicly. Currently, organisations have established their own processes and mechanisms to receive, disseminate and share information on vulnerabilities, and the Facebook group mentioned above (D5.5), which discloses incidents on a regular basis, is contributing to a cultural shift in this regard and has encouraged voluntary disclosure. Beyond that, there is no framework in place and only some organisations are obliged to report to CERT-IS. Banks have to report within 24 hours according to the FSA guidance. After the GDPR comes into force companies will have 72 hours to report to the DPA. Additionally, financial institutions and telecommunication companies inform affected customers, usually via email or a publicly available status page. Changes are expected with the implementation of GDPR, NIS and the Police Directive into Icelandic law when incident reporting both towards relevant authorities and data subjects involved (if applicable) will be required for by law.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Standards, Organisations, and Technologies*, the following set of recommendations are provided to the Republic of Iceland. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

ADHERENCE TO STANDARDS

R5.1 Adopt a nationally agreed baseline of cybersecurity related standards and good practices across the public and private sectors, including standards in procurement and software development.

R5.2 Establish a body within government to assess the level of adoption of standards across public and private sectors. Apply metrics to monitor compliance.

R5.3 Promote discussions on how standards and good practices can be used to address risk within critical infrastructure supply chains by both government and infrastructure organisations.

INTERNET INFRASTRUCTURE RESILIENCE

R5.4 Enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors.

R5.5 Conduct regular assessments of processes according to international standards and guidelines together with assessment of national information infrastructure security and critical services that drive investment in new technologies.

R5.6 Identify and map points of critical failure across the Internet infrastructure.

SOFTWARE QUALITY

R5.7 Develop a catalogue for secure software platforms and applications within the public and private sectors and share with all stakeholders.

R5.8 Establish software quality and functional requirements in public and private sectors, including policies on software updates.

R5.9 Promote the use of reliable software applications that adhere to international standards and good practices in the public and private sectors.

R5.10 Monitor and assess the quality of software used in public and private sectors.

TECHNICAL SECURITY CONTROLS

R5.11 Promote user understanding of the importance of anti-malware software and network firewalls.

R5.12 Establish policies for technical security control deployment in critical infrastructure and ISPs.

R5.13 Keep technical security controls up-to-date within the public and private sector, monitor their effectiveness and review on a regular basis.

R5.14 Conduct penetration testing of technical security controls to upstream user and private/public sector protection.

CRYTOGRAPHIC CONTROLS

R5.15 Encourage the development and dissemination of cryptographic controls across all sectors and users for protection of data at rest and in transit, according to international standards and guidelines.

R5.16 Raise public awareness of secure communication services, such as encrypted/signed emails.

R5.17 Promote deployment of state-of-the-art tools, such as SSL or TLS, by web service providers, to secure all communications between servers and web browsers.

R5.18 Develop encryption and cryptographic control policies within the public and private sectors based on previous assessments, and regularly review the policies for effectiveness.

CYBERSECURITY MARKETPLACE

R5.19 Consider promoting the production of cybersecurity products by domestic providers in accordance with market needs.

R5.20 Ensure that cybersecurity technology development abides by secure coding guidelines, good practices and adheres to internationally accepted standards.

R5.21 Promote the establishment of a market for cyber-insurance and encourage information-sharing among participants of the market.

RESPONSIBLE DISCLOSURE

R5.22 Develop a responsible vulnerability-disclosure framework or policy with all stakeholders involved (product vendors, customers, security vendors and public) and facilitate its adoption in the private sector, including a disclosure deadline, a schedule for resolution and an acknowledgment report.

R5.23 Encourage software and service providers to address bug and vulnerability reports.

R5.24 Encourage sharing of technical details of vulnerabilities among critical infrastructure organisations and ISPs.

R5.25 Publish the analysis of the technical details of vulnerabilities and disseminate advisory information according to different individual roles and responsibilities.

ADDITIONAL REFLECTIONS

Overall, the representation and composition of stakeholder groups was balanced and comprehensive. The MoTLG extended invitations to stakeholders in advance of the review, and while it is difficult to ascertain whether all relevant experts were present, the input gathered over the three days was key to ensuring a successful review.

This was the eighteenth country review that GCSCC has supported directly. Iceland has begun the process of developing different aspects of cybersecurity capacity across all dimensions, including through implementing the action plan of the National Cybersecurity Strategy and revisiting legal frameworks and regulation.

These efforts will establish the foundations for more advanced capacity in the future. GCSCC hopes that this review will offer useful insights to Iceland and that the review's recommendations will contribute to continuing work on enhancing cybersecurity capacity across all five dimensions of the CMM.

APPENDIX

SUMMARY OF REVIEW RESULTS

CAPACITY FACTORS	STAGE OF MATURITY	REFERENCES	RECOMMENDATIONS
D1.1 National Cybersecurity Strategy	**Established**	National Cybersecurity Strategy (NCSS) 2015-2026 https://www.government.is/media/innanrikisraduneyti-media/media/frettir-2015/Icelandic_National_Cyber_Security_Summary_loka.pdf https://www.stjornarradid.is/news/article/2015/07/03/National-Cyber-Strategy-for-Iceland-released/ The Ministry of Transport and Local Government (MoTLG) https://www.government.is/news/article/2017/05/01/Two-new-ministries-commence-operation/	**R1.1** Ensure that the National Cybersecurity Strategy content includes, at a minimum: explicit links to national risks, priorities, objectives, and business development, raising public awareness, mitigating cybercrime, and protecting critical infrastructure from external and internal threats. **R1.2** Encourage the promotion and implementation of the National Cybersecurity Strategy by multiple stakeholders across government and other sectors. **R1.3** Administer a discrete cybersecurity budget line in order to allocate and manage resources. **R1.4** Conduct regular scenario and real-time cyber exercises that provide a concurrent picture of national cyber resilience. **R1.5** Collect and evaluate relevant metrics, monitoring processes and data in order to inform decision-making. **R1.6** Include in the NCSS provision for the protection of critical infrastructure from insider threats.
D1.2 Incident Response	**Formative to Established**	CERT-IS https://www.cert.is/en/node/2.html https://www.cert.is/en/node/2.html Telecommunication Act no. 81/2003 http://www.althingi.is/lagas/nuna/2003081.html#G47A	**R1.7** Develop an operational central registry of national level cybersecurity incidents and implement guidelines of the GDPR and the NIS. **R1.8** Improve incident identification and analysis in response and conduct regular, systematic updates to the national level incident registry. **R1.9** Ensure that the human and financial resources allocated to incident response are adequate to the cybersecurity threat environment by

		Art. 47 and regulation no. 475/2013 https://www.stjornartidindi.is/Advert.aspx?ID=f5282f2a-6827-4d98-9fc2-0afd611243d6 Nordic Financial CERT https://www.nordea.com/en/press-and-news/news-and-press-releases/the-digital-hub/2017/2017-04-10-collaboraration-is-key-in-fighting-cybercrime.html Nordic National CERT Collaboration https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf	conducting regular scenario exercises designed to test human, organisational and financial capacities. **R1.10** Promote coordinated national incident response between public and private sectors, with lines of communication prepared for times of crisis. **R1.11** Develop a culture of risk assessment and management predictive methods to assess risk, its propagation and its aggregation for the national and CI domain. **R1.12** Establish mechanisms for regional and international cooperation for incident response between organisations to resolve incidents as they occur. **R1.13** Promote a platform for the reporting and sharing of incidents across sectors.
D1.3 Critical Infrastructure (CI) Protection	**Formative**	Parliamentary Resolution on a National Security Policy for Iceland (no. 26/145) https://www.government.is/media/utanrikisraduneyti-media/media/Varnarmal/National-Security-Policy-ENS.pdf Global Influenza Preparedness Plan http://www.landlaeknir.is/servlet/file/store93/item19632/Pandemic%20Influenza%20Preparedness%20Plan_March.06_.pdf Financial Supervisory Authority (FSA) https://en.fme.is/ Annual Report of the Financial Supervisory Authority 2016 https://en.fme.is/media/utgefid-efni/FME-arsskyrsla-2016-ENSKA-29072016.pdf	**R1.14** Perform detailed audits of CI assets as it relates to cybersecurity on a regular basis and disseminate CI asset audit lists to relevant stakeholders. **R1.15** Implement regular audit practices to assess network and system dependencies to inform continuous reassessment of risk portfolio. Identify and establish specific auditing processes. **R1.16** Develop a strategy for strengthening formal coordination regarding Critical National Infrastructure (CNI) and information sharing between public and private sector. **R1.17** Establish a mechanism for regular vulnerability disclosure with defined scope for reporting incidents between CI asset owners and the government. **R1.18** Promote strategic engagement between government and CI. **R1.19** Define formal internal and external CI communication strategies across sectors, with clear points of contact. **R1.20** Optimize the legal framework concerning CNI by amending existing legislation or enacting new regulations as needed to encompass incident prevention, detection and response. **R1.21** Continue to invest in capability of Board Members and Senior Leaders of CI organisations to understand cyber-risk intelligence, in both private and public sectors, so that relevant individuals can lead in the face of crisis and take their part in risk management more generally.

			R1.22 Use CI risk management procedures to create a national response plan including the participation of all vital entities.
D1.4 **Crisis Management**	**Formative**	ENISA risk assessment exercises https://www.enisa.europa.eu/topics/cyber-exercises	**R1.23** Prioritise crisis management exercises, especially at a local level, and communicate the value of these exercises to all sectors. **R1.24** Conduct compromised communications scenarios and exercises to test emergency response asset interoperability and effective functionality and incorporate the results of the exercises to inform strategic investment in future emergency response assets. **R1.25** Plan the exercises by engaging relevant participants, outlining their role in the exercise, and articulating the benefits and incentives for participation.
D1.5 **Cyber Defence Consideration**	**Start-up**	Defence Act No 34/2008 https://www.government.is/topics/foreign-affairs/national-security/ Iceland Crisis Response Unit (ICRU) https://www.government.is/topics/foreign-affairs/icru/ NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) https://ccdcoe.org/about-us.html https://ccdcoe.org/cyber-security-strategy-documents.html The Tallinn Manual 2.0 https://ccdcoe.org/tallinn-manual.html Trident Juncture 2018 https://forsvaret.no/en/exercise-and-operations/exercises/nato-exercise-2018 Memorandum of Understanding (MOU) with NATO http://www.nicp.nato.int/iceland-signs-new-mou-on-	**R1.26** Review compliance of the National Security Strategy with international law and its consistency with national and international rules of engagement in cyberspace. **R1.27** Form a formal Research Cluster comprised by stakeholders from Government, Academia and Intelligence working on national cyber resilience. This Cluster will be working towards resilience on national CI (see D1.3). **R1.28** Initiate discussions regarding the participation and membership to NATO CCDCOE and participation to exercises.

		cyber-defence-cooperation/index.html	
D1.6 Communications Redundancy	**Formative**		**R1.29** Undertake outreach to, and education of key stakeholders in the need for digital and communications redundancy. **R1.30** Test the interoperability and function of emergency response assets under compromised communications scenarios to inform strategic investment in future emergency response assets based on the results of these scenario exercises. **R1.31** Allocate resources to hardware integration, technology stress testing, personnel training and crisis simulations drills.

Dimension 2 Cyber Culture ~~And~~ and Society

D2.1 Cybersecurity Mind-set	**Formative**		**R2.1** Enhance efforts at all levels of government, especially officials, and the private sector to employ cybersecurity good (proactive) practices. Design systems that enable users across society to embed secure practices more easily into their everyday use of the Internet and online services. **R2.2** Routinize cross-sectorial cooperation and information sharing among private and public sector organisations on cybersecurity risks and good practice. **R2.3** Identify vulnerable groups and high-risk behaviour across the public, in particular young people, to inform targeted, coordinated awareness campaigns, as recommended in R3.1.
D2.2 Trust and Confidence on the Internet	**Formative to Established**		**R2.4** Establish ISP programmes to promote trust in their services based on measures of effectiveness of these programmes. **R2.5** Promote data protection by default and data protection by design as a tool for transparency in the provision of e-governance services (including e-health and e-police). Implement feedback mechanisms for use to ensure that the e-services are continuously improved and trust is strengthened among users.

			R2.6 Employ processes for gathering user feedback within government agencies in order to ensure efficient management of online content. **R2.7** Ensure that the private sector applies security measures to establish trust in e-commerce services, including informing users of the utility of deployed security solutions.
D2.3 User Understanding of Personal Information Protection Online	**Formative**		**R2.8** Promote the understanding of protection of personal information online among users and promote the development of their skills to manage their privacy online. **R2.9** Encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making. **R2.10** Promote the compliance to web standards that protect the anonymity of users. **R2.11** Promote data protection by default and by design as a tool for transparency. **R2.12** Develop user-consent policies designed to notify practices on the collection, use or disclosure of sensitive personal information.
D2.4 Reporting Mechanisms	**Formative**	Barnaheill - Save the Children Iceland www.barnaheill.is INHOPE http://www.saft.is/wp-content/uploads/2013/10/SAFT_2013_annual_report_lowres.pdf	**R2.13** Establish reporting mechanisms for reporting online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents in accordance with GDPR, NIS directive. **R2.14** Encourage different stakeholders (public-private sector, Police, DPA, CERT-IS) to coordinate the reporting mechanisms and their roles and responsibilities, and to collaborate and share good practices to improve the mechanisms. **R2.15** Establish awareness programmes to promote the regular use of reporting mechanisms by public and private sectors, and their use as an investment in loss prevention and risk control. **R2.16** Establish awareness programmes to promote cyber security and data protection in the public sphere as well as within private entities that process a great amount of personal data on a daily basis, i.e. financial institutions, insurance, IT, marketing etc. **R2.17** Employ effectiveness metrics for all existing mechanisms and ensure that they contribute to their improvement.

D2.5 **Media and Social Media**	**Formative**	Freedom House Report https://freedomhouse.org/report/freedom-net/2016/iceland The Media Commission http://fjolmidlanefnd.is/english/ Crime & Safety Report https://www.osac.gov/Pages/ContentReportDetails.aspx?cid=21376 Iceland Review http://icelandreview.com/news/2015/11/30/increasingly-dangerous-internet-attacks-iceland Grapevine https://grapevine.is/news/2015/12/09/vodafone-falls-prey-to-cyber-attack/ The Hacker News http://thehackernews.com/2013/11/vodafone-iceland-hacked-and-exposed.html	**R2.18** Encourage media and social media providers to further extend the coverage beyond threat reporting and focus on informing the public about proactive and actionable cybersecurity measures, as well economic and social impacts. **R2.19** Encourage a frequent discussion about cybersecurity on social media. **R2.20** Ensure that the debate in social and mainstream media and the attitudes expressed inform policymaking.

Dimension 3 Cybersecurity Education, Training and Skills

D3.1 **Awareness-raising**	**Formative**	Heimili og skóli (Home and School) http://www.heimiliogskoli.is/ Safer Internet Center Iceland (SAFT) http://www.saft.is/ SAFT Annual Report 2013 http://www.saft.is/wp-content/uploads/2013/10/SAFT_2013_annual_report_lowres.pdf Netöryggi www.netöryggi.is Safer Internet Day http://www.eccisland.is/en/about-ecc-net/news/safe-internet-day-2017	**R3.1** Develop a national cybersecurity awareness-raising programme with specified target groups, focusing on the most vulnerable users. **R3.2** Appoint a designated organisation (from any sector) to lead the cybersecurity awareness-raising programme. **R3.3** Engage relevant stakeholders from public and private sectors in the development and delivery of the awareness-raising programme as well as for the creation and utilisation of programmes and materials. **R3.4** Create a single online portal linking to appropriate cybersecurity information and disseminate the cybersecurity awareness programme via this platform. **R3.5** Enact evaluation measurements to study effectiveness of the awareness programmes at a level where they

		The 5 Commandments For Safer Internet Use http://www.eccisland.is/sites/default/files/atoms/files/safe_internet_day_2017.pdf	inform future campaigns taking into account gaps or failures. **R3.6** Promote awareness of risks and threats at lower levels of the government. **R3.7** Develop a dedicated awareness-raising programme for executive managers within the public and private sectors, particularly those in the financial and telecommunications sectors. **R3.8** Promote awareness regarding the protection of personal information online. **R3.9** Promote awareness raising efforts of cybersecurity crisis management at the executive level **R3.10** Develop operational cyber security self-education websites.
D3.2 Framework for Education	**Formative**	University of Iceland http://english.hi.is/ Reykjavík University https://en.ru.is/ Ministry of Education, Science and Culture https://www.government.is/ministries/ministry-of-education-science-and-culture/ Icelandic Centre for Research (RANNIS) https://en.rannis.is/ ECRI Institute https://www.ecri.org/about/Pages/default.aspx https://www.ecri.org/Resources/In_the_News/Cybersecurity_Its_Clinical_Too(Trustee).pdf NTNU, Master in Information Security https://www.ntnu.edu/studies/mis	**R3.11** Create cybersecurity education programmes for instructors of cybersecurity to ensure that skilled staff is available to teach newly formed cybersecurity courses. **R3.12** Create accredited cybersecurity-specific degree courses at the university level, in addition to the other existing cybersecurity-related courses in the various Icelandic universities, in cooperation with other European/international universities. **R3.13** Promote efforts by Universities and other bodies to hold seminars/lectures on cybersecurity issues aimed at non-specialists, in cooperation with other European/international universities. **R3.14** Allocate additional resources to cybersecurity education for public universities, dedicated to national cybersecurity research and laboratories at universities. **R3.15** Establish cooperation agreements with European/International Universities in order students to enrol to programmes abroad. **R3.16** Provide more opportunities for individuals (such as students and experts) to gain experience, through internships and apprenticeships, in cooperation with other European/international universities, in order to enhance their expertise by combining education and practical training.

			R3.17 Inform cybersecurity education priorities through broad consultation across government, private sector, academia and civil society, linked to the National Cybersecurity Strategy. **R3.18** Promote competitions and initiatives for students by government and/or industry in order to increase the attractiveness of cybersecurity careers. **R3.19** Ensure the sustainability of research programs. **R3.20** Develop effective metrics to ensure that educational and skill enhancement investments meet the needs of the cybersecurity environment.
D3.3 Framework for Professional Training	**Formative**	Syndis https://www.syndis.is/owasp-top-10-training	**R3.21** Establish more structured cybersecurity training programmes to develop skills towards building a cadre of cybersecurity-specific professionals. **R3.22** Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, and models and operation of these tools. **R3.23** Train general IT staff on cybersecurity issues so that they can react to incidents as they occur. **R3.24** Ensure that affordable security professional certification is offered across sectors within the country. **R3.25** Develop a central platform for sharing training information for experts and create a national-level register of cybersecurity experts. **R3.26** Establish requirements for joint cybersecurity training for the public and private sector and develop collaborative training platforms. **R3.27** Establish job creation initiatives for cybersecurity within organisations and encourage employers to train staff to become cybersecurity professionals. **R3.28** Begin to implement metrics evaluating take-up of ad-hoc training courses, seminars, online resources, and certification offerings.

Dimension 4 Legal and Regulatory Frameworks

D4.1 **Legal Frameworks**	**Established**	Regulatory Framework of the European Union https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf Alþingi https://www.althingi.is/pdf/Althingi2013_enska.pdf National report submitted in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21 Iceland https://www.upr-info.org/sites/default/files/document/islande/session_26_-_octobre_2016/a_hrc_wg.6_33_isl_1_e_0.pdf Electronic Communications Act (ECA) No. 81 from March 2003: https://www.stjornarradid.is/publications/legislation/lex/2018/01/16/Electronic-Communications-Act-No.-81-26-March-2003/ Act on the Post and Telecom Administration (APTA) No. 69, from March 2003: https://www.stjornarradid.is/publications/legislation/lex/2018/01/04/Act-on-the-Post-and-Telecom-Administration-No.-69-24-March-2003/ APTA Amendment No. 62 https://www.pfs.is/upload/files/Act%20no.62_2012.pdf Criminal Proceedings Act: https://www.government.is/publications/legislation/lex/2018/01/15/Law-on-	**R4.1** Continue to review existing legal and regulatory mechanisms for ICT security to identify where gaps and overlaps may exist and amend or enact new laws accordingly. Monitor the enforcement of the legislative frameworks and ensure that it informs resources allocation and legal reform. Put mechanisms in place for keeping ICT legal frameworks in harmony with national cybersecurity-related ICT policies, international law, standards and good practices. **R4.2** Ensure that international and regional trends and good practices inform the assessment and amendment of domestic legal frameworks protecting human rights online and associated resource planning. In order to meet dynamic changes in the application of technology to human rights, identify procedures to amend and update legal frameworks as needed. **R4.3** Continue to actively contribute to the global discourse on human rights on the Internet. Foster research on human rights on the Internet and ensure that measures are in place to exceed minimal baselines specified in international agreements. Continue to actively contribute to the global discourse on human rights and move the focus on human rights on the Internet. **R4.4** Ensure that the GDPR and the Police Directive on the processing of personal data is successfully implemented and legal mechanisms are in place that enable. Identify international and regional trends and good practices to inform the assessment and amendment of data-protection laws and associated resource planning. **R4.5** Improve national child protection online legislation to comply with regional and international law and standards. **R4.6** In order to meet dynamic changes in the application of technology to consumer protection, develop and implement procedures to amend and update legal frameworks as needed. **R4.7** Review the legislation on intellectual property online through consultation with key stakeholders and through public discourse to reflect changes in national priorities and the international ICT landscape.

		Criminal-Procedure-No.-88-2008-Exerpts/ Regulation on protection, functionality, and quality of IP communications services", No. 1223 from 2007 https://www.pfs.is/upload/files/REGULATION_no.1223_IP%20communication.pdf Icelandic Media Law http://fjolmidlanefnd.is/wp-content/uploads/2011/12/Log-um-fjolmidla_ensk-thyding_mai2015.pdf Act No 28/2001 on Electronic Signatures: https://www.stjornarradid.is/publications/legislation/lex/2018/02/01/Merchants-and-Trade-Act-No-28-2001-on-electronic-signatures/ Regulation No. 780/2011 http://www.neytendastofa.is/lisalib/getfile.aspx?itemid=2736 Privacy Protection Act"), No. 77/2000 https://www.personuvernd.is/information-in-english/greinar/nr/438 European Parliament and of the Council 1995 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML Rules No. 299/2001 on the Security of Personal Data https://www.personuvernd.is/information-in-english/greinar/nr/442 Regulation in the Protection of Information in the Public Communications Networks no 1221/2007 https://www.pfs.is/library/Skrar/Innflutt/PDF/REGULATION_no.1221_Protectio	**R4.8** Develop and implement measures to exceed minimal baselines for substantive and procedural cybercrime frameworks specified in international treaties where appropriate, which includes procedures to amend those frameworks as needed. **R4.9** Ensure that in the case of cross-border investigation, procedural law stipulates what actions need to be conducted under particular case characteristics, in order to successfully investigate cybercrime.

		n%20of%20information.pdf Data Protection Authority (DPA) https://www.personuvernd.is/information-in-english/greinar/nr/438 Freedom House https://freedomhouse.org/report/freedom-net/2016/iceland The constitution http://www.government.is/constitution/ https://www.upr-info.org/sites/default/files/document/islande/session_26_-_octobre_2016/a_hrc_wg.6_33_isl_1_e_0.pdf Media Law http://fjolmidlanefnd.is/wp-content/uploads/2011/12/Log-um-fjolmidla_ensk-thyding_mai2015.pdf Information Act No. 140/2012 https://www.government.is/publications/legislation/lex/2018/01/19/The-Information-Act-No.-140-2012/ UN Universal Declaration of Human Rights and Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe https://treaties.un.org/pages/showDetails.aspx?objid=080000028014a40b Icelandic Human Rights Centre (ICEHR) http://www.humanrights.is UN Convention on the Rights of the Child: https://www.government.is/topics/social-welfare-and-families/

Act No 62/2005
www.neytendastofa.is/lisalib/getfile.aspx?itemid=1402

European Parliament and Council Directive 1999/93/EB
https://portal.etsi.org/esi/Documents/e-sign-directive.pdf

Forum of European Supervisory Authorities
http://www.fesa.eu/index.html

Copyright Act No. 126/2011
http://www.wipo.int/edocs/lexdocs/laws/is/is/is108is.pdf

Icelandic Media Law
http://fjolmidlanefnd.is/wp-content/uploads/2011/12/Log-um-fjolmidla_ensk-thyding_mai2015.pdf

General Penal Code No. 19
http://www.althingi.is/altext/stjt/2006.074.html

Articles 257 and 228
http://www.parliament.am/library/Qreakan/islandia.pdf

Act on Collection of Evidence Relating to Alleged Violations of Intellectual Property Rights, No. 53/2006
https://www.stjornarradid.is/publications/legislation/lex/2018/01/15/Act-on-Collection-of-Evidence-Relating-to-Alleged-Violations-of-Intellectual-Property-Rights-No.-53-2006/

Law on Criminal Procedure 88/2008:
https://www.stjornarradid.is/publications/legislation/lex/2018/01/15/Law-on-Criminal-Procedure-No.-88-2008-Exerpts/

		EU ICT Security Policy https://joinup.ec.europa.eu/community/epractice/news/iceland-boosts-ict-security-measures-shares-policy	
D4.2 Criminal Justice System	**Formative**	International Association of Prosecutors http://www.iap-association.org/ Council of Europe http://www.coe.int/en/web/cybercrime/trainings	**R4.10** Invest in advanced investigative capabilities in order to allow the investigation of complex cybercrime cases, supported by regular testing and training of investigators. **R4.11** Allocate resources dedicated to fully operational cybercrime units based on strategic decision making in order to support investigations, especially at the local level. **R4.12** Enhance training and education of prosecutors and judges on cybercrime and data protection. Additional resources should be allocated for this purpose. **R4.13** Establish a formal mechanism to enable the exchange of information and good practices between prosecutors and judges to ensure efficient and effective prosecution of cybercrime cases. **R4.14** Collect and analyse statistics and trends regularly on cybercrime investigations, on cybercrime prosecutions and on cybercrime convictions.
D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime	**Established**	Cooperation with Interpol https://www.interpol.int/Member-countries/Europe/Iceland Cooperation with Europol https://www.europol.europa.eu/agreements/iceland Council of Europe Reservations and Declarations for Treaty No.185 - Convention on Cybercrime http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=CZVDo71s&_coeconventions_WAR_coeconventionsportlet_enVigueur=false&_coeconventions_WAR_coeconventionsportlet_searchBy=state&_coeconventions_WAR_coeconventionsportlet_c	**R4.15** Allocate resources to support the exchange of information between public and private sectors domestically and enhance legislative framework and communication mechanisms. **R4.16** Enhance established informal cooperation mechanisms between Internet Service Providers and PTA, DPA and law enforcement with clear communication channels.

		odePays=ICE&_coeconventions_WAR_coeconventionsportlet_codeNature=3	

Dimension 5 Standards, Organisations and Technologies

D5.1 Adherence to Standards	**Formative**	Financial Inspectorate Director (FSA) https://en.fme.is/ Public Procurement Act, No. 120/2016 https://www.stjornarradid.is/media/fjarmalaraduneyti-media/media/frettatengt2016/act-on-public-procurment-no.-120-2016.pdf ISO 29 115 https://www.iso.org/standard/45138.html Ríkiskaup, Government public procurement office https://www.rikiskaup.is/	**R5.1** Adopt a nationally agreed baseline of cybersecurity related standards and good practices across the public and private sectors, including standards in procurement and software development. **R5.2** Establish a body within government to assess the level of adoption of standards across public and private sectors. Apply metrics to monitor compliance. **R5.3** Promote discussions on how standards and good practices can be used to address risk within critical infrastructure supply chains by both government and infrastructure organisations.
D5.2 Internet Infrastructure Resilience	**Established**	The Global Competitiveness Report 2016-2017 http://www3.weforum.org/docs/GCR2016-2017/05FullReport/TheGlobalCompetitivenessReport2016-2017_FINAL.pdf OECD https://data.oecd.org/iceland.htm	**R5.4** Enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors. **R5.5** Conduct regular assessments of processes according to international standards and guidelines together with assessment of national information infrastructure security and critical services that drive investment in new technologies. **R5.6** Identify and map points of critical failure across the Internet infrastructure.

D5.3 **Software Quality**	**Start-up to Formative**		**R5.7** Develop a catalogue for secure software platforms and applications within the public and private sectors and share with all stakeholders. **R5.8** Establish software quality and functional requirements in public and private sectors, including policies on software updates. **R5.9** Promote the use of reliable software applications that adhere to international standards and good practices in the public and private sectors. **R5.10** Monitor and assess the quality of software used in public and private sectors.
D5.4 **Technical Security Controls**	**Formative to Established**		**R5.11** Promote user understanding of the importance of anti-malware software and network firewalls. **R5.12** Establish policies for technical security control deployment in critical infrastructure and ISPs. **R5.13** Keep technical security controls up-to-date within the public and private sector, monitor their effectiveness and review on a regular basis. **R5.14** Conduct penetration testing of technical security controls to upstream user and private/public sector protection.
D5.5 **Crypto-graphic Controls**	**Formative to Established**		**R5.15** Encourage the development and dissemination of cryptographic controls across all sectors and users for protection of data at rest and in transit, according to international standards and guidelines. **R5.16** Raise public awareness of secure communication services, such as encrypted/signed emails. **R5.17** Promote deployment of state-of-the-art tools, such as SSL or TLS, by web service providers, to secure all communications between servers and web browsers. **R5.18** Develop encryption and cryptographic control policies within the public and private sectors based on previous assessments, and regularly review the policies for effectiveness.

D5.6 **Cyber-security Marketplace**	**Start-up to Formative**		**R5.19** Consider promoting the production of cybersecurity products by domestic providers in accordance with market needs. **R5.20** Ensure that cybersecurity technology development abides by secure coding guidelines, good practices and adheres to internationally accepted standards. **R5.21** Promote the establishment of a market for cyber-insurance and encourage information-sharing among participants of the market.
D5.7 **Responsible Disclosure**	**Formative**		**R5.22** Develop a responsible vulnerability-disclosure framework or policy with all stakeholders involved (product vendors, customers, security vendors and public) and facilitate its adoption in the private sector, including a disclosure deadline, a schedule for resolution and an acknowledgment report. **R5.23** Encourage software and service providers to address bug and vulnerability reports. **R5.24** Encourage sharing of technical details of vulnerabilities among critical infrastructure organisations and ISPs. **R5.25** Publish the analysis of the technical details of vulnerabilities and disseminate advisory information according to different individual roles and responsibilities.

The review was conducted in cooperation with the *Ministry of Transport and Local Government*, of Iceland.

Global Cyber Security Capacity Centre

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

Cybersecurity Capacity Portal: www.sbs.ox.ac.uk/cybersecurity-capacity