Deploying the Cybersecurity Capacity Maturity Model for Nations in Iceland: findings and recommendations

Dr. Maria Bada, Lead Researcher
Global Cyber Security Capacity Centre
University of Oxford
Maria.Bada@cs.ox.ac.uk
@MariaBadaOxford

Reykjavik 30th November 2017

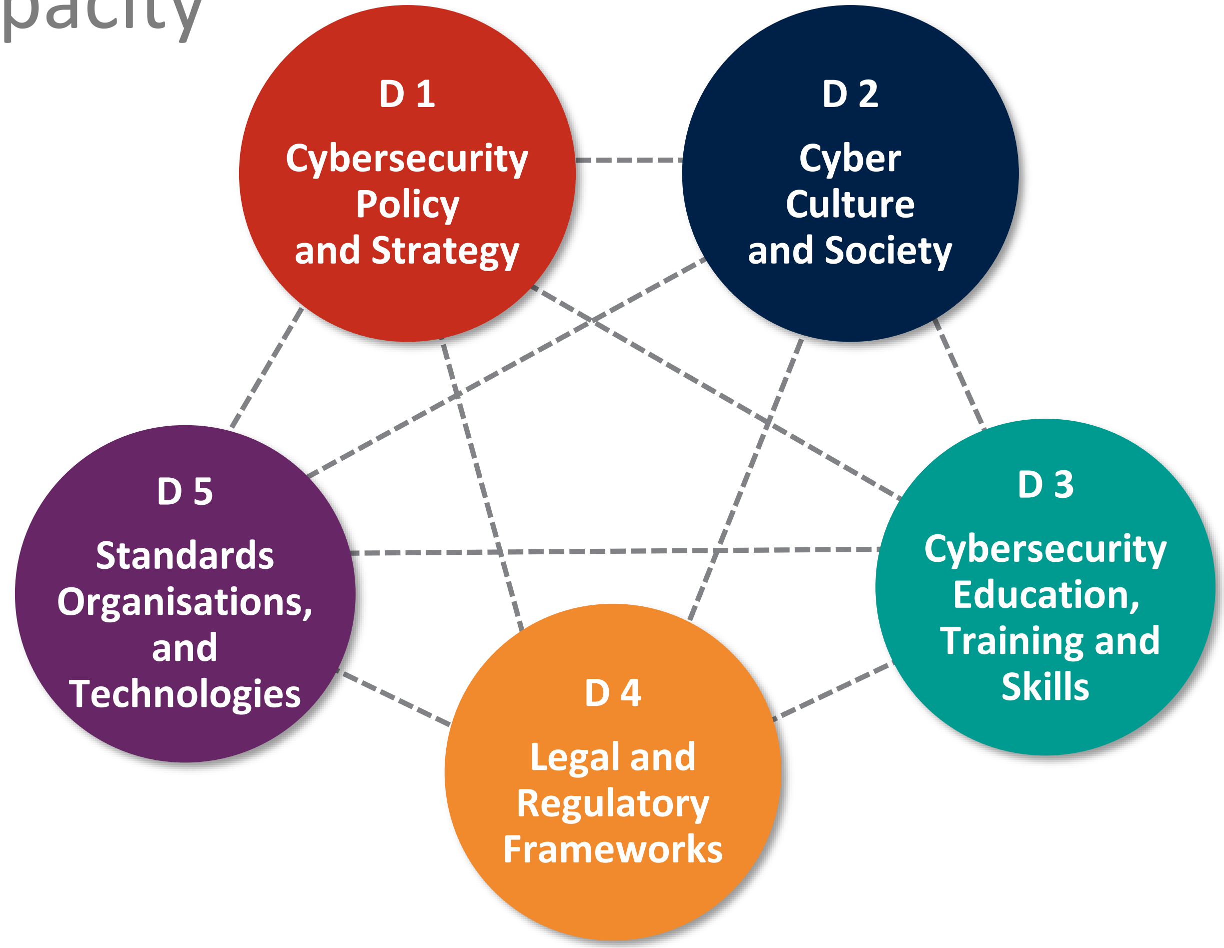
Global
Cyber Security
Capacity Centre

OXFORD
MARTIN
SCHOOL

UNIVERSITY OF
OXFORD

Cybersecurity Capacity Maturity Model for Nations (CMM)

The **5 DIMENSIONS** of Cybersecurity Capacity



D 1

Cybersecurity Policy and Strategy

D 2

Cyber Culture and Society

D 3

Cybersecurity Education, Training and Skills

D 4

Legal and Regulatory Frameworks

D 5

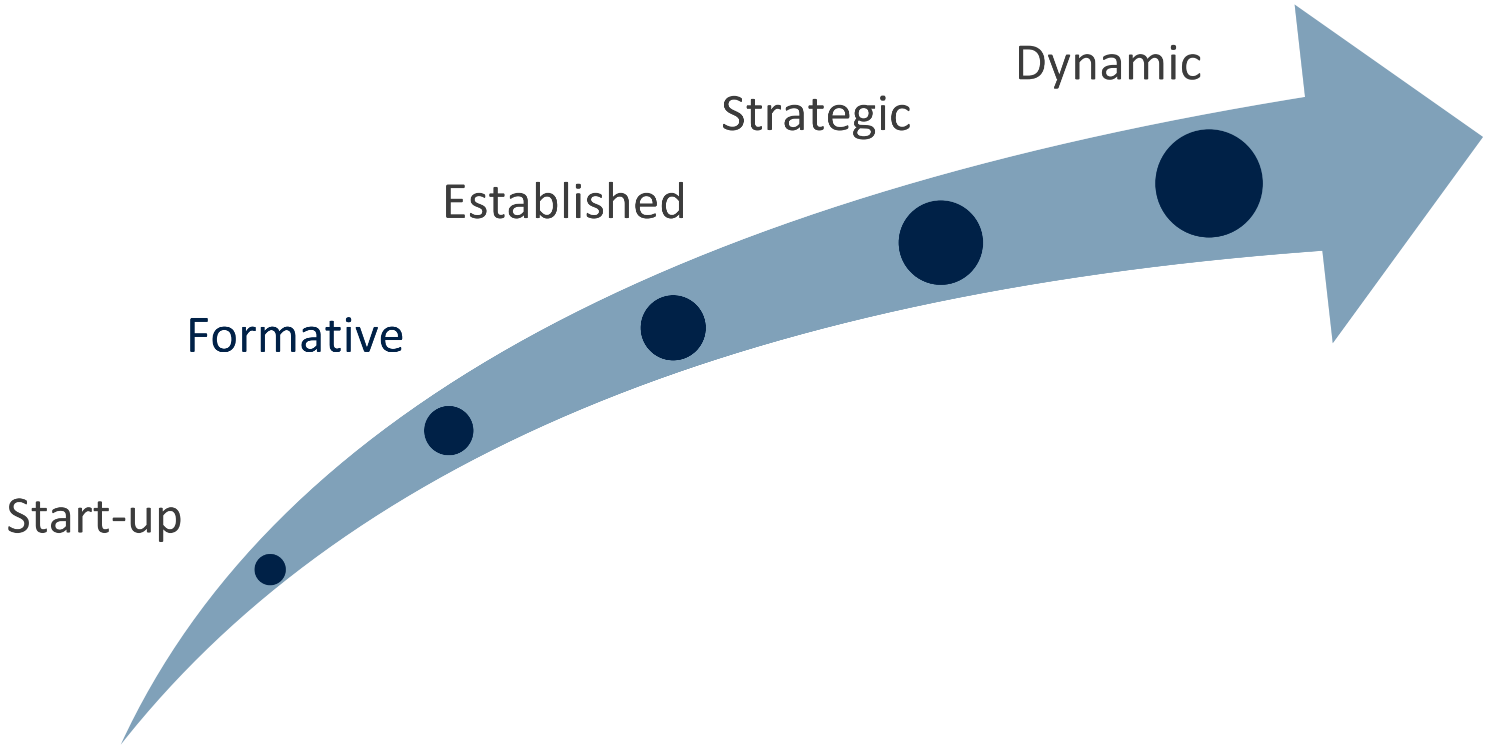
Standards Organisations, and Technologies

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Stages of Maturity



Start-up

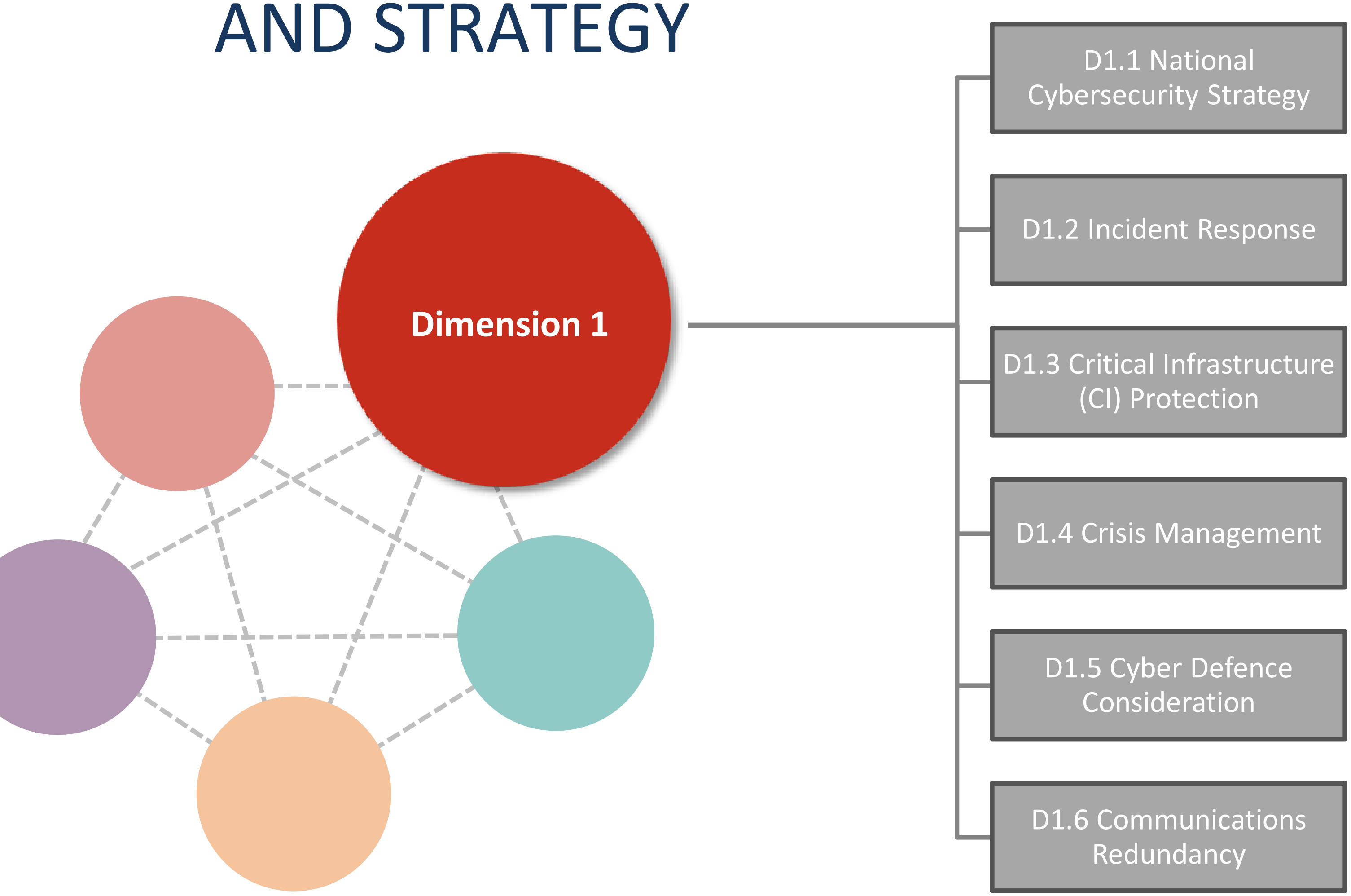
Formative

Established

Strategic

Dynamic

CYBERSECURITY POLICY AND STRATEGY

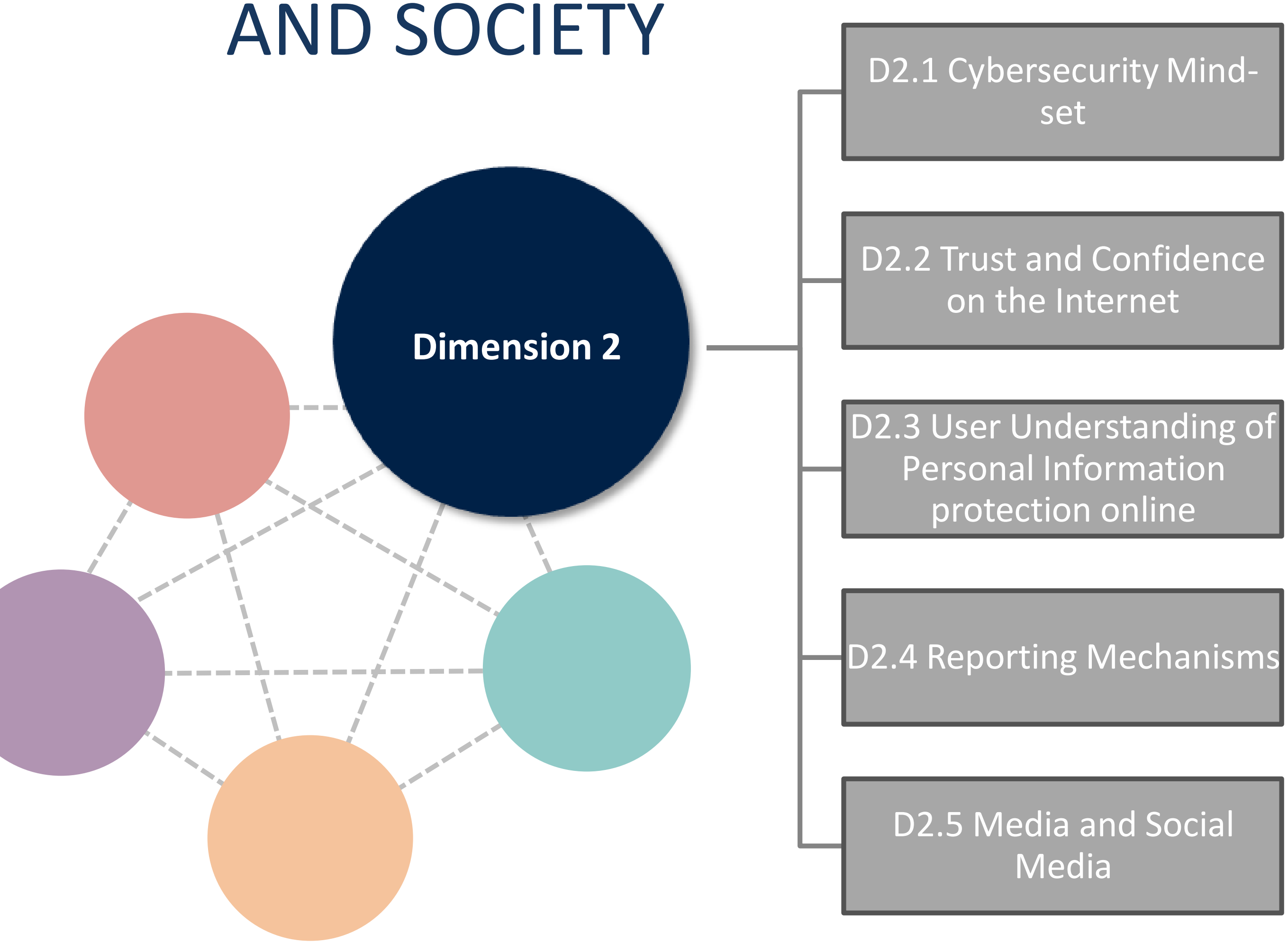

Dimension 1
D1.1 National Cybersecurity Strategy
D1.2 Incident Response
D1.3 Critical Infrastructure (CI) Protection
D1.4 Crisis Management
D1.5 Cyber Defence Consideration
D1.6 Communications Redundancy

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

CYBERSECURITY CULTURE AND SOCIETY



Dimension 2

D2.1 Cybersecurity Mind-set

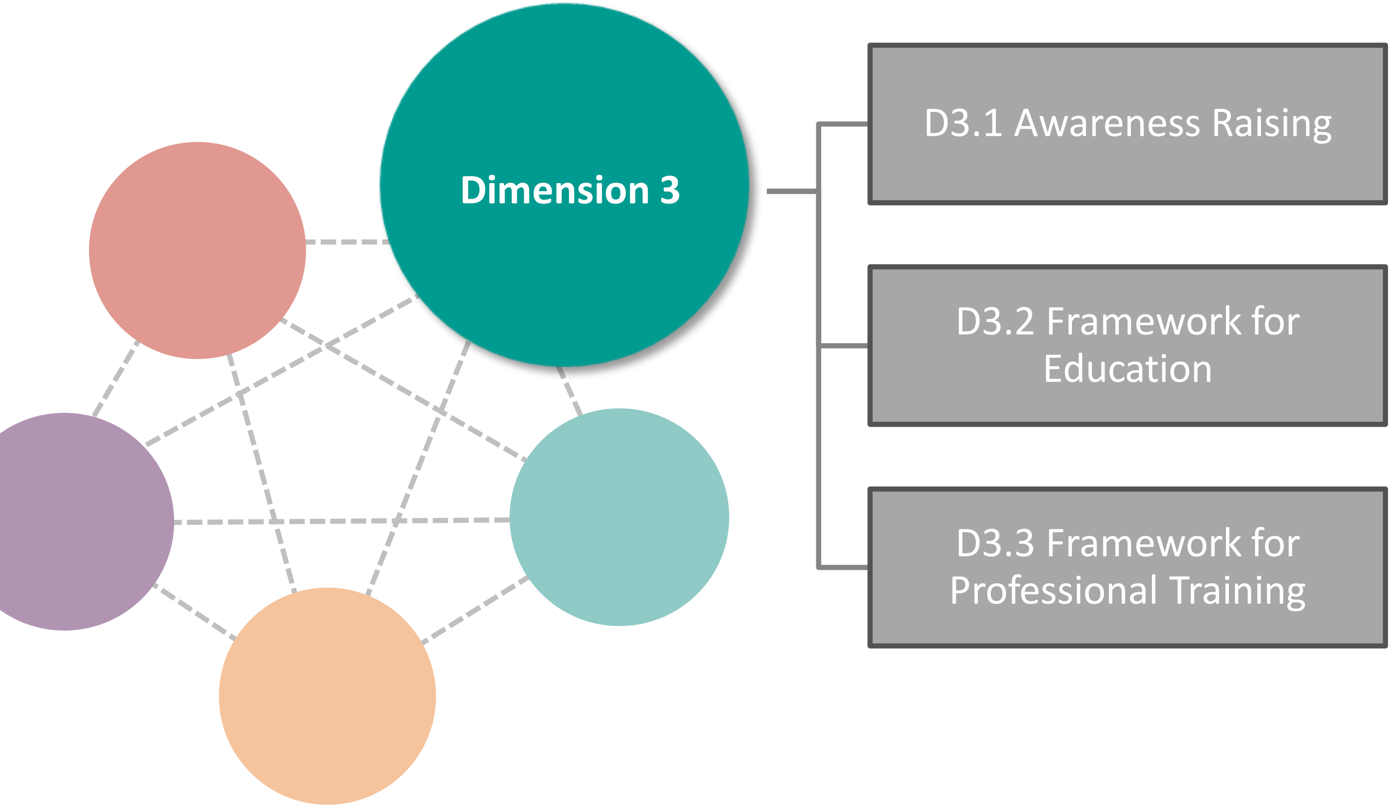
D2.2 Trust and Confidence on the Internet

D2.3 User Understanding of Personal Information protection online

D2.4 Reporting Mechanisms

D2.5 Media and Social Media

CYBERSECURITY EDUCATION, TRAINING AND SKILLS

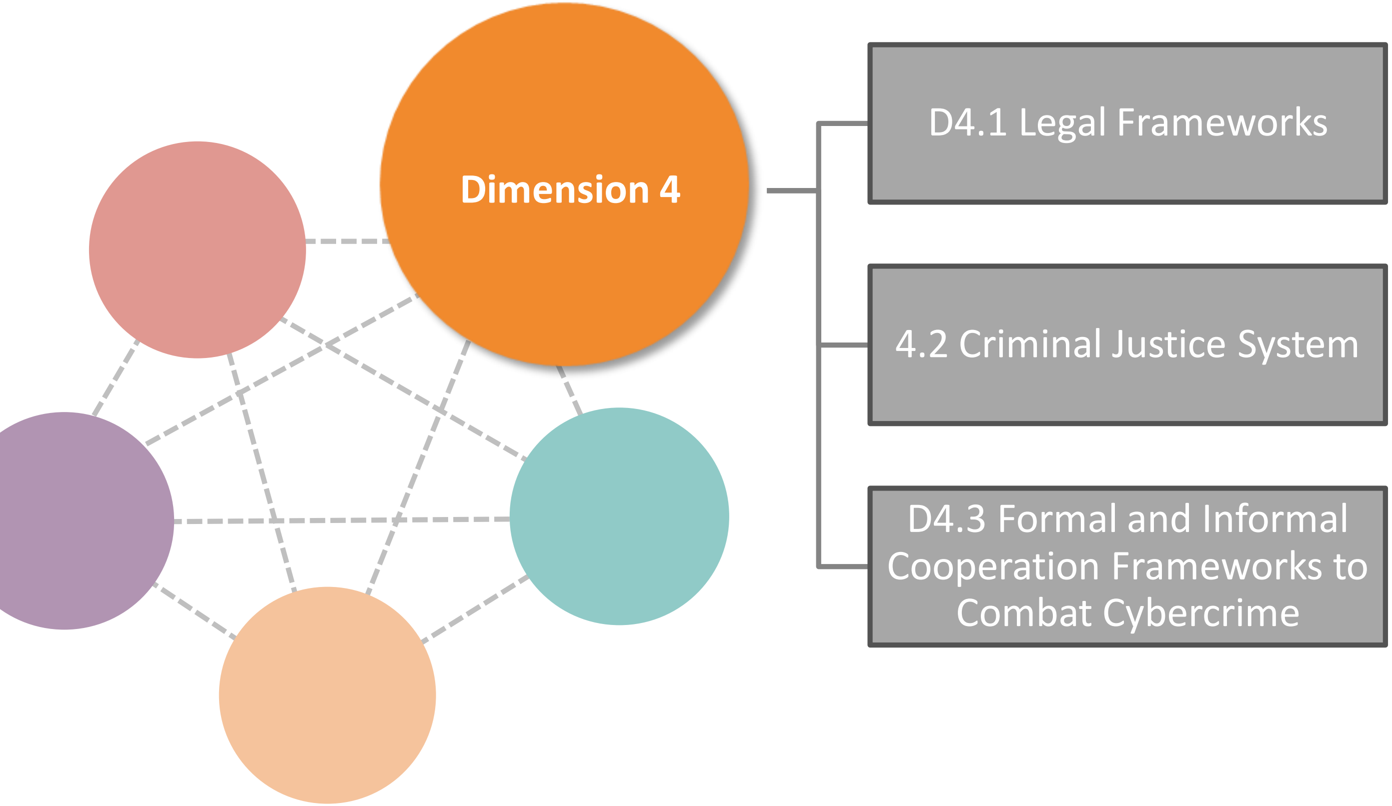


D3.1 Awareness Raising

D3.2 Framework for Education

D3.3 Framework for Professional Training

LEGAL AND REGULATORY FRAMEWORKS



Dimension 4

D4.1 Legal Frameworks

4.2 Criminal Justice System

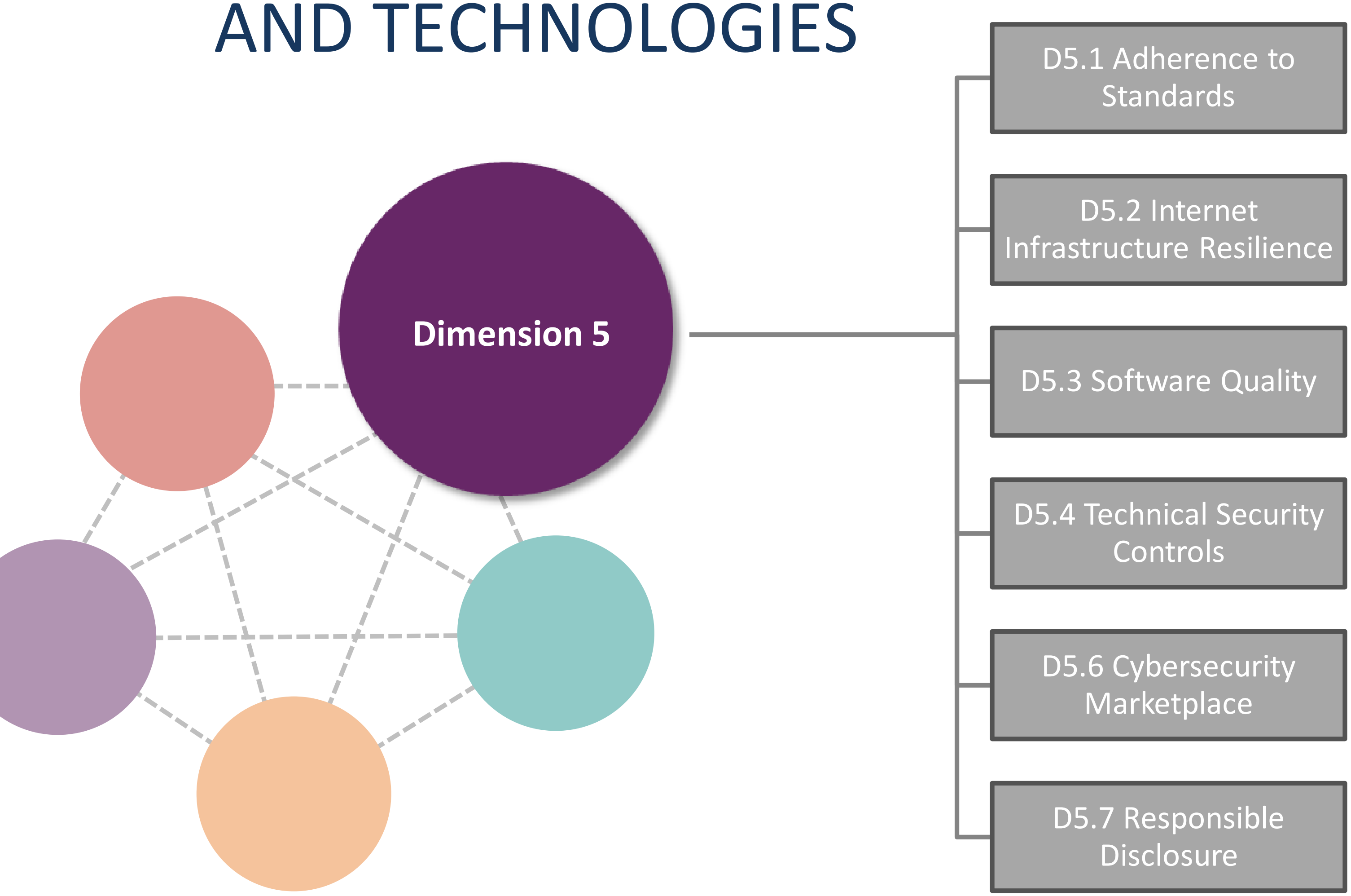
D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

STANDARDS, ORGANISATIONS AND TECHNOLOGIES



Dimension 5

D5.1 Adherence to Standards

D5.2 Internet Infrastructure Resilience

D5.3 Software Quality

D5.4 Technical Security Controls

D5.6 Cybersecurity Marketplace

D5.7 Responsible Disclosure

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

CYBERSECURITY CAPACITY REVIEW
Republic of Iceland

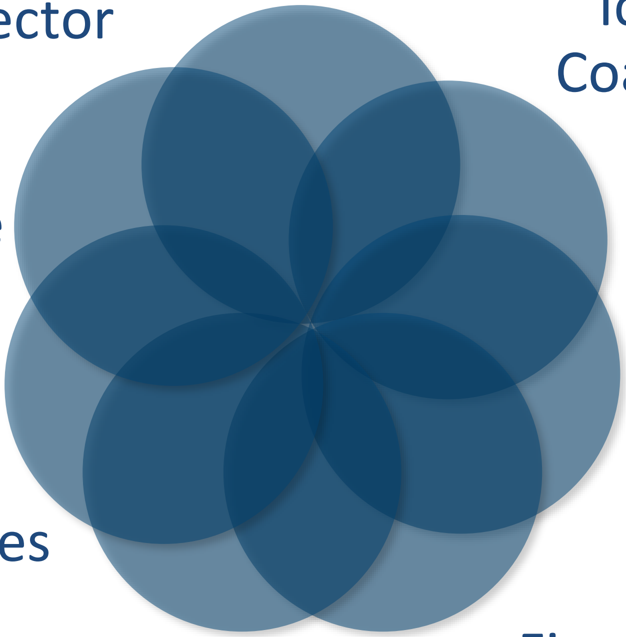
Methodology

Hosted by Iceland’s Ministry of Transport and Local Government (MoTLG)

Over the period 21–23 June 2017

- In-country focus group discussions with key stakeholders
- 10 sessions over 3 days
- Research team from the GCSCC

Stakeholder Clusters



Government

Icelandic Coast Guard

Academia/ Civil Society

Internet registries

Finance sector

Legislators

Public Prosecution

Health Authorities

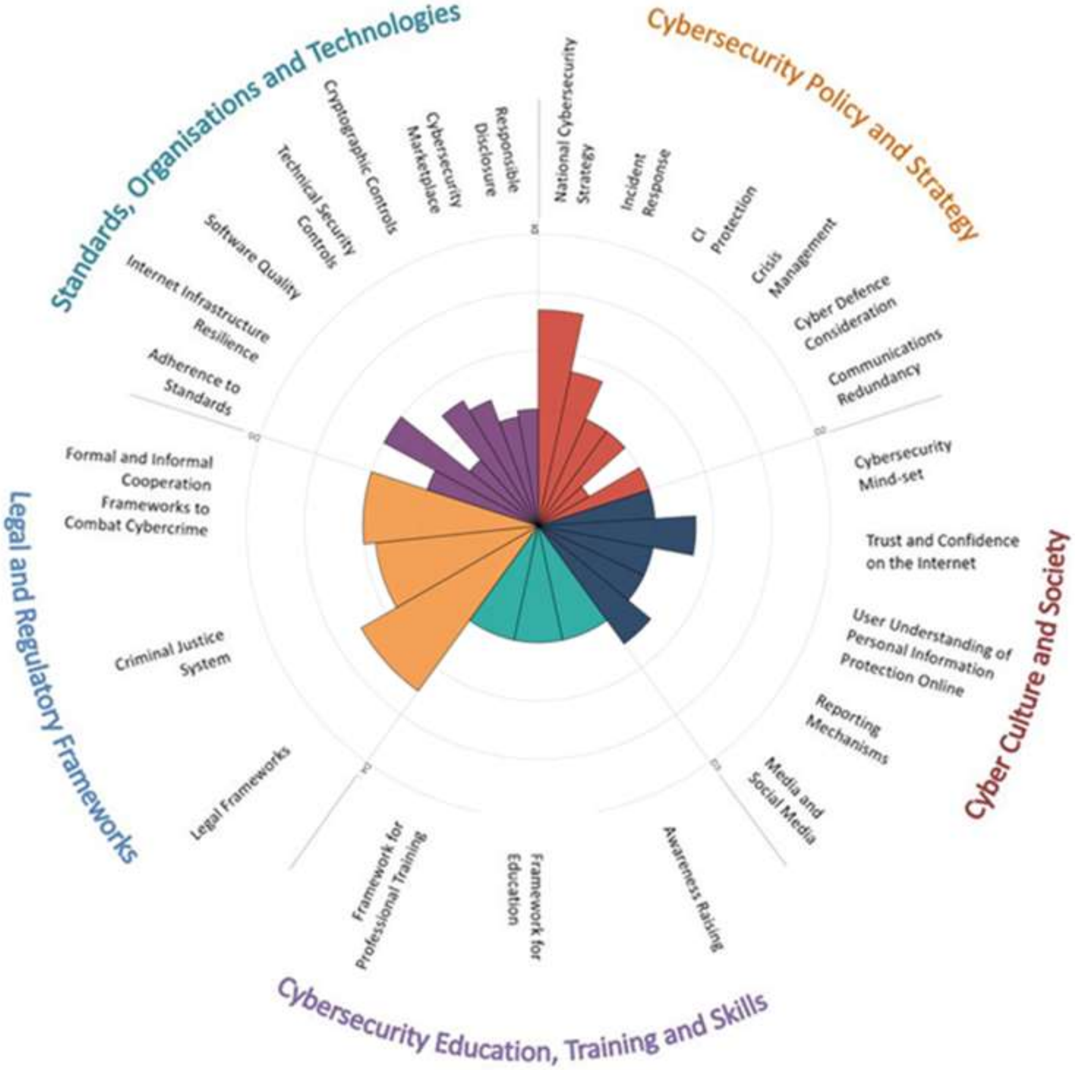
CERT and IT

Critical Infrastructure

Private sector

CMM Review in Iceland
Findings

Overall representation of the cybersecurity capacity in the Republic of Iceland

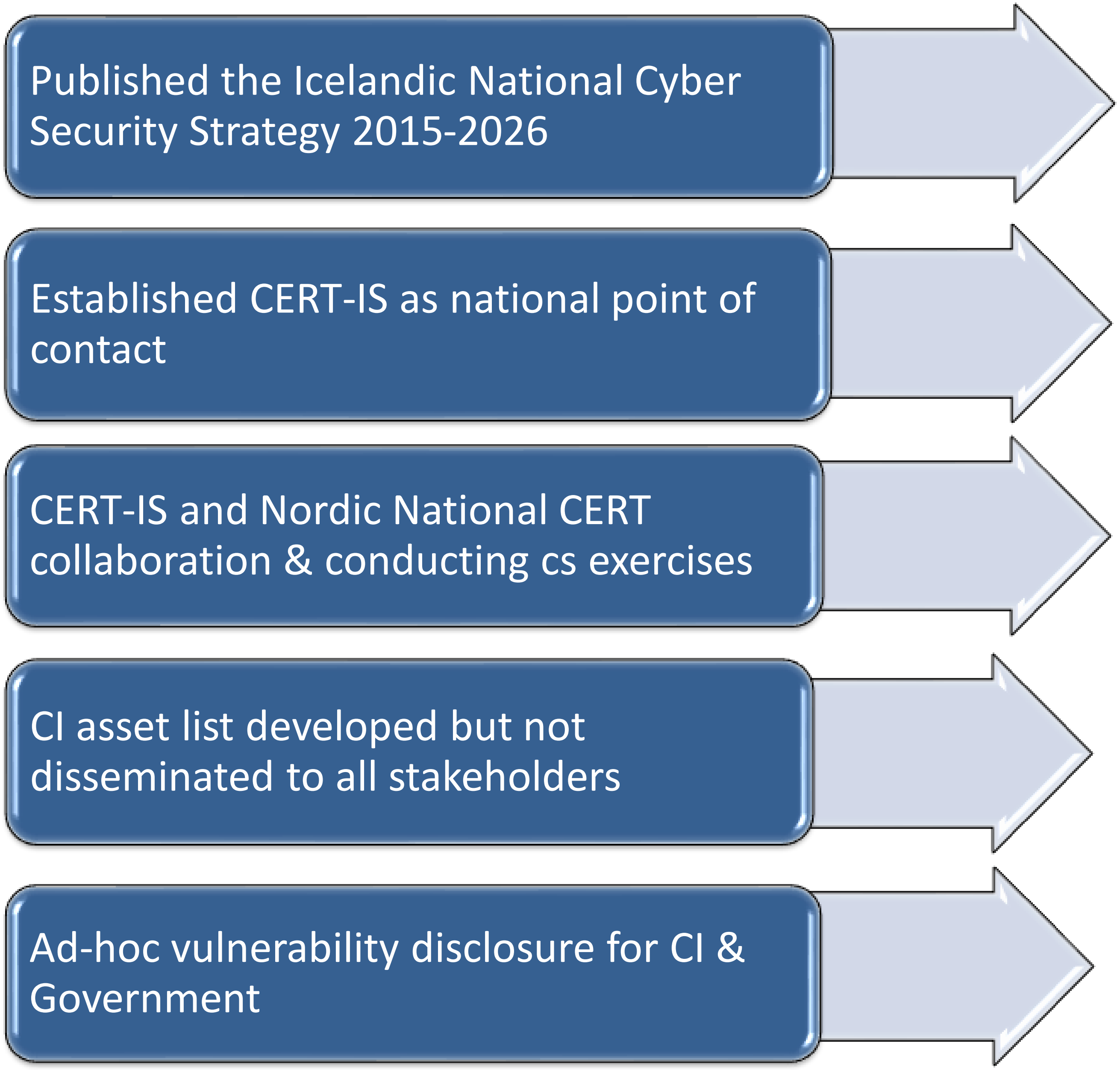


Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Cybersecurity Policy and Strategy



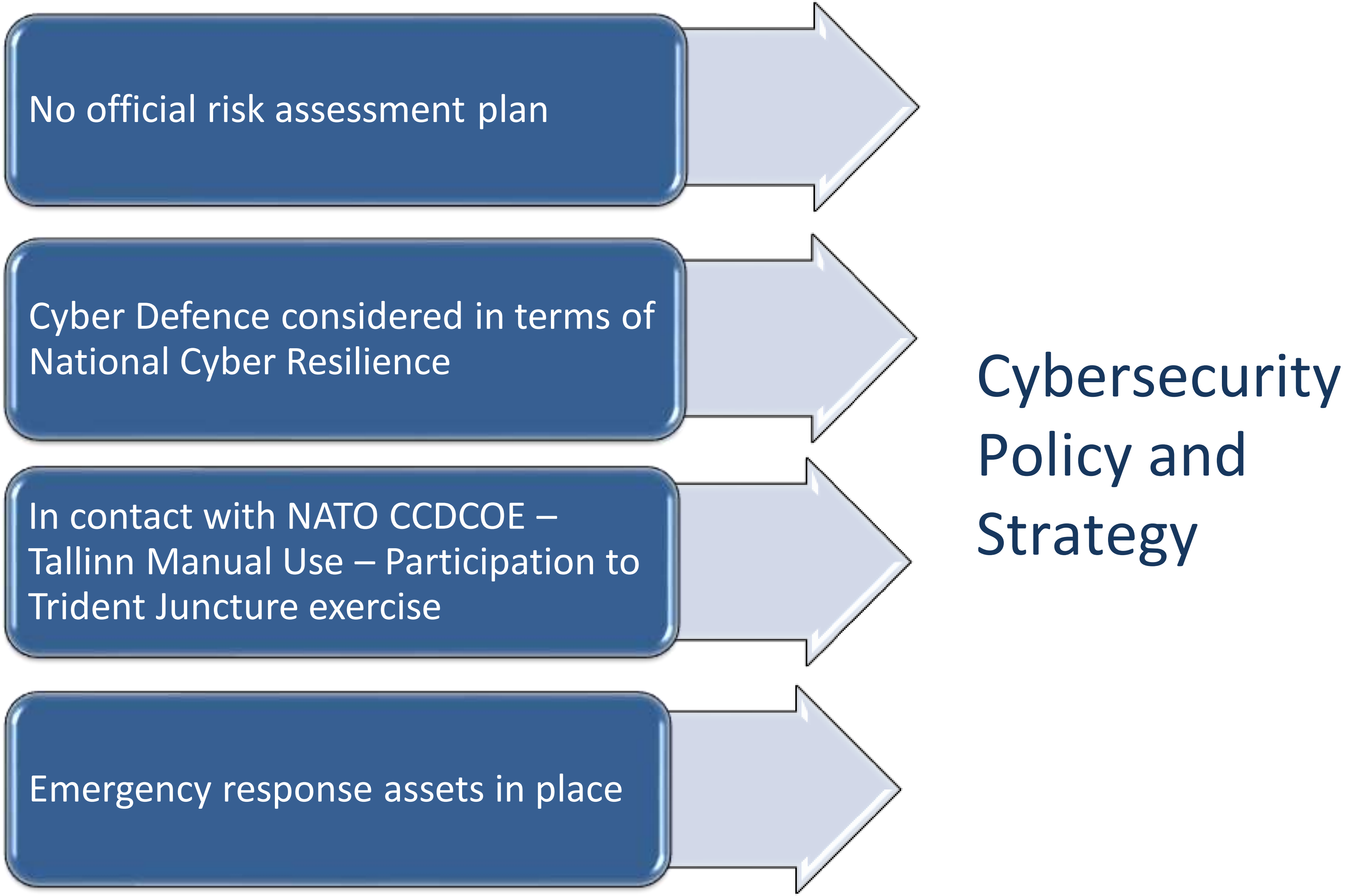
Published the Icelandic National Cyber Security Strategy 2015-2026

Established CERT-IS as national point of contact

CERT-IS and Nordic National CERT collaboration & conducting cs exercises

CI asset list developed but not disseminated to all stakeholders

Ad-hoc vulnerability disclosure for CI & Government



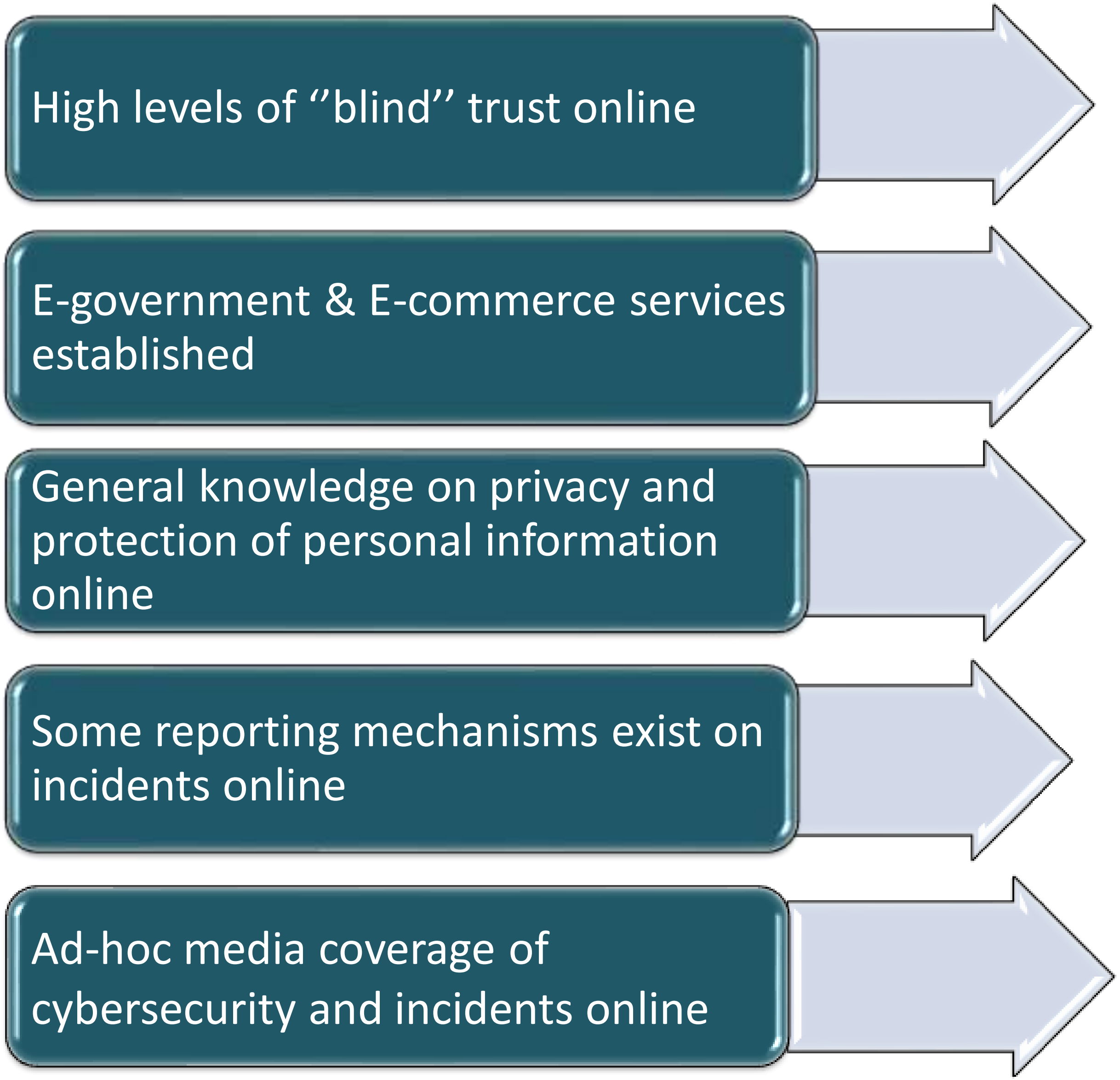
No official risk assessment plan

Cyber Defence considered in terms of National Cyber Resilience

In contact with NATO CCDCOE – Tallinn Manual Use – Participation to Trident Juncture exercise

Emergency response assets in place

Cybersecurity Policy and Strategy



High levels of ''blind'' trust online

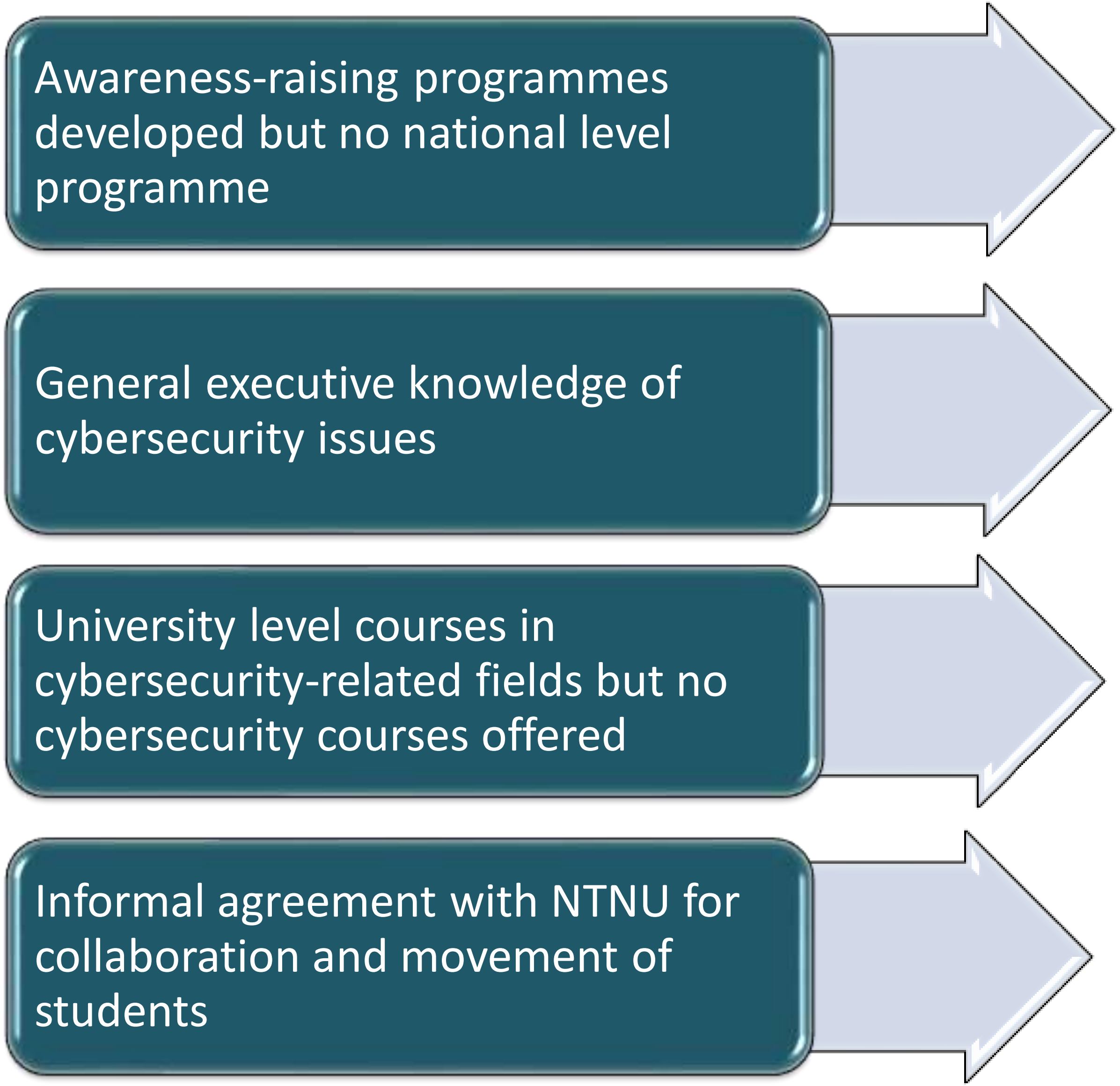
E-government & E-commerce services established

General knowledge on privacy and protection of personal information online

Some reporting mechanisms exist on incidents online

Ad-hoc media coverage of cybersecurity and incidents online

CYBERSECURITY CULTURE AND SOCIETY



Awareness-raising programmes developed but no national level programme

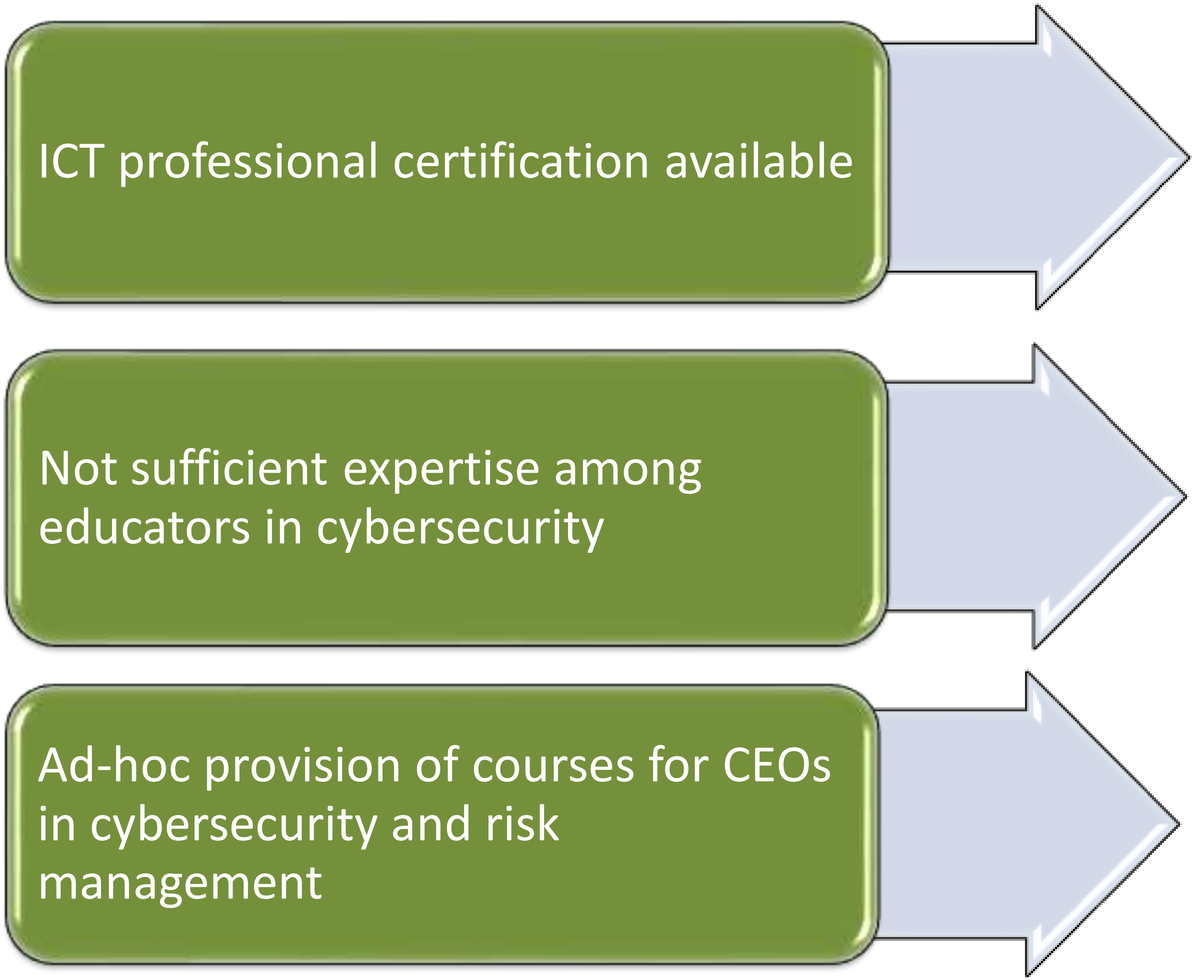
General executive knowledge of cybersecurity issues

University level courses in cybersecurity-related fields but no cybersecurity courses offered

Informal agreement with NTNU for collaboration and movement of students

CYBERSECURITY EDUCATION, TRAINING AND SKILLS

CYBERSECURITY EDUCATION, TRAINING AND SKILLS

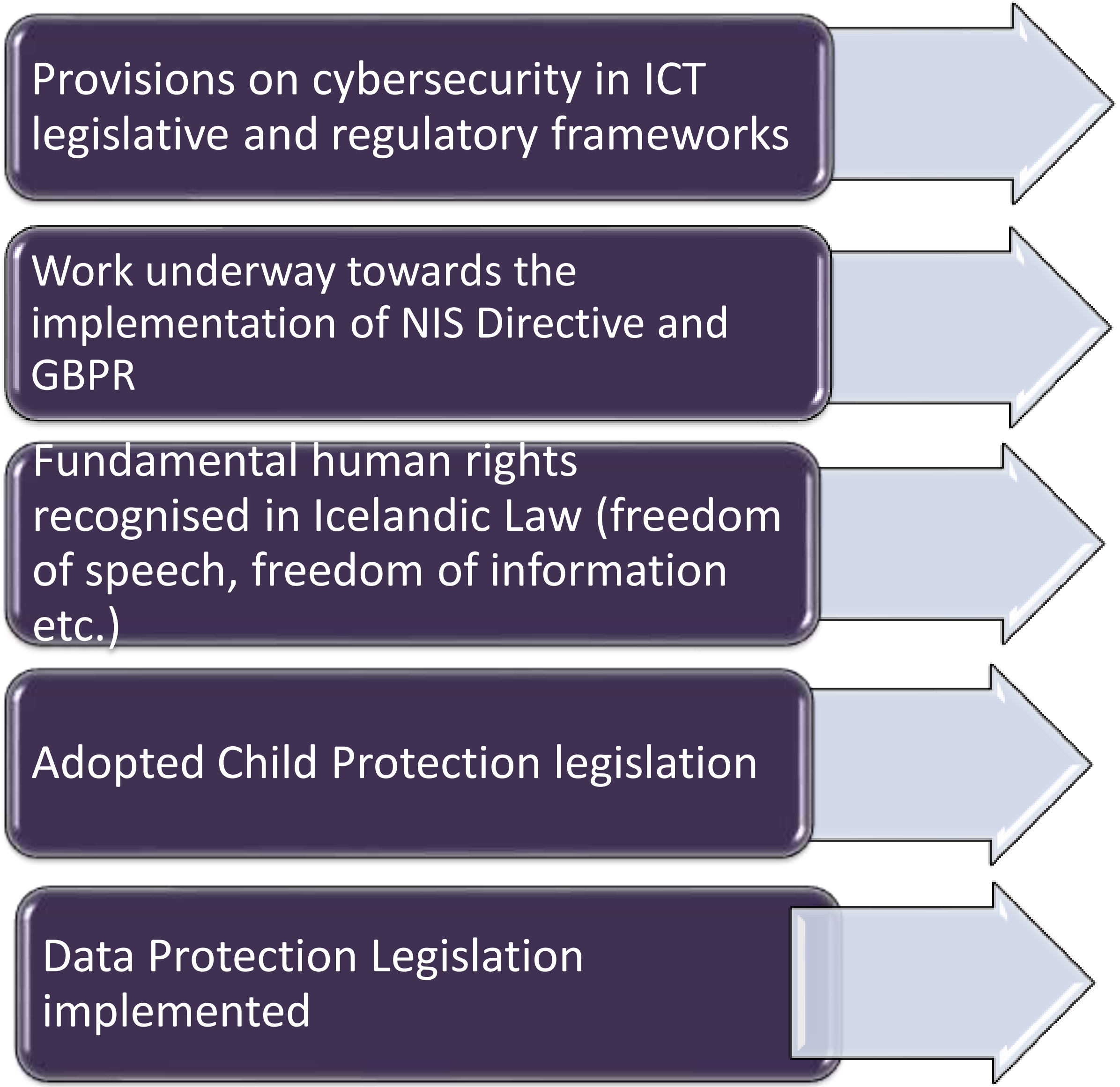


ICT professional certification available

Not sufficient expertise among educators in cybersecurity

Ad-hoc provision of courses for CEOs in cybersecurity and risk management

LEGAL AND REGULATORY FRAMEWORKS



Provisions on cybersecurity in ICT legislative and regulatory frameworks

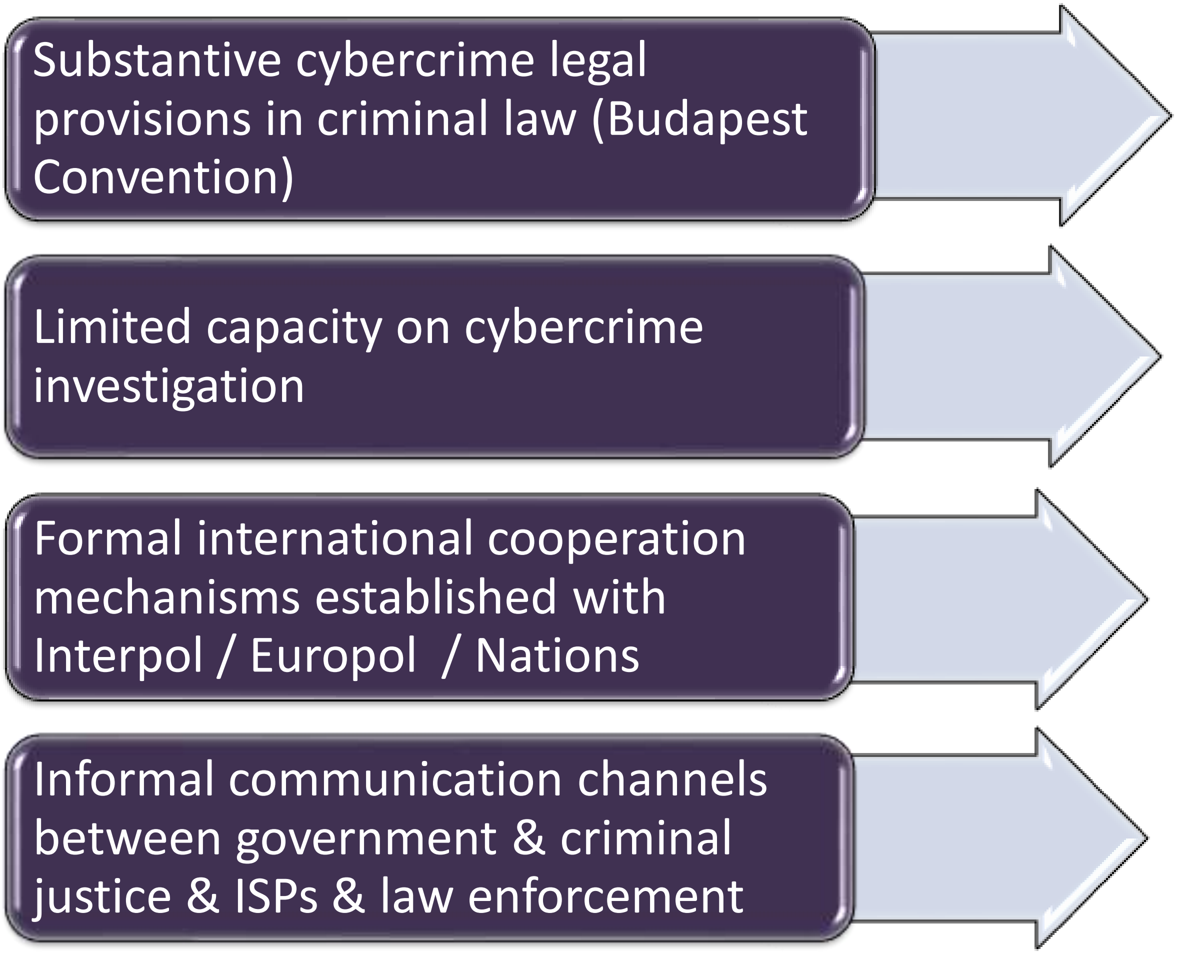
Work underway towards the implementation of NIS Directive and GBPR

Fundamental human rights recognised in Icelandic Law (freedom of speech, freedom of information etc.)

Adopted Child Protection legislation

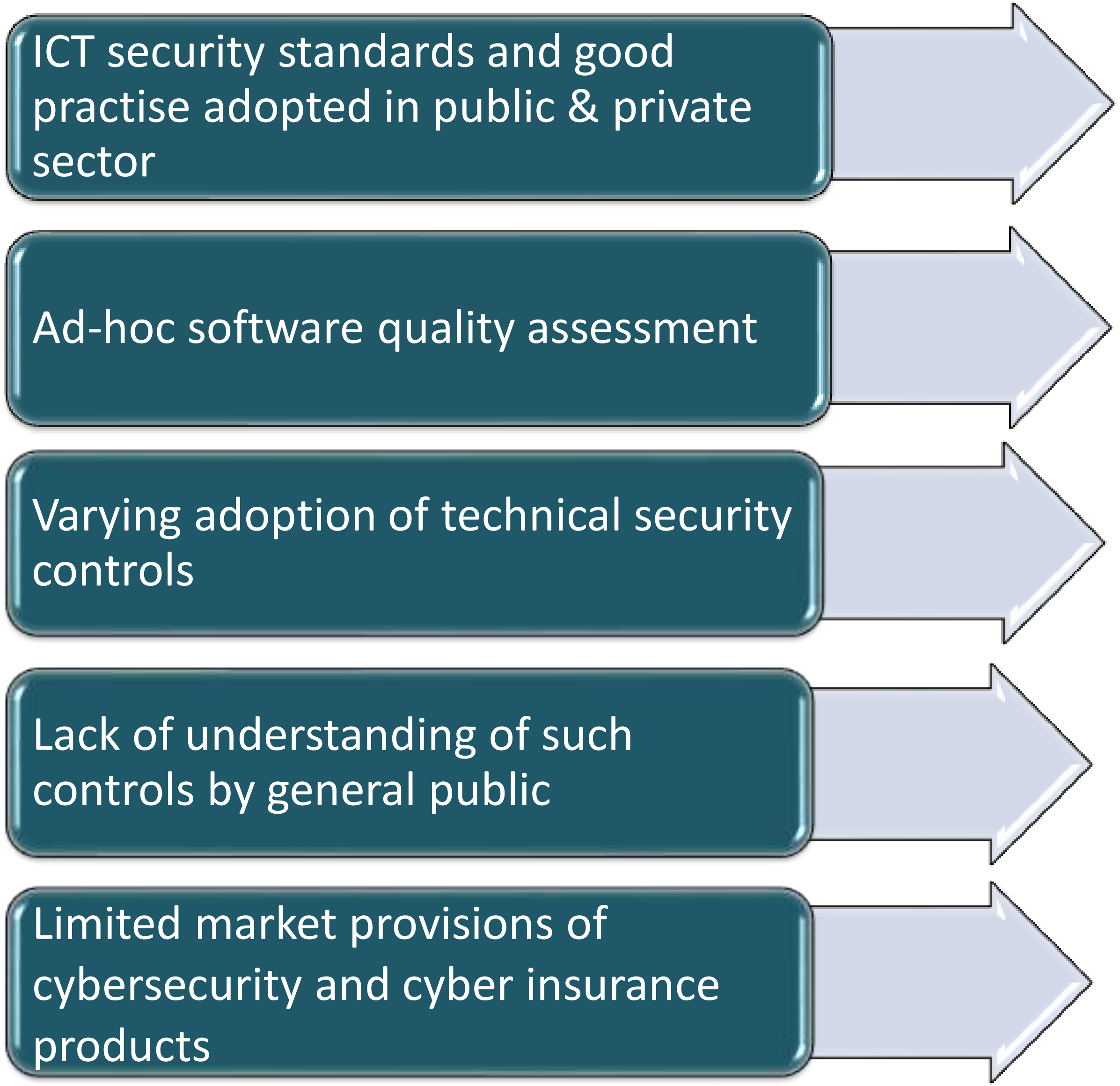
Data Protection Legislation implemented

LEGAL AND REGULATORY FRAMEWORKS



- Substantive cybercrime legal provisions in criminal law (Budapest Convention)
- Limited capacity on cybercrime investigation
- Formal international cooperation mechanisms established with Interpol / Europol / Nations
- Informal communication channels between government & criminal justice & ISPs & law enforcement

STANDARDS, ORGANISATIONS AND TECHNOLOGIES



- ICT security standards and good practise adopted in public & private sector
- Ad-hoc software quality assessment
- Varying adoption of technical security controls
- Lack of understanding of such controls by general public
- Limited market provisions of cybersecurity and cyber insurance products

Limited market provisions of cybersecurity and cyber insurance products

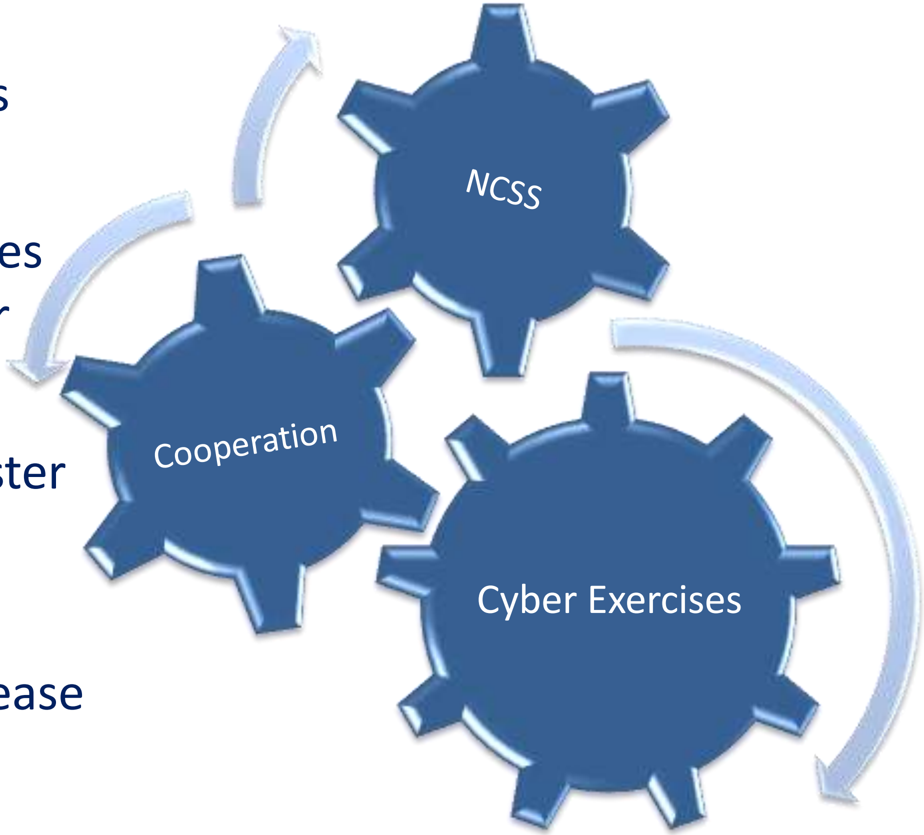
No official vulnerability disclosure framework at place

STANDARDS, ORGANISATIONS AND TECHNOLOGIES

CMM Review in Iceland
Recommendations

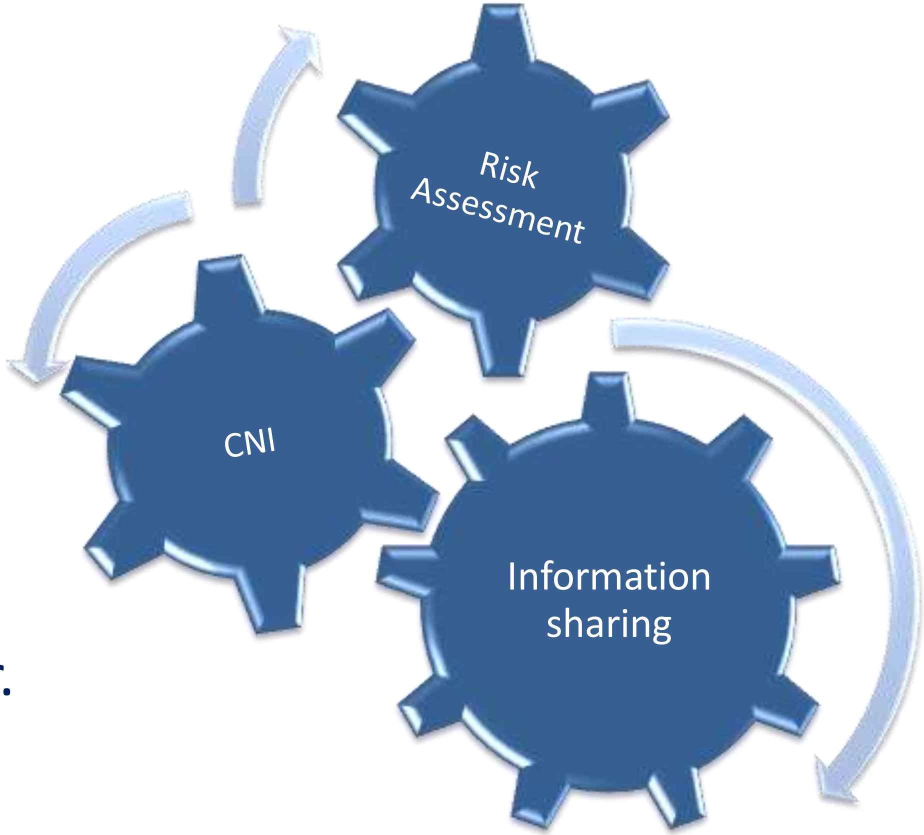
CYBERSECURITY POLICY AND STRATEGY
Recommendations

- Encourage the implementation of the National Cyber Security Strategy across government and other sectors.
- Conduct regular scenario cyber exercises that provide a picture of national cyber resilience.
- Form a multi-stakeholder research cluster to work on national cyber resilience.
- Promote cooperation between stakeholders and other nations to increase incident response capacity (Nordic National CERT Collaboration).



CYBERSECURITY POLICY AND STRATEGY
Recommendations

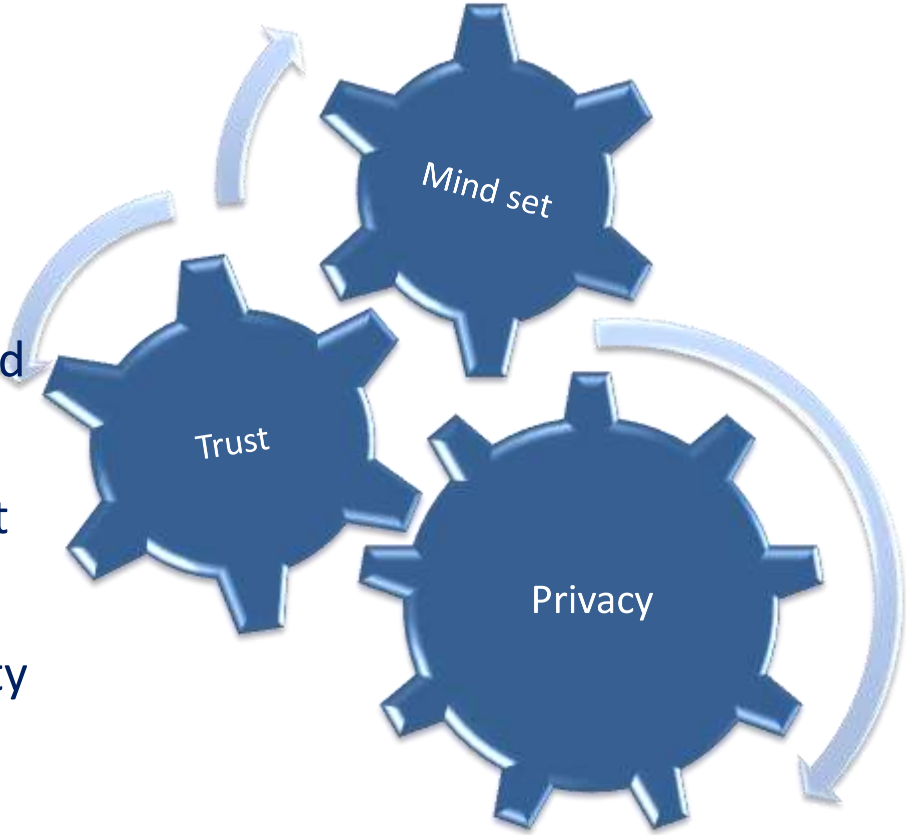
- Develop a national risk assessment plan.
- Strengthen formal coordination regarding CNI protection.
- Promote information sharing between public & private sector.



CYBERSECURITY CULTURE AND SOCIETY

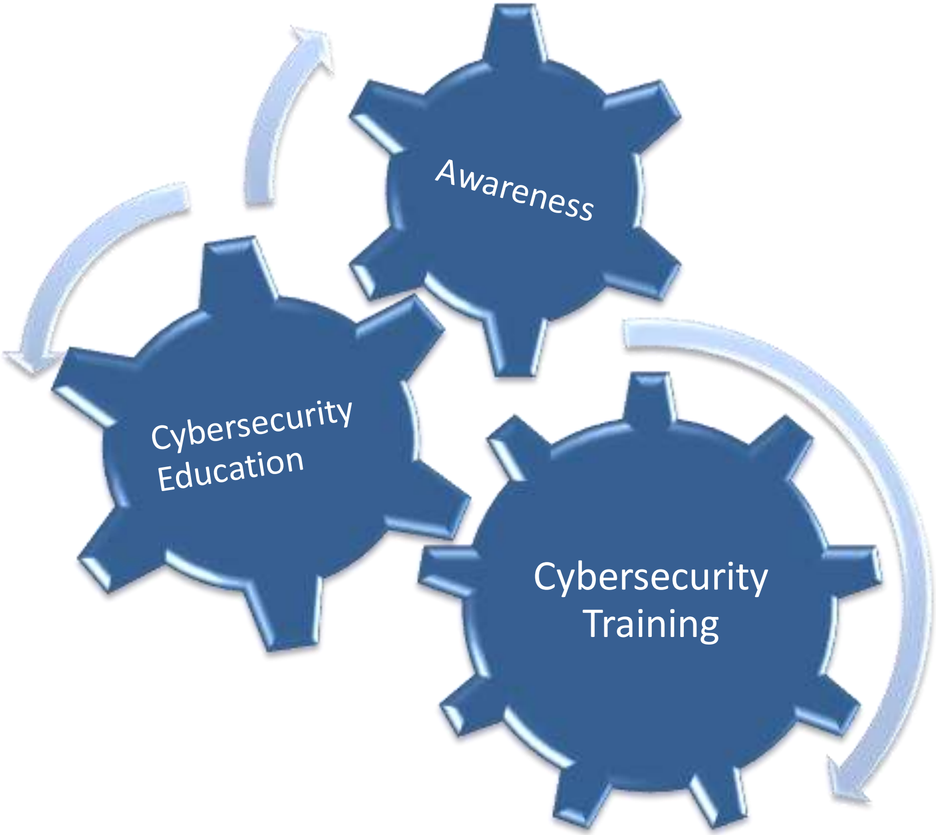
Recommendations

- The Icelandic online culture is described by ‘’blind’’ trust.
- Promote data protection online.
- Coordinate reporting mechanisms on child abuse and other online incidents.
- Apply security measures to establish trust in e-commerce services.
- Encourage discussions about cybersecurity on social media.



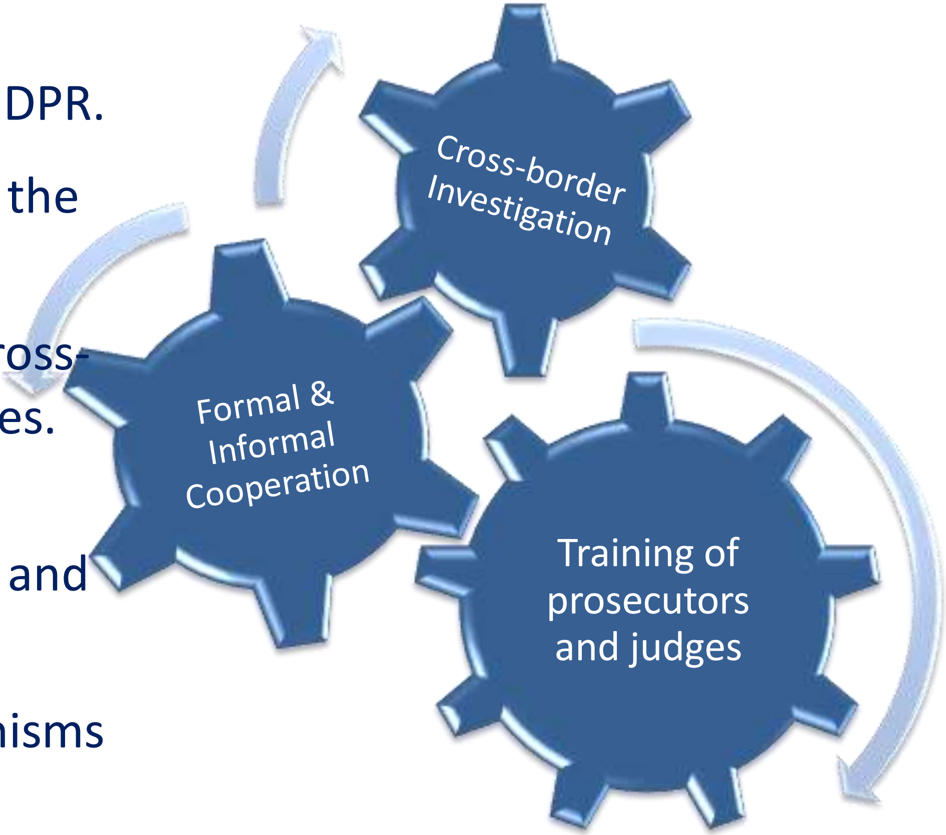
CYBERSECURITY EDUCATION, TRAINING AND SKILLS
Recommendations

- Develop a National Cybersecurity Awareness programme.
- Create cybersecurity education programmes.
- Establish cooperation agreements with European/International Universities.
- Establish cybersecurity training programmes for professionals.
- Develop a central platform for sharing training information for experts.



LEGAL AND REGULATORY FRAMEWORKS
Recommendations

- Coordinate work towards the implementation of NIS Directive and GDPR.
- Identify international trends to inform the amendment of data protection laws.
- Ensure procedural law provisions on cross-border investigation of cybercrime cases.
- Enhance training and education of prosecutors and judges on cybercrime and data protection.
- Enhance informal cooperation mechanisms between ISPs, law enforcement, government & criminal justice.


Cross-border Investigation
Formal & Informal Cooperation
Training of prosecutors and judges

STANDARDS, ORGANISATIONS AND TECHNOLOGIES Recommendations

- Promote cybersecurity standard adoption in all sectors.
- Conduct regular assessments of processes on national information infrastructure security & critical services.
- Promote user understanding of deployment of security controls.
- Develop a responsible vulnerability disclosure framework with all stakeholders involved.

Standards
Responsible Disclosure
Security Controls

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Thank you!

Global Cyber Security Capacity Centre
Oxford Martin School, University of Oxford
34 Broad Street, Oxford OX1 3BD, UK
Phone: +44(0)1865 287903
cybercapacity@oxfordmartin.ox.ac.uk

www.oxfordmartin.ox.ac.uk/cybersecurity

Global
Cyber Security
Capacity Centre

OXFORD
MARTIN
SCHOOL

UNIVERSITY OF
OXFORD