CMM 2021 Edition

Launch

25 March 2021

Global Cyber Security Capacity Centre

OCSC Oceania Cyber Security Centre

C3SA

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

CMM End-user Value and Capacity-building Impact

According to a a recent evaluation of the CMM in 2020

- Drives increased **cybersecurity awareness and capacity building** and contributes to greater collaboration within government;
- Helps enable **networking and collaboration** with business and wider society;
- Enhances **internal credibility** of cybersecurity agenda within governments;
- Helps define **roles and responsibilities** within governments;
- Increases **funding** for cybersecurity capacity building; and
- Is foundational to country **strategy and policy** development.

Global Cyber Security Capacity Centre

OCSC Oceania Cyber Security Centre

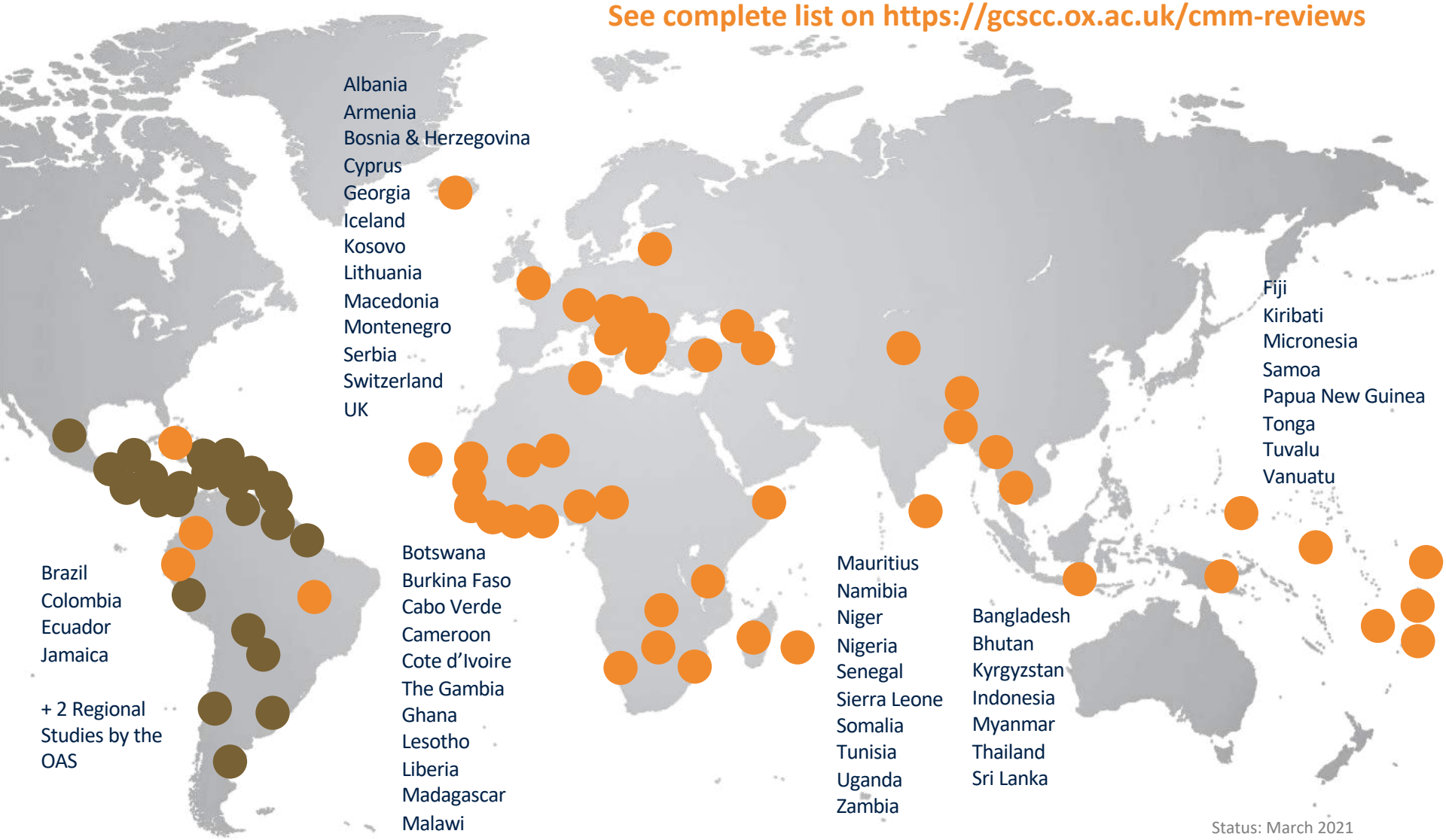
C3SA

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Over 85 National Cybersecurity Capacity Reviews

See complete list on https://gcscc.ox.ac.uk/cmm-reviews



Albania
Armenia
Bosnia & Herzegovina
Cyprus
Georgia
Iceland
Kosovo
Lithuania
Macedonia
Montenegro
Serbia
Switzerland
UK

Brazil
Colombia
Ecuador
Jamaica

+ 2 Regional Studies by the OAS

Botswana
Burkina Faso
Cabo Verde
Cameroon
Cote d'Ivoire
The Gambia
Ghana
Lesotho
Liberia
Madagascar
Malawi

Mauritius
Namibia
Niger
Nigeria
Senegal
Sierra Leone
Somalia
Tunisia
Uganda
Zambia

Bangladesh
Bhutan
Kyrgyzstan
Indonesia
Myanmar
Thailand
Sri Lanka

Fiji
Kiribati
Micronesia
Samoa
Papua New Guinea
Tonga
Tuvalu
Vanuatu

Status: March 2021

Global Cyber Security Capacity Centre

OCSC Oceania Cyber Security Centre

C3SA

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

CMM 2021 Edition Decision Process

The decision to considering reviewing the CMM was taken based on two key factors:

1) **Operational Environment and Risks**

2) **Changing Cybersecurity Control Landscape**

How it all started…

- CMM revision process formally begun in 2019

- Collection of evidence from:
  - CMM Implementers
  - Global Constellation partners (OCSC, C3SA)
  - Countries who used the CMM
  - Consultation with the GCSCC's Expert Advisory Panel (EAP)
  - Cybersecurity experts

Autumn 2019 - March 2020

- Consultation: Discussion of the content of the change proposals for each Dimension
- Personalised email invitations (almost 300) sent out including EAP members, global constellation and strategic partners and cybersecurity experts
- For each Dimension at least 3-4 online conference calls took place (18 in total); alongside 1-1- calls with partners and other experts.
- Feedback was gathered during a CMM Revision Workshop held in Melbourne alongside the OCSC/GCSCC Annual Conference February 2020
- More than 150 individuals contributed to different steps of the revision process

Inclusion in the proposed CMM 2021 Edition

- Each change must have been proposed by partners, users, or expert advisors. It must be based on experience in deploying the CMM and feedback from a country which has used the CMM or from a member of the international stakeholder community with particular insight into changing environments that need be taken into account;

- The change must have been discussed with the GCSCC Expert Advisory Panel, regional, strategic and implementation partners and other experts during the online conference calls and/or one-to-one online meetings. Clear consensus must have been reached amongst the attendees;

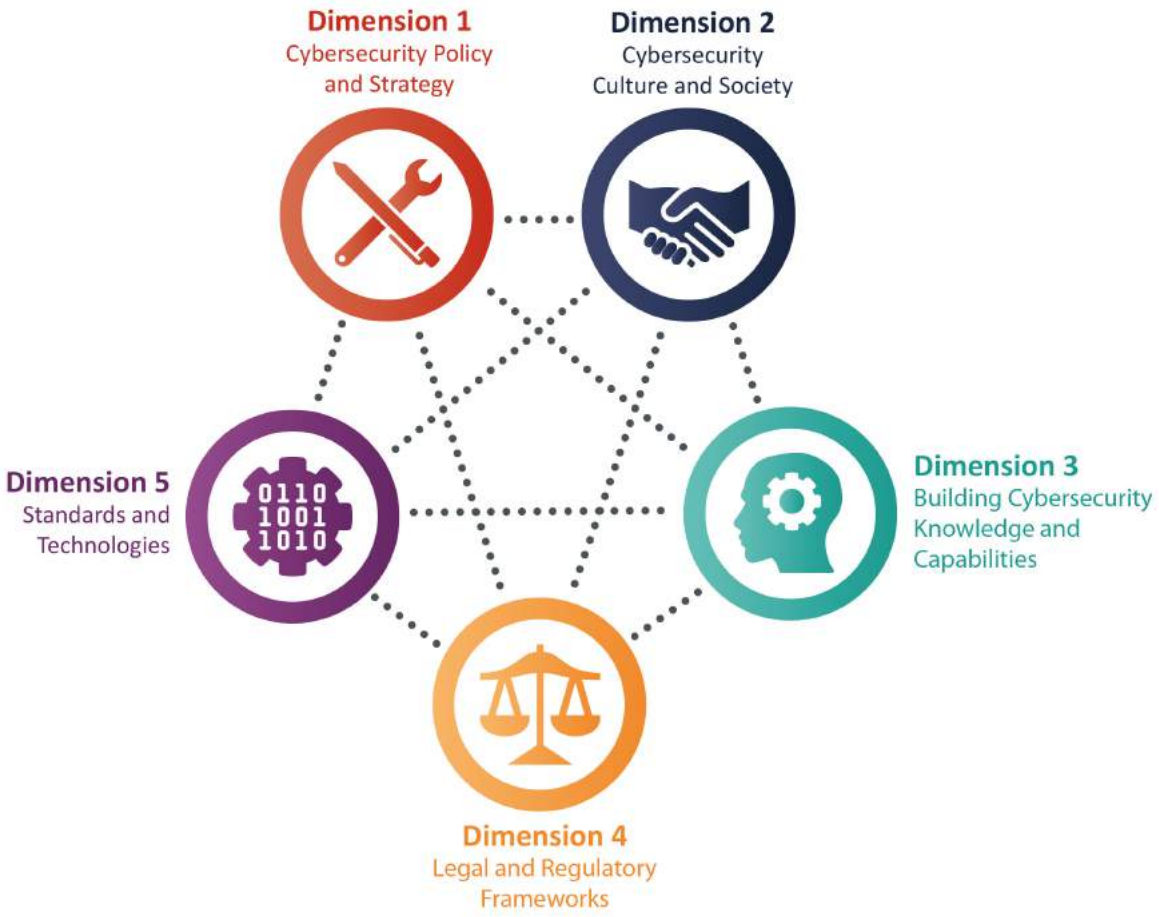
- The change must have been discussed at the CMM Revision Workshop in February 2020. Clear consensus must have been reached amongst attendees;

- Global Constellation partners and strategic and implementation partners must have been consulted; and

- Members of the GCSCC Technical Board must agree that the changes are desirable.

Cybersecurity Capacity Maturity Model for Nations (CMM)

- spanning five *Dimensions* and 23 *Factors* including almost 800 indicators
- developed and reviewed in global multi-stakeholder consultation processes
- suitable for self-assessment of current capacity
- creating a comprehensive benchmark of current position and how to increase maturity



Global Cyber Security Capacity Centre

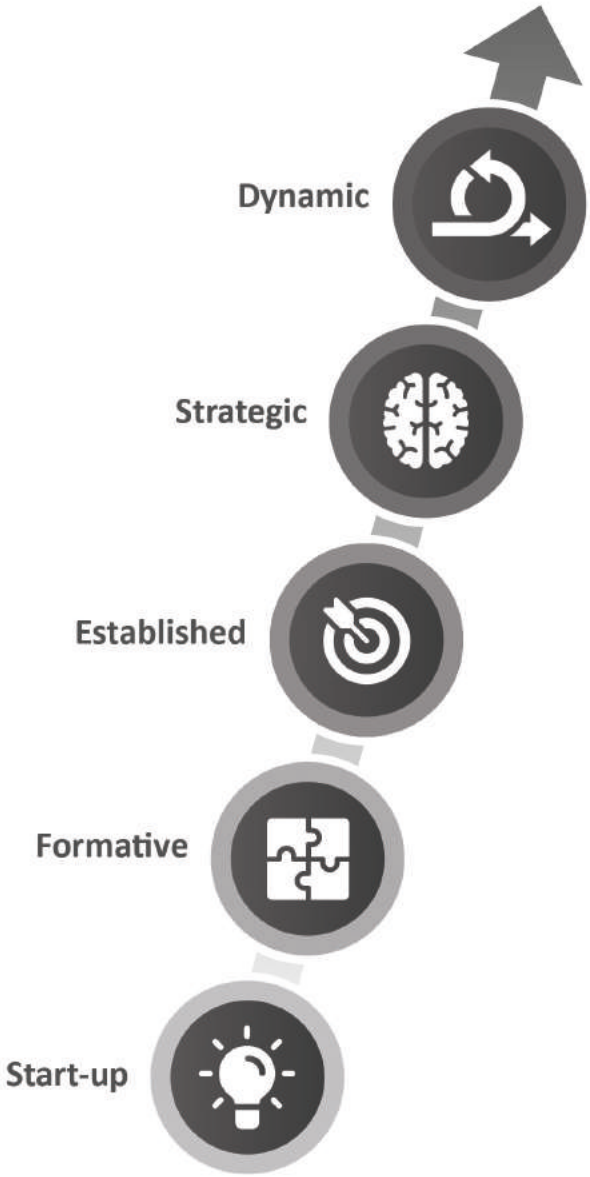
OCSC Oceania Cyber Security Centre

C3SA

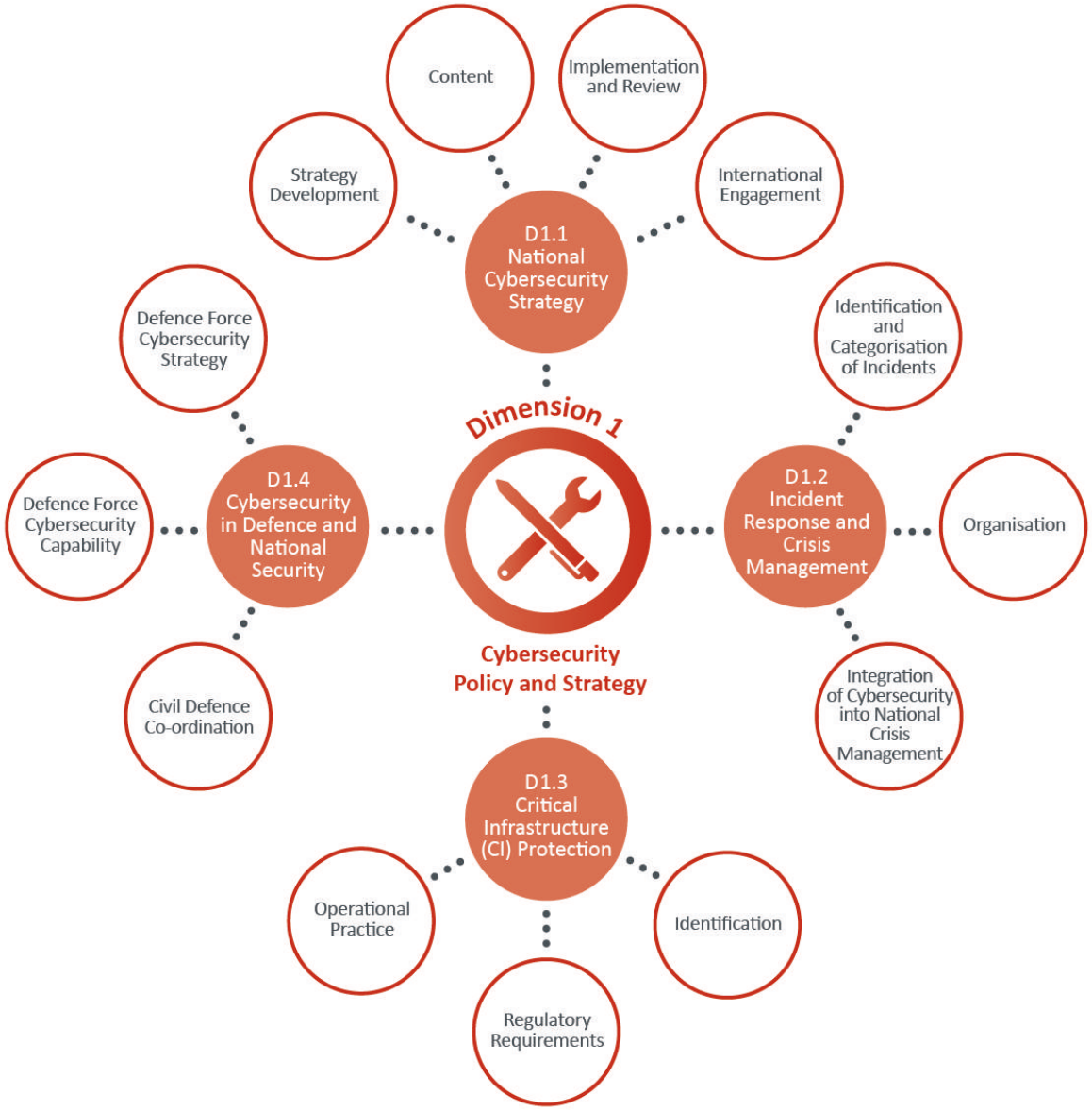
OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

5 Stages of Maturity



Dimension 1: Cybersecurity Policy and Strategy



Global Cyber Security Capacity Centre
OCSC Oceania Cyber Security Centre
C3SA
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD

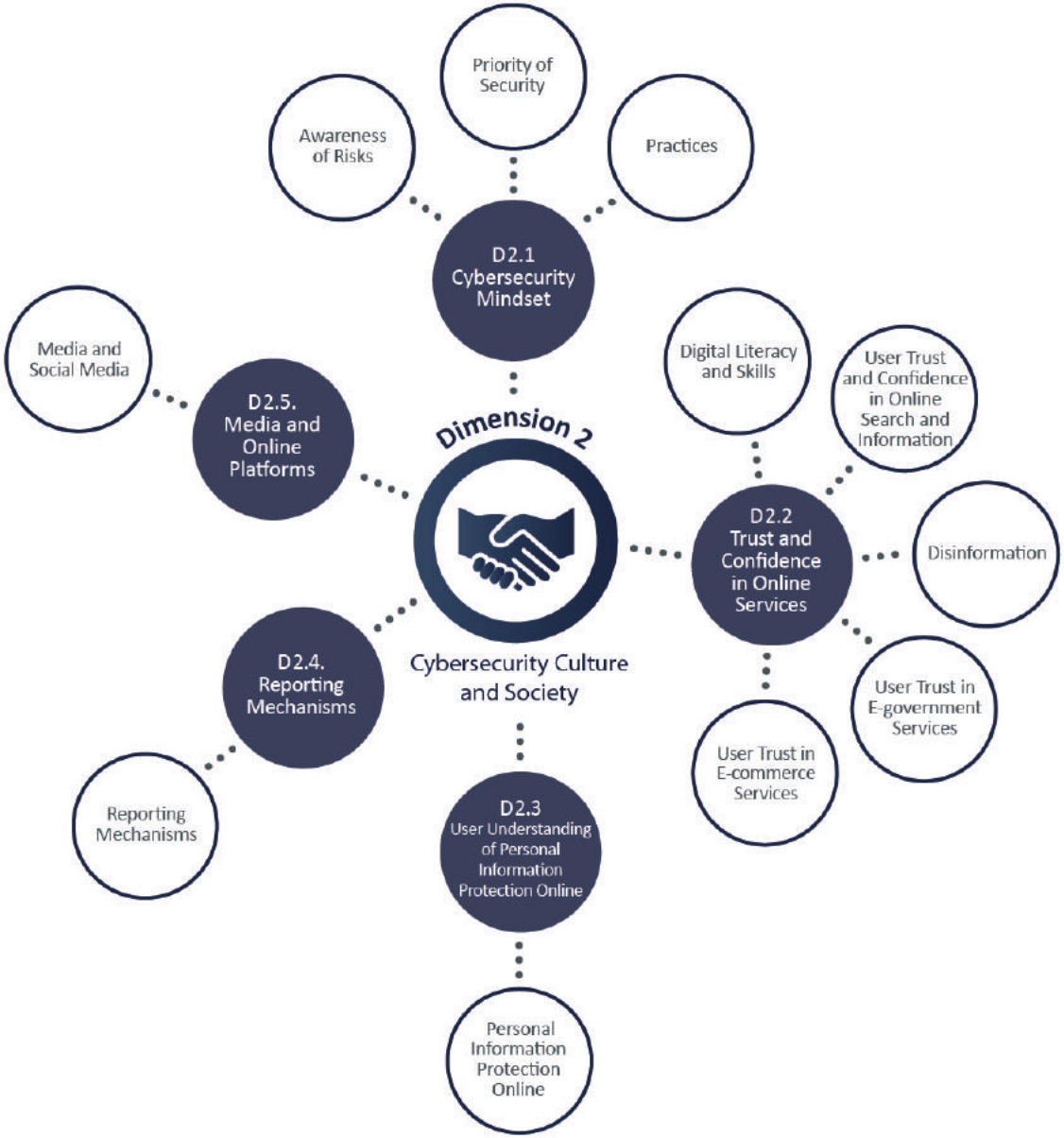
CMM 2016	CMM 2021 Edition
Factor 1.1: National Cybersecurity Strategy Aspects: • Strategy Development • Organisation • Content	**Factor 1.1: National Cybersecurity Strategy** Aspects: • Strategy Development • Content • Implementation and Review • International Engagement
Factor 1.2: Incident Response Aspects: • Identification of Incidents • Organisation • Coordination • Mode of Operation	**Factor 1.2: Incident Response and Crisis Management** Aspects: • Identification and Categorisation of Incidents • Organisation • Integration of Cybersecurity into National Crisis Management

Dimension 1

Cybersecurity Policy and Strategy

CMM 2016	CMM 2021 Edition
Factor 1.3: Critical Infrastructure (CI) Protection Aspects: • Identification • Organisation • Risk Management and Response	**Factor 1.3: Critical Infrastructure (CI) Protection** Aspects: • Identification • Regulatory Requirements • Operational Practice
Factor 1.4: Crisis Management Aspect: • Crisis Management	~~**Factor 1.4. National Crisis Management**~~ (removed and merged into Factor 1.2)
Factor 1.5: Cyber Defence Aspects: • Strategy • Organisation • Coordination	**Factor 1.4: Cybersecurity in Defence and National Security** Aspects: • Defence Force Cybersecurity Strategy • Defence Force Cybersecurity Capability • Civil-Defence Coordination
Factor 1.6: Communications Redundancy • Communications Redundancy	~~**Factor 1.6: Communications Redundancy**~~ (removed, was split and merged relevant parts with D1.2 and D5.2 on Internet Infrastructure)

Dimension 2: Cybersecurity Culture and Society


Priority of Security
Awareness of Risks
Practices
D2.1 Cybersecurity Mindset
Media and Social Media
D2.5. Media and Online Platforms
Dimension 2
Cybersecurity Culture and Society
Digital Literacy and Skills
User Trust and Confidence in Online Search and Information
D2.2 Trust and Confidence in Online Services
Disinformation
User Trust in E-government Services
User Trust in E-commerce Services
D2.4. Reporting Mechanisms
Reporting Mechanisms
D2.3 User Understanding of Personal Information Protection Online
Personal Information Protection Online

Dimension 2

Cybersecurity Culture and Society

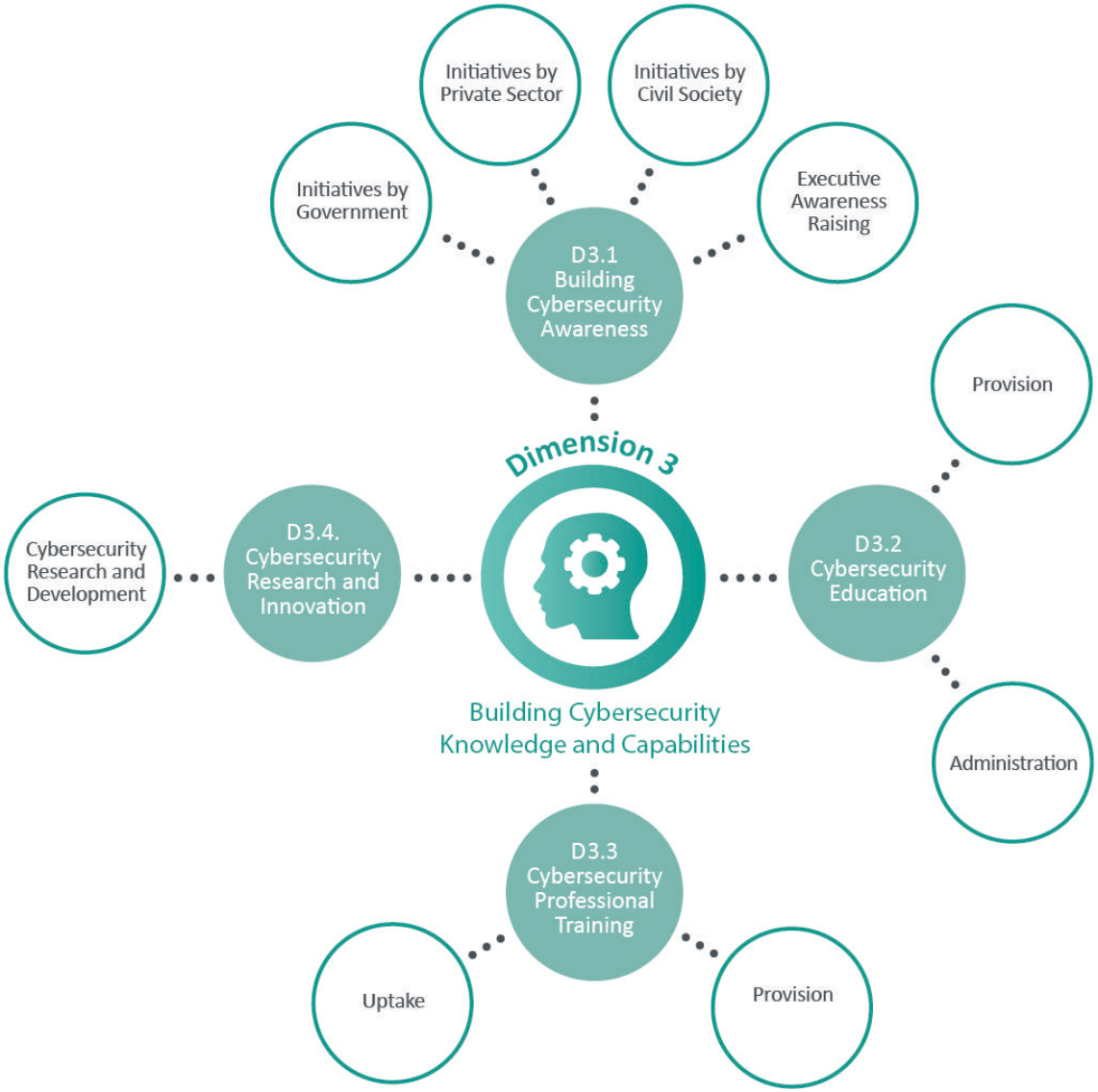
CMM 2016	CMM 2021 Edition
Factor 2.1: Cybersecurity Mindset Aspects: • Government • Private sector • Users	**Factor 2.1: Cybersecurity Mindset** Aspects: • Awareness of Risks • Priority of Security • Practices
Factor 2.2: Trust and Confidence on the Internet Aspects: • User Trust and Confidence on the Internet • User Trust in E-government Services • User Trust in E-commerce Services	**Factor 2.2: Trust and Confidence in Online Services** Aspects: • Digital Literacy and Skills • User Trust and Confidence in Online Search and Information • Disinformation • User Trust in E-government Services • User Trust in E-commerce Services
Factor 2.3: User Understanding of Personal Information Protection Online Aspects: • User Understanding of Personal Information Protection Online	**Factor 2.3: User Understanding of Personal Information Protection Online** Aspects: • Personal Information Protection Online

Dimension 2

Cybersecurity Culture and Society

CMM 2016	CMM 2021 Edition
Factor 2.4: Reporting Mechanisms Aspects: • Reporting Mechanisms	**Factor 2.4: Reporting Mechanisms** Aspects: • Reporting Mechanisms
Factor 2.5: Media and Social Media Aspects: • Media and Social Media	**Factor 2.5: Media and Online Platforms** Aspects: • Media and Social Media

Dimension 3: Building Cybersecurity Knowledge and Capabilities



Global Cyber Security Capacity Centre

OCSC Oceania Cyber Security Centre

C3SA

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Dimension 3

Building Cybersecurity Knowledge and Capabilities

CMM 2016	CMM 2021 Edition
Factor 3.1: Awareness Raising Aspects: • Awareness Raising Programmes • Executive Awareness Raising	**Factor 3.1: Building Cybersecurity Awareness** Aspects: • Initiatives by Government • Initiatives by Private sector • Initiatives by Civil society • Executive Awareness Raising
Factor 3.2: Framework for Education Aspects: • Provision • Administration	**Factor 3.2: Cybersecurity Education** Aspects: • Provision • Administration
Factor 3.3: Framework for Professional Training Aspects: • Provision • Uptake	**Factor 3.3: Cybersecurity Professional Training** Aspects: • Provision • Uptake
	Factor 3.4: Cybersecurity Research and Innovation (new factor and aspect added) Aspect: • Cybersecurity Research and Development

Dimension 4: Legal and Regulatory Frameworks

Global Cyber Security Capacity Centre

OCSC Oceania Cyber Security Centre

C3SA

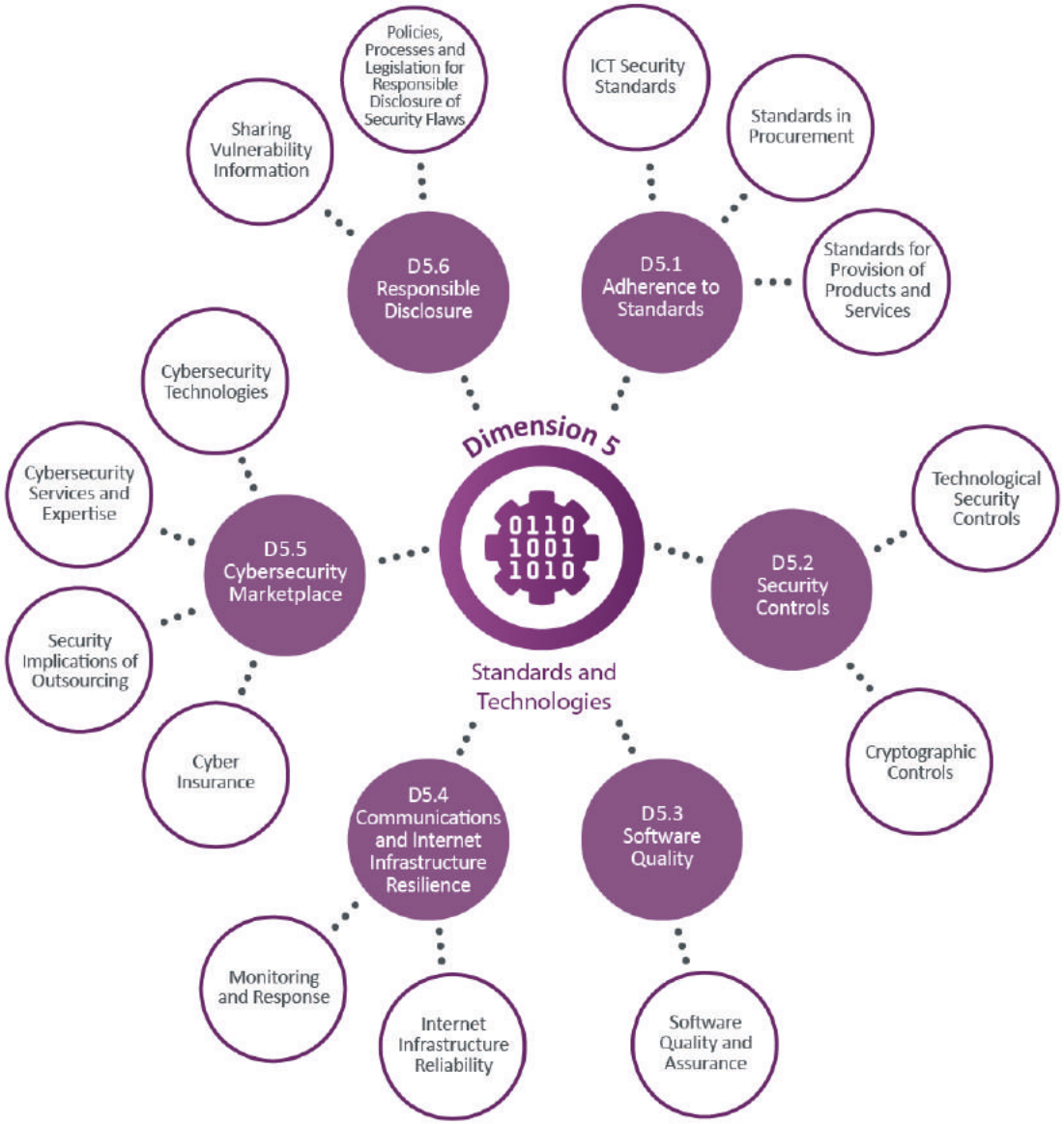
OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

CMM 2016	CMM 2021 Edition
Factor 4.1: Legal Frameworks Aspects: • Legislative Frameworks for ICT Security • Privacy, Freedom of Speech & Other Human Rights Online • Data Protection Legislation • Child Protection Online • Consumer Protection Legislation • Intellectual Property Legislation • Substantive Cybercrime Legislation • Procedural Cybercrime Legislation	**Factor 4.1: Legal and Regulatory Provisions** Aspects: • Substantive Cybercrime Legislation • Legal and Regulatory Requirements for Cybersecurity • Procedural Cybercrime Legislation • Human Rights Impact Assessment ~~• Legislative Frameworks for ICT Security~~ ~~• Privacy, Freedom of Speech & Other Human Rights Online~~ ~~• Data Protection Legislation~~ ~~• Child Protection Online~~ ~~• Consumer Protection Legislation~~ ~~• Intellectual Property Legislation~~
-	**Factor 4.2: Related Legislative Frameworks** • Data Protection Legislation • Child Protection Online • Consumer Protection Legislation • Intellectual Property Legislation

CMM 2016	CMM 2021 Edition
Factor 4.2: Criminal Justice System Aspects: • Law Enforcement • Prosecution • Courts	**Factor 4.3: Legal and Regulatory Capability and Capacity** Aspects: • Law Enforcement • Prosecution • Courts • Regulatory Bodies
Factor 4.3: Formal and Informal Cooperation Frameworks to Combat Cybercrime Aspects: • Formal Cooperation • Informal Cooperation	**Factor 4.4: Formal and Informal Co-operation Frameworks to Combat Cybercrime** Aspects: • Law Enforcement Co-operation with Private Sector • Co-operation with Foreign Law Enforcement Counterparts • Government-Criminal Justice Sector Collaboration

Dimension 5: Standards and Technologies


Dimension 5
0110
1001
1010
Standards and Technologies
D5.1 Adherence to Standards
ICT Security Standards
Standards in Procurement
Standards for Provision of Products and Services
D5.2 Security Controls
Technological Security Controls
Cryptographic Controls
D5.3 Software Quality
Software Quality and Assurance
D5.4 Communications and Internet Infrastructure Resilience
Internet Infrastructure Reliability
Monitoring and Response
D5.5 Cybersecurity Marketplace
Cyber Insurance
Security Implications of Outsourcing
Cybersecurity Services and Expertise
Cybersecurity Technologies
D5.6 Responsible Disclosure
Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
Sharing Vulnerability Information

Dimension 5

Standards and Technologies

CMM 2016	CMM 2021 Edition
Factor 5.1: Adherence to Standards Aspects: • ICT Security Standards • Standards in Procurement • Standards in Software Development	**Factor 5.1: Adherence to Standards** Aspects: • ICT Security Standards • Standards in Procurement • Standards for Provision of Products and Services
Factor 5.2: Internet Infrastructure Resilience Aspects: Internet Infrastructure Resilience	**Factor 5.2: Communications and Internet Infrastructure Resilience** Aspects: • Internet Infrastructure Reliability • Monitoring and Response
Factor 5.3: Software Quality Aspects: • Software Quality	**Factor 5.3: Software Quality** Aspects: • Software Quality and Assurance

Dimension 5
Standards and Technologies

Factor 5.4: Technical Security Controls Aspects: • Technical Security Controls	**Factor 5.4: Security Controls** Aspects: • Technological Security Controls • Cryptographic Controls
Factor 5.5: Cryptographic Controls Aspects: • Cryptographic Controls	~~**Factor 5.5: Cryptographic Controls**~~ Cryptographic controls was merged into Security Controls (above) as a new aspect.
Factor 5.6: Cybersecurity Marketplace Aspects: • Cybersecurity Technologies • Cyber Insurance	**Factor 5.5 Cybersecurity Marketplace** Aspects: • Cybersecurity Technologies • Cybersecurity Services and Expertise • Security Implications of Outsourcing • Cyber Insurance
Factor 5.7: Responsible Disclosure Aspects: • Responsible Disclosure	**Factor 5.6: Responsible Disclosure** Aspects: • Sharing Vulnerability Information • Policies, Processes and Legislation for Responsible Disclosure of Security Flaws

Global Cyber Security Capacity Centre
OCSC Oceania Cyber Security Centre
C3SA
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD

CMM 2021 Edition

will be available on

https://gcscc.ox.ac.uk/the-cmm

Discussion and questions

Thank you for your attention!

Global
Cyber Security
Capacity Centre

Department of Computer Science
University of Oxford
15 Parks Road, Oxford OX1 3QD, UK
Phone: +44(0)1865 287903
cybercapacity@cs.ox.ac.uk

www.oxfordmartin.ox.ac.uk/cybersecurity
https://gcscc.ox.ac.uk

@CapacityCentre

https://www.linkedin.com/company/global-cyber-security-capacity-centre/