

CMM 2021 Edition

Launch

25 March 2021



Global
Cyber Security
Capacity Centre



OCSC
Oceania Cyber Security Centre



C3SA



CMM End-user Value and Capacity-building Impact

According to 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.



Over 85 National Cybersecurity Capacity Reviews

See complete list on <https://gcsc.ox.ac.uk/cmm-reviews>



Status: March 2021

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.



Global
Cyber Security
Capacity Centre



OCSC
Oceania Cyber Security Centre

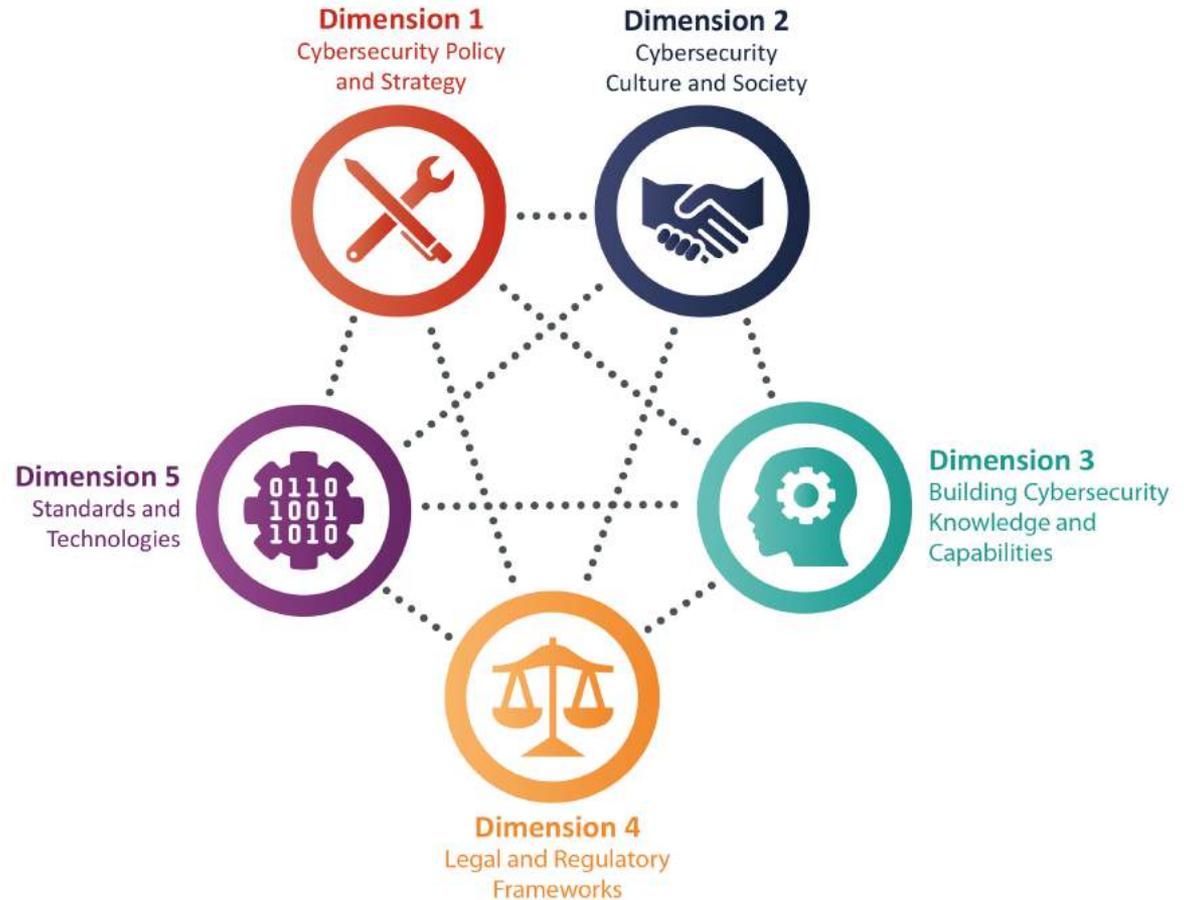


C3SA

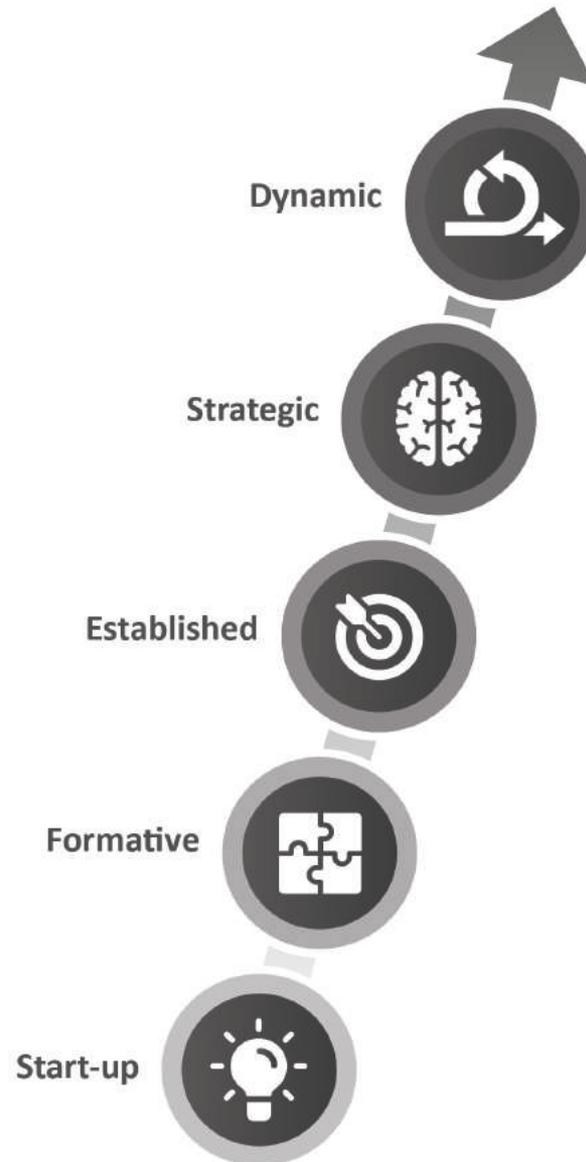


Cybersecurity Capacity Maturity Model for Nations (CMM)

- 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



5 Stages of Maturity





Dimension 1: Cybersecurity Policy and Strategy





CMM 2016	CMM 2021 Edition
<p>Factor 1.1: National Cybersecurity Strategy</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Strategy Development • Organisation • Content 	<p>Factor 1.1: National Cybersecurity Strategy</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Strategy Development • Content • Implementation and Review • International Engagement
<p>Factor 1.2: Incident Response</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Identification of Incidents • Organisation • Coordination • Mode of Operation 	<p>Factor 1.2: Incident Response and Crisis Management</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Identification and Categorisation of Incidents • Organisation • Integration of Cybersecurity into National Crisis Management

CMM 2016	CMM 2021 Edition
<p>Factor 1.3: Critical Infrastructure (CI) Protection</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Identification • Organisation → • Risk Management and Response → 	<p>Factor 1.3: Critical Infrastructure (CI) Protection</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Identification • Regulatory Requirements • Operational Practice
<p>Factor 1.4: Crisis Management</p> <p>Aspect:</p> <ul style="list-style-type: none"> • Crisis Management 	<p>Factor 1.4: National Crisis Management (removed and merged into Factor 1.2)</p>
<p>Factor 1.5: Cyber Defence</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Strategy • Organisation → • Coordination 	<p>Factor 1.4: Cybersecurity in Defence and National Security</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Defence Force Cybersecurity Strategy • Defence Force Cybersecurity Capability • Civil-Defence Coordination
<p>Factor 1.6: Communications Redundancy</p> <ul style="list-style-type: none"> • Communications Redundancy 	<p>Factor 1.6: Communications Redundancy (removed, was split and merged relevant parts with D1.2 and D5.2 on Internet Infrastructure)</p>



Dimension 2: Cybersecurity Culture and Society

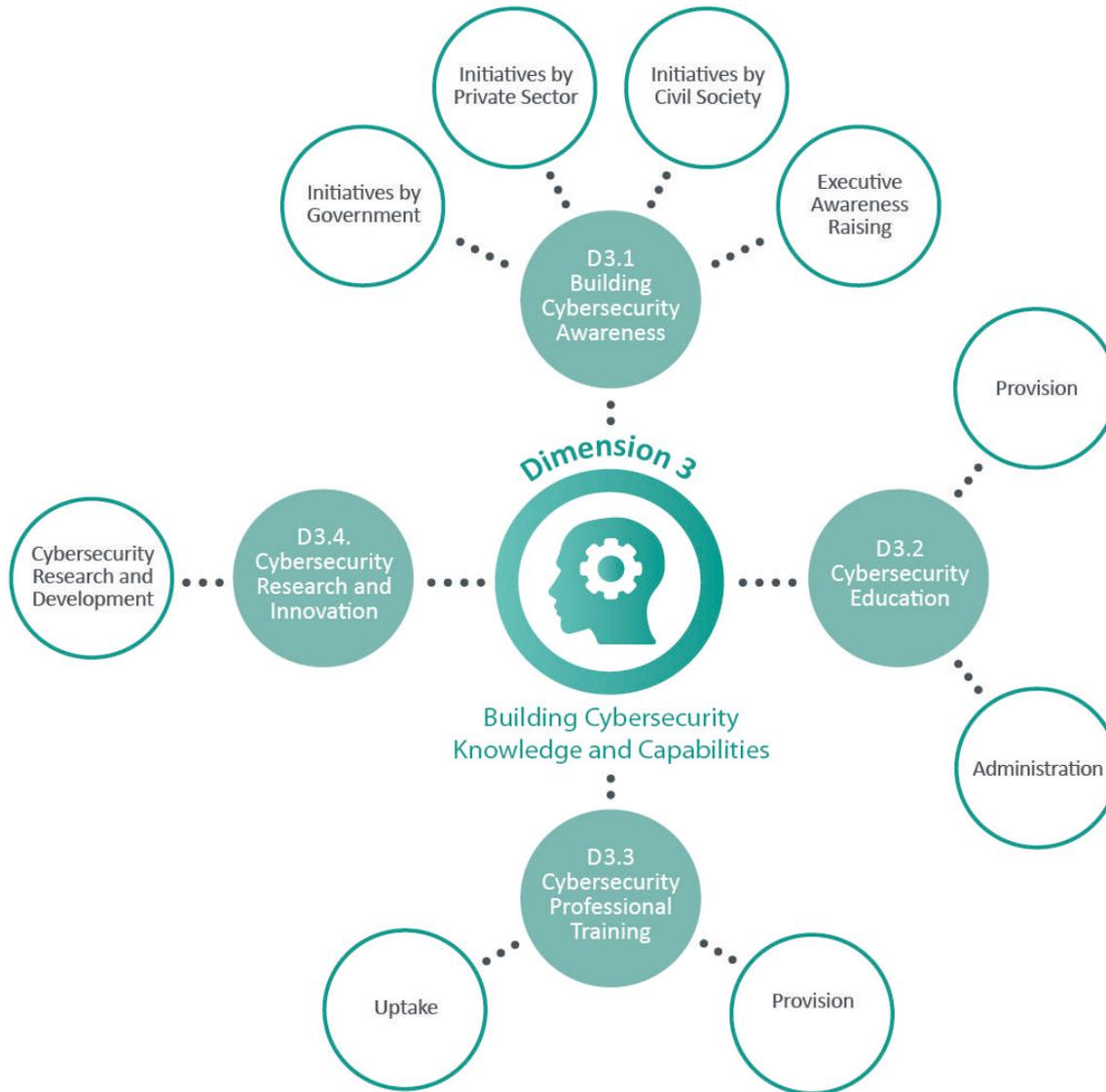


CMM 2016	CMM 2021 Edition
<p>Factor 2.1: Cybersecurity Mindset</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Government • Private sector • Users 	<p>Factor 2.1: Cybersecurity Mindset</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Awareness of Risks • Priority of Security • Practices
<p>Factor 2.2: Trust and Confidence on the Internet</p> <p>Aspects:</p> <ul style="list-style-type: none"> • User Trust and Confidence on the Internet • User Trust in E-government Services • User Trust in E-commerce Services 	<p>Factor 2.2: Trust and Confidence in Online Services</p> <p>Aspects:</p> <ul style="list-style-type: none"> • 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
<p>Factor 2.3: User Understanding of Personal Information Protection Online</p> <p>Aspects:</p> <ul style="list-style-type: none"> • User Understanding of Personal Information Protection Online 	<p>Factor 2.3: User Understanding of Personal Information Protection Online</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Personal Information Protection Online

CMM 2016	CMM 2021 Edition
<p>Factor 2.4: Reporting Mechanisms</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Reporting Mechanisms 	<p>Factor 2.4: Reporting Mechanisms</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Reporting Mechanisms
<p>Factor 2.5: Media and Social Media</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Media and Social Media 	<p>Factor 2.5: Media and Online Platforms</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Media and Social Media



Dimension 3: Building Cybersecurity Knowledge and Capabilities



CMM 2016	CMM 2021 Edition
<p>Factor 3.1: Awareness Raising</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Awareness Raising Programmes • Executive Awareness Raising 	<p>Factor 3.1: Building Cybersecurity Awareness</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Initiatives by Government • Initiatives by Private sector • Initiatives by Civil society • Executive Awareness Raising
<p>Factor 3.2: Framework for Education</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Provision • Administration 	<p>Factor 3.2: Cybersecurity Education</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Provision • Administration
<p>Factor 3.3: Framework for Professional Training</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Provision • Uptake 	<p>Factor 3.3: Cybersecurity Professional Training</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Provision • Uptake
	<p>Factor 3.4: Cybersecurity Research and Innovation (new factor and aspect added)</p> <p>Aspect:</p> <ul style="list-style-type: none"> • Cybersecurity Research and Development

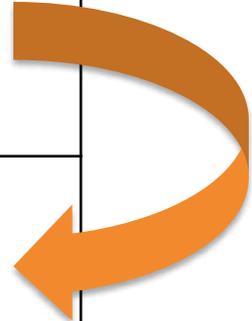


Dimension 4: Legal and Regulatory Frameworks

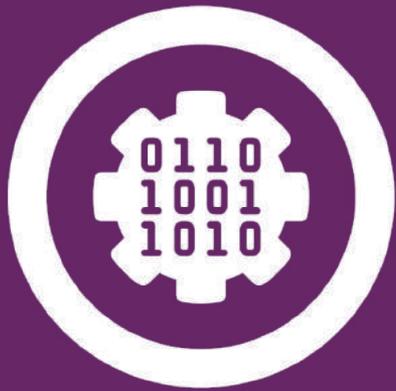




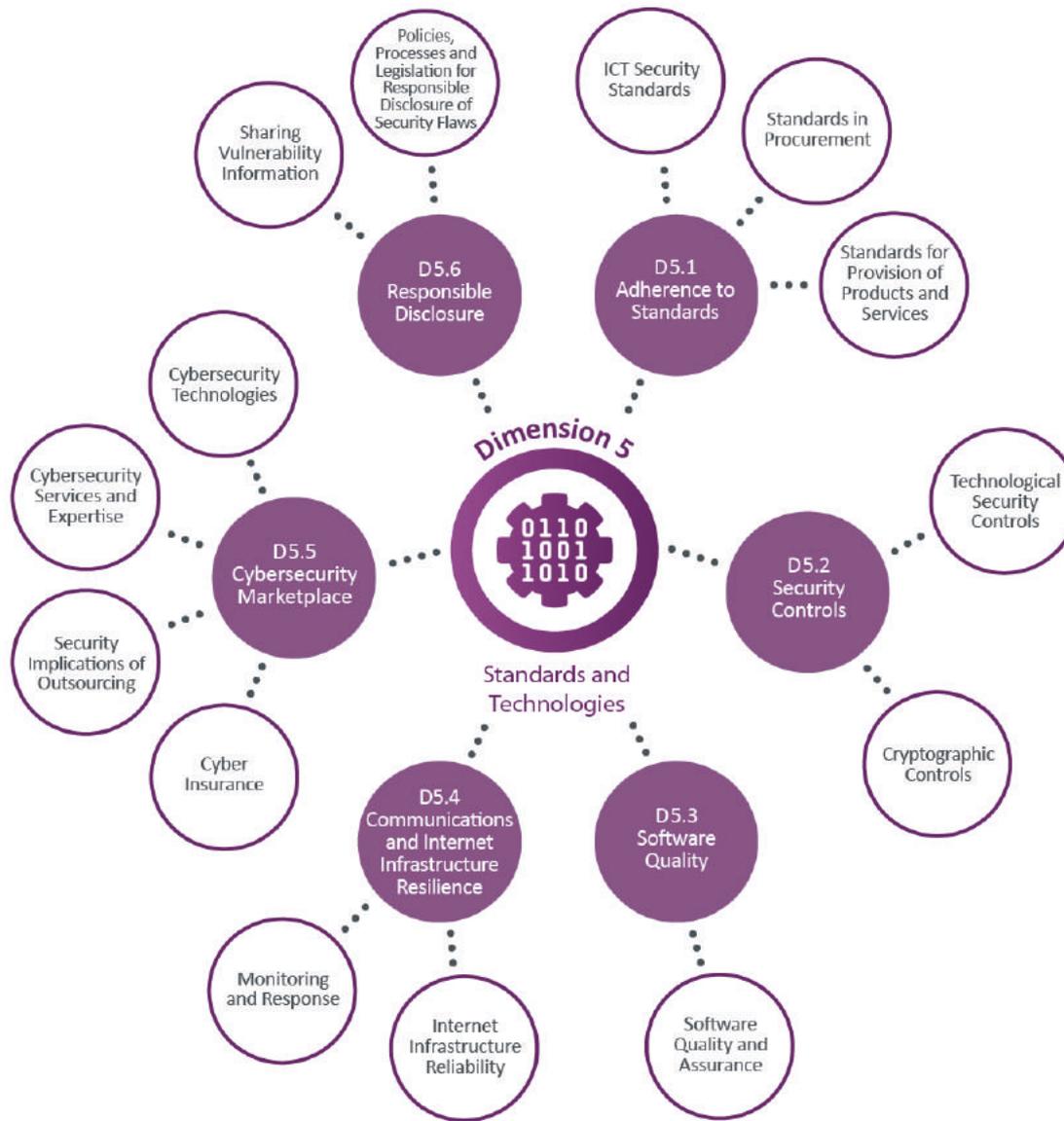
CMM 2016	CMM 2021 Edition
<p>Factor 4.1: Legal Frameworks</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Legislative Frameworks for ICT Security • Privacy, Freedom of Speech & Other Human Rights Online • Data Protection Legislation • Child Protection Online • Consumer Protection Legislation • Intellectual Property Legislation • Substantive Cybercrime Legislation • Procedural Cybercrime Legislation 	<p>Factor 4.1: Legal and Regulatory Provisions</p> <p>Aspects:</p> <ul style="list-style-type: none"> • 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
-	<p>Factor 4.2: Related Legislative Frameworks</p> <ul style="list-style-type: none"> • Data Protection Legislation • Child Protection Online • Consumer Protection Legislation • Intellectual Property Legislation



CMM 2016	CMM 2021 Edition
<p>Factor 4.2: Criminal Justice System</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Law Enforcement • Prosecution • Courts 	<p>Factor 4.3: Legal and Regulatory Capability and Capacity</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Law Enforcement • Prosecution • Courts • Regulatory Bodies
<p>Factor 4.3: Formal and Informal Cooperation Frameworks to Combat Cybercrime</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Formal Cooperation • Informal Cooperation 	<p>Factor 4.4: Formal and Informal Co-operation Frameworks to Combat Cybercrime</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Law Enforcement Co-operation with Private Sector • Co-operation with Foreign Law Enforcement Counterparts • Government-Criminal Justice Sector Collaboration



Dimension 5: Standards and Technologies





CMM 2016	CMM 2021 Edition
<p>Factor 5.1: Adherence to Standards</p> <p>Aspects:</p> <ul style="list-style-type: none"> • ICT Security Standards • Standards in Procurement • Standards in Software Development 	<p>Factor 5.1: Adherence to Standards</p> <p>Aspects:</p> <ul style="list-style-type: none"> • ICT Security Standards • Standards in Procurement • Standards for Provision of Products and Services
<p>Factor 5.2: Internet Infrastructure Resilience</p> <p>Aspects:</p> <p>Internet Infrastructure Resilience</p>	<p>Factor 5.2: Communications and Internet Infrastructure Resilience</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Internet Infrastructure Reliability • Monitoring and Response
<p>Factor 5.3: Software Quality</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Software Quality 	<p>Factor 5.3: Software Quality</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Software Quality and Assurance

<p>Factor 5.4: Technical Security Controls</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Technical Security Controls 	<p>Factor 5.4: Security Controls</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Technological Security Controls • Cryptographic Controls
<p>Factor 5.5: Cryptographic Controls</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Cryptographic Controls 	<p>Factor 5.5: Cryptographic Controls</p> <p>Cryptographic controls was merged into Security Controls (above) as a new aspect.</p>
<p>Factor 5.6: Cybersecurity Marketplace</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Cybersecurity Technologies • Cyber Insurance 	<p>Factor 5.5 Cybersecurity Marketplace</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Cybersecurity Technologies • Cybersecurity Services and Expertise • Security Implications of Outsourcing • Cyber Insurance
<p>Factor 5.7: Responsible Disclosure</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Responsible Disclosure 	<p>Factor 5.6: Responsible Disclosure</p> <p>Aspects:</p> <ul style="list-style-type: none"> • Sharing Vulnerability Information • Policies, Processes and Legislation for Responsible Disclosure of Security Flaws

CMM 2021 Edition

will be available on

<https://gcsc.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://gcsc.ox.ac.uk>



@CapacityCentre



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