This commission remains open for additional co-sponsorship. It is currently sponsored by: Australia; Botswana; Belize; Chile; Colombia; Dominican Republic; Ecuador; Fiji; Germany; Georgia; Iceland; Japan; Malawi; Mauritius; Netherlands; Norway; Paraguay; Peru; Switzerland; Tanzania; Uganda; United Kingdom; Vanuatu; Global Cyber Security Capacity Centre; Cybersecurity Capacity Centre for Southern Africa; Oceania Cyber Security Centre; Commonwealth Telecommunications Organisation; Global Forum on Cyber Expertise; Organization of American States; Asia-Pacific Telecommunity (APT)

The Cybersecurity Capacity Maturity Model: Driving needs assessments and national strategies

---

'*Capacity-building should … correspond to nationally identified needs and priorities… and be tailored to specific needs and contexts'*. A/75/816 (OEWG 2021 Final Report)

What is the Cybersecurity Capacity Maturity Model (CMM)?

1. The Cybersecurity Capacity Maturity Model[1] (CMM) is a first-of-its-kind model to review cybersecurity capacity maturity enabling nations to self-assess, benchmark, better plan investments and national cybersecurity strategies, as well as set priorities for capacity development.

2. Crucially these are guided assessments where experts can support nations and organisations to understand their current situation and how they can make progress in a way that is tailored to their circumstances.

3. This stakeholder developed and implemented model has led to enormous improvements in States capacity building efforts, and to their ability to cooperate internationally on capacity building and in countering malicious cyber activity.

Why undertake a Cybersecurity Capacity Maturity Model (CMM) assessment?

4. Undergoing a basic needs assessment and developing a national cyber strategy enables States to make the most of international cooperation. This need was recognised in our consensus framework as early as 2013[2]. It is beyond time to make it real.

5. Undertaking a CMM review bridges traditional siloes of expertise, strengthens networks and relationships between stakeholders, and creates evidence-bases that can be used to underpin investment cases as well as national cybersecurity strategies.

---

[1] For more on the CMM, please contact: cybercapacity@cs.ox.ac.uk
[2] See A/68/98, Final Report of the 2013 GGE, paragraph 30.

6. At least 87 States – including the UK – have taken this first step since 2015 using the CMM designed by the Global Cyber Security Capacity Centre (GCSCC) in Oxford. 36 states have gone on to use the process a second time to review their strategy. But that leaves many others who may not have had that opportunity through this or a similar process.

How can I undertake a Cybersecurity Capacity Maturity Model (CMM)?

7. Delivery of the CMM is a global effort delivered through a range of well-known stakeholders from the World Bank (with funding from the Korea Internet and Security Agency and the Government of Japan) to the International Telecommunication Union, and through regional institutions such as the Organization of American, the Inter-American Development Bank, the Commonwealth Telecommunications Organisation, the Oceania Cyber Security Centre (sponsored by the Australian State of Victoria), and the Cybersecurity Capacity Centre for Southern Africa (C3SA, sponsored by the Government of Norway).

What role for Member States and the Open Ended Working Group?

8. *The OEWG provides an opportunity to ensure that all States who wish to work through the CMM or similar model to conduct an initial needs assessment and develop a national strategy, can do so.*

9. We call on all Member States to prioritise their own cybersecurity capacity maturity and recognise the role of these models in enabling international cooperation. By sharing opportunities for best practice we can support practical progress towards identifying States' needs, improving coordination and ensuring that States are appropriately matched to existing opportunities which support international cooperation.

10. We call on the OEWG to:
    a. Promote the routes by which States can access support – including funding – to conduct the CMM through the above organisations and through the Global Forum for Cyber Expertise (GFCE);
    b. Promote alternative routes for those who do not wish to complete a full guided assessment, including the online guides provided by the Oxford GCSCC Centre[3] and the 'national cybersecurity strategy cycle catalogue' available through the GFCE's Cybil Portal; and
    c. Welcome UNIDIR's ongoing research and highlight tracking global progress against the movement for States to assess their priority needs and aims and

[3] The CMM is openly published and freely available enabling countries to utilise it without support if they so wish.

develop national strategies, perhaps through voluntary reporting using the Survey of National Implementation, as a possible area of future work.