



The Cyber Security Body Of Knowledge



Topic Guide updates

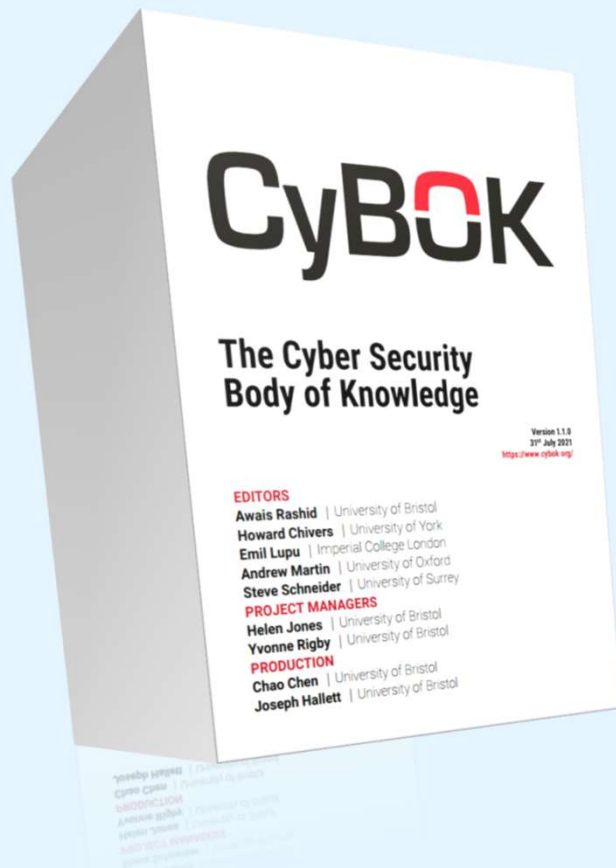
Cloud Security and Security-Informed Safety

Andrew Martin

Professor of Systems Security
University of Oxford

contact@cybok.org
www.cybok.org

CyBOK: a living document set



- responsive mode updates
 - change requests open
- proactive review
 - a theme at a time
- accompanying documents for
 - emerging themes
 - cross-cutting knowledge
 - (long-term development)

transparency

rigorous processes

peer review

community consensus

So far

Security Economics Knowledge Guide Issue 1.0.0

Tyler Moore | University of Tulsa

EDITOR
Yulia Cherdantseva | Cardiff University

REVIEWERS
Ross Anderson | University of Cambridge
Daniel Arce | University of Texas at Dallas
Rainer Böhm | University of Innsbruck
Jason Nurse | University of Kent

AI for Security Topic Guide Issue 1.0.0

Matilda Rhode | Airbus

EDITOR
Awais Rashid | University of Bristol

REVIEWERS
Elisa Bertino | Purdue University
Daisuke Mashima | Advanced Digital Sciences Center
Guillermo Suarez-Tangil | IMDEA Networks Institute

Security and Privacy of AI Knowledge Guide Issue 1.0.0

Lorenzo Cavallaro | University College London

Emiliano De Cristofaro | University College London

EDITOR
Steve Schneider | University of Surrey

REVIEWERS
James Muir | BAE Systems Digital Intelligence
Jose Such | King's College London
Yang Zhang | CISPA

transparency

rigorous processes

peer review

community consensus

Topic Guide in Progress: **Cloud Security**

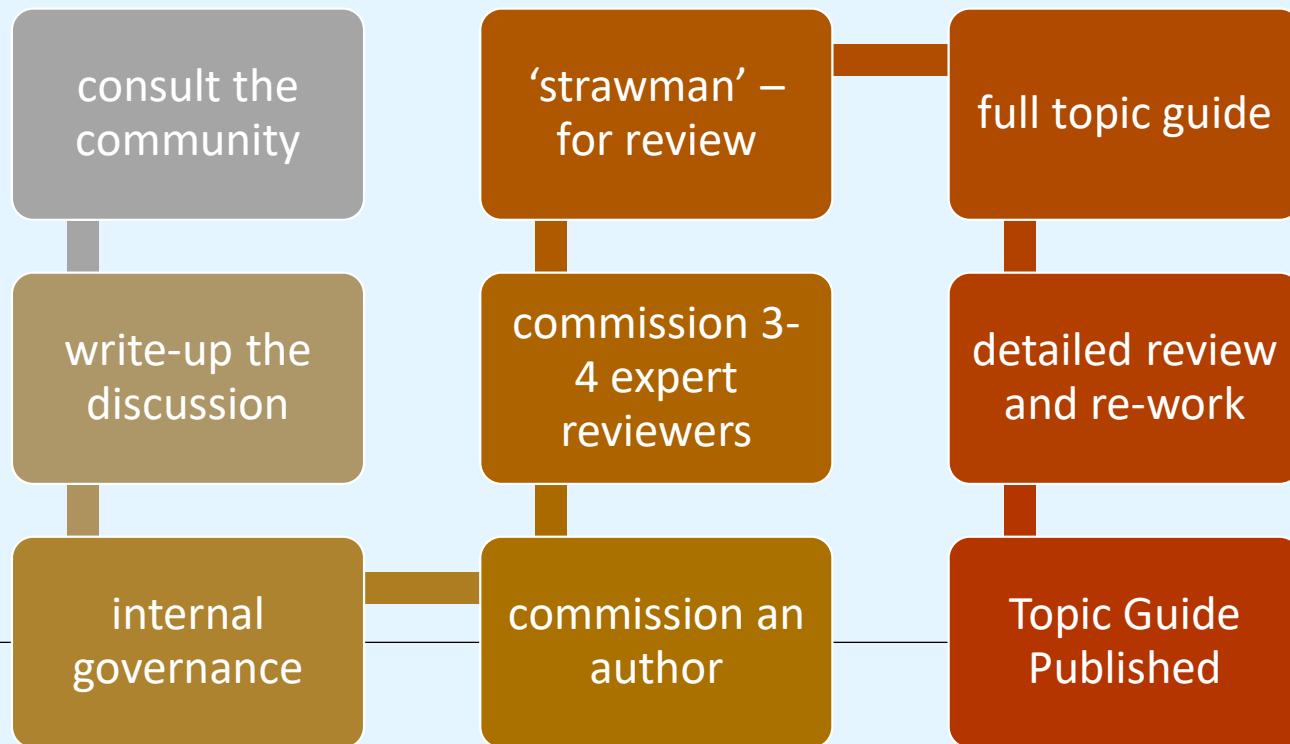
- Identified as a cross-cutting theme/topic
- Relevant to many CyBOK KAs
 - including OS/virtualization, networking, distributed systems, AAA, Law & Regulation
- Lots of practitioner knowledge – and emerging stable architecture models
- Small pockets of academic expertise
 - much research on details; not so much on the big picture

Cloud Security Topic Guide

- **2023/24:** lots of scoping discussions
- Author identified
- **May 2025:** *strawman* for expert review
- **summer 2025:** authoring and review; copy editing
- **autumn 2025:** published TG

Topic Guide in Progress: Cloud Security

- CyBOK was invited by DSTL to consider developing a Topic Guide in *Security-Informed Safety*
- *Following our usual process:*



Workshop outcomes

- Strong agreement on the need
 - With some dissent
 - Noting much pre-existing work in regulations, codes of practice; not much that is discursive or expository.
- Topic guide needs to explain differences of approach in safety and security
 - Should consider the intellectual and engineering inter-play of the two themes
- Need sector-specific discussions
 - automotive, rail, nuclear, off-shore, aviation
- Nod to emerging concerns
 - e.g. security of AI in safety-critical settings

discussion questions

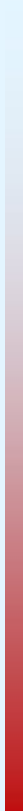
1. Is there a coherent body of established knowledge in this area, sufficient to warrant the creation of a substantive guide to the topic?
2. What material from the core CyBOK should be part of such a guide?
3. How can we make an indicative list of topics to be included (preferably with a structure/narrative arc to link them)?
4. What are the key references to draw upon and cite? (Other Bodies of Knowledge; Standards; seminal papers; textbooks).

Current state, and plans

- Recruiting author, establishing scope, and strawman
 - we will follow the process described
- **Extra phase of work:**
 - CyBOK has had multiple rounds of 'small projects' for supporting materials
 - (practical labs, instruction material, evaluations in particular contexts, etc.)
 - all outputs freely available under OGL
 - We will issue an open call for small projects specifically in Security-informed safety
 - Objectives of developing resources, and broadening awareness/take-up of the ideas
 - Based on previous experience, we would expect take-up by a range of academic and SMEs, typically: we offer up to £5k for a small project to produce some useful resources (to be published under OGL).
 - Project team reviews one-page proposals and funds the most promising/best focussed.

In summary

- Working on:
 - **Topic Guide in Cloud Security**
 - publication later in 2025
 - **Topic Guide in Security-Informed Safety**
 - **Resources supporting Security-Informed Safety**
 - Teaching materials, curricula, practical labs, evaluations: depending on what the community offers and produces
- Informal input welcome in all published CyBOK



CyBOK

contact@cybok.org
www.cybok.org

