CyBOK

CyBOK: Cyber Security Body of Knowledge

Process

This document defines the processes to be followed by the CyBOK project in all aspects of the development of the Cyber Security Body of Knowledge, and supporting documents. It meets the project's commitment to "Detail and publish the process for developing, consulting, and publishing the CyBOK and its major phases."

1. Phase One: Scoping

The main thrust of Phase I is to establish the scope for CyBOK: that is, identifying the key knowledge areas to be covered. The intention of this phase is that it will enable the project sponsors and members to agree a consensus, determining in broad terms what is in and out of scope. The intention is to match the wider community's consensus about the extent of the topic of cyber security.

1.1. Data Mining

As many static sources of evidence as possible will be mined for information, including:

1. previously-published bodies of knowledge in this and related areas
2. systematic descriptions of the field from industry and professional bodies
3. papers, contents lists, and calls from relevant academic conferences and journals
4. relevant trade conferences and publications

We will use these sources to generate a *Straw Man Scope Document*, which will be shared with sponsors and will complement the active data collection activities described below. The Straw Man *may* also be shared more publicly.

1.2. Active Data Collection

Input will be solicited from the wide Cyber Security community – researchers and practitioners – across the UK and internationally, though a number of means:

1. *Interviews with key experts*, will be conducted nationally and internationally to elicit views on the scope of CyBOK and the knowledge areas to be covered.
2. *Workshops with researchers and practitioners in the UK* will be organised.
3. *Community views on key topic areas* will be gathered through a survey of academia and industry (nationally and internationally) that will be made available on the CyBOK web site.
4. *A call for short position papers* will be set up to invite contributions from the national and international community towards the identification of knowledge areas.

The resulting data set will be held by the project team but will not be ready for wide dissemination at this time. Informal mention of emerging themes, and recurring questions regarding scope, will of course need to feature in interviews and workshops.

1.3. Analysis, Synthesis and Establishment of Scope

The third part of this phase will entail analysing and synthesising the insights from the various consultations and mapping studies, to define the scope of CyBOK and the knowledge areas to be covered. This will be a mix of systematic and ad hoc processes, undertaken by the project team.

We will run birds-of-a-feather sessions (BoFs) at major international conferences to gain feedback on the list of emerging knowledge areas. Advice will also be sought from our international academic advisors and the Professional Advisory Board. Online consultations will be run with the cyber security community to gain feedback before finalising the knowledge areas and scope of the CyBOK..

Deliverable: *Report defining the CyBOK scope*.

- This will be published and made available publicly. It will substantially be fixed for the duration of the project, but may be subject to minor updates as needed.
- There will be around 10-15 resulting knowledge areas (KAs) that will formulate the top-level topics within CyBOK. These will be normative for the project overall, and once agreed will be changed only following consultation with the advisory groups, and consent from the sponsor.
- Each KA will be accompanied by a 50-150 word summary (prose or keywords) describing the extent of the KA. This will be *indicative,* and may be subject to change in the detailed drafting process. A KA strawman text that diverges (by omission, or by adding a lot of extra topics) substantially (in the opinion of the KA Editor or expert review panel) will need approval from the Project Management Board.
- The scoping document will also present an *indicative* list of knowledge areas that are relevant but out of scope (including prerequisite knowledge that is not itself about cyber security). Such a list will emerge during the drafting process (below), but capturing a first draft here serves several purposes: (i) determining what is *not* in scope is valuable in its own right; (ii) where the same prerequisite is needed by more than one KA, it will be helpful for each to refer to the same authoritative external source, rather than introducing confusion with competing sources.

2. Phase 2: Developing Knowledge Areas

Development of each KA will be overseen by a **KA Editor**, who will normally be a member of the Project Management Board.

2.1. Initial Drafting and Review

Knowledge Areas will be assigned to a **KA author** (or authors) by a process defined below.

Each Knowledge Area will also have a **KA expert review panel**. This panel will normally include five international experts who will provide detailed scrutiny of the knowledge area description and comments to the authors. Review panel members will be selected by a process also defined below.

Each author will be invited to write a description of the KA, according to guidance given in the *Author Guidelines.* Authors will have access to the Scoping Document, and will be asked to determine the scope of their KA as an initial step. Development of the KA will be via an iterative process, with at least three steps:

- The KA author or authors will prepare a ***strawman*** proposal for initial review and feedback by the expert panel for that KA (see below).
- The author(s) will prepare a full draft (***woodenman***[1]) which will be reviewed by the Review Panel, generating feedback for the authors. This step may be repeated if multiple iterations are required to revise the KA description.

[1] Borrowing nomenclature from "Ada - The Project, The DoD High Order Language Working Group", ACM SIGPLAN Notices Vol. 28, No. 3, March 1993.

- Once all feedback from the expert review panel has been addressed, the author(s) will then prepare a draft for public release (***tinman***) which will be copyedited, and distributed for community consultation.

In developing the KA description, authors will need to refine the account of topics which are relevant but out of scope for the KA. Such topics may be expected to be covered in another KA (cross-dependency) or in external documentation (prerequisite).

The written content will remain embargoed, confidential to the authors and expert panel reviewers, until it has been formally reviewed by the Project Management Board (which may seek input from the Professional Advisory Board and International Academic Advisors as needed). Once the content has been approved, it will be copy- edited, prior to the launch of a public review phase.

2.2. Public Review Phase

Following the private review process defined above, the resulting 'tinman' fair draft of the KA will be made available publically and announced, with public review invited.

As well as individual contributions here, we will undertake wide community consultation on the drafts through online community engagement, as well as via workshops held nationally and internationally (co- located with major international conferences).

To avoid overburdening authors and editors, we will manage this public feedback using a system akin to bug tracking and management. During our workshops and calls for online feedback, we will encourage those commenting to offer constructive suggestions for improvement, discouraging purely negative comments. It will be the role of the KA Editor, supported by the expert review panel for that KA, to prioritise such feedback and help filter duplicates and irrelevancies. The authors, thus, will only receive review feedback that they can and should act upon.

The collection of comments will be time-limited, and authors will also be asked to undertake updates within a set time frame.

2.3. Provisional Release

Following completion of the public review phase, the resulting draft KA (***'ironman'***) will be made available publically. It would be regarded as stable at this stage, but further 'bug' reports may be filed. The KA Editor will decide whether (and when) to act upon these, or to invite additional review as needed. If re-drafting is needed, this will be referred back to the Author, but only on a timetable agreed by the Project Management Board.

2.4. Full Release

When all KAs are complete, and dependencies/inconsistencies are resolved, the collection of KAs and prerequisite lists will be published as a completed CyBOK (**'steelman'**).

Maintenance (further review and bug reports) will continue through a separate project, if judged appropriate by the sponsors.

3. Author and Reviewer Selection

3.1. Knowledge Area Editors

Each Knowledge Area (KA) will be assigned to one of the five members of the Project Management Board, who will act as the KA Editor for those areas. The role of the editor will be to ensure the overall process of delivery of appropriate text on that topic. We will ensure that KAs are assigned to editors where they have strong domain knowledge, in order that they will be able to recruit relevant expert authors and reviewers. In the event that a KA is discovered for which none of the investigators feels equipped with suitable domain knowledge, the project will seek advice from its International Academic Advisors to supplement the board's knowledge and identify potential authors. However, one of the board members will remain responsible for that area in an oversight role.

3.2. Author Selection

Authors will be selected through a two- step process: (i) During the workshops and consultations during the scoping work in Phase I, we will seek community input on the internationally leading figures suitable for writing contributions to CyBOK on particular topics. (ii) Once the KAs have been finalised, KA editors will utilise this community input along with their own extensive knowledge of the national and international research community to draw up a list of leading candidates to author each KA description. In some cases, KAs may be authored by one individual and, in others, two or three individuals. The KA editor will produce a list of 10 leading candidate authors along with their brief resumes and influential publications. We will only select candidate authors who will carry weight with the target community, with a strong track record of scholarly work and high quality publications.

The Project Management Board will rank the candidate authors for each KA. The ranked lists will be presented to the Professional Advisory Board and International Academic Advisors and their input sought before they are finalised. Once the ranked lists are finalised, the KA editors will approach the candidate authors (or co-authors) in rank order to discuss whether they will be able and willing to take on the role.

3.3. Expert Reviewer Selection and Review Process

The review process is designed as a two-stage process to ensure thorough peer review of the submitted KA descriptions while managing the overhead for the authors. Each KA description is first scrutinised by an expert review panel before being released for public review and consultation.

Each KA Editor will take the role of chair of an expert review panel to examine the candidate documents from KA authors. This panel will normally include five international experts who will provide detailed scrutiny of the knowledge area description and comments to the authors. As with the author selection process, the KA Editor will solicit and identify candidates, to be prioritised by the Project Management Board and reviewed by the Academic Advisors and Professional Advisory Board prior to finalisation.