

TERMS OF REFERENCE

SECURITY Community of Expertise

1 Status

The Security Community of Expertise (SCoE) reports to the Policy and Public Affairs Board (PPAB) as a Standing Group to develop long term policy capability in “security” (see 2.3).

2 Purpose

The principal aims of the Security Community of Expertise are:

- 2.1 To serve/enable the public good and enhance the UK economic and social well being – in relation to information security, identity and privacy matters and associated risks and exposures.
- 2.2 To act as a source of professionally-recognised expertise for informing BCS policy in the security, identity and privacy fields, advising and influencing the wider security arena, underpinning the outward-facing role of the BCS and providing a means of encouraging wider membership of the Society.
- 2.3 To provide advice to the PPAB, Engineering and Science Board, Professionalism Board and BCS Academy on:
 - Information & Communication Technology (ICT) Security
 - Information & Communication Technology (ICT) Audit
 - Information Confidentiality, Integrity and Availability [the 3 fundamental tenets of IT and IS Governance]
 - Information Privacy
 - Risk Management associated with all aspects of Information and Privacy Assurance
 - Security Management, including: People, Process, Technology and Innovation
 - Privacy Management
 - Identity Management
 - Security and Privacy Design
 - Security Standards (including Compliance with Information Regulatory and Statutory Requirements)
 - And other associated specialisms

For simplicity these headings are hereafter identified by the term “Security”.

- 2.4 To encourage cooperation between the various players within the security specialisms – both internally and externally, in the public and private sectors. This will include bringing in other parts of BCS for workshops, debates, seminars etc. as necessary to achieve the above aims.
- 2.6 To contribute to the growth of BCS new products and services for members, related to all security specialisms.
- 2.7 To influence public policy by contributing to appropriate consultations on behalf of BCS and reflecting outward from the Institute across the membership and to the general public, corporations and government.

3 Key Responsibilities

In support of its purpose the SCoE will:

- 3.1 Ensure that its membership comprises an active group of key professionals who between them are able to survey the Security area.
- 3.2 Agree on an expert professional view on selected issues arising within its sphere of responsibility. Where possible agree these with other professional bodies, such as the joint ETF initiatives and responses to Government consultations with IET and RAEng; the Cyber Security Skills Partnership with IET, RAEng, IAAC, CESG, e-Skills, BIS and others.
 - 3.2.1 Write and publish White Papers and Position Papers for BCS on these topics.
 - 3.2.2 By so doing, seek to influence government, regulators and industry to make computing safer for the public and to educate them.
- 3.3 Respond to public consultations as and when appropriate through the Government Relations Group of the PPAB.
- 3.4 Actively research ideas and develop proposals for products, services, recommendations, conferences, seminars and any other activity which may benefit the BCS membership and the wider community in the security field.
- 3.5 Carry out Thought Leadership Debates and generate Hot Topic meetings on Security issues.
- 3.6 Work closely with all the BCS Specialist Groups, Branches, Committees, Panels and Working Groups that have an interest in all or part of the security field.
- 3.7 Develop relationships with outside bodies in the security field for mutual development of policies, increased profile, products and services. (see also 3.2 for specific examples)/
- 3.8 Provide security content on the BCS website and/or eBCS & Elite Newsletters, IT NOW and other BCS publications.
- 3.9 SCoE will be responsible for ensuring that all its members receive appropriate training as prescribed by Trustee Board from time to time.

4 Strategic Planning and Management

- 4.1 In consultation with BCS HQ staff and the PPAB, the Security CoE will produce annual business plans with associated budgets.
- 4.2 The SCoE will monitor its success in achieving its Annual Plan. This will be considered by the PPAB during the annual business planning process.

5 Constitution and Membership

- 5.1 All appointments to the Security CoE, with the exception of the Chair, shall be subject to approval by PPAB, following the recommendation of the Security CoE Chair.

- 5.2 Membership of the Security CoE will be granted on the basis of demonstration of seniority level, security strategy development, adequate qualifications, industry experience, recognition by peers, and evidence of an appropriate track record.
- 5.3 Membership of the Security CoE shall comprise:
- Chair, appointed by the PPAB.
 - A deputy Chair, who is not an automatic candidate for the role of Chair
 - There will be a maximum of 25 members who should be Professional Members of the Institute.
- 5.4 Appointments for all members shall be for three years initially, thereafter on an annual basis for a maximum of six years.
- 5.5 SCoE members, representing specific constituents (e.g. the ISSG) may appoint an alternative to represent them on SCoE business with the prior agreement of the SCoE Chair.
- 5.6 Actions and decisions of the CoE must be agreed by a majority of the members present, with a requirement that, as a minimum, a meeting quorum of one quarter of the total current membership of the CoE, rounded up to the next whole number, must be in attendance.
- 5.7 Each member must be prepared to contribute to matters within his or her competence that are discussed by the panel, and must fairly represent the views of the panel in all significant respects when discussing the actions of the panel with others.
- 5.8 All members must commit reasonable time and effort to the work of the CoE and make reasonable efforts to attend meetings. If a member fails to attend three consecutive meetings, the CoE may terminate his or her membership of the CoE, unless the non-attendance was owing to illness or other reasonable cause.
- 5.9 On the recommendation of the Chair of the CoE, the PPAB may cancel or suspend the membership of the CoE where the member's actions have, in the opinion of the PPAB and of the SCoE, been detrimental to the work of the CoE.
- 5.10 In the event that the Chair is unable to attend and chair a particular meeting, the Chair of the CoE may delegate his/her deputy, or in his/her absence another member from amongst the panel, to chair that particular meeting.
- 5.11 In the event of a tied vote, the Chair or acting chair shall have an additional casting vote.
- 5.12 In order to maintain a wide portfolio of awareness and inclusion, there will be representatives from academia, industry, and the public sector within the CoE membership

6 List of Boards, Committees, Expert Panels, Working Groups and Standing Committees that have representation on the Security Community of Expertise

- Information Security Specialist Group (ISSG)
- Information Risk Management & Audit Specialist Group (IRMA)

- Information Privacy Expert Panel (IPEP)
- Forensics and Cyber-Security Specialist Group
- Young Professionals Information Security Group

7 Approval and Review

These Terms of Reference are approved by the PPAB. The Security Community of Expertise will review them on an annual basis.