

# The UK Cyber Security Council

The role of the Council  
and the influence of  
CyBOK

## About the Council

### Formation

### Vision, role & mission

### What we do

### The four pillars

### The Council and CyBOK

### What can you do?

# VISION, ROLE & MISSION

Our **vision** is a shared vision: for the UK to be one of the most secure places anywhere in the world to do business in cyberspace\*.

Our **role** in achieving this vision is to be the umbrella body for existing professional organisations and to drive progress towards meeting the key challenges faced by the profession.

In that role, our **mission** is:

- ▶ to be the self-regulatory body for, and voice for, the cyber security profession
- ▶ to develop, promote and provide stewardship of the highest possible standards of expertise, excellence, professional conduct and practice in the profession, for the benefit of the public.

\*As set out in the original National Cyber Security Strategy 2016-2021

About the Council

What we do

The four pillars

The Council and  
CyBOK

What can you do?

# WHAT WE DO

In order to **champion the cyber security profession** across the UK, **provide broad representation** for the industry, **accelerate awareness** and **promote excellence in the profession**, the Council:

- ▶ delivers thought leadership, career tools and education resources to the cyber security sector and those seeking to enter the sector
- ▶ helps influence government, industry and academia with the aim of developing and promoting UK cyber security excellence globally; and
- ▶ takes action to grow the UK's cyber security skills base.

About the Council

What we do

The four pillars

Professional  
development

The Council and  
CyBOK

What can you do?

# PROFESSIONAL DEVELOPMENT

Key purposes of the Council:

- ▶ supporting the professional development of those working or aspiring to work in the cyber security profession
- ▶ supporting employers and individuals as they make decisions about skills, development and recognition through certification and Chartered Status
- ▶ establishing a professional qualification framework, mapping criteria to appropriate skills and qualifications.

About the Council

What we do

The four pillars

Professional  
development

Outreach &  
diversity

The Council and  
CyBOK

What can you do?

# OUTREACH & DIVERSITY

Key purposes of the Council:

- ▶ broadening the skills base and overcoming actual and perceived barriers to entry and progression
- ▶ building a vibrant and inclusive network of industry, government and education partners that will provide events and attract people into cyber security from all parts of society
- ▶ promoting cyber security as an attractive and rewarding career option for people of all ages and at any stage of their career, whether already in the industry or new to it.

About the Council

What we do

The four pillars

Professional  
development

Outreach &  
diversity

Professional  
ethics

The Council and  
CyBOK

What can you do?

# PROFESSIONAL ETHICS

Key purposes of the Council:

- ▶ building and maintaining public confidence in the industry, its organisations and practitioners
- ▶ developing and maintaining a Code of Ethics and Guiding Principles for Individuals, to ensure organisations and individual professionals maintain the highest possible standards themselves and challenge any unethical behaviour by others
- ▶ enforcing through member bodies the Code of Ethics

About the Council

What we do

The four pillars

Professional  
development

Outreach &  
diversity

Professional  
ethics

Thought  
leadership &  
influence

The Council and  
CyBOK

What can you do?

# THOUGHT LEADERSHIP & INFLUENCE

Key purposes of the Council:

- ▶ informing Government policy and regulation development by:
  - ▶ acting as an expert body on education and skills for the cyber security profession
  - ▶ identifying where new policies are required; and
  - ▶ advising on regulations or statutes that include an aspect of cyber security.
- ▶ forging and nurturing essential international links
- ▶ working with industry and regulators to further the cause of the sector and to ensure needs are understood on both sides
- ▶ working with relevant bodies to agree standards that define cyber security.

About the Council

What we do

The four pillars

The Council and  
CyBOK

Why CyBOK is  
important to the  
Council

What can you do?

# WHY CYBOK IS IMPORTANT TO US

CyBOK is the source of the knowledge content in two key products for the Council:

- ▶ The Careers Framework
- ▶ The Qualification Framework

About the Council

What we do

The four pillars

The Council and  
CyBOK

Why CyBOK is  
important to the  
Council

The  
Qualifications  
Framework

What can you do?

# THE CAREERS FRAMEWORK

## Helping

Prospective practitioners (and advisers) identify:

- ▶ suitable initial roles
- ▶ helpful qualifications
- ▶ potential career paths

Current practitioners identify:

- ▶ appropriate sideways careers moves
- ▶ prospects for upwards progression
- ▶ helpful qualifications

Managers and recruiters define:

- ▶ cyber security team structures
- ▶ job and person descriptions
- ▶ appropriate qualifications for roles
- ▶ Valuable experience outside cyber for IT for candidates

About the Council

What we do

The four pillars

The Council and  
CyBOK

Why CyBOK is  
important to the  
Council

The  
Qualifications  
Framework

Specialisms

What can you do?

# SPECIALISMS

- ▶ Used to define pathways and roles in the Careers Framework
- ▶ Descriptive, not prescriptive
- ▶ Compatible with existing standards
- ▶ Flexible enough to meet the varying needs of organisations

About the Council

What we do

The four pillars

The Council and  
CyBOK

Why CyBOK is  
important to the  
Council

The  
Qualifications  
Framework

Specialisms

The 16  
specialisms we  
are using

What can you do?

# THE 16 SPECIALISMS WE ARE USING

- ▶ Digital Forensics
- ▶ Threat Intelligence
- ▶ Incident Response
- ▶ Vulnerability Management
- ▶ Network Monitoring & Intrusion Detection
- ▶ Security Testing
- ▶ Data Protection & Privacy Management
- ▶ Cryptography & Communications Security
- ▶ Identity & Access Management
- ▶ Secure Operations
- ▶ Secure Development
- ▶ Secure Architecture & Design
- ▶ Cyber Security Risk Assessment & Management
- ▶ Cyber Security Audit & Assurance
- ▶ Cyber Security Control & Management
- ▶ Cyber Security generalist

About the Council

What we do

The four pillars

The Council and  
CyBOK

Why CyBOK is  
important to the  
Council

The  
Qualifications  
Framework

Specialisms

The 16  
specialisms we  
are using

An example of  
mapping  
knowledge to  
specialisms

What can you do?

# EXAMPLE: MAPPING KNOWLEDGE

- ▶ What is the relevant knowledge?
  - ▶ These knowledge elements are ones that an experienced practitioner in an incident response role will typically use, although not always to the same level of detail.
  - ▶ They are most likely to have a very good understanding of the Specialist Knowledge, which is essential to performing the role.
  - ▶ They may still a good understanding of the Related Knowledge but not to quite the same degree.
  - ▶ They may have much less detailed understanding of the elements of Wider Knowledge, which provides context for their work.
  - ▶ It is not expected that someone coming into such a role would have all this knowledge initially.

About the Council

What we do

The four pillars

The Council and  
CyBOK

Why CyBOK is  
important to the  
Council

The  
Qualifications  
Framework

Specialisms

The 16  
specialisms we  
are using

An example of  
mapping  
knowledge to  
specialisms

What can you do?

# EXAMPLE: MAPPING KNOWLEDGE

## Incident Response

- ▶ Specialist Knowledge
  - ▶ Security Operations & Incident Management

If you are working in a role which has responsibility for the security of cyber-physical systems you will also need:
  - ▶ Cyber-Physical Systems Security
- ▶ Related knowledge
  - ▶ Malware & Attack Technologies
  - ▶ Adversarial Behaviours
- ▶ Wider Knowledge
  - ▶ Human Factors
  - ▶ Forensics
  - ▶ Network Security
  - ▶ Hardware Security

About the Council

What we do

The four pillars

The Council and  
CyBOK

Why CyBOK is  
important to the  
Council

The  
Qualifications  
Framework

Specialisms

The 16  
specialisms we  
are using

An example of  
mapping  
knowledge to  
specialisms

SPARE

What can you do?

# THE QUALIFICATION FRAMEWORK

- ▶ A consistent presentation of each cyber security qualification
- ▶ A system for matching qualifications to specialism
- ▶ Matching process
  - ▶ Qualification syllabus
  - ▶ Knowledge Areas per specialism
  - ▶ Assess extent of match
  - ▶ Copy results into Careers Framework pathways

About the Council

What we do

The four pillars

The Council and  
CyBOK

What can you do?

# WHAT CAN YOU DO?

Once the Council is operational, there will be opportunities for:

- ▶ Organisations to work with the Council, including options for membership
- ▶ Practitioners and experts to volunteer and support the work of the Council