CyBOK

# The Cyber Security Body of Knowledge

## Tabular representation of CyBOK Broad Categories, Knowledge Areas and their descriptions

**June 2020**
http://www.cybok.org

| S.NO | 1- Human, Organizational, and Regulatory Aspects | |
|---|---|---|
| 1 | Risk Management and Governance | Security management systems and organizational security controls, including standards, best practices, and approaches to risk assessment and mitigation. |
| 2 | Law and Regulation | International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare. |
| 3 | Human Factors | Usable security, social and behavioural factors impacting security, security culture and awareness as well as the impact of security controls on user behaviours. |
| 4 | Privacy and Online Rights | Techniques for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems. |
| | 2- Attacks and Defences | |
| 5 | Malware and Attack Technologies | Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches. |
| 6 | Adversarial Behaviours | The motivations, behaviours, and methods used by attackers, including malware supply chains, attack vectors, and money transfers. |
| 7 | Security Operations and Incident Management | The configuration, operation, and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence. |
| 8 | Forensics | The collection, analysis, and reporting of digital evidence in support of incidents or criminal events. |
| | 3- Systems Security | |
| 9 | Cryptography | Core primitives of cryptography as presently practiced and emerging algorithms, techniques for analysis of these, and the protocols that use them. |
| 10 | Operating Systems and Virtualization Security | Operating systems protection mechanisms, implementing secure abstraction of hardware, and sharing of resources, including isolation in multiuser systems, secure virtualization, and security in database systems. |
| 11 | Distributed Systems Security | Security mechanisms relating to larger-scale coordinated distributed systems, including aspects of secure consensus, time, event systems, peer-to-peer systems, clouds, multitenant data centers, and distributed ledgers. |
| 12 | Authentication, Authorization, and Accountability | All aspects of identity management and authentication technologies, and architectures and tools to support authorization and accountability in both isolated and distributed systems. |
| | 4- Software and Platform Security | |
| 13 | Software Security | Known categories of programming errors resulting in security bugs, and techniques for avoiding these errors—both through coding practice and improved language design—and tools, techniques, and methods for detection of such errors in existing systems. |
| 14 | Web and Mobile Security | Issues related to web applications and services distributed across devices and frameworks, including the diverse programming paradigms and protection models. |
| 15 | Secure Software Lifecycle | The application of security software engineering techniques in the whole systems development lifecycle resulting in software that is secure by default. |
| | 5- Infrastructure Security | |
| 16 | Network Security | Security aspects of networking and telecommunication protocols, including the security of routing, network security elements, and specific cryptographic protocols used for network security. |
| 17 | Hardware Security | Security in the design, implementation, and deployment of general-purpose and specialist hardware, including trusted computing technologies and sources of randomness. |
| 18 | Cyber-Physical Systems Security | Security challenges in cyber-physical systems, such as the Internet of Things and industrial control systems, attacker models, safe-secure designs, and security of large-scale infrastructures. |
| 19 | Physical Layer and Telecommunications Security | Security concerns and limitations of the physical layer including aspects of radio frequency encodings and transmission techniques, unintended radiation, and interference. |