

FAQ Sheet for EBK

1. What is the IT Security EBK?

The EBK is a single framework that maps IT security competencies, such as incident management, and functions, such as manage or design, to both government and private sector IT security roles, such as digital forensics professional. Although sample job titles are listed within the document, roles are used because they are typically more descriptive than job titles and provide utility regardless of a specific organization or context. This high level approach means that the EBK provides insight for career paths for all IT security related professionals, no matter what organization or agency.

2. Is this product somehow related to the Information Assurance Workforce Improvement Program that is dictated by Manual DoD 8570.01-M?

Yes, it is related in that the development team used the results of the DoD job task analysis (Critical Work Functions) as inputs to the EBK. The DoD IASS was a core document used to shape the competency areas and functions captured in the IT Security Competency and Functional Framework. The IASS was developed by the Defense-wide IA Program (DIAP) as part of the DoD 8570-Workforce Improvement Program.

The IT Security EBK reflects the vast contribution of resources to date and builds directly upon the work of established references and best practices from the public and private sectors, which were used in the development process and are reflected within the content of the document. The IT Security EBK is a resource that can be used by organizations for workforce development and planning, by consumers for personal development, or by other groups as useful within their programs. It is not tied to a specific technology, allowing broad application in a variety of environments.

3. Is this a mandate?

The EBK is not mandated by existing policy nor is it intended to represent a standard, directive, or policy by DHS. It should be viewed as a complement to existing, widely used models for describing IT security processes such as the National Institute of Standards and Technology (NIST) or Committee on National Security Systems (CNSS) guidance on IT security training. It was developed as a resource tool to aid the public and private sectors, as well as higher education in developing curriculum, planning role-based training, instructional design for IT security courses, and IT security workforce professional development (e.g., career paths, certification options) to ensure that we have the most qualified and appropriately trained IT security workforce possible.

4. How would the federal government utilize this framework?

The federal government, a large customer of the certification industry, could potentially utilize the IT Security EBK through the Information Systems Security Line of Business (ISS LOB) initiative. The ISS LOB, an interagency program led by the Office of Management and Budget (OMB) and DHS, seeks to streamline specific security project relevant to all federal agencies including role-based, specialized security training. The IT Security EBK could be used to identify which competency-based topics would be

beneficial for various security roles, therefore helping to shape the federal government's role-based training requirements.

5. Will the IT Security EBK developers seek accreditation?

DHS may eventually seek inclusion in the overall accreditation process by working with the American National Standards Institute (ANSI) to ask certification providers to identify how their testing objectives map to the IT Security EBK. Alternatively, DHS may pursue other avenues for working with certification providers to identify how certifications map to the content and roles within the framework.

6. Is Certification and Accreditation (C&A) mentioned in the IT Security EBK?

Because DHS-NCSD provides the *IT Security EBK* for use across the public and private sectors, topics that are not applicable to these areas have not been included in this version. For example, the certification and accreditation (C&A) process, which is mandated by the Office of Management and Budget (OMB) Circular A-130 and applies only to systems that house Federal data, has not been included as a key term, concept, or function within a competency. The absence of C&A from the EBK is not meant to diminish its importance to IT security practitioners within the public sector—it is still a key term, but has not been included here because of its limited applicability across academia and private sector.

7. How often with the IT Security EBK be updated?

The EBK will continue to be revised approximately every two years with input from subject matter experts (SME), to ensure that it remains a useful and up-to-date resource for the community.