EXPLORING THE CHANGES TO THE CISSP DOMAINS

Brett J. L. Landry
College of Business, University of Dallas
Irving, TX 75062
blandry@udallas.edu 972-636-8633

Sandra Blanke
College of Business, University of Dallas
Irving, TX 75062
sblanke@udallas.edu

ABSTRACT

Recently ISC2, the organization that provides the Certified Information Systems Security Professionals (CISSP) exam and CISSP certification announced new changes for the 10 domains in the Common Body of Knowledge (CBK). This announcement has many security individuals rushing to ñBoot Campsò and other training programs to prepare and take the exam prior to the exam change date of January 2012. For individuals not taking the exam before the end of 2011 it is important to understand the changes outlined in this paper and obtain an understanding of the new knowledge subjects that will be required to become a CISSP in 2012 and beyond. This paper outlines these changes and discusses potential changes to coincide with the National Initiative of Cybersecurity Education (NICE).

INTROUCTION

The CISSP was the first credential in the field of Information Security accredited by the American National Standards Institute (ANSI) to International Standards Organizations (ISO) Standard 17024:2003. Today it is still a globally recognized standard of achievement and an objective measure of excellence. The CISSP exam is administered by the International Information Systems Security Certification Consortium (ISC)². The exam is designed around the security triad of confidentiality, integrity, and availability across ten domains that comprise the Common Body of Knowledge (CBK). In September 2011, (ISC)² announced that the CBK is was to change effective January 1, 2012. This paper sets out to examine the changes listed in the CISSP Candidate Information Bulletin (CIB) found on the (ISC)² website (. The ten domains are Access Control, Telecommunications and Network Security, Information Security Governance and Risk, Software Development Security, Cryptography, Security Architecture and Design, Security Operations, Business Continuity and Disaster Recovery Planning, Legal Regulations, Investigations and Compliance, and Physical (Environmental) Security. This review will examine the differences in the 2009 and 2012 CIB and not repeat the material topics that are unchanged.

Domain 1: Access Control

The changes to Access Control Domain are that there is an explained description under sections B and C as well as a new section D. Section B, *Understand access control attacks* now includes subsets of *threat modeling, asset, valuation, vulnerability analysis and asset aggregation.* Under Section C, *Assess Effectiveness of Access Controls,* two sections have been added*: user entitlement and access review and audit.* The new section D, *Identify and access provision lifecycle* gives examples of provisioning, review, and revocation without any additional details.

Domain 2: Telecommunications and Network Security

The first thing to be observed with Domain 2 is that section A has been changed from *Establish secure data communications* to *Understand secure network architecture and design*. This change includes IP and Non-IP protocols and segmentation. This is an important change in the area of security as so many of today's data breaches are as a result of flat, non-segmented networks. Raising the awareness of segmentation in the CBK is certainly a good thing. An additional topic, A.3, has been added to include Implications of multi-layer protocols. Under section B.1, Hardware now specifically includes wireless access points and B.2 transmission media gives examples of wired, wireless, and fiber. Under section C.3 Remote access has replaced Virtual Private Networks to include screen scraper, virtual application / desktop and telecommuting.

Domain 3: Information Security Governance and Risk

Domain 3 includes a number of small changes. Section 3.F is new with Manage third-party governance and tangible and intangible asset valuation is new within understand and apply risk management concepts. Professional ethics has been removed from this domain and has been moved to domain nine. Two new components have been added; (1) develop and implement information security strategies and (2) assess the completeness and effectiveness of the security program.

Domain 4: Software Development Security

Domain 4 has been renamed from Application Development Security to Software Development Security. Section A.5, Perform Risk Analysis has been removed and the other changes revolve around replacing application with security. Specifically certification and accreditation, Auditing and Logging and Corrective actions have been removed from Section C. It cannot be assumed that these concepts are actually leaving the CBK, but it is surprising that they have been removed and it is not clear where or if they are being addressed in other domains or another certification.

Domain 5: Cryptography

A new section has been added under Cryptography called Understand the cryptographic lifecycle has been added and using cryptography for email security has been replaced with using cryptography for application security. Other than that no changes are suggested for Cryptography.

Domain 6: Security Architecture and Design

There is only one change for domain six and that is the addition of Distributed Systems (cloud computing, grid computing and peer to peer) under *Software and system vulnerabilities and threats.* These are important topics and additions to the content of this domain.

Domain 7: Security Operations

In Domain 7, Personnel Privacy and Safety has been moved to Domain 10. Other small changes for this domain includes changing section D from *prevent and respond to attacks* to *implement preventative measures against attacks.*

Domain 8: Business Continuity and Disaster Recovery

Domain 8 is another of the domains that does not have any changes in this revision. We could argue that after the major natural disasters of 9-11 and Hurricane Katrina, and the disasters after data breaches that this domain could include more than just creating your disaster recovery plan and which archive bits are flipped in each variety of backup schemes. Ideally, newer DR schemes such as SANs to SANs replication should be covered at a minimum. Landry and Koger's (2006) work on the ten myths of disaster recovery would be a good inclusion here as well for a real world perspective.

Domain 9: Legal Regulations, Investigations, and Compliance

There are three small changes for Domain 9. Hardware/embedded device analysis has been added under *understand forensic procedures and* Section B on *understanding professional ethics* has been added. Additionally, a new section F has been added entitled Ensure security in contractual agreements and procurement processes (cloud computing, outsourcing, and vendor governance.)

Domain 10: Physical (Environmental) Security

The only change to Domain 10 is that *understand personnel privacy and safety* has been moved from a previous domain and added to this domain. Interesting enough, is that biometrics, multifactor authentication, and social engineering were not added to the domain.

National Initiative on Cybersecurity Education

The National Institute of Standards and Technology (NIST) has recently released the National Initiative on Cybersecurity Education (NICE) to address the issues of workforce development. The NICE framework outlines seven broad categories and thirty-one job roles. The seven categories or tracks are: securely provision, operate and maintain, protect and defend, investigate, operate and collect, analyze, and support. Additionally, NIST has outlined KSAs for many of these job roles to give guidance to employers and educators on defining job roles. NICE will serve as the national educational standards that U. S. NSA and DHS Academic Centers of Excellence (CAE) Universities will have to map to as CNSS 4021-4027. Since NICE

is holistic in that it includes all areas of IT and not just traditional firewall type security, both CAE students and practitioners will see NICE as a better framework than the CBK.

Conclusions

The 2012 revisions to the CISSP CBK are minor. Instructors and students should not be worried about major changes for the upcoming 2012 exams. However, the real issue is that the changes to the CBK are not enough to update the exam to match current and newer technologies, business strategies, and newer models such as NICE.

References

Landry, B. J. L., & Koger, M. S. (2006) Dispelling 10 common disaster recovery myths: Lessons learned from hurricane Katrina and other disasters. *ACM Journal of Educational Resources in Computing (JERIC).* 6(4).

ISC² (2011) *CISSP® - Certified Information Systems Security Professional. Retrieved from* https://www.isc2.org/cissp/default.aspx

National Institute for Standards and Technology. (2011) *The National Initiative for Cybersecurity Education (NICE). Retrieved from csrc.nist.gov/nice/*