Review Questions for Multiple Attempts - Secure Software Design D487

All answers must be in your own words. The copying and pasting of answers is not permitted.

1. What are the major phases of the SDLC?
2. Explain how the Common Computer Vulnerabilities and Exposures (CVE) aids in identifying threats and vulnerabilities.
3. Explain the advantages and disadvantages of the Waterfall Software Development methodology.
4. Explain the advantages and disadvantages of the Agile Software Development methodology.
5. What should a Privacy Impact Assessment include?
6. How does a programmer use Data Flow Diagrams in developing software?
7. An information security specialist ranks threats based upon which two factors? Explain each one.
8. Explain what is involved in black box testing.
9. What happens during the code review process?
10. What are the essential steps in Change Management?
11. What are the different elements of policy compliance analysis?
12. How is penetration testing different from vulnerability scanning? What type of software should undergo this form of testing?
13. What is a Software Security Champion? What is his or her area of expertise?
14. How does the STRIDE model aid in identifying threats?
15. How would you use the DREAD model in developing secure software?
16. Self Check – Learning a new discipline works at different levels. Think DIK – Data, Information, Knowledge. With *Data* understanding, you know definitions and terms. For example, you can explain what a fuzzer does. *Information* understanding means you can describe the relationships between different data. For example, what is the difference between the SDL and the SDLC? What are the differences between STRIDE and PASTA? How are the threat methodologies similar? You can apply concepts and discuss them comfortably at the *Knowledge* level of understanding. For example, before you ship a software product, what security factors must you consider? Why are those factors important?

    Before trying an Objective Assessment, ensure you have the knowledge level of understanding. We aim not only to have you memorize isolated facts but also to use those facts to foster skills to deploy in the information security profession. For practice, answer the questions below.

17. Explain what a fuzzer does.
18. What is the difference between the SDL and the SDLC?
19. What are the differences between STRIDE and PASTA? How are the threat methodologies similar?
20. Before you ship a software product, which security factors must you consider? Why are those factors important?

21.