Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 20 of the official CISSP study guide. Here are the top things you need to know from this chapter on software development security.

Explain the basic architecture of a relational database management system, know the structure of relational databases, be able to explain the function of tables, rows and columns, know how relationships are defined between tables and the roles of various types of keys, describe the database security threats posed by aggregation and inference, explain how expert systems, machine learning and neural networks function.

Expert systems consists of two core components, a knowledge base that contains a series of if then rules and an inference engine that uses that information to draw conclusions about other data. Machine learning techniques attempt to algorithmically discover knowledge from datasets.

Neural networks simulate the functioning of the human mind to a limited extent by arranging a series of layered calculations to solve problems. Neural networks require extensive training on a particular problem before they're able to offer solutions.

Understand the models of system development. Know that the waterfall model describes a sequential development process that results in the development of a finished product. Developers may step back only one phase on the process if errors are discovered. The spiral model uses several iterations of the waterfall model to produce a number of fully specified and tested prototypes. Agile development models place an emphasis on the needs of the customer and quickly developing new functionality that meets those needs in an iterative fashion.

Explain the scrum approach to agile software development. Scrum is an organized approach to implementing the agile philosophy. It relies on daily scrum meetings to organize and review work. Development focuses on short sprints of activity that deliver finished products. Integrated product teams or IPTs are an early effort at this approach that was used by the US Department of Defense. Describe software development maturity models.

Know that maturity models help software organizations improve the maturity and quality of their software processes by implementing an evolutionary path from Ad hoc chaotic processes to mature, disciplined software processes. Be able to describe the SW-CMM, ideal and SAMM models.

Understand the importance of changing configuration management. Know the three basic components of the change management process request control, change control and release control and how they contribute to security.

Explain how software configuration management controls the versions of software used in an organization, understand how the auditing and logging of changes mitigates risk to the organization, understand the importance of testing. Software testing should be designed as part of the development process. Testing should be used as a management tool to improve the design, development and production processes.

Explain the role of DevOps and DevSecOps in the modern enterprise. DevOps approaches seek to integrate software development and operations activities by embracing automation and collaboration between teams. DevSecOps approaches expand on the DevOps model by introducing security operations activities into the integrated model. Continuous integration and delivery CICD techniques automate the DevOps and DevSecOps Pipelines.

Know the role of different coding tools in a software development ecosystem. Developers write code in different programming languages, which is then either compiled into machine language or

executed through an interpreter. Developers may make use of software development tool sets and integrated development environments to facilitate the code writing process. Software libraries create shared and reusable code, whereas code repositories provide a management platform for the software development process.

Explain the impact of acquired software on the organization. Organizations may purchase commercial off the shelf for COTS software to meet their requirements and they may also rely on free open-source software. All of this software expands the potential attack surface and requires security review and testing. Those are the study essentials that you'll need to know for Chapter 20, software development security.