7. Oracle's Approach to Engineering Secure Cloud Services

The Oracle Cloud Services development process follows the Oracle Software Security Assurance (OSSA) program. The OSSA is Oracle's methodology for incorporating security into the design, building, testing, and maintenance of its services.

From initial architecture considerations to service post-release, all aspects of cloud services development consider security. Here is a summary of secure software development phases we go through:

- Design Phase: Security training about guiding security principles and Oracle's secure coding standards help ensure that our engineers, architects and product managers make the best security decisions possible. Assessing threats during architectural risk analysis meetings help us identify potential security issues as early in the development lifecycle as possible.
- Coding Phase: We address standard vulnerability types through the use of secure coding standards and patterns. In this phase we use static code analysis tools to identify security flaws and fix all significant security findings before our services move to testing phase.
- Testing Phase: Our internal security professionals and independent security consultants use Oracle internal tools, third party tools for dynamic analysis and fuzz testing, and manual testing to identify potential security issues.
- Prior to service release: Before we release a cloud service, Oracle validates that the functionality being developed meets Oracle's cloud security requirements. We use independent security professionals to evaluate and monitor the product for potential security issues.

See the **Oracle Software Security Assurance** online documents to learn more about OSSA.