1. Identifying the Need for Security in Your Software Projects

- Identify Security Requirements and Expectations
  Identify Factors That Undermine Software Security
  Find Vulnerabilities in Your Software
  Gather Intelligence on Vulnerabilities and Exploits

2. Handling Vulnerabilities

- Handle Vulnerabilities Due to Software Defects and Misconfiguration
  Handle Vulnerabilities Due to Human Factors
  Handle Vulnerabilities Due to Process Shortcomings

3. Designing for Security

- Apply General Principles for Secure Design
  Design Software to Counter Specific Threats

4. Developing Secure Code

- Follow Best Practices for Secure Coding
  Prevent Platform Vulnerabilities
  Prevent Privacy Vulnerabilities

5. Implementing Common Protections

- Limit Access Using Login and User Roles
  Protect Data in Transit and At Rest
  Implement Error Handling and Logging
  Protect Sensitive Data and Functions
  Protect Database Access

6. Testing Software Security

- Perform Security Testing
  Analyze Code to find Security Problems
  Use Automated Testing Tools to Find Security Problems

7. Maintaining Security in Deployed Software

- Monitor and Log Applications to Support Security
  Maintain Security after Deployment