**1. Planning:**

* **Security Requirements:** Define security requirements alongside functional requirements. Include compliance with standards and regulations.
* **Risk Assessment:** Perform an initial risk assessment to identify potential security threats and vulnerabilities.

**2. Development:**

* **Secure Coding Practices:** Implement coding standards that emphasize security, such as input validation and error handling.
* **Static Code Analysis:** Use tools to automatically check code for security vulnerabilities during development.

**3. Testing:**

* **Penetration Testing:** Simulate attacks to identify vulnerabilities that may not be evident through automated tools.
* **Dynamic Analysis:** Test running applications to find security issues in real-time.

**4. Deployment:**

* **Security Configuration:** Ensure that security configurations are set correctly before deploying the software.
* **Monitoring:** Set up monitoring to detect and respond to security incidents promptly.

**5. Maintenance:**

* **Patch Management:** Regularly update software to fix known vulnerabilities.
* **Incident Response:** Have a plan in place to respond to security incidents effectively.