Sungard AS proposes a Code Review a as a vital step towards the advancement of Your Company's cyber resilience goals by providing organizations with a deep technical security review of a Web application leading to improvement of the overall security of the Web application.

Due to the size of applications in today's modern environment, automatic vulnerability scanning is employed to provide a wide analysis of the code. Although this may lead to many false positives being discovered, it maximizes time spent on discovering known vulnerabilities in the code.

After vulnerability scanning was completed, the Sungard AS tester validated vulnerabilities to filter out false positives. The results were saved to disk to be included in the vulnerability matrix. Risk ratings were assigned to each of the vulnerabilities, along with a business risk, remediation procedure and effort required to remediate.

A manual review is then carried out on the code to provide a deeper dive on certain areas of the code where known high risk vulnerabilities may exist.

This analysis is based upon the OWASP Code Review Methodology and covers the following areas:

- Input validation
- Source code design
- Information leakage and improper error handling
- Direct object reference
- Resource usage
- API usage
- Best practices violation
- Weak Session Management
- Using HTTP GET query strings

The OWASP Secure Code Review Process diagram below illustrates the operational process of analyzing the security of an application. This process and its phases are followed to ensure a logical and comprehensive review is undertaken.