

Source Code Review

The source code of an application is the human programmer's definition of how a system should behave. Unfortunately the human element introduces scope for error, which is commonly seen through well-known security vulnerabilities and conditions such as buffer overflows.

Even the smallest of programs can contain coding errors (sometimes non-obvious) that might lead to conditions enabling undesired behaviour of the running program. As software provides the interface to systems and applications, the possibility of exploitation and manipulation of coding errors to circumvent the security controls of IT systems and networks becomes of great concern. Similarly, the reliability of software is paramount in maintaining business continuity, and organisations cannot afford the downtime that may result from denial of service attacks enabled through inherent coding errors and software bugs.

IRM's Source Code Review service evaluates source code for common programming errors that may result in application compromise, or in the unintended behaviour of systems and processes. The result is comprehensive coverage and assured protection from vulnerabilities during any phase of the application lifecycle.

A complete source code review includes the following phases:

- **Objectives Establishment**

IRM will determine the area of review, depth of audit and timeline depending on requirements specified and realised by the code reviewer and client. The area of review will depend on type of code (technology, platform) and application logic being implemented. At this stage, the security requirements of the application and its intended behaviour will be discussed.

- **Preliminary Scan**

Interesting areas within the code will be identified using automated source code scanning utilities. Potential areas of vulnerability flagged by the code scanning utilities will be further drilled down in subsequent stages.

- **Code Analysis**

Code for each component of the application will be evaluated by deriving various input zones and trust boundaries. Coverage will be ensured by examining vulnerabilities corresponding to application logic and the development platform. Issues flagged by the code scanning utility will also be reviewed.

- **Deliverables**

IRM will deliver a formal report including an executive summary, a risks and recommendations table detailing the high level results of the assessment and a detailed description of each issue discovered including remediation advice.

About IRM

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.