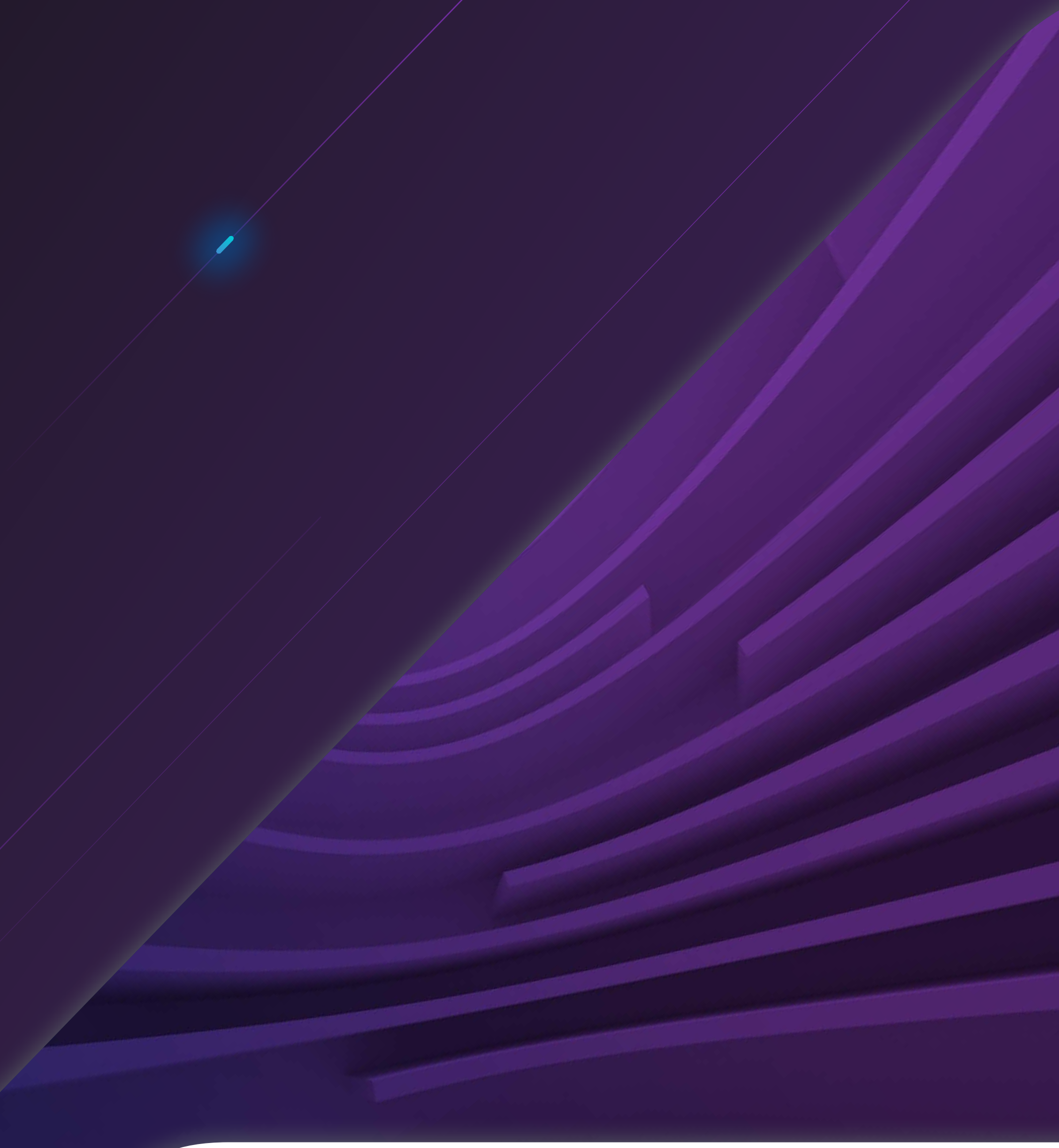
BISHOPFOX

METHODOLOGY

Secure Code Review



Bishop Fox's Secure Code Review methodology identifies code-level vulnerabilities by combining automated and manual testing techniques.

Assessments begin by understanding the architecture performing detailed analysis of the applications underlying construction. Next, the assessment team analyzes the software composition to inventory the open-source components and flag potential issues. The team then performs a static-code analysis by executing an automated review against all customer developed codebases. Finally, the team manually validates the automated findings confirming automated results and identifies issues within critical functionality including security-related components as well as components and functionality related to specific threats identified in a Threat model if this service has also been contracted. The methodology outlined in this document provides a detailed look at the step-by-step process and delineation of responsibilities that are critical to accomplishing predetermined objectives.

Summary of Engagement

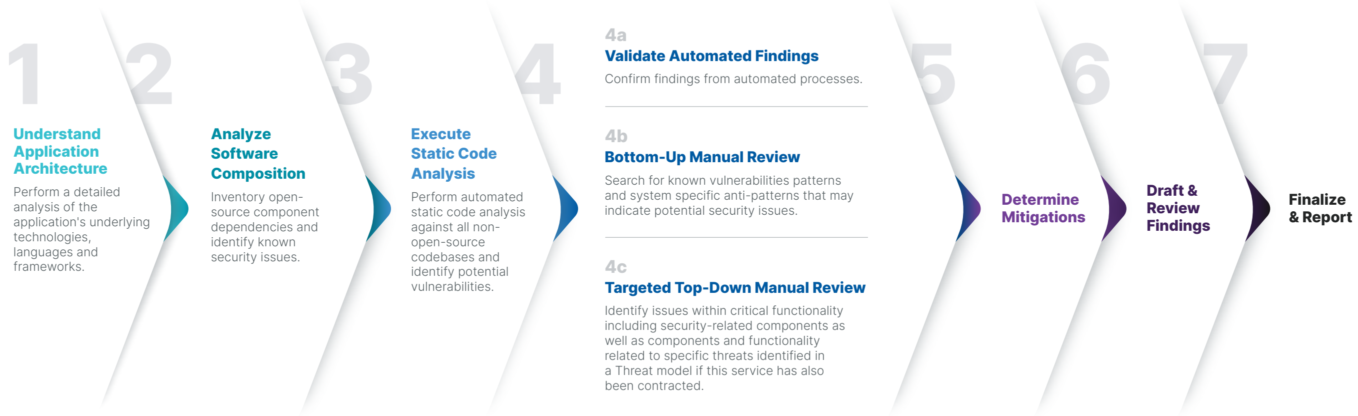
Before the engagement can begin, Bishop Fox's consultants require the codebase for assessment.

Once the codebase has been provided, Bishop Fox's Secure Code Review team can begin the engagement. The team initiates phase one by understanding the application architecture to gather a detailed perspective of the applications' underlying languages, frameworks, and configurations, as well as security-related components such as authentication, access control, user and session management, cryptography, etc. Next, the team can complete analysis of the software composition, inventorying open-source component dependencies to identify known , security issues. Lastly, Phase 1 of the Secure Code Review methodology, Bishop Fox will execute a static code analysis leveraging automated technology against all non-open-source codebases to identify potential vulnerabilities.

Next, the team will then validate the automated static analysis results to confirm vulnerabilities identified, and perform manual analysis of the source code searching for known vulnerability patterns and language- or framework-specific anti-patterns that may indicate security issues. The team then performs a top-down manual code review to identify issues within critical functionality including security-related components as well as components and functionality related to specific threats identified in a Threat Model if this service has also been contracted.

Once Bishop Fox has identified codebase weaknesses, the assessment concludes with a detailed reporting of all security issues discovered within the target codebase alongside comprehensive remediation recommendations and steps. It is important to note that the primary outcome of this engagement is ensuring your security teams understand all Code-base exposures and prioritization of remediation against the likelihood of attack, business impact, and required resource allocation.

High-level Process



1

Understand Application Architecture

Perform a detailed analysis of the application's underlying technologies, languages and frameworks.

2

Analyze Software Composition

Inventory open-source component dependencies and identify known security issues.

3

Execute Static Code Analysis

Perform automated static code analysis against all non-open-source codebases and identify potential vulnerabilities.

4

4a

Validate Automated Findings

Confirm findings from automated processes.

4b

Bottom-Up Manual Review

Search for known vulnerabilities patterns and system specific anti-patterns that may indicate potential security issues.

4c

Targeted Top-Down Manual Review

Identify issues within critical functionality including security-related components as well as components and functionality related to specific threats identified in a Threat model if this service has also been contracted.

5

Determine Mitigations

6

Draft & Review Findings

7

Finalize & Report

Methodology Details

Phase 1: Pre-assessment

The following assessment requirements must be met before the start of fieldwork activities to ensure the timely and successful completion of the project.

Pre-assessment Requirements	
ARCHITECTURE REVIEW	The assessment team requires detailed application information, including but not limited to: • Any available documentation related to the application • Source Code
SOFTWARE COMPOSITION ANALYSIS	The assessment team requires a detailed inventory, such as a Software Bill of Materials (SBOM) specifying the open-source components, libraries, and modules required by the application.
AUTOMATED/ MANUAL CODE REVIEW	The assessment team requires access to the application source code, which may include but is not limited to: • Complete, build-quality application source code • Any related libraries used in the application

	Bishop Fox	Client
Understand application architecture	✓	✓
Provide application information		✓
Provide source code		✓

Phase 2: Comprehensive Manual Code Review

In this phase, automated tools have informed the team of potential risks and vulnerabilities in the code. The team will leverage that information as well as additional techniques to manually confirm and review the findings.

VALIDATE AUTOMATED FINDINGS	Although automated static analysis tools reduce the amount of time required to identify many well known and understood vulnerability patterns in source code, these tools are by nature designed to err on the side of caution and subsequently produce an elevated level of false positives. The assessment team manually reviews all findings to eliminate false positives and uncover any additional findings.
BOTTOM-UP MANUAL REVIEW	Bishop Fox will perform automated and manual searches for known vulnerability patterns and system-specific anti-patterns that may indicate potential security issues in the codebase. The identified candidate points will be analyzed to identify data flows from untrusted input, while examining intermediate code for mitigation measures.
TARGETED TOP-DOWN MANUAL REVIEW	Identity issues in critical functionality including security-related components such as authentication, access control, input validation, encryption/data protection, user and session management, configuration, error handling, and logging. If a Threat Model has been completed, Bishop Fox will perform additional analysis to uncover additional findings from the perspective of the threat model.

	Bishop Fox	Client
Validate automated findings through manual review	✓	
Perform manual techniques to uncover additional codebase weaknesses	✓	
Analyze candidate points to uncover concerning patterns in the codebase	✓	
Manually review critical functionality in the codebase for security flaws	✓	

Phase 3: Analysis & Reporting

Bishop Fox reports contain an executive-level summary of the engagement, which includes the assessment goals, a synthesis of the highest-impact findings, and high-level recommendations. Within each finding, detailed information including identification of the vulnerable code module(s) is provided and the assessment team builds a holistic view of the business risk it represents by performing the following technical analysis activities.

LIKELIHOOD DETERMINATION	For each vulnerability, the assessment team determines the likelihood that it will be exploited based on the following factors: • Threat-source motivation and capability • Nature of the vulnerability • Existence and effectiveness of controls
IMPACT ANALYSIS	For each vulnerability, the assessment team analyzes and determines the impact of successful exploitation as it affects the organization and its customers in the areas of confidentiality, integrity, and availability of systems and data.
SEVERITY DETERMINATION	Bishop Fox determines severity ratings using in-house expertise and industry-standard rating methodologies such as the Open Web Application Security Project (OWASP) and the Common Vulnerability Scoring System (CVSS) to evaluate the likelihood and impact of exploitation. The team weighs those factors to classify the overall severity as critical, high, medium, or low. The severity of each finding is determined independently of the severity of other findings.

	Bishop Fox	Client
Likelihood determination	✓	
Impact analysis	✓	✓
Severity determination	✓	

Appendix

Delineation of Responsibilities	Bishop Fox	Client
Phase 1: Pre-Assessment Requirements		
Understand application architecture	✓	✓
Provide application information		✓
Provide source code		✓
Phase 2: Comprehensive Manual Code Review		
Validate automated findings through manual review	✓	
Perform manual techniques to uncover additional codebase weaknesses	✓	
Analyze candidate points to uncover concerning patterns in the codebase	✓	
Manually review critical functionality in the codebase for security flaws	✓	
Phase 3: Analysis & Reporting		
Likelihood determination	✓	
Impact analysis	✓	✓
Severity determination	✓	