indium

Make Technology Work

S3T
Shared Services Security Testing

White Paper

www.indiumsoftware.com

Introduction

Organizations today are literally borderless and really virtual. These are times where lack of data integrity, breach of information and confidentiality and data leakages can make or break organizations. Companies are not only hurt financially on account of this but also take severe beating in their brand image and investor confidence. The changes in technology – while enabling higher productivity and increased efficiencies – are also being fast out-paced by greater exposure and dangers from the hackers and their methods. Top on the priority list of every IT leader, is the need to ensure that the networks, applications, infrastructure and processes are secure and safe. Further, the need for compliance to regulatory provisions is mandatory and increased audit oversight on information assurance brings information security and data protection to the core of any organization's growth plans.

Business Value of Independent Testing

Primary drivers in any testing engagement are Visibility and Deep-dive analysis to the specific problem area. An Independent testing team provides this value in an extremely effective and efficient manner. Leveraging independent testing firms, clients have the confidence and comfort that their information assurance goals are being implemented by impartial and objective experts using the right mix of tools, standards and processes. Having the expertise of implementing such frameworks across multiple client engagements, Independent testing firms enable cross-pollination of best-fit practices and benchmarking of processes and metrics.

The rigor of a clearly defined and implemented process and guidelines is at the core of ensuring that the enterprise goals of Information Assurance are realized.

SOPs & Templates

Whitepapers

Frameworks and Tools

Checklists

Objective of S3T

To provide assurance to organization that data Confidentiality and Integrity are maintained by testing the IT controls – at pre-defined life cycle stages or periodicity based on client needs.

This objective is realized through the following dimensions:

- **Independent 3rd party view –** focus on objective, un-biased and formal view.
- Unified & Aligned enterprise - wide Information Assurance process integrating into the application development life cycle; aligning the information security objectives/ compliance standards to the overall business objectives.
- **Line of evidence –** document test artifacts and reports.
- **Provide transparency and visibility –** frequent reporting and close monitoring of execution progress.
- Creation of re-usable artifacts and a robust knowledge management process.
- **Optimizing the investments in infrastructure and resources –** leveraging the automation tools, jump start kits for faster time to market. Implementing an offshore based delivery to optimize the total cost of ownership (TCO).

- **Year on year improvements in key metrics –** through continuous improvement and delivery excellence initiatives.

Guideposts of S3T

The central tenets of the S3T framework include:

- **Authentication –** establishing identity – building on you know, you have and you are factors – an important and critical aspect of the security assurance.
- **Authorization –** assign permission and defining levels of access and privileges based on organization specific needs.
- **Auditing –** keeping track of events to ensure non-repudiation. Primarily ensures that the authentication and authorization checks and controls are effective.
- **Confidentiality –** data is protected from unauthorized access – ensuring privacy – both forms of data that is stored in systems and data that is in transmission.
- **Integrity –** content not tampered (unauthorized alteration, modification or deletion) – either in transit or in stored systems.
- **Availability –** remains available and accessible for authorized users. Mitigate Denial of Service attacks.

The 'Shop Floor' Factory Concept

The S3T model is implemented as an integral part of the application/system development life cycle. The S3T implements a toll gate process where the team tests the various compliance and security policies as provided in the mandate.

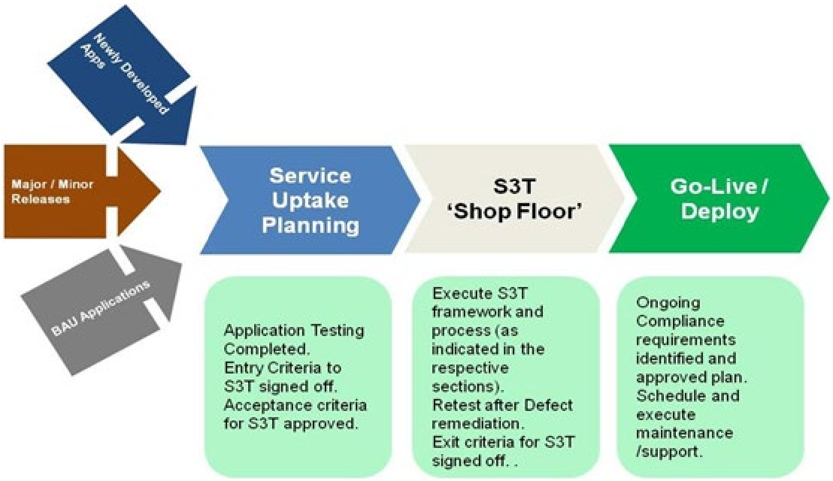
Traditionally, there could be three work streams that could feed into the S3T shop floor:

a) Newly Developed Applications – all new applications that are ready for deployment after completing the system and integration testing – will go through the S3T shop floor for the specific compliance testing.

b) Major and Minor releases – the frequent upgrades/patches are checked for compliance prior to deployment.

c) BAU Applications – all the existing/in-scope applications could be on a periodic basis scanned and tested for compliance parameters. Some clients have used the Gold, Silver and Bronze classification of applications and have different periodicities for compliance testing.

The Security Testing Framework and Process are depicted in the pictures below that enable detailed step-by-step activities towards implementation of the S3T objectives.

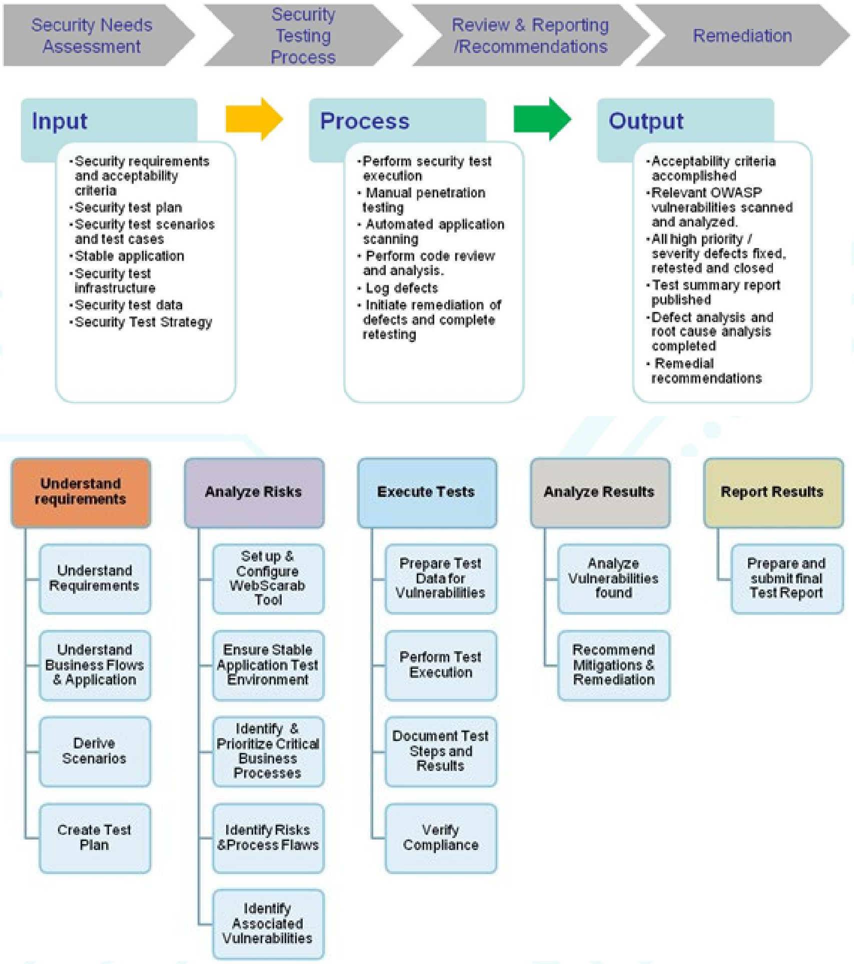


Application Testing Completed.
Entry Criteria to S3T signed off.
Acceptance criteria for S3T approved.

Execute S3T framework and process (as indicated in the respective sections).
Retest after Defect remediation.
Exit criteria for S3T signed off. .

Ongoing Compliance requirements identified and approved plan.
Schedule and execute maintenance /support.

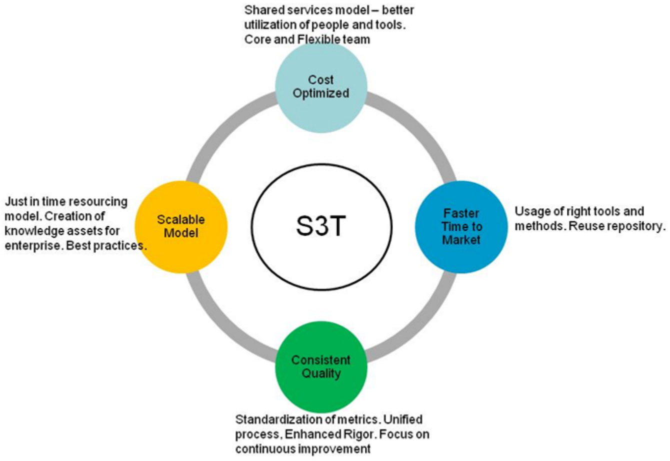
iAVA – Indium's Application Vulnerability Analysis


Security Needs Assessment
Security Testing Process
Review & Reporting /Recommendations
Remediation
Input
•Security requirements and acceptability criteria
•Security test plan
•Security test scenarios and test cases
•Stable application
•Security test infrastructure
•Security test data
•Security Test Strategy
Process
•Perform security test execution
• Manual penetration testing
• Automated application scanning
• Perform code review and analysis.
• Log defects
• Initiate remediation of defects and complete retesting
Output
•Acceptability criteria accomplished
•Relevant OWASP vulnerabilities scanned and analyzed.
•All high priority / severity defects fixed, retested and closed
•Test summary report published
•Defect analysis and root cause analysis completed
• Remedial recommendations
Understand requirements
Understand Requirements
Understand Business Flows & Application
Derive Scenarios
Create Test Plan
Analyze Risks
Set up & Configure WebScarab Tool
Ensure Stable Application Test Environment
Identify & Prioritize Critical Business Processes
Identify Risks &Process Flaws
Identify Associated Vulnerabilities
Execute Tests
Prepare Test Data for Vulnerabilities
Perform Test Execution
Document Test Steps and Results
Verify Compliance
Analyze Results
Analyze Vulnerabilities found
Recommend Mitigations & Remediation
Report Results
Prepare and submit final Test Report

A Shared Services Model

Clients have reaped multiple benefits in a shared services model for implementing specific service lines. Typical benefits of a 'factory-like' shared services model include: Optimized Costs – both from efficient utilization of tools and creating an 'on-demand' resourcing model that is implemented in a core vs. flexible team context.

Time to Market (read Time to Value) – usage of right tools, leveraging different time zones for test life cycles, implementation of re-use to enhance faster time to market are some of the key drivers in a shared services model.


Shared services model – better utilization of people and tools. Core and Flexible team
Cost Optimized
Just in time resourcing model. Creation of knowledge assets for enterprise. Best practices.
Scalable Model
S3T
Faster Time to Market
Usage of right tools and methods. Reuse repository.
Consistent Quality
Standardization of metrics. Unified process. Enhanced Rigor. Focus on continuous improvement

Consistent Quality – the primary advantage of the shared services model stems from the fact that the processes (entry and exit criteria) and project level metrics are standardized that enables enhanced rigor and focus on continuous improvement initiatives.

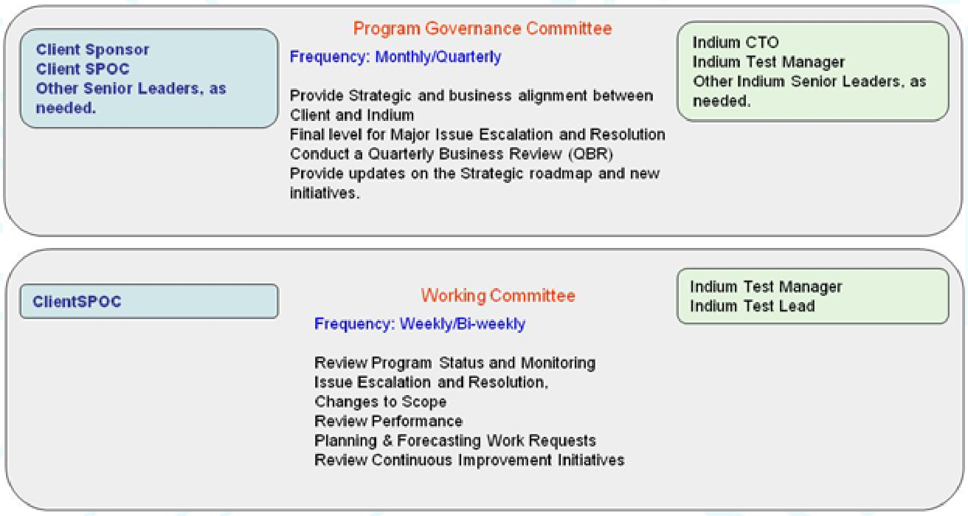
Scalable Model – the shared services model is built on the premise to ensure that the team can be ramped up and down based on the bandwidth needed for executing the service requests. A robust knowledge management and training process ensures such rapid scaling up and down of resources. Specialization and creation of accelerator kits, related to tools, processes and client specific assets is a key lever for scalability.

Program Governance

The figure below indicates the key aspects of Program Governance that is performed at two levels:

- Overall Program level and
- Project level

Respective stakeholders from client and Indium are involved in this to enable a friction-less implementation of the desired objectives.



Client Sponsor
Client SPOC
Other Senior Leaders, as needed.

Program Governance Committee

Frequency: Monthly/Quarterly

Provide Strategic and business alignment between Client and Indium
Final level for Major Issue Escalation and Resolution
Conduct a Quarterly Business Review (QBR)
Provide updates on the Strategic roadmap and new initiatives.

Indium CTO
Indium Test Manager
Other Indium Senior Leaders, as needed.

ClientSPOC

Working Committee

Frequency: Weekly/Bi-weekly

Review Program Status and Monitoring
Issue Escalation and Resolution,
Changes to Scope
Review Performance
Planning & Forecasting Work Requests
Review Continuous Improvement Initiatives

Indium Test Manager
Indium Test Lead

Indium offers this comprehensive S3T framework with the following accelerators:

- Jump Start Kit – with process, checklist, expertise and experience
- Life Cycle Integration approach and recommendations
- Flexibility of leveraging commercial (HP Mercury, IBM Rational et al) and Open Source tools
- Focus on re-use and year on year productivity improvements
- Training of business analysts and developers

☎

INDIA

Chennai | Bengaluru | Mumbai
Toll-free: 1800-123-1191

USA

Cupertino | Princeton | Boston
Toll-free: +1 888 207 5969

UK

London

SINGAPORE

+65 9630 7959

MALAYSIA

Kuala Lumpur
+60 (3) 2298 8465

🌐

Sales Inquiries
sales@indiumsoftware.com

General Inquiries
info@indiumsoftware.com