



# Let's get to the future, faster. **Together.**

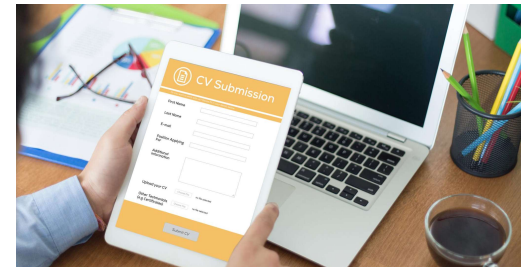
**Prepared for:** Application Security  
As a Service



# Assessment as a Service

## Introduction

Assessment as a Service is a comprehensive package offered by LTIMindtree, designed to help organizations efficiently and flexibly conduct technical assessments. This service enables enterprises to evaluate the costs, benefits, and impacts of various initiatives at the organizational level.



## What is it?

### Conduct Assessments

Assessment as a Service is a solution that enables organizations to perform assessments with ease. This feature offers flexibility and convenience to both assessors and participants, allowing assessments to be taken from any location at any time.

### Flexible and Efficient Way to Conduct Assessments

Assessment as a Service provides a flexible and efficient method for organizations to conduct assessments. This service simplifies the scheduling process for organizations and facilitates a seamless experience for participants, resulting in a streamlined and effective assessment process.



# Benefits of Assessment as a Service

## ● Increased Efficiency

Assessment as a Service enables remote assessments, saving time and money associated with scheduling and administering them. It also provides instant feedback and results, reducing the time required for grading and evaluation.

## ● Flexibility

Assessment as a Service offers organizations the flexibility to conduct assessments anytime and anywhere. This makes it easier for organizations to schedule assessments and for participants to take them.

## ● Scalability

Assessment as a Service allows organizations to scale assessments up or down based on their needs, facilitating efficient management of assessment resources.

## ● Improved User Experience

This service allows participants to take assessments from anywhere, making it more convenient and accessible.

This results in a better user experience and higher engagement. Additionally, it provides instant results and feedback, helping participants understand their strengths and weaknesses and offering opportunities for improvement.






# Objectives & Scope

The key objective is to assess customer's

- Current application security posture leveraging risk-based approach
- DevSecOps maturity assessment for in scope applications

Mapped to applicable standards and frameworks including OWASP, SANS, PCI-DSS, HIPAA and other industry practices

Key Activities:	Understanding of Application Landscape	Maturity Assessment	Recommendation
<ol style="list-style-type: none"> <li>1. Review existing security assessment activities for in-scope apps aligned with processes, tools &amp; technologies, and industry frameworks.</li> <li>2. Conduct DevSecOps Maturity assessment for the applications</li> <li>3. Identify potential gaps, associated risks to arrive at a risk score and current DevSecOps maturity level</li> <li>4. Provide recommendations for achieving target maturity state, actionable insights for application security posture enhancement</li> </ol>	 <ul style="list-style-type: none"> <li>• Identify the master application inventory along with criticality levels and type of apps (web, mobile, API, container)</li> <li>• Identify application security assessment activities</li> <li>• Access to current documentation in terms of process, policies, procedures, standards, security audit / VM reports, guidelines and architecture as applicable for in-scope apps</li> <li>• Define Secure SDLC framework</li> </ul>	 <ul style="list-style-type: none"> <li>• Perform DevSecOps maturity assessment to identify current As-Is state for in-scope apps</li> <li>• Review and Assess previous Security Audit / Compliance Reports / Other security Reports</li> <li>• Define desired maturity level as per organizational goals</li> <li>• Develop operating model to bridge the gap between the current state and the envisioned maturity level</li> </ul>	 <ul style="list-style-type: none"> <li>• Identify, organize, and prioritize actions for managing and addressing the gaps</li> <li>• Actionable Recommendations aligned with security control framework for             <ul style="list-style-type: none"> <li>– Target DevSecOps maturity state with short term and long terms goals</li> <li>– Risk treatment plan and remediation roadmap</li> </ul> </li> <li>• Final Recommendation Report</li> </ul>

# Assessment Methodology

	<b>Stakeholder Interviews</b>	Involves gathering data for threat analysis, risk assessment and metrics collection
	<b>Build and Deployment</b>	Focuses on security practices in the CI/CD pipeline and deployment processes
	<b>Implementation</b>	Covers secure coding and infrastructure hardening practices
	<b>Culture and Organization</b>	Addresses organizational culture, education, and processes that support security initiatives
	<b>Test and Verification</b>	Focuses on testing practices to validate security measures and ensure continuous improvement
	<b>Existing Security Reports</b>	Analysis of existing security reports including code review, penetration testing etc.

# Key Components & Frameworks for Assessment

## Application Security

### Application Security Requirements:

- Identify relevant industry regulations and compliance standards
- Assess the customer's current application security posture.

### DevSecOps Adoption:

- Evaluate the existence and enforcement of security activities integrated in CI/CD pipelines
- Identify any gaps or areas for improvement.

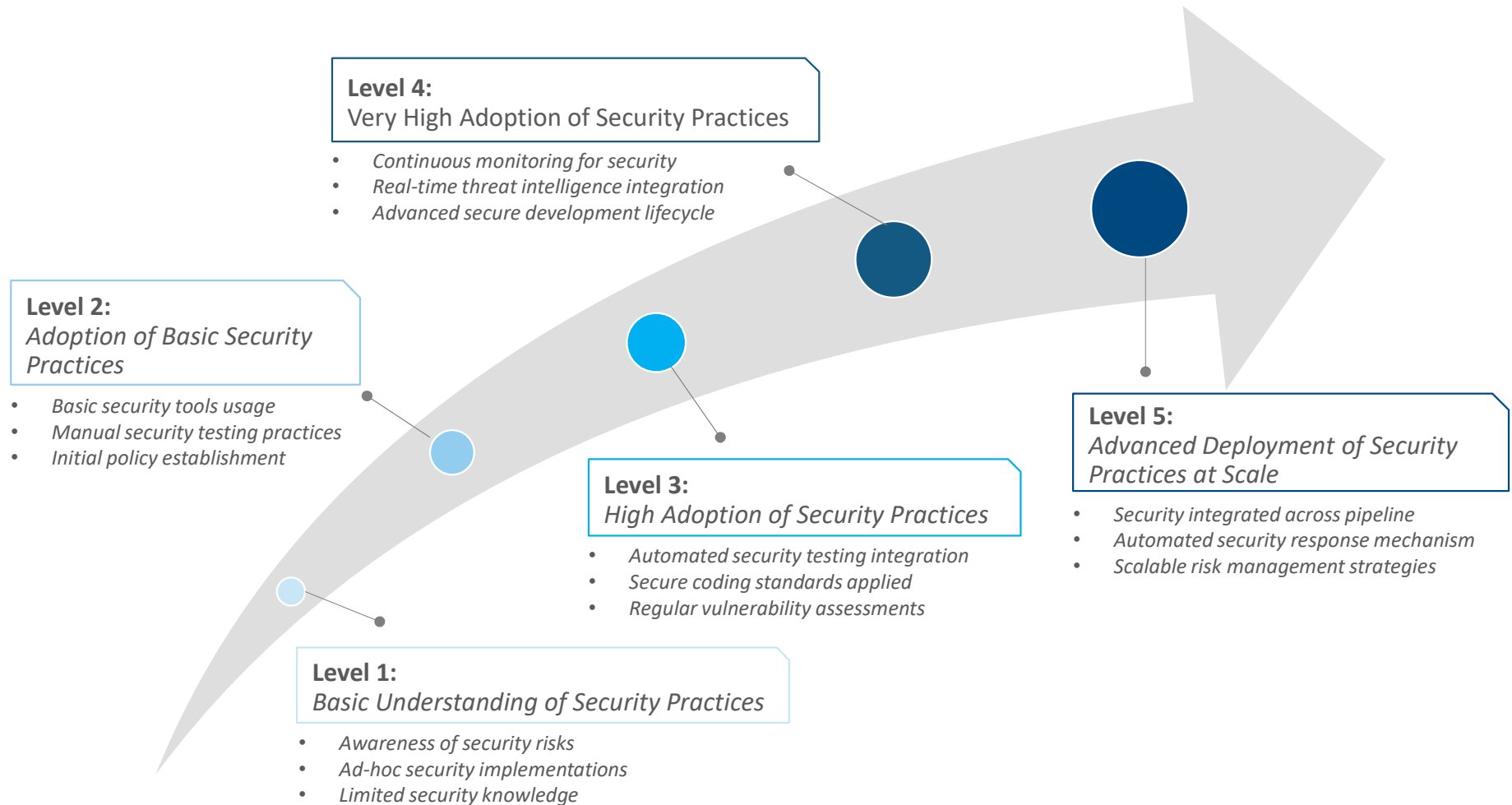
### Assessment and Reporting:

- Assess the customer's ability to track user activity and generate audit reports.
- Identify any gaps in application security assessment activities

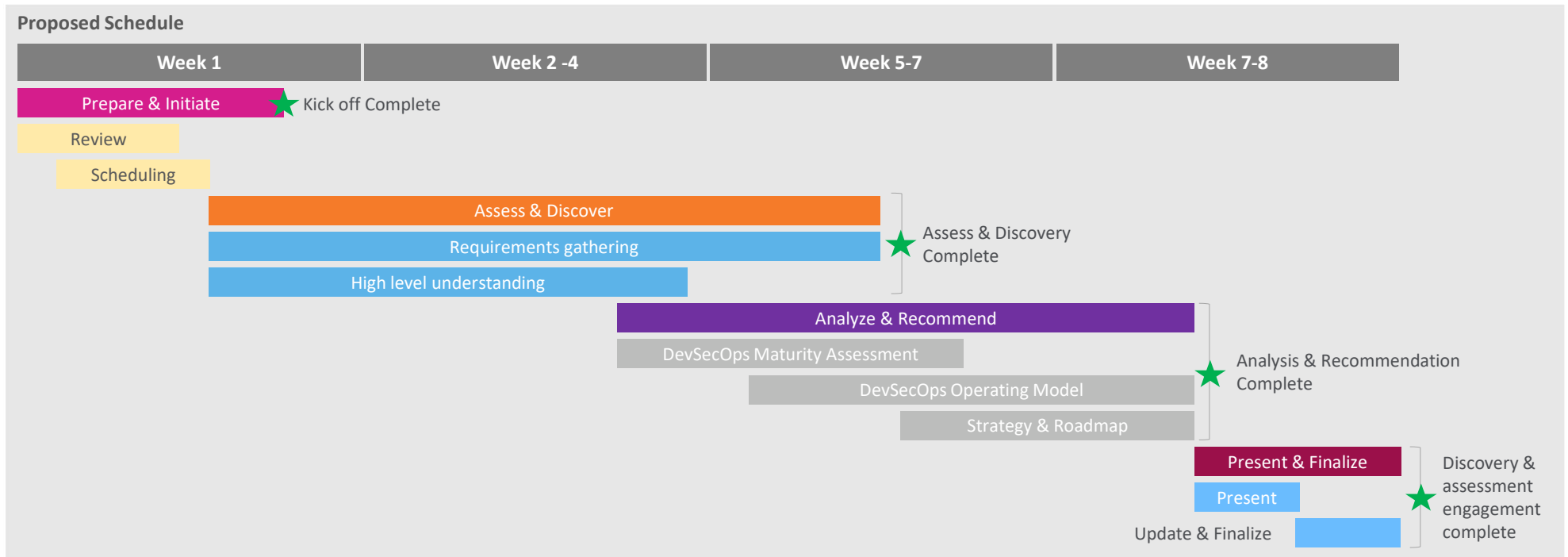
## Accelerator Frameworks

- DevSecOps Maturity Assessment Questionnaires
- DevSecOps Operating Model
- OWASP DevSecOps Maturity Model (DSOMM)

# Leveraging OWASP DevSecOps Maturity Model (DSOMM)



# Assessment Plan on a Page (Indicative)



## Deliverables

### Assessment Report:

- A detailed document outlining our findings, gaps, and recommendations.

### Roadmap for Implementation with a plan:

- Recommend specific solutions to address the identified gaps
- High-level plan with effort estimation, cost analysis, target operating model with business impact analysis.
- Risks, Assumptions, Issues, and Dependencies with a mitigation plan.
- DevSecOps maturity roadmap



## Pricing Model



Options for fixed-price assessments or hourly consulting rates.



Potential for subscription-based support for ongoing assessments.



Microsoft and LTIM joint collaboration

Contact us for more details.

Let's get to the future, faster, Together

Thank you