



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

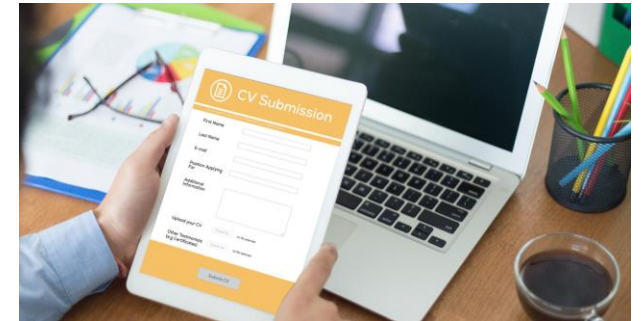
**Prepared for:** Azure Cloud Compliance  
Assessment As a Service



# 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 Azure Cloud compliance / security posture leveraging risk-based approach

Mapped to applicable standards and frameworks including CSA CCM, CIS, ISO 27001, NIST CSF and industry best practices

## Assessment Scope

- Review existing security controls as mapped to Azure Cloud environment aligned with processes, tools & technologies, and governance frameworks.

## Assessment of Existing Environment

- **Gap Analysis-** Identify potential compliance gaps, associated risks to arrive at a risk score and current cyber security maturity score
- **Recommendation** - Provide recommendations for achieving target state, actionable insights for compliance posture enhancement and risk remediation

## Understanding Existing Cloud Environment



- Define in scope environment
- Define in scope controls aligned mapped to applicable control framework and compliance requirements
- Access to current documentation in terms of process, policies, procedures and standards, security audit / VM reports, asset inventory, network design and architecture as applicable to the scope of controls
- Define Risk Modeling Matrix
- Define Cybersecurity Maturity Framework

## Gap Analysis



- Understanding of current As – IS state for in scope controls and assets mapped
- Review and Assess previous Security Audit / Compliance Reports / Other security Reports
- Compare current controls implementation state viz-a-viz security framework and conduct gap analysis and identify gaps along with associated risks.
- Consolidated Risk score as well as mapped to control domains







## Recommendation



- Identify, organize, and prioritize actions for managing and addressing cybersecurity risk
- Actionable Recommendations aligned with security control framework for
  - Short term and long terms goals
  - Risk treatment plan and remediation roadmap
- Final Recommendation Report



# Assessment Methodology

	<b>Stakeholder Interviews</b>	Gather insights from key personnel to understand the operational context.
	<b>Policy Review</b>	Evaluate current access policies, role definitions, and governance frameworks.
	<b>Technology Audit</b>	Reference specific Technology requirements and assess the same
	<b>Control Framework Mapping</b>	Identify and map specific control framework standards for the assessment
	<b>Documentation Review</b>	Review of existing Process, Procedures and Standards documentation and configurations
	<b>Existing Security Reports</b>	Analysis of existing security reports including penetration testing etc.

# Key Components & Frameworks for Assessment

## Governance and Compliance

### Compliance Requirements:

- Identify relevant industry regulations and compliance standards
- Assess the customer's current Azure cloud compliance posture.
- Reference Control Framework under consideration
- Reference to UCF Framework as required

### Governance Policies:

- Evaluate the existence and enforcement of governance policies for data access, retention, and privacy.
- Identify any gaps or areas for improvement.

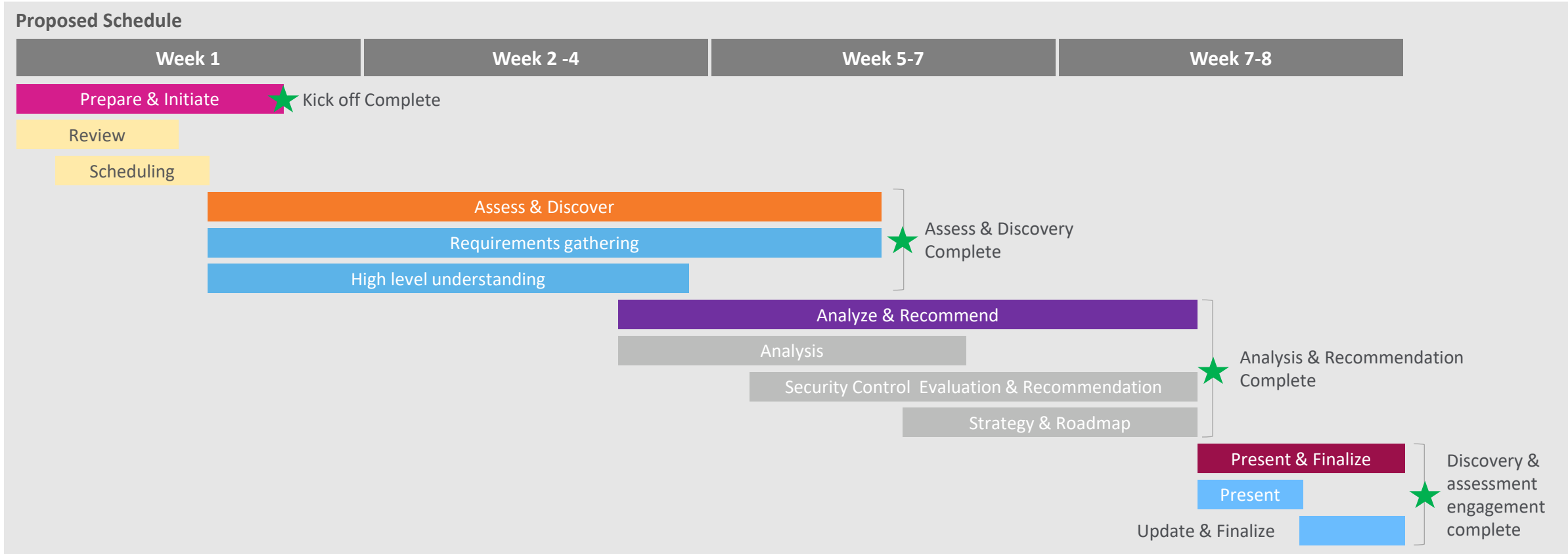
### Assessment and Reporting:

- Assess the customer's ability to track user activity and generate audit reports.
- Identify any gaps in logging or monitoring capabilities

## Accelerator Frameworks

- Framework to Control Mapping based Assessment Questionnaire
- Unified Compliance Framework for Compliance Posture Analysis
- Risk Modeling Framework

# Assessment Plan on a Page (Indicative)



## Deliverables

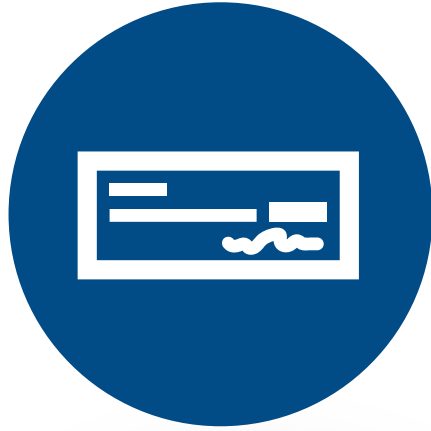
### Assessment Report:

- 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.
- Cybersecurity maturity roadmap

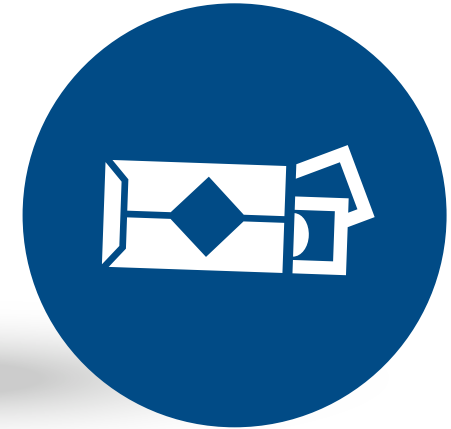
# Pricing Model



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