# AWS FTR (Foundational Technical Review) 2023 for

vaultastic

## Contents



## Background

Mithi delivers its products as SaaS services from the AWS cloud platform. To keep these services secure, reliable, and your data safe, Mithi integrates and leverages many AWS services in the cloud.

Besides this, Mithi also has stringent processes to onboard new members to the cloud team., secure access to the cloud resources, review the audit logs, scan for vulnerabilities, and more.

To benefit all our customers and put them at ease about the safety and security of the cloud, Mithi, in collaboration with AWS, has completed an independent foundational technical review of the cloud platform and processes, which covers various aspects of cloud security, availability, and performance.

## About AWS FTR

The AWS Foundational Technical Review (FTR) enables us to identify and remediate our software or solutions risks. The FTR helps you identify AWS Well-Architected best practices for our software or solution.

This document outlines the scope of the audit and the process followed to receive our logo from AWS.

## The Validation

The successful FTR audit done in September 2023 has earned Mithi this logo.


## The Scope

The FTR audit focuses on aligning our solution with a specific set of AWS best practices around security, performance, and operational processes that are most critical for customer success. This audit does not cover additional initiatives from the partner (Mithi) to ensure security, such as periodic VAPT audits by certified auditors.

### Access to the AWS resources

This point covered the access security related to the AWS account carrying the cloud resources composing our platform. The best practices include using only IAM accounts with MFA for accessing this account and creating an SOP/runbook to handle any exceptions here

### Communication from AWS

Here, we reviewed and ensured that there were separate, redundant contacts aligned to each line of communication regarding the events/alerts in the cloud infrastructure. This contact assignment ensures accurate and quick remediation of any alert, even if some team members are absent.

### Audit logging

Here, the review ensured the use of the cloud audit logging tool to enable governance, compliance, operational auditing, and risk auditing of our AWS account. These management events enable cross-region, cross-accounts, and the logs centrally collated into secure, IAM-controlled storage in a separate AWS account. The log protection makes it computationally infeasible to modify, delete, or forge CloudTrail log files without detection.

### Identity and Access Management

IAM is one of the most critical aspects of the FTR. Here, the review ensures adherence to the best practices of creating identities and access rights for working with the AWS resources. These include but are not limited to separate identities for each human, MFA, strong password policies with frequent rotation, automatic disabling of unused accounts, least privilege access, and more.

### High Availability

This part of the audit stressed automatic backups of the databases, compute instances, storage volumes, and cloud storage to recover from administrative, logical, or physical error scenarios. The audit also ensured that backups were integral and a process to test data restoration periodically to help meet our RTO objectives.

The disaster recovery portion of the audit reviewed our definition of RPO RTO and ensured that we could meet these requirements by performing an actual DR drill. The FTR required us to test failover to DR to ensure that RTO and RPO are met periodically and after significant updates. The DR test must include accidental data loss, instance, and Availability Zone (AZ) failures. We complied successfully.


### Sensitive data and access to the elastic cloud store

This cloud storage resource carries high-volume business-critical email data. The FTR audit focused on ensuring appropriate access levels and automatically monitoring these rights with defined alerts to ensure the buckets remain secure.

The FTR also stresses segregating sensitive data such as PII or PHI, and business-critical email information and ensuring clear policies to store these securely. The audit verifies that encryption protects sensitive information at rest and in transit.

Any access to the sensitive data in the cloud stores is logged comprehensively throughout the system. Implementing application- and resource-level auditing and logging to monitor all access to data and quickly identify unauthorized access.

## The Audit process:

The FTR audit process starts with a self-assessment checklist shared with the assigned AWS solution architect (SA - expert). The SA reviews the self-assessment and prepares responses or remediation requests.

The self-assessment is followed by a deep dive joint call with the AWS expert and our team comprising the CISO, the cloud infrastructure, and the operational people. During this meeting, the expert reviews each point in the expansive FTR framework to verify that the partner (Mithi) adheres to the guidelines.

The expert highlights gaps and expects the partner to remediate these within the specific timelines.

Only when the expert is satisfied will the partner receive the FTR logo.

This process repeats after 12 months.

*Document Revision:*

| | |
|---|---|
| *Created on* | *6th Dec 2021* |
| *Last Modified* | *6th Oct 2023* |