# Azure Assessment

CASE STUDY

**PARTNER: Xoriant Corporation**

**WEB SITE**: www.xoriant.com

**LOCATION**: Sunnyvale, California

**ORG SIZE**: 4000+ employees

**PARTNER PROFILE**:

Xoriant is a trusted global security services partner focused on Enterprise clients in Financial Services, Healthcare and Manufacturing. With 20 years in business, 4000+ employees and $220M+ in revenue we bring proven experience, mature processes and measurable outcomes to each engagement.

Microsoft | Go-To-Market Services

# Xoriant Advanced Security Assessment for an Enterprise Transportation Company

## SITUATION

- The Client, one of the leading government undertakings for postal and high-speed railway services, wanted to get an independent security assessment for the Azure environment to comply with the ISO27001:2013 certification audit
- As part of the assessment, they wanted to review the customer's Azure architecture and implementation in accordance with Microsoft's Azure recommended security best practices and patterns

## SOLUTION

Xoriant helped the customer to identify the security gaps in their Azure environment and provided a mitigation plan based on Microsoft's Azure recommended security best practices.

Assessment performed based on these parameters:

- Review the customer's Azure architecture and implementation
- Security Roles, Access Controls, Policies & Recommendations
- Azure network security & network controls
- Virtual Machine vulnerabilities assessment using Azure Security Center
- Data Security, Data Collection & Storage
- Azure Identity Management and access control
- Azure database Security & Security Monitoring

## BENEFITS

- Xoriant team performed an independent and thorough review of client's environment, identified various security risks associated with areas of non-compliance, and recommended mitigations to reduce risks.
- After mitigating risks based on mitigation plan, client was found to be compliant with all the controls as per their SOA for the ISO27001 external audit; this resulted in increased operational efficiency and huge profits for end customers in terms of productivity gain, reduced turnaround time, reduced risks, more secured data, and fewer network failures.