



SMBCTEX-003 – Expert Design Review

Project Title: IX-RD-PS-Infinity-01 Migración y modernización infraestructura Infinity

Document Title: Expert Design Review

Document Code: SMBCTEX-003

Version: 1.0

Date: June 3, 2025

Prepared by: Intcomex Cloud

Reviewed by: Julio Diaz

1. Purpose of Review

This document presents an expert technical review of the cloud solution architecture and deployment for Infinity Gifts Souvenirs. The evaluation focuses on alignment with AWS best practices across the five pillars of the AWS Well-Architected Framework: **Operational Excellence**, **Security**, **Reliability**, **Performance Efficiency**, and **Cost Optimization**.

2. Summary of Findings

Category	Review Result	Summary Comment
Operational Excellence	Meets Best Practices	Monitoring, runbooks, and automation in place.
Security	Meets Best Practices	IAM, encryption, logging, and root security enforced.
Reliability	Acceptable with Caveats	Single-AZ limits high availability.
Performance Efficiency	Meets Best Practices	Right-sized resources and scalable components used.
Cost Optimization	Meets Best Practices	Cost models used; lean infrastructure setup.

3. Detailed Review

3.1 Operational Excellence

- **Strengths:**
 - CloudWatch is used for proactive alerting (CPU, RAM, disk).
 - CloudTrail logs are active across regions.
 - Sessions held with client for training and knowledge transfer.

- Use of QA/test environments for validation and release testing.

- **Recommendations:**

- Implement versioned runbooks for maintenance and incident response.
- Introduce automation for patch application, not just scanning.

3.2 Security

- **Strengths:**

- IAM roles follow the least privilege model.
- Root user access is protected by MFA.
- SSL/TLS configured via AWS Certificate Manager.
- IAM policies segregate admin/dev/test access effectively.

- **Recommendations:**

- Enable AWS Config for deeper compliance and audit trail tracking.
- Rotate IAM credentials regularly (automated reminders or tooling).

3.3 Reliability

- **Strengths:**

- Automated backups via AWS Backup with defined RTO (2h) and RPO (24h).
- DR strategy exists and is aligned with the client's needs.
- Infrastructure is provisioned via Terraform, ensuring consistent redeployment.

- **Concerns:**

- The use of **a single Availability Zone** limits fault tolerance and high availability.
- No mention of multi-region replication or cross-AZ failover.

- **Recommendations:**

- Consider a Multi-AZ deployment for RDS and EC2 if SLA or customer demand increases.
- Document incident response procedures in the event of AZ outages.

3.4 Performance Efficiency

- **Strengths:**

- EC2 and RDS instance types are appropriate for workload size (t3.medium).



- CloudWatch metrics used to guide resource sizing.
- Application layer uses IIS with appropriate EBS backing volumes.
- **Recommendations:**
 - Evaluate use of Auto Scaling Groups (ASGs) for web tier redundancy if traffic increases.
 - Consider Amazon CloudFront if public-facing web access expands.

3.5 Cost Optimization

- **Strengths:**
 - AWS Pricing Calculator used to model TCO before deployment.
 - Deployment strategy (single AZ, minimal instances) meets budget constraints.
 - Terraform enables consistent decommissioning of unused resources.
- **Recommendations:**
 - Implement budget alerts via AWS Budgets.
 - Review Reserved Instances or Savings Plans based on usage after 3–6 months.

4. Compliance Alignment

- IAM roles and password policies align with AWS and client requirements.
- Logging (CloudTrail, CloudWatch) supports security audits.
- Data encryption at rest and in transit is enforced using AWS-managed keys.
- Backup and DR planning is well-documented.

5. Risks & Mitigation Strategies

Risk	Impact	Mitigation
Single-AZ Failure	High	Evaluate cost-benefit of Multi-AZ deployments
Manual Patch Deployment Delay	Medium	Automate patch installation after scan approval
No Config or Conformance Packs	Medium	Deploy AWS Config for deeper compliance checks

6. Final Verdict

The solution for Infinity Gifts Souvenirs has been **well-architected and meets the necessary operational, security, and cost-efficiency requirements** for its current scale and needs. The use of Terraform, IAM, encryption, and CloudWatch ensures the environment is manageable and secure. However, to prepare for future growth and risk reduction, **multi-AZ failover and automation of routine tasks** should be planned.

7. Reviewer's Notes

- **Overall Readiness for Production:** Yes
- **Recommended Improvements Priority:** Moderate (non-blocking)
- **Re-review Suggested:** In 6–12 months post go-live or after significant scale change