FTR Self-Assessment: Guided Breakdown of Key Focus Areas

Use this guide to better understand what AWS looks for during the **Foundational Technical Review (FTR)**. These four pillars—**Security, Resilience, Performance, and Supportability**—are essential to passing the review and maintaining customer trust.

---

1. Security

Goal: Ensure your solution protects customer data and is built using secure AWS best practices.

Key Questions:

- Are IAM roles and permissions scoped to least privilege?
- Is customer data encrypted at rest and in transit?
- Are secrets (API keys, credentials) managed using AWS Secrets Manager or equivalent?
- Are security groups configured to restrict access appropriately?

What AWS Wants:
Secure-by-design architecture using built-in AWS services like KMS, IAM, WAF, and GuardDuty.

---

2. Resilience

Goal: Ensure your solution is fault-tolerant and can recover from failure scenarios.

Key Questions:

- Do you use multiple Availability Zones or Regions?
- Is auto-scaling or failover configured?
- Do you have backup and restore mechanisms in place?
- Are health checks used with load balancers or managed services?

What AWS Wants:
High availability with clear disaster recovery (DR) planning and automated recovery options.

---

3. Performance

Goal: Deliver a solution that meets SLAs under variable workloads.

Key Questions:

- Are services appropriately sized (compute, memory, storage)?
- Are you using monitoring tools like Amazon CloudWatch or X-Ray?
- Do you implement caching where necessary (e.g., ElastiCache, CloudFront)?
- Is your architecture optimized to minimize latency?

What AWS Wants:
A well-architected, scalable solution that performs efficiently as usage grows.

---

4. Supportability

Goal: Ensure your team can monitor, troubleshoot, and support the solution effectively.

Key Questions:

- Do you have logging and alerting in place?
- Are logs centralized (e.g., CloudWatch Logs, OpenSearch)?
- Is there a documented escalation process or support plan?
- Do you track SLAs and SLOs?

What AWS Wants:
Clear operational visibility with active monitoring and customer support capabilities.

Tips for Completing the FTR Self-Assessment Thoroughly and Accurately

Completing the **FTR self-assessment** is your first step to passing the full review. Use these best practices to ensure accuracy, reduce friction, and show your team is ready for co-sell alignment.

---

1. Assign a Technical Owner

Designate someone who deeply understands your product's architecture and AWS usage to lead the assessment. This is not a task for a generalist.

---

2. Treat It Like an Audit

Don't just check boxes—provide evidence. Link to architecture diagrams, security policies, Terraform scripts, and monitoring screenshots to prove each control is in place.

---

3. Use the AWS Well-Architected Framework

Align each answer with one of the five Well-Architected pillars (especially Security, Reliability, and Operational Excellence). AWS reviewers love to see this.

---

4. Use Native AWS Services Where Possible

Leverage AWS-native tools like IAM, CloudTrail, CloudWatch, and KMS. It simplifies your explanation and builds trust in your architecture.

---

5. Be Honest About Gaps

If you're working on a feature (e.g., DR plan in progress), note that honestly and explain your timeline. AWS is supportive when there's a plan in place.

---

6. Centralize Your Responses

Create a central document or knowledge base that includes:

- Self-assessment answers
- Links to relevant documentation or dashboards
- Screenshots or proof-of-concept material

---

7. Review Internally Before Submitting

Have a second technical stakeholder review your submission for completeness and clarity. A fresh set of eyes can catch assumptions or vague answers.