

# Post-M&A Security Integration Plan - 90-Day Roadmap

## Objective

This document presents a 90-day roadmap for post-merger security and compliance integration. It is based on best practices applied during the integration of a major Caribbean beverage operation into an existing corporate structure. The goal is to rapidly align both organizations under a unified security governance model while minimizing operational risk.

## Phase 1: Initial Assessment (Days 1-30)

- Conduct full security posture review of acquired entity.
- Map existing policies, standards, and procedures.
- Perform gap analysis against ISO 27001, NIST CSF, and corporate standards.
- Identify high-risk vulnerabilities requiring immediate attention.
- Establish communication and reporting lines with key stakeholders.

## Phase 2: Rapid Mitigation (Days 31-60)

- Implement quick-win security measures for critical gaps.
- Deploy endpoint protection, MFA, and enhanced logging.
- Align incident response procedures across entities.
- Begin integration of compliance reporting tools.
- Initiate training sessions for security awareness.

## Phase 3: Process Integration (Days 61-90)

- Standardize governance documentation and approval processes.
- Integrate access control systems and IAM.
- Consolidate vendor security assessment processes.
- Align disaster recovery and business continuity plans.
- Finalize merged Common Controls Framework (CCF).

## Expected Outcomes

- Unified governance, risk, and compliance (GRC) structure.
- Reduced security vulnerabilities.
- Aligned security culture and awareness.
- Compliance readiness for regulatory and audit requirements.
- Long-term resilience and operational continuity.