# Business Continuity & Security Playbooks

## Status: Planned - Q1 2026

**Expected Duration:** 5-7 weeks  
**Target Audience:** Organizations requiring formal incident response capabilities  
**Prerequisites:** Security Roadmap Workshop or equivalent strategic planning

## Purpose & Problem Solved

Many organizations lack structured incident response procedures and disaster recovery plans that integrate security considerations with business continuity requirements. When security incidents occur, response is often ad-hoc, leading to extended downtime, compliance violations, and ineffective remediation.

This engagement develops comprehensive playbooks that integrate security incident response with business continuity planning, ensuring coordinated and effective response to various threat scenarios.

## Expected Deliverables

* Security incident response playbooks for common threat scenarios
* Business continuity procedures with security integration points
* Crisis communication templates for security incidents
* Disaster recovery testing framework with security validation
* Roles and responsibilities matrix for incident response teams
* Evidence preservation and forensic readiness procedures
* Post-incident review and improvement processes
* Integration with existing business continuity and IT service management

## Integration with E2 Portfolio

**Natural Progressions:** - Security Roadmap Workshop → Business Continuity & Security Playbooks (implements strategic preparedness) - Security Architecture Review → Business Continuity & Security Playbooks (addresses resilience recommendations) - Essential Eight → Business Continuity & Security Playbooks (backup and recovery maturity) - Business Continuity & Security Playbooks → Advanced Security Operations (future module)

**Complementary Services:** - Advanced Threat Detection (future module) - Security Metrics and Reporting (future module)

## Key Focus Areas

* **Incident Response:** Structured procedures for security event management
* **Business Integration:** Aligning security response with business continuity requirements
* **Communication Management:** Coordinated messaging during security incidents
* **Evidence Handling:** Forensic readiness and legal compliance during incidents
* **Recovery Validation:** Ensuring security integrity during disaster recovery
* **Continuous Improvement:** Learning from incidents to enhance preparedness

## Express Early Interest

Contact Engage Squared to participate in early requirements gathering and scenario planning.

**Contact:** E2 Security Operations Practice  
**Requirements Gathering:** Customer workshops planned for Q3 2025