Organization: _____ **Calendar Year:** 202___ **Program Owner:** _____ **Executive Sponsor:** _____

TOOL 1: ANNUAL EXERCISE CALENDAR BUILDER (SELECTION, SEQUENCING & OUTCOMES)

Balance exercises across critical business functions, vary scenario types, sequence to build on lessons learned, and avoid operational surge periods.

Ex ID	Target Function / Unit	Target Audience	Target Date	Scenario & Threat Type	Exercise Type	Expected Capability Outcome
EX-01	Customer Payments & Settlement	Payment Ops, Treasury, IT Ops	Q1 • Feb 18	Core Payment Gateway Cloud Outage	Functional Simulation	Validate manual settlement workaround within 4-hour RTO; verify queue integrity.
EX-02	Supply Chain & Logistics Hub	Procurement, Logistics, Warehouse	Q2 • May 12	Tier-1 Distribution Center Fire / Loss	Tabletop Walkthrough	Activate secondary 3PL routing; confirm stock allocation priority rules.
EX-03	Enterprise IT & Core Infrastructure	SecOps, Network Ops, SysAdmins	Q3 • Aug 20	Ransomware Encryption Incident	Technical Failover & DR	Restore air-gapped immutable backup; achieve data integrity within 8h RPO.
EX-04	Executive Crisis Management	C-Suite, Legal, Media, HR	Q4 • Nov 10	Multi-Site Disruption & Media Leak	Full-Scale Simulation	Test executive decision thresholds, public comms release, and regulatory disclosure.
EX-05						
EX-06						
EX-07						
EX-08						

CALENDAR DISTRIBUTION, SEASONAL BUFFERS & STAKEHOLDER COORDINATION

Coordination Factor	Analysis & Organizational Constraints	Calendar Implementation Rule
Testing Cadence by Function	Risk assessments and regulatory mandates dictate minimum testing intervals for critical vs secondary functions.	Critical tier: Min 1x annually; High risk: 2x annually; Supporting functions: 1x per 24 months.
Seasonal & Cycle Buffers	Peak commercial volumes, quarterly financial closings, customer freezes, and major product launches.	Black out Q4 holiday peak (retail), month-end close (finance), or planned major code releases.
Stakeholder Consultation	Advance review by Business Units, IT, Corporate Comms, Legal, and Compliance to secure operational buy-in.	Circulate draft calendar 60 days prior; lock dates with Steering Committee approval.
Change Trigger Integration	Implementation of new technology, core vendor migration, restructuring, or facility consolidation.	Schedule ad-hoc validation within 90 days of major system or operating model go-live.

TOOL 2: EXERCISE SELECTION & RISK TARGETING WORKSHEET

Ground annual exercise selection in risk assessments, business impact analyses, recent disruptions, and vulnerability analyses to ensure maximum organizational value.

Target ID	Critical Business Function	Risk Driver / Threat Vector	Targeting Rationale	Vulnerability / Gap	Proposed Exercise Scenario	Priority	Cal Qtr
TR-01	Customer Digital Banking App	Cloud hosting regional outage; DNS poisoning	High-Impact / High-Prob	Automated failover unproven since Q2 redesign	Simulated primary cloud region cutoff; measure DNS cutover speed	**P1 - High**	Q1
TR-02	Inbound Raw Material Receiving	Sole-source overseas vendor insolvency	Emerging Threat / SPOF	Single Tier-1 supplier delivers 60% of critical component	Tabletop: Vendor declares force majeure; activate dual-sourcing	**P2 - Med**	Q2
TR-03	Patient Medication Dispensing	Automated dispensing pharmacy network outage	Recent Disruption Analysis	Network near-miss revealed manual record lag	Functional drill: 100% manual charting and dual-nurse verification	**P1 - High**	Q3
TR-04							
TR-05							
TR-06							
TR-07							
TR-08							

RISK SCORING & MULTI-YEAR OBJECTIVES MAPPING

Targeting Evaluation Checklist:
[ ] **BIA Grounding:** Every critical function with MTPD ≤ 24h represented in calendar.
[ ] **Threat Spectrum:** Mix of physical, cyber, vendor, infrastructure, and human loss vectors.
[ ] **Past Incident Loop:** All Sev-1 / Sev-2 disruption findings addressed by validation exercises.
[ ] **Audit & Regulatory Fit:** Meets supervisory testing mandates without redundancy.

Multi-Year Objective Alignment:
• **Year 1 Goal:** Establish repeatable baseline testing across 100% of critical tier functions.
• **Year 2 Goal:** Transition from tabletops to functional simulations and automated failover tests.
• **Year 3 Goal:** Integrate cross-functional crisis management and external tier-1 vendor failover.
• **Target Maturity Milestone:** Progress from Current State to Target State on scheduled pathway.

TOOL 3: MATURITY SELF-ASSESSMENT SHEET (CURRENT VS. TARGET STATE)

Assess current maturity across core program dimensions, establish realistic target states, and document concrete evidence for ratings.

Program Dimension	Maturity Level Criteria (Levels 1–5)	Current State (1–5)	Target State (1–5)	Evidence for Current Rating	Required Progression Action
1. Program Governance & Oversight	1: Ad Hoc • 2: Continuity Mgr • 3: Steering Comm & Charter • 4: Exec Comm & Multi-year budget • 5: Board oversight	**Level 2**	**Level 3**	BC lead named, but no formal cross-functional steering committee charter exists.	Draft and sign Steering Committee charter; secure executive sponsor signature.
2. Annual Calendar & Scope	1: Unscheduled • 2: Basic schedule • 3: Risk-based calendar • 4: Integrated IT/Ops • 5: Full-scale & vendor partner runs	**Level 2**	**Level 3**	Tabletops conducted in 3 departments, but without risk-based annual calendar.	Deploy Calendar Builder; map all BIA critical functions into scheduled annual slots.
3. Scenario Design & Relevance	1: Generic script • 2: Single-threat • 3: Varied BIA threats • 4: Dynamic & emerging • 5: Multi-vector crisis simulation	**Level 2**	**Level 4**	Repeating same building fire script annually; no cyber/vendor scenarios tested.	Develop 4 new threat inject scripts: Cloud outage, Ransomware, 3PL supplier halt.
4. Performance Metrics & Tracking	1: Attendance only • 2: Completion counts • 3: Balanced inputs/outputs • 4: RTO/RPO outcome data • 5: Benchmark index	**Level 1**	**Level 3**	Only tracking attendance sheets; no remediation closure times recorded.	Implement Tool 4 Findings Log & Tool 5 Executive Dashboard metric calculations.
5. Continuous Improvement Loop	1: Informal notes • 2: Action list • 3: Centralized log • 4: Lessons repository • 5: Institutional learning culture	**Level 2**	**Level 3**	Actions logged in email; no central tracking of overdue remediation items.	Establish formal remediation log with steering committee review cadence.
6. Integration with BCM & IT DR	1: Isolated • 2: Departmental • 3: Coordinated BCM/DR • 4: Fully integrated ops • 5: Ecosystem & partner resilience	**Level 2**	**Level 4**	IT DR exercises run separately from business unit continuity walkthroughs.	Design joint operational-technical exercises pairing system failover with staff workarounds.

MATURITY PROGRESSION PATHWAY SUMMARY

Executive Maturity Target: Advance overall program maturity from **Level 1.8 (Initial)** to **Level 3.2 (Managed)** over 24 months.
Key Milestone Gates: (1) Charter signed by Q1; (2) Risk-targeted calendar published by Q2; (3) Metric tracking active by Q3; (4) Formal Executive Leadership Report presented by Q4.

TOOL 4: CONTINUITY EXERCISE RECORD & FINDINGS LOG

Record all conducted exercises, log deviations from planned calendar, document operational findings, and track corrective action remediation to closure.

Log ID	Date Run	Function / Unit	Scenario Tested	Status / Dev	Key Operational Findings & Gaps	Corrective Action & Owner	Due Date	State
FND-01	Feb 18	Payment Settlement	Cloud Gateway Outage	On Sched	Primary manual token generation procedure failed; secondary operator lacked MFA credentials.	Provision backup MFA tokens; rewrite SOP. (J. Vance, SecOps)	Mar 15	**Closed**
FND-02	May 12	Supply Chain Hub	Tier-1 Warehouse Fire	+2 Wks Dev	3PL alternate carrier contract required 48h activation notice, exceeding 12h BIA MTPD.	Renegotiate SLA to 4h standby activation window. (T. Chen, Supply)	Jun 30	**Closed**
FND-03	Aug 20	Enterprise IT / DR	Ransomware Encryption	On Sched	Air-gapped backup restored cleanly, but database indexing took 11h vs 8h RTO target.	Upgrade storage IOPS tier for indexing engine. (M. Ross, IT DR)	Oct 15	**In Prog**
FND-04								
FND-05								
FND-06								
FND-07								
FND-08								
FND-09								

CALENDAR DEVIATION & CORRECTIVE ACTION GOVERNANCE RULES

• **Deviation Threshold:** Any exercise postponed >30 days requires Steering Committee notification and documented re-schedule date.
• **Fundamental Gap Escalation:** Gaps causing RTO breach or life-safety hazard trigger immediate executive review and mandatory re-test within 60 days.
• **Closure Standard:** A corrective action cannot be closed on verbal confirmation; closing requires operational artifact proof (updated SOP, config change ticket, re-test log).

TOOL 5: EXECUTIVE LEADERSHIP REPORTING PACKAGE TEMPLATE

EXECUTIVE RESILIENCE SUMMARY • ANNUAL / QUARTERLY GOVERNANCE REPORT

Prepared for: Executive Leadership Team & Risk Committee • Reporting Period: [Q / Year] • Program Owner: [Name]

Program Performance Metric	Target Benchmark	Actual Result	Status	Executive Interpretation & Action
Annual Calendar Completion Rate	≥ 90% planned	100% (4 of 4 completed)	**ON TRACK**	All planned critical functions validated on schedule.
Critical Business Functions Tested	100% Tier-1 functions	100% (12 of 12)	**ON TRACK**	Full baseline coverage achieved across customer-facing operations.
Operational Gaps Identified / Closed	≥ 85% closure in 60d	88% (15 of 17 closed)	**ON TRACK**	Exercises actively identifying valid vulnerabilities; fast remediation.
Average Gap Remediation Time	≤ 45 calendar days	34 days avg	**ON TRACK**	Business units remediating findings well within governance tolerance.
RTO Compliance Achievement Rate	100% inside MTPD	92% (11 of 12 inside)	**MONITOR**	1 IT DR indexing delay identified; hardware upgrade approved.
Recovery Procedure Activation Time	≤ 30 minutes	22 minutes avg	**ON TRACK**	Staff activation speed improved 35% over prior-year baseline.
Personnel Readiness Confidence	≥ 85% positive	89% post-exercise	**ON TRACK**	Measured improvement in operational confidence during stress simulation.

STRATEGIC MATURITY & INVESTMENT RECOMMENDATIONS

Maturity Progression Status:
• **Current Baseline:** Level 2.6 (Transitioning Initial → Managed).
• **Year-End Target:** Level 3.0 (Full Managed Program certification).
• **Key Accomplishments:** Formal charter in place; standardized findings log implemented; all Tier-1 recovery procedures validated.

Steering Committee Action Requests:
1. **Capital Approval:** Fund air-gapped database IOPS expansion ($____).
2. **Vendor Mandate:** Enforce 4h standby recovery SLA across Tier-1 suppliers.
3. **Next Calendar Lock:** Approve 202___ Annual Calendar draft by Nov 30.

TOOL 6: REGULATORY & SUPERVISORY AUDIT EVIDENCE INDEX

Maintain comprehensive, tamper-evident records of all exercise activities, participant rosters, after-action analyses, and corrective actions to satisfy supervisory and auditor scrutiny.

Compliance Evidence Category	Required Audit Artifact Description	Storage Location / File Reference	Verification Sign-off
Program Charter & Policy	Executive-signed BCM policy, governance charter, and annual testing mandate defining program authority and scope.	`/BCM-Governance/Charter-2026.pdf`	[ ] Verified
Annual Approved Calendar	Formal annual calendar showing planned dates, functions, and scenario types signed by Steering Committee.	`/BCM-Calendars/Calendar-2026-Final.pdf`	[ ] Verified
Exercise Packages	Exercise plan, scenario briefing, master inject timeline (MSEL), and participant attendance sign-in sheets.	`/BCM-Exercises/2026/EX-[01-04]-Packs/`	[ ] Verified
After-Action Reports (AAR)	Formal after-action reports detailing timeline, participant feedback, observed RTO/RPO metrics, and gap analyses.	`/BCM-AAR/2026/AAR-[01-04]-Signed.pdf`	[ ] Verified
Corrective Action Proofs	Remediation proof artifacts: change tickets, updated SOPs, training rosters, and formal re-test records.	`/BCM-Remediation/CAP-[01-17]-Evidence/`	[ ] Verified
Executive Briefings	Quarterly and annual reporting slide decks and briefing memos presented to Executive Leadership and Board.	`/BCM-Executive/QBR-[1-4]-Board-Reports/`	[ ] Verified

AUDIT DEFENSE PROTOCOLS & DOCUMENT RETENTION STANDARDS

• **Retention Window:** Retain all exercise packs, attendance logs, and after-action reports for a minimum of 3 to 7 years (as dictated by applicable industry regulation and organizational document policy).
• **Inspection Readiness:** Ensure all completed exercises carry signed attendance logs and documented closure dates within 30 days of exercise execution.
• **Regulator Walkthrough:** Use the Executive Reporting Template (Tool 5) as the primary narrative brief, cross-referenced to specific evidence folders in this dossier index.