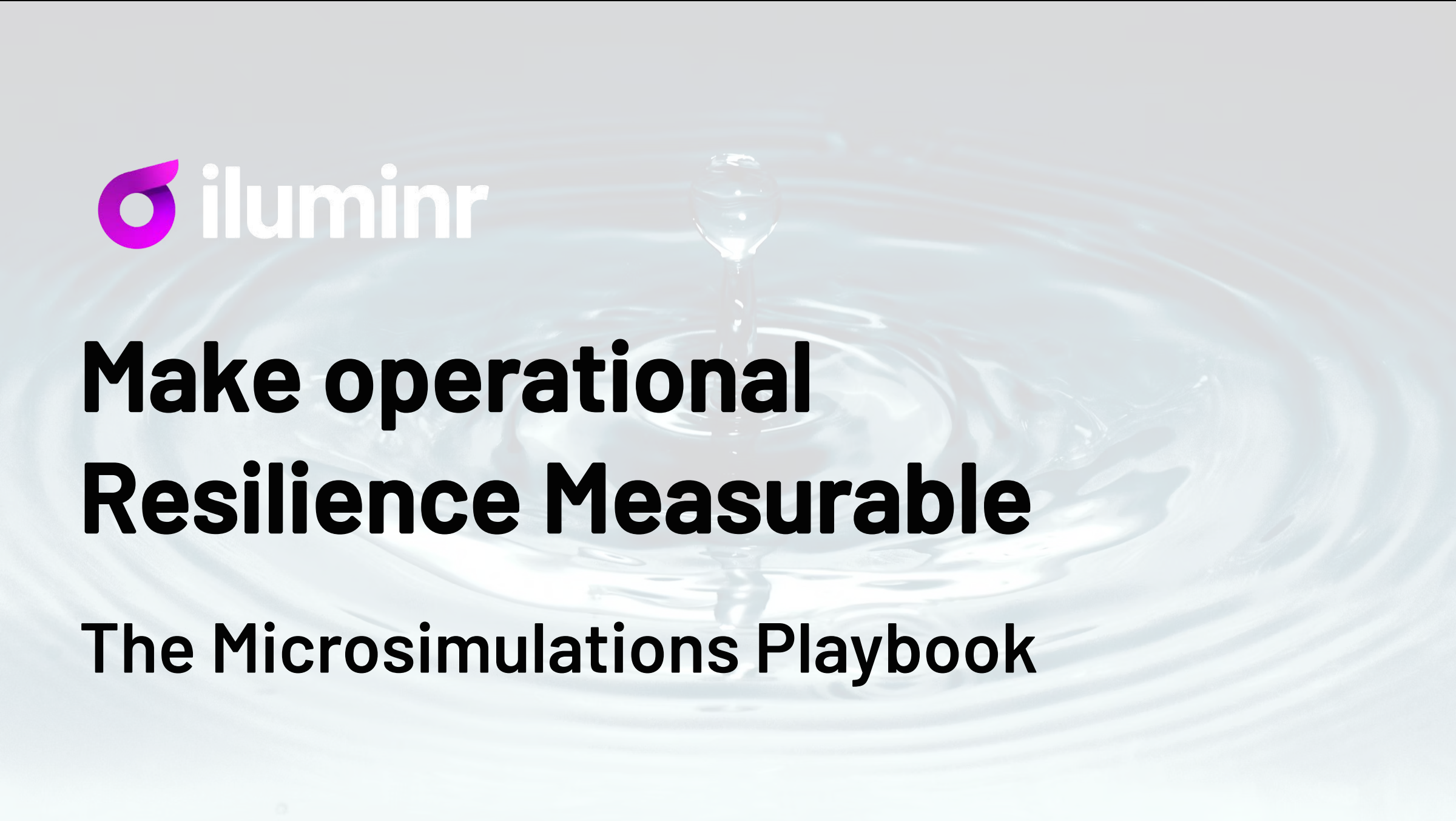


iluminr

Make operational Resilience Measurable

The Microsimulations Playbook

The Unmet Challenge: Why Traditional Resilience Exercises Are Failing

Despite mounting regulatory pressure for "business-as-usual" operational resilience testing, many firms are struggling.

Traditional large-scale, annual exercises are unsustainable and resource-intensive, leading to team burnout and significant operational disruption.

Moreover, they are increasingly **failing to meet evolving regulatory expectations**.

Regulators across jurisdictions are demanding a fundamental shift towards continuous, data-driven assurance.

They expect firms to move beyond episodic, box-ticking drills and demonstrate true resilience capability.

Frequent & Integrated Testing

Testing must be regular and embedded into daily operations, not a standalone, occasional event.

Risk-Focused Scenarios

Testing should prioritize critical business services and their potential impact, aligning with a true risk-based approach.

Severe & Challenging

Scenarios must be genuinely disruptive and plausible, pushing organizational limits beyond comfortable boundaries.

Regulators require firms to:

- Establish clear impact tolerances for service disruption.
- Rigorously map critical resources, dependencies, and supporting infrastructure.
- Provide verifiable evidence of their ability to maintain operations within tolerance under stress.
- Evolve testing methodologies from theoretical, desk-based reviews to empirical, data-driven validation.

Without a strategic transformation in testing methodology, firms will continue to face the dilemma of regulatory non-compliance versus unsustainable operational burden.

Microsimulations—with their bite-sized scope, high frequency, and rich evidence collection—represent a practical and scalable solution.

They make operational resilience testing continuous, efficient, and truly regulator-ready across the enterprise.

This playbook translates supervisory expectations into a repeatable Microsimulation programme aligned to requirements across key financial jurisdictions, offering the urgent shift needed to meet these demands.

United Kingdom (FCA • PRA • Bank of England)

The Financial Conduct Authority emphasizes the evolution of testing approaches in its 2024 guidance:

> "You must develop and keep up to date testing plans... identifying 'severe but plausible scenarios', varying in nature, severity and duration." (FCA, 2024)

> "Scenario testing... should become **part of business as usual** and be **reviewed on a regular basis**." (FCA, 2024)

> "Scenario testing should be **evolving** from **judgement, desk-based** approaches to **empirical data**, including **penetration tests, disaster recovery/failover tests, and simulations**." (FCA, 2024)

The Prudential Regulation Authority reinforces these expectations in SS1/21:

> "Firms are expected to **test regularly their ability to remain within impact tolerances** in **severe but plausible** disruption scenarios." (PRA, SS1/21)

> "Testing should include a range of **severe but plausible scenarios**, with **increasing sophistication over time**." (PRA, SS1/21)

EMEA (EU/EEA)

The Digital Operational Resilience Act (DORA) mandates structured testing programs:

> "Financial entities... shall **establish, maintain and review a... digital operational resilience testing programme**." (DORA, Art. 24)

> "Ensure, **at least yearly**, that appropriate tests are conducted on **all ICT systems and applications supporting critical or important functions**." (DORA, Art. 24)

> "Financial entities... **shall carry out at least every 3 years** advanced testing by means of **TLPT**." (DORA, Art. 26)

The European Central Bank's supervisory exercises reveal gaps in current approaches:

> "The 2022 climate risk stress test was a **useful learning exercise**... revealed many **deficiencies, data gaps and inconsistencies** across institutions." (ECB, 2022)

Canada (OSFI)

The Office of the Superintendent of Financial Institutions (OSFI) emphasizes regular testing and robust business continuity in its Guideline E-21 on Operational Resilience:

> "FRFIs should regularly **test their ability to remain within impact tolerances** and to **recover from disruptions**." (OSFI, Guideline E-21)

> "Testing programs should be **adaptable and evolve** to reflect changes in the FRFI's operating environment, risks, and critical functions." (OSFI, Guideline E-21)

> "FRFIs should identify potential **severe but plausible scenarios** that could disrupt their critical functions and assess the impact of these disruptions." (OSFI, Guideline E-21)

> "FRFIs should develop, maintain and periodically review their business continuity plans, taking into account different types of disruptions and their potential impact." (OSFI, Guideline B-10)

Ireland (Central Bank of Ireland)

The Central Bank of Ireland (CBI) highlights the importance of comprehensive testing and a continuous improvement approach in its Cross Industry Guidance on Operational Resilience:

> "Firms should conduct **regular testing** of their operational resilience capabilities, including scenario-based testing, to ensure the continued effectiveness of their arrangements." (CBI, Cross Industry Guidance)

> "Testing should include a range of **severe but plausible scenarios** to challenge the firm's operational resilience framework and identify areas for improvement." (CBI, Cross Industry Guidance)

> "The firm should be able to demonstrate, through **verifiable evidence**, that its operational resilience framework is effective and capable of withstanding severe disruption." (CBI, Cross Industry Guidance)

> "Firms should ensure that their business continuity plans are comprehensive, regularly reviewed, and tested to ensure they remain fit for purpose." (CBI, Cross Industry Guidance)

United States (Fed • OCC • FFIEC)

US regulators focus on outcome-based resilience and regular testing:

> "Operational resilience is **the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard**..." (Federal Reserve)
>
> "...the outcome of effective operational risk management combined with sufficient... resources to prepare, adapt, withstand, and recover..." (Federal Reserve)
>
> "Notably, the impacts of most concern are not financial; **this is not a problem that capital or liquidity can solve**." (OCC, 2024)
>
> "Ensuring that critical operations... can withstand or recover... **requires... regular testing**." (OCC, 2024)

Australia & New Zealand (APRA • RBNZ)

APRA's CPS 230 (effective 2025) mandates:

> Business continuity plans must be "**regularly tested with severe but plausible scenarios**. A **systematic testing program**... covering all critical operations and **includes an** annual **business continuity exercise**...testing the ability to meet tolerance levels **in a range of severe but plausible scenarios**." (APRA, CPS 230)

What Supervisors Observe

Regulatory observations reveal significant gaps between expectations and current industry practices.

FCA (UK)

Firms should evolve beyond "**judgement, desk-based**" approaches to **empirical** testing, including **simulations**.

Many organizations rely too heavily on subjective assessments, rather than objective evidence from realistic testing.

ECB (EU)

Climate stress tests exposed "**deficiencies, data gaps, and inconsistencies**" across institutions.

When faced with stress testing, firms often discover their data collection and analysis capabilities are insufficient.

ECB Cyber (EU)

Banks have response/recovery frameworks, but "**areas for improvement remain**."

Documented frameworks do not guarantee effective execution during actual disruptions.

RBNZ (NZ)

Exercises were **resource-intensive** but improved banks' **capability** and **identified risks**.

Traditional large-scale exercises deliver value, but at a significant cost that limits frequency.

These observations highlight a critical gap: supervisors expect testing that is frequent, realistic, evidenced, and embedded in business-as-usual operations.

Current Industry Challenges

- Infrequent testing (annual/quarterly)
- Predominantly desk-based, theoretical approaches
- Limited empirical evidence of resilience
- Resource-intensive exercises, limiting frequency
- Insufficient coverage of critical functions
- Gap between documented procedures and execution

Regulatory Expectations

- Regular, business-as-usual testing
- Empirical, data-driven approaches
- Objective evidence within tolerances
- Sustainable cadence for critical functions
- Evolving sophistication over time
- Proven execution capabilities under stress

This misalignment between expectations and current practices creates both regulatory risk and a significant opportunity to improve operational resilience.

Microsimulations offer a practical bridge.

Microsimulations Defined: A New Approach

Frequent

Run weekly to monthly.Minimal preparation allows for sustainable cadence without team burnout.

Targeted

Narrow scope focusing on specific dependencies, processes, teams, or failure modes.

Evidenced

Produce hard evidence: timestamps, artifacts, metrics, and objective measurements.

Chainable

Can be linked into campaigns.These cumulatively approximate end-to-end crises.

Unlike traditional large-scale exercises, Microsimulations:

- Are **risk-based**, mapped to important business services and critical operations.
- Instrument outcomes against **impact tolerances** and **time-bound recovery objectives**.
- Feed **lessons learned** into control improvements, playbooks, and vendor obligations.
- Require minimal preparation and disruption to business operations.
- Build an **evidence base** that satisfies regulatory requirements.

Why Microsimulations Are the Only Practical Way Forward

Cadence

Only frequent, small tests can satisfy "business-as-usual / regular / annual" expectations without burning out teams or disrupting operations.

Coverage

Micro-scope allows comprehensive annual coverage of all critical/important functions (as required by DORA Art. 24).

It also enables thorough testing of UK impact tolerance pathways.

Evidence

Each run yields objective evidence for supervisors, moving beyond desk-based assertions to empirical proof of capabilities.

Evolution

Complexity can be incrementally increased over time (as required by PRA SS1/21).

This progresses from tabletop exercises to live-fire failover and threat-led penetration testing.

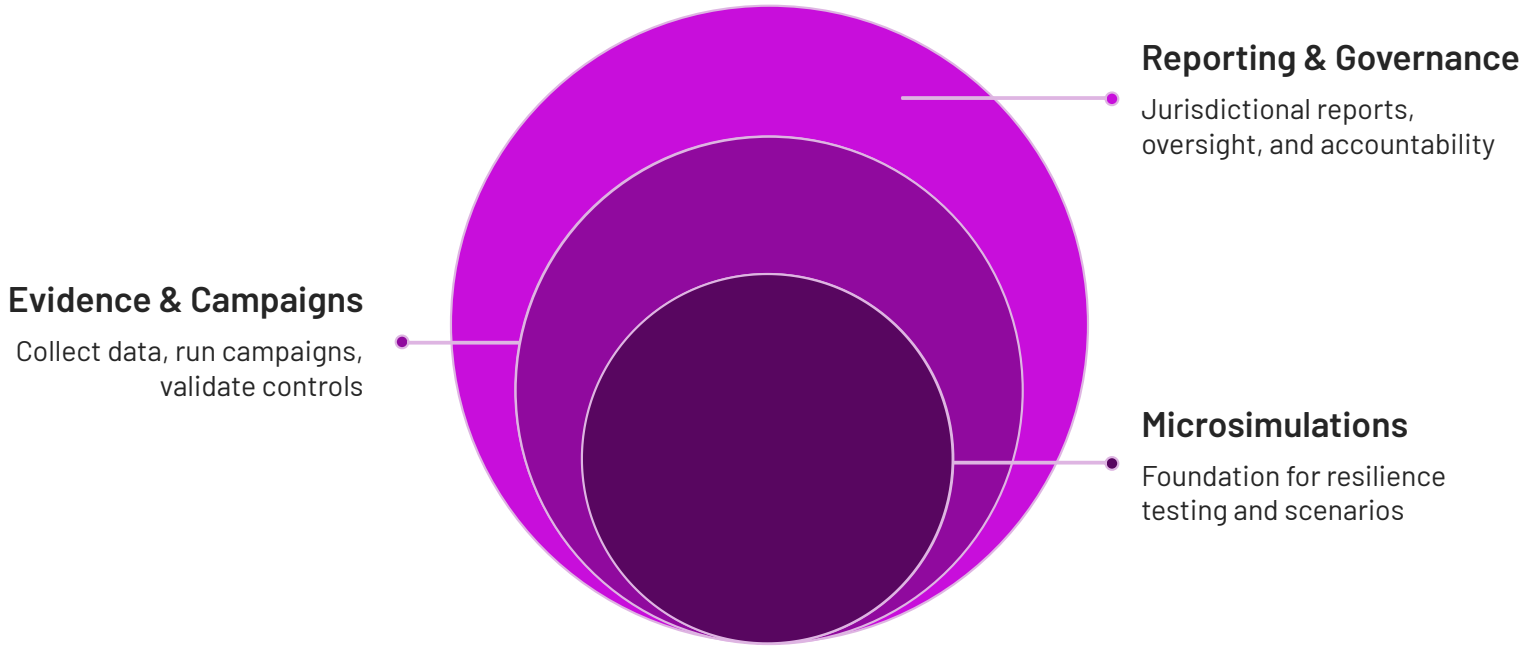
By breaking down testing into manageable components, while maintaining links to the broader resilience framework, Microsimulations transform operational resilience. It shifts from an episodic, resource-intensive exercise into a continuous, embedded capability. This approach generates ongoing evidence of compliance with regulatory expectations.

Mapping Regulatory Requirements to Microsimulation Design

Jurisdiction	Regulatory Expectation	Microsimulation Response
UK (FCA/PRA)	Severe-but-plausible scenarios; regular testing; evolving sophistication; BAU; map tolerances	Weekly/monthly micro-exercises (IBS & resource maps); progressive difficulty
EU (DORA/ECB)	Testing programme; annual tests across all critical/important functions; TLPT ≥ 3-yearly; recovery-focused cyber stress	Rolling microsim coverage (100% annual functions); TLPT-ready scope from micro-findings; dedicated recovery sprints
US (Fed/OCC/FFIEC)	Outcome focus; tolerances for disruption; regular testing; third-party dependencies	Micro-exercises for critical ops, SLAs, vendors; explicit tolerance checks; vendor simulations
AU (APRA CPS 230)	Systematic testing; annual enterprise exercise; severe-but-plausible	Year-round microsims feeding one annual cross-entity event; severity ladder mapped to tolerance
NZ (RBNZ)	Capability development via exploratory stress; quantify impacts	Microsims that quantify business/financial impacts and improve models over time

Implementing Across Regulatory Regimes

A well-designed Microsimulation programme can satisfy multiple regulatory requirements simultaneously through a layered approach:



iluminr

Key Alignment Principles

- **Universal coverage:** Test all critical/important functions annually.
- **Jurisdictional emphasis:** Tailor exercises to specific regulatory priorities.
- **Evidence standardisation:** Collect consistent evidence for diverse regulatory submissions.
- **Graduated severity:** Implement a severity ladder mapping to regulatory "severe but plausible" definitions.
- **Integrated remediation:** Ensure lessons learned drive control improvements aligned with regulatory expectations.

This mapping approach ensures that a single, well-designed Microsimulation programme can satisfy multiple regulatory regimes without duplicating effort or creating silos of compliance activity.

12-Week Programme Blueprint: From Implementation to BAU

Establishing an effective Microsimulation programme requires a structured approach. The following 12-week blueprint provides a roadmap for implementing Microsimulations and integrating them into business-as-usual operations.

Phase 1 — Stand-up (Weeks 1–4)

1

- Define **scope**: important business services, critical operations, tolerances, dependencies, and key vendors.
- Build **scenario library**: include common failure modes (e.g., data loss, cyber encryption, DNS failure, staff/facility outage, vendor outage, corrupted reference data).
- Instrument **evidence pack**: define run sheets, metrics, and artifacts; automate capture of tickets, logs, and communication transcripts.
- Establish governance framework and reporting templates.

Phase 2 — Pilot (Weeks 5–8)

2

- Run 4–6 Microsimulations across diverse services and domains.
- Calibrate **severity** ladder and **acceptance criteria**: tolerance compliance, time-to-detect/recover, and communication quality.
- Initiate specific **campaigns** (e.g., Payments Week, Cloud Week) and cross-functional injects.
- Refine evidence collection and reporting based on pilot learnings.

Phase 3 — Scale (Weeks 9–12)

3

- Expand to a weekly cadence, ensuring full annual coverage of all critical and important functions.
- Schedule the annual enterprise exercise (APRA).
- Curate TLPT scope (DORA) using insights from micro-evidence and weakness heatmaps.
- Establish comprehensive **governance**: Board reporting, remediation tracking, vendor obligations, and a continuous improvement loop.
- Train additional facilitators and expand participation across the organization.

Critical Success Factors

- **Executive sponsorship:** Secure early commitment from senior leadership.
- **Clear ownership:** Designate accountable individuals for each phase and workstream.
- **Realistic scoping:** Start with a manageable scope and expand gradually.
- **Technology enablement:** Implement tools to automate evidence collection and reporting.
- **Integrated remediation:** Establish clear processes for tracking and implementing lessons learned.

Following this structured approach ensures that Microsimulations become embedded in organizational processes and generate the evidence needed to demonstrate regulatory compliance.

6 Key Metric Categories

Tolerance Adherence

- Percentage of Microsimulations within impact tolerances.
- Distribution of tolerance breaches by cause.
- Trend analysis of tolerance performance.
- Root cause analysis of tolerance breaches.

Recovery Performance

- Time-to-detect (TTD): Incident identification speed.
- Time-to-contain (TTC): Speed to halt incident spread.
- Time-to-recover (TTR): Service restoration speed.
- Comparison of actual performance vs. objectives.

Control Efficacy

- Failed control rate during Microsimulations.
- Repeated-failure trend across exercises.
- Mean time to remediate (MTTR) identified gaps.
- Control performance by type (preventative, detective, corrective).

Third-Party Performance

- Vendor inject outcomes vs. contractual obligations.
- Evidence of third-party exercise participation.
- Third-party engagement and response time.
- Quality of third-party incident communications.

Coverage

- Annual critical/important function testing coverage.
- Scenario family coverage across risk landscape.
- Environment coverage (production-like/dev/test).
- Staff participation and role coverage in exercises.

Learning Loop

- Percentage of identified lessons implemented.
- Retest pass-rate for remediated controls.
- Time to implement lessons learned.
- Performance metric improvement post-lessons.

Evidence Format and Presentation

When presenting evidence to supervisors, consider these best practices:

- **Standardisation:** Use consistent formats for evidence collection across all exercises.
- **Traceability:** Ensure clear links between test scenarios, important business services, and regulatory requirements.
- **Visualisation:** Present metrics in dashboards that highlight trends and patterns.
- **Contextualisation:** Provide narrative context that explains metric performance.
- **Remediation:** Document how identified issues are tracked, prioritised, and resolved.

Systematic collection and presentation of these metrics will empirically demonstrate to supervisors that operational resilience capabilities are robust and regularly tested.

While a well-designed Microsimulation programme addresses core requirements across jurisdictions, regulatory nuances require targeted compliance checks.

United Kingdom (FCA/PRA)

- IBS and impact tolerances are fully mapped. Tolerance dashboards live.
- Quarterly micro-campaigns run for each IBS pathway. Microsimulations are logged with evidence.
- Annual maturity uplift achieved per FCA/PRA guidance, progressing from tabletop to live failover exercises.
- Board-approved self-assessments completed, with evidence-based conclusions on impact tolerances.

European Union/EEA (DORA/ECB)

- DORA testing programme approved by management body. Documented governance in place.
- Annual tests cover all critical functions. A comprehensive evidence pack is maintained.
- TLPT readiness established. Scoping dossier built from micro-evidence; three-year plan in place.
- Recovery drills aligned with ECB's cyber-stress focus. Relevant metrics captured.

United States (Fed/OCC/FFIEC)

- Defined tolerances for critical operation disruption are documented and formally approved.
- Regular testing cadence established. Executive visibility and reporting maintained.
- Third-party dependencies included in scenario injects, ensuring contractual alignment.
- Evidence aligned to Fed's "outcome" framing and OCC's baseline focus on critical operations.

Australia & New Zealand (APRA/NZ)

- Systematic programme documented per CPS 230. Governance framework in place.
- Annual enterprise exercise scheduled, with board visibility and participation.
- Severe-but-plausible scenario library maintained. Scenarios mapped to Australian financial system.
- Capability development metrics tracked. Quantifiable impact assessments integrated.

Cross-Jurisdictional Harmonisation

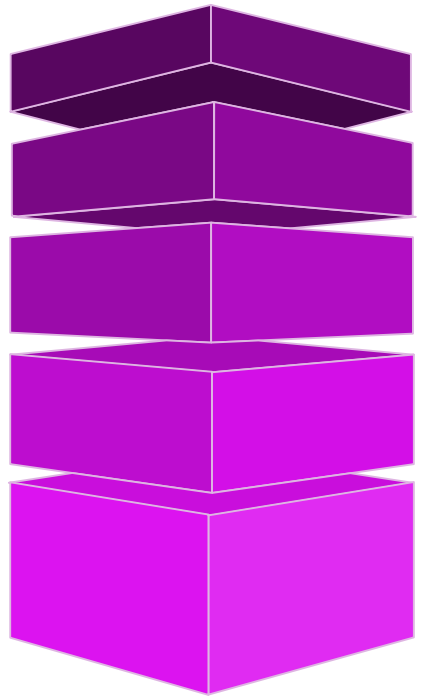
For firms operating across multiple jurisdictions, these checklists can be integrated into a comprehensive framework that addresses all requirements while minimising duplication. Key harmonisation steps include:

- **Common terminology mapping:** Create correspondence tables for jurisdiction-specific terms (e.g., "important business services" vs. "critical operations").
- **Evidence reusability:** Design evidence formats that satisfy multiple regulatory regimes.
- **Governance alignment:** Establish unified governance structures that address all jurisdictional requirements.
- **Consolidated reporting:** Develop reporting templates that can be adapted for different supervisory audiences.

By addressing these jurisdiction-specific requirements within a common framework, firms can efficiently demonstrate compliance across multiple regulatory regimes without maintaining separate programmes.

Operating Model & Roles

A successful Microsimulation programme requires clear ownership and accountability across the organisation. The following operating model defines key roles and responsibilities for implementation and ongoing operation.



Board & Exec

Provide governance, strategic direction and accountability.

Service Owners

Own service continuity plans and implement simulations.

Vendors & Partners

Deliver external capabilities, integrate systems and support exercises.

Resilience Office

Coordinate programme, report to Board & Exec and manage interactions.

Risk & Audit

Assess controls, validate outcomes and provide independent assurance.

Board & Executive Committee

- Set risk appetite, impact, and tolerance levels
- Review outcomes quarterly via standardized reporting
- Approve remediation priorities and resource allocation
- Provide visible sponsorship and participate in selected exercises
- Challenge assumptions

Resilience Office

- Own program methodology, scenario library, and metrics
- Coordinate Microsimulation calendar and campaign planning
- Facilitate exercises and document outcomes
- Maintain evidence repository for regulatory submissions
- Track remediation progress and maturity

Service Owners

- Run service-specific Microsimulations with support
- Maintain resource maps and dependency documentation
- Implement service-specific remediation actions
- Ensure staff participation and capability development
- Integrate lessons learned

Risk & Audit Functions

- Provide independent challenge to scenario design and outcomes
- Sample evidence to verify quality and completeness
- Include Microsimulation outcomes in risk reporting
- Verify remediation effectiveness through targeted testing

Vendors & Partners

- Participate in relevant Microsimulation injects
- Share evidence of their own resilience capabilities
- Implement agreed remediation actions within contract
- Participate in joint planning and lessons learned reviews

Governance Cadence

Effective governance requires regular touchpoints at different organisational levels:

Forum	Frequency	Key Focus
Board Risk Committee	Quarterly	Program effectiveness, tolerance breaches, strategic risks
Executive Committee	Monthly	Cross-functional issues, resource allocation, priority remediation
Operational Resilience Working Group	Bi-weekly	Microsimulation outcomes, campaign planning, lessons implementation
Service Owner Review	Weekly	Service-specific results, technical remediation

This operating model ensures clear accountability and fosters collaboration across organisational boundaries.

Sample 90-Day Microsimulation Schedule

Week A (Payments)

Focus: DNS resolution failure, failover, & communications

- Exercise DNS resolution.
- Assess payment processing impact.
- Test automated failover procedures.
- Evaluate internal and external communications.
- Measure time-to-detect and time-to-recover.
- Check tolerance compliance.

Week B (Customer Support)

Focus: Staff outage, surge routing, vulnerable-customer.

- Simulate significant staff unavailability.
- Test surge capacity and alternate routing.
- Evaluate prioritization of vulnerable customers.
- Assess customer communications quality.
- Check notifications.

Week C (Core Banking)

Focus: Storage corruption, restore, & data reconciliation

- Inject simulated storage corruption.
- Focus on core banking data.
- Test data restore procedures.
- Verify data validation processes.
- Exercise reconciliation procedures.
- Review affected systems.

Week D (Cloud)

Focus: Region impairment, network segmentation, & IAM break-glass

- Simulate cloud region availability issues.
- Focus on key workloads.
- Test network segmentation.
- Exercise Identity and Access Management (IAM) break-glass procedures.
- Evaluate multi-region resilience.

This cycle repeats with raised severity levels and additional complexity, including cross-border dependencies, market infrastructure interactions, and third-party injects. Each subsequent cycle builds on lessons from previous iterations, creating a continuous improvement loop.

Campaign Structure

Microsimulations can be grouped into themed campaigns that focus on specific aspects of operational resilience:

Payment Systems Resilience

Series of Microsimulations testing dependencies in payment processing chain.

Data Integrity

Testing of data corruption, loss, and reconciliation capabilities.

Cloud Infrastructure

Focused testing of cloud-based services and multi-region resilience.

Third-Party Dependencies

Exercises involving key vendors and service providers.

Cyber Resilience

Response and recovery capabilities for cyber disruption scenarios.

By structuring Microsimulations into these thematic campaigns, firms can ensure comprehensive coverage while building focused expertise in specific resilience domains. This approach also allows for targeted reporting to different stakeholders based on their areas of interest and responsibility.

Evidence Pack Structure for Regulators

Executive Summary

- Overview of Microsimulation program & methodology
- Key findings & themes from recent exercises
- Summary of tolerance compliance & improvement trends
- High-priority remediation actions & timeline
- Forward plan for program development

Methodology Documentation

- Microsimulation approach & scenario selection
- Mapping to important business services & critical operations
- Severity classification framework & tolerance definitions
- Governance framework & decision-making process

Exercise Catalogue

- Inventory of completed Microsimulations (dates & scope)
- Coverage analysis of critical functions & services
- Participation records (staff, teams, third parties)
- Scenario descriptions & severity classifications
- Links to detailed run sheets & artifacts

Quantitative Metrics

- Tolerance compliance statistics & trend analysis
- Recovery time performance (TTD, TTC, TTR) & benchmarks
- Control efficacy measurements & failure patterns
- Third-party performance metrics vs. obligations
- Coverage statistics & participation metrics

Qualitative Insights

- Thematic analysis of recurring challenges & strengths
- Root cause analysis of significant findings
- Effectiveness assessment of response & recovery procedures
- Communication quality evaluation (internal & external)
- Decision-making effectiveness under stress

Remediation Tracking

- Inventory of identified issues needing remediation
- Prioritization framework & implementation timeline
- Progress updates & completion evidence
- Effectiveness validation through retesting
- Escalation process for stalled remediation

Jurisdiction-Specific Supplements

In addition to the core components, evidence packs should include supplements tailored to specific regulatory requirements:

UK Supplement

- Impact tolerance mapping & compliance
- Important business service linkage
- FCA/PRA self-assessment
- Sophistication evolution evidence

US Supplement

- Critical operations resilience
- Third-party dependency testing
- Alignment to Fed/OCC guidance
- Outcome-based effectiveness

EU/EEA Supplement

- DORA testing program documentation
- Critical/important function coverage
- TLPT readiness & scoping
- Digital operational resilience framework

AU/NZ Supplement

- CPS 230 compliance
- Annual enterprise exercise documentation
- Severe-but-plausible scenario justification
- Capability development & impact quantification

By structuring evidence in this way, firms can efficiently demonstrate compliance to supervisors while maintaining a consistent approach across jurisdictions.

The modular design allows for customization without duplicating effort, ensuring regulatory submissions are both comprehensive and efficient.

Microsimulation Scenario Design Principles

Effective Microsimulation scenarios must balance realism, severity, and practicality.

Core Design Principles

Risk-Based Selection

Scenarios should be informed by the organization's risk assessment.

Focus on the most critical dependencies.

Specific Focus

Each scenario should target a specific process, system, or dependency.

Avoid attempting to test everything at once.

Severe but Plausible

Scenarios should stretch capabilities.

Avoid extremes that might be dismissed as unrealistic or impossible to prepare for.

Evidence-Generating

Design should facilitate objective evidence collection.

This evidence demonstrates capability and identifies gaps.

Scenario Documentation Template

Each Microsimulation scenario should be documented consistently to ensure clarity and traceability:

Scenario Identification

- Unique ID and descriptive name
- Severity classification & rationale
- Service/function mapping
- Regulatory linkage
- Tolerance thresholds & measurement criteria

Scenario Details

- Detailed disruption description
- Timeline of events
- Affected systems, processes, & teams
- Impacted internal & external dependencies
- Previous findings & vulnerabilities

Execution Guidelines

- Required participants & roles
- Evidence collection points & methods
- Inject sequence & timing
- Success criteria & evaluation framework

By applying these design principles, firms can develop Microsimulation scenarios that effectively test resilience capabilities.

This also generates the necessary evidence to satisfy regulatory expectations.

Scenario Severity Ladder

A graduated approach to scenario severity allows firms to progressively increase challenge while maintaining credibility:

Severity Level	Characteristics	Example
Level 1: Routine	Single component failure with established workarounds; limited duration; isolated impact.	Temporary outage of a redundant system component with auto failover.
Level 2: Challenging	Multiple related failures; extended duration; potential tolerance pressure.	Regional data centre outage, manual recovery needed.
Level 3: Severe	Complex, multi-faceted disruption; significant duration; tolerance breach likely.	Cyber attack affecting multiple systems with data integrity concerns.
Level 4: Extreme	Unprecedented scale; market-wide implications; multiple tolerance breaches.	Simultaneous disruption of critical market infrastructure and internal systems.

Scenario Categories and Examples

iluminr

Microsimulation Facilitation Guide

Facilitator Role and Responsibilities

- **Exercise management:** Guide scenario execution, maintaining focus and pace.
- **Reality enforcement:** Ensure realistic conditions by limiting "magic solutions" and enforcing constraints.
- **Evidence collection:** Capture key decisions, actions, and timestamps throughout the exercise.
- **Participant engagement:** Keep all participants involved and challenge assumptions appropriately.
- **Time management:** Maintain the exercise schedule while allowing for valuable exploration.

Before the Exercise

Preparation Checklist

- Distribute pre-reading material 48 hours before.
- Brief observers on roles and monitoring areas.
- Test technology platforms or tools.
- Prepare inject cards and supporting materials.
- Review previous exercise findings for follow-up.

Participant Briefing

- Clearly explain Microsimulation purpose and scope.
- Set expectations about realism; "no magic solutions."
- Describe evidence collection and its use.
- Encourage honest responses, not "perfect" answers.
- Explain exercise artificiality vs. reality.

During the Exercise

Launch

Begin with a clear scenario introduction and initial conditions.

Record the official start time.

Injects

Deliver scenario injects at planned intervals.

Capture reaction times and initial responses.

Facilitation

Guide discussion with probing questions.

Challenge assumptions and "too easy" solutions.

Capture

Document decisions, actions, and timelines.

Collect artifacts and evidence of capabilities.

Facilitation Techniques

Reality Enforcement

- **The "So What?" Challenge:** Ask for concrete next steps and immediate implications.
  Example: "You've notified the vendor, so what? How long until they respond? What's your interim solution?"
- **Resource Constraints:** Introduce limitations to test adaptability.
  Example: "That person is unavailable. Who else can do this?"
- **Time Pressure:** Impose strict deadlines for decision-making.
  Example: "The CEO needs an update in 10 minutes. What can you tell her?"
- **Escalation Reality:** Highlight the practicalities and timelines of approvals.
  Example: "That requires senior approval. How long will that take? What's your contingency?"

Evidence Extraction

- **Process Verification:** Request demonstration of documented procedures.
  Example: "Show me where that procedure is documented."
- **Tool Demonstration:** Ask participants to show how they would use a specific system.
  Example: "Can you show us how you would actually do that in the system?"
- **Decision Logging:** Record key decisions, the decision-maker, and their rationale.
  Example: "I'm capturing that decision. Who made it and what was the rationale?"
- **Timeline Construction:** Establish expected completion times for actions.
  Example: "Let's record when you would expect that action to be complete."

After the Exercise

01

Immediate Debrief

Conduct a structured discussion immediately after the exercise while details are fresh. Use the "what went well, what didn't, what could improve" framework.

02

Evidence Compilation

Organise all collected evidence, including timeline, decisions, actions, and artifacts. Identify any gaps requiring follow-up.

03

Findings Documentation

Document key findings, including tolerance assessments, control effectiveness, and improvement opportunities.

04

Remediation Planning

Develop specific, actionable remediation items with clear ownership and timelines for implementation.

Effective facilitation transforms Microsimulations from theoretical exercises into practical demonstrations of capability.

These exercises generate valuable evidence for regulatory purposes and drive genuine improvements in operational resilience.

Key Findings and Themes

Strengths Identified

- Strong detective controls across payment systems
- Effective cross-team collaboration during customer service disruptions
- Improved recovery time in cloud-based workloads
- Clear escalation paths and decision rights

Improvement Areas

- Data reconciliation processes exceed tolerance
- Third-party response coordination ownership needed
- Backup systems not regularly load tested
- Communication templates require pre-approval

Technology Enablement for Microsimulations

Scenario Management

Centralised repository for scenario development, version control, and reuse.

It enables consistent formatting, tagging to business services, and systematic severity classification.

Exercise Execution

Tools for delivering injects, capturing responses, and recording timestamps. Supports both tabletop and technical exercises with appropriate workflow guidance.

Evidence Collection

Structured templates for capturing decisions, actions, and artifacts. Automated collection of system logs, communications, and performance metrics where possible.

Analytics & Reporting

Dashboards displaying key metrics, trends, and compliance status. Customisable views for different stakeholders from operational teams to board level.

Remediation Tracking

Workflow management for identified issues, from assignment through implementation to verification. Integration with existing risk and control systems.

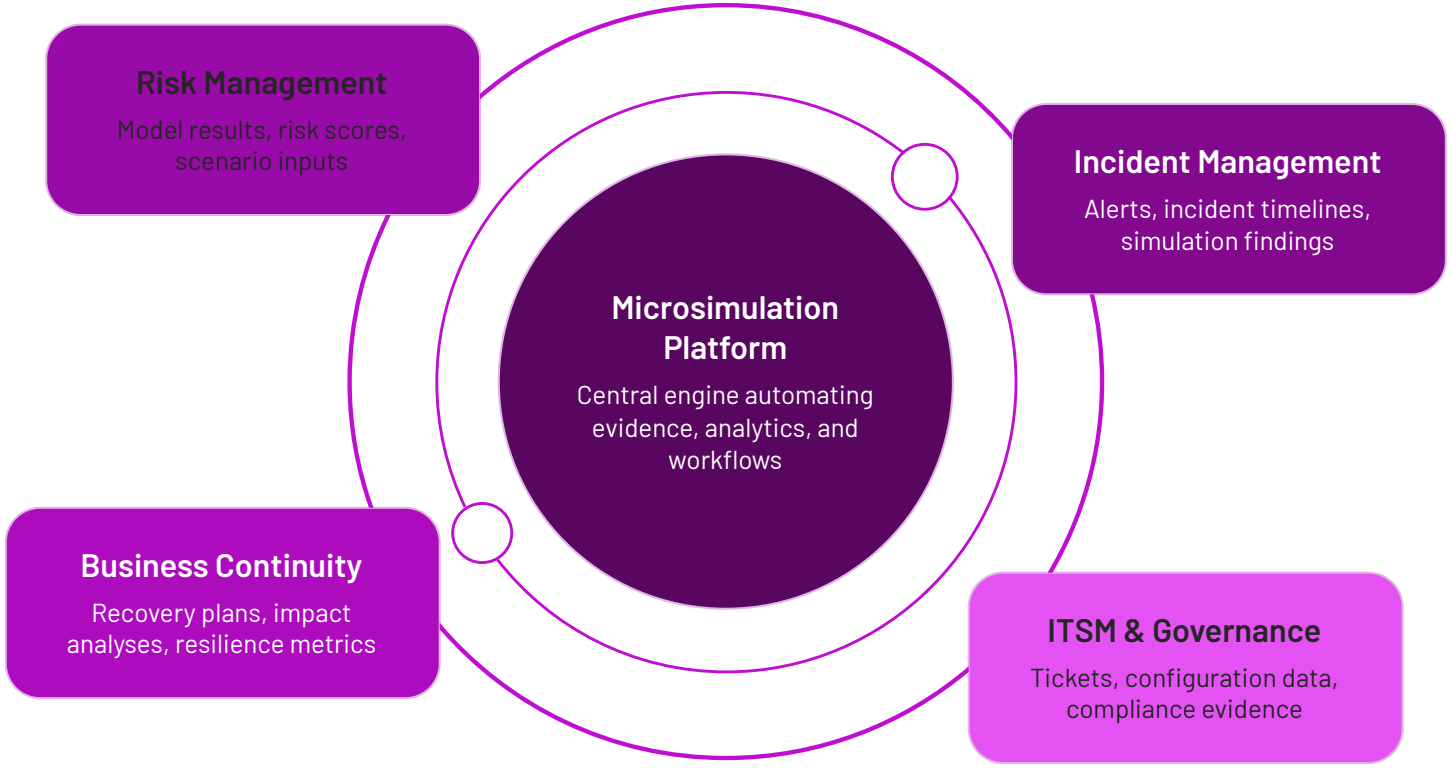
Regulatory Documentation

Template-driven generation of regulatory submissions with appropriate formatting and evidence linking.

It also provides jurisdiction-specific supplements.

Integration Points

Microsimulation technology should integrate with existing enterprise systems to maximise efficiency and avoid duplication:



iluminr

Build vs. Buy Considerations

Custom Development Approach

Advantages:

- Tailored to specific organizational processes
- Full control over features and development roadmap

Disadvantages:

- Significant initial development investment
- Requires dedicated technical resources for maintenance
- May lack industry best practices
- Longer time to implement benefits

Specialised Platform Approach

Advantages:

- Faster implementation and time to value
- Incorporates industry best practices and standards
- Regular updates for regulatory compliance
- Lower internal resource requirements

Disadvantages:

- May require process adaptation
- Less control over feature development priorities

Implementation Roadmap

Phase 1: Foundation

Implement core scenario management and evidence collection capabilities. Focus on standardised templates and basic reporting.

Phase 2: Integration

Connect with key enterprise systems for incident management, risk tracking, and communication platforms.

Phase 3: Automation

Implement automated evidence collection, metrics calculation, and regulatory report generation.

Phase 4: Advanced Analytics

Deploy predictive analytics, pattern recognition, and AI-assisted scenario development.

Effective technology enablement transforms microsimulations from manual, resource-intensive activities into efficient, evidence-rich exercises.

These exercises scale across the enterprise while maintaining consistency and quality.

Third-Party Integration in Microsimulations

Third-party dependencies represent a significant source of operational risk that must be included in Microsimulation programmes.

Effectively integrating vendors, partners, and market infrastructure providers into testing requires a structured approach that balances practicality with thoroughness.

The Regulatory Imperative

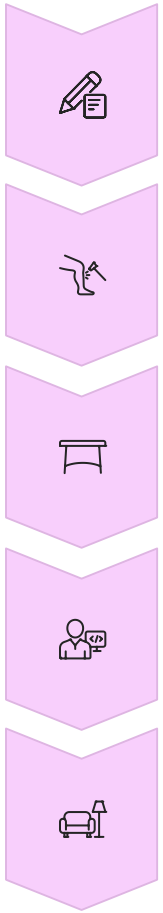
Regulators across jurisdictions explicitly expect third-party dependencies to be included in resilience testing:

> "This is not a problem that capital or liquidity can solve."
>
> "Ensuring that critical operations... can withstand or recover... requires... regular testing." (OCC, 2024)

This statement from the OCC highlights the need to test operational capabilities—including those that depend on third parties—rather than simply maintaining financial buffers.

Similar expectations exist across UK, EU, and Australia/New Zealand regulatory frameworks.

Third-Party Integration Spectrum



Document Review

Review vendor resilience documentation and contractual SLAs without direct involvement.

Simulated Response

Internal teams role-play vendor responses based on documented procedures and past experience.

Tabletop Participation

Vendor representatives participate in discussion-based exercises focused on coordination.

Technical Exercise

Actual technical testing involving vendor systems in test/development environments.

Live Simulation

Coordinated testing with vendors in production-like conditions with actual system interactions.

Contractual Considerations

Effective third-party testing requires appropriate contractual provisions:

Testing Rights

- Explicit right to include vendor in resilience testing.
- Minimum participation frequency and scope.
- Required seniority and expertise of participating staff.
- Notice periods and scheduling constraints.

Evidence Requirements

- Types of evidence vendor must provide.
- Format and timeliness of delivery.
- Right to verify vendor's own testing.
- Regulatory submission permissions.

Remediation Obligations

- Timelines for addressing identified issues.
- Verification procedures for remediation effectiveness.
- Escalation for unresolved issues.
- Continuous improvement expectations.

Practical Implementation Approaches

Tiered Approach

Categorize third parties by criticality. Apply different testing requirements to each tier, with the most critical receiving the most rigorous testing.

Piggyback Method

Coordinate with vendors to participate in their own resilience exercises. This reduces burden while maintaining coverage.

Community Testing

Collaborate with industry peers who use the same vendors to conduct joint exercises, increasing leverage and sharing insights.

Gradual Implementation

Begin with lower-intensity involvement (documentation, tabletop). Progressively move toward technical testing as relationships mature.

Measuring Third-Party Performance

Metric	Description	Target
Response Time	Time from notification to active engagement	Per contract SLA
Communication Quality	Clarity, accuracy, and usefulness of status updates	≥4/5 rating
Resolution Time	Time to resolve simulated issues	Per contract SLA
Participation Rate	Percentage of invited exercises with active participation	≥90%
Remediation Completion	Percentage of identified issues remediated on schedule	≥85%

Effective third-party integration in Microsimulations not only satisfies regulatory expectations.

It also strengthens the resilience of critical service delivery chains and provides early warning of potential vulnerabilities in the broader ecosystem.

Microsimulation Programme Maturity Model

Operational resilience testing capabilities evolve over time, progressing through stages of increasing sophistication and effectiveness.

This maturity model provides a framework for assessing current capabilities and planning future development of a Microsimulation programme.

Maturity Dimensions

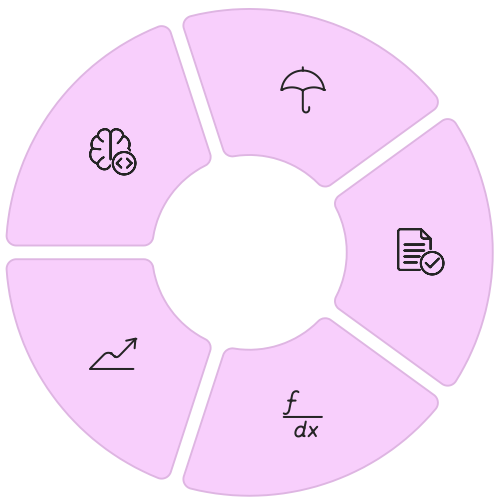
Programme maturity should be assessed across multiple dimensions:

Methodology

Rigour and sophistication of testing approaches, from theoretical discussions to technical verification.

Improvement

Effectiveness of the feedback loop in driving tangible resilience enhancements.



Coverage

Breadth and depth of testing across critical business services and their dependencies.

Evidence

Quality, objectivity, and comprehensiveness of evidence collected during testing.

Integration

Degree to which testing is embedded in business-as-usual operations and governance.

Maturity Levels

Level 1: Initial

Exercises are ad hoc and infrequent, with limited scope and methodology. They are primarily discussion-based, with minimal evidence collection. There is also limited connection to business services or regulatory requirements.

Level 2: Developing

Exercises are regular but still relatively infrequent, using basic methodology. Some standardization exists in approach and documentation. Evidence collection is limited, focusing on process verification rather than empirical data.

Level 3: Defined

Established programme with consistent methodology and governance. Regular exercises cover major business services. There is a mix of discussion-based and limited technical testing. Evidence collection is standardized, with basic metrics.

Level 4: Managed

Comprehensive programme with high-frequency Microsimulations integrated into Business-as-Usual (BAU) operations.There is extensive coverage across all important services and dependencies. Evidence collection is strong, utilizing quantitative metrics, with a clear link to tolerances and regulatory requirements.

Level 5: Optimising

Sophisticated programme with a continuous improvement cycle. It features technology-enabled automation for evidence collection and analysis.There is comprehensive coverage with increasing technical depth. Integration with vendor and industry-wide testing is in place, and the programme includes predictive capabilities based on past exercise data.

Dimension	Level 1 Indicators	Level 3 Indicators	Level 5 Indicators
Methodology	Discussion-based only. Subjective assessment; no formal scenarios.	Structured scenarios. Mix of discussion & technical verification. Standardised approach.	Advanced technical testing. Automated verification. Intelligence-led scenarios; sophisticated injects.
Coverage	Limited to select high-profile services. Minimal third-party inclusion.	Covers major services & dependencies. Some third-party participation.	Comprehensive coverage of all services, dependencies, & third parties. Varied severity levels.
Evidence	Minimal documentation. Primarily qualitative observations.	Standardised evidence collection. Basic metrics; tolerance assessment.	Automated evidence collection. Comprehensive metrics; predictive analytics. Regulatory-ready evidence packs.
Integration	Siloed exercises. Limited connection to business operations.	Regular schedule; established governance. Basic BAU integration.	Fully embedded in operations. Continuous testing culture. Board-level visibility & engagement.
Improvement	Ad hoc follow-up. Limited tracking of issues.	Structured remediation process. Tracked actions with ownership.	Closed-loop verification. Trend analysis; predictive risk identification. Demonstrable improvement over time.

Common Challenges and Solutions

Resource Constraints

Challenge: Limited staff availability for exercise participation and facilitation, especially when attempting to increase testing frequency.

Solution:

- Implement a "minimum viable participation" model; allow asynchronous input for non-essential staff.
- Create a trained facilitator pool across departments.
- Use technology to streamline evidence collection and reporting.

Stakeholder Resistance

Challenge: Perception of exercises as disruptive, theoretical, or not adding value to busy operational teams.

Solution:

- Demonstrate direct business value by linking exercises to recent incidents
- Create "resilience champions" within business units.
- Produce actionable insights that solve real operational problems.
- Recognise and reward participation

Silo Mentality

Challenge: Difficulty coordinating across organisational boundaries, particularly with technology teams and third parties.

Solution:

- Establish cross-functional working groups with clear terms of reference.
- Create shared objectives and metrics that span organisational boundaries.
- Implement "resilience by design" principles in change management processes.
- Executive sponsorship of cross-silo collaboration.

Methodology Challenges

Scenario Design

Challenge: Developing scenarios that are both severe but plausible, avoiding unrealistic "doomsday" scenarios and overly simplistic tests.

Solution:

- Ground scenarios in actual incidents from within the organisation or industry.
- Use external threat intelligence to inform scenario design.
- Implement a severity classification framework with clear criteria.
- Ensure the risk function reviews scenarios for plausibility.

Evidence Quality

Challenge: Collecting objective, meaningful evidence rather than subjective assessments or theoretical capabilities.

Solution:

- Implement standardised evidence templates with specific artifacts for each exercise type.
- Use technology to automate evidence collection where possible.
- Require demonstration rather than assertion of capabilities.
- Have independent observers validate evidence quality.

Exercise Artificiality

Challenge: Exercises feeling contrived or participants finding unrealistic workarounds that wouldn't be available in real incidents.

Solution:

- Increase realism through unannounced elements, limited information, and actual system access (in test environments).
- Train facilitators in reality enforcement techniques.
- Incorporate recent real incidents into scenario design to enhance credibility.

Sustainability Challenges

Programme Fatigue

Challenge: Maintaining momentum and engagement over time, particularly after initial regulatory deadlines pass.

Solution:

- Vary exercise formats to maintain interest.
- Celebrate successes and improvements.
- Link programme to actual incident reduction and service improvements.
- Refresh scenarios regularly with current threats.

Remediation Follow-Through

Challenge: Ensuring identified issues are actually fixed rather than just documented and tracked.

Solution:

- Implement a closed-loop verification for remediation effectiveness.
- Include remediation metrics in executive reporting.
- Retest specific issues in subsequent exercises.
- Link remediation completion to performance objectives.

Evolving Regulation

Challenge: Adapting the programme to keep pace with changing regulatory expectations across multiple jurisdictions.

Solution:

- Establish a regulatory horizon scanning process.
- Design the programme for flexibility with modular components.
- Maintain relationships with supervisors to understand direction.
- Participate in industry working groups on resilience.

Operationalising Microsimulations with iluminr

Scenario Studio

Curate and tag Microsimulations to critical services, vendors, and tolerances.

Manage a comprehensive library of scenarios with version control and reusability.

One-Click Runs

Launch injects, capture run-sheets, timestamps, and communications automatically.

Streamline exercise execution with guided workflows and artifact management.

Evidence Pack

Generate exportable dossiers per jurisdiction with mapped requirements.

Standardise evidence collection and presentation.

Analytics

Monitor tolerance compliance, heatmaps, and vendor performance.

Visualise trends, patterns, and time-to-recover metrics across exercises.

Technology Benefits

Efficiency Gains

- **Time savings:** Automate manual tasks like evidence collection and report generation.
- **Resource optimisation:** Enable smaller teams to manage comprehensive programmes.
- **Standardisation:** Ensure consistent approach across different business units and geographies.
- **Reusability:** Create modular scenarios and evidence templates for repurposing.

Quality Improvements

- **Evidence rigour:** Capture objective, timestamped evidence automatically.
- **Comprehensive metrics:** Calculate complex metrics consistently across all exercises.
- **Pattern recognition:** Identify trends and systemic issues across multiple exercises.
- **Regulatory alignment:** Map evidence directly to specific regulatory requirements.

Implementation Best Practices

01

Start with Core Capabilities

Begin with essential functionality like scenario management and evidence collection before expanding to advanced analytics.

02

Integrate with Existing Systems

Connect with incident management, risk, and communication platforms to leverage existing investments and streamline workflows.

03

Train Facilitators

Develop a pool of trained facilitators who can effectively use the technology to run engaging, evidence-rich exercises.

04

Iterative Enhancement

Continuously refine the technology implementation based on user feedback and evolving programme requirements.

Governance Framework

Technology platforms should support robust governance of the Microsimulation programme:

- **Approvals workflow:** Structured process for scenario approval, scheduling, and evidence validation.
- **Waivers management:** Track exceptions with justification and time limits.
- **Tracking learnings:** Comprehensive database for identified issues, remediation actions, and verification.

Final Word: From Event to Capability

> Across regions, supervisors want continuous, evidenced, severe-but-plausible testing that matures over time.
>
> Microsimulations are the only scalable way to meet that bar—turning resilience from a once-a-year event into a **measurable operating capability**.

Technology enablement is key to this transformation, making Microsimulations sustainable, evidence-rich, and truly embedded in business-as-usual operations.

By implementing purpose-built technology platforms, firms can satisfy regulatory expectations while building genuine resilience capabilities that protect customers, preserve market integrity, and safeguard the organisation's future.

Through the consistent application of Microsimulations, supported by technology such as iluminr, operational resilience evolves from a compliance exercise into a strategic advantage.

This capability allows the organisation to adapt, respond, and thrive in an increasingly complex and uncertain operational environment.