

ENTREPRENEURSHIP LIBRARY · VOLUME 3

Bad-Week Resilience Pack_____

Fragility, recovery, absence, cash, exits, and a 90-day build.

Gaurav Tiwari

Companion to *Built for Bad Weeks*

Run one plausible shock at a time. Protect the essential promise and evidence. Use qualified professional support for security, privacy, employment, insurance, tax, finance, and legal obligations.

Contents

Bad-Week Test Deck	3
Fragility Map	5
Founder-Absence Rehearsal	7
Downside Cash Scenarios	9
Platform and Vendor Exit Checklist	11
90-Day Resilience Plan	13

Bad-Week Test Deck

Run each scenario separately. Rewrite it with a duration and measurable effect.

- ☐ Largest customer leaves or pauses.
- ☐ Founder is unavailable for 2 weeks.
- ☐ Primary acquisition route loses half its qualified demand.
- ☐ Critical supplier fails during active commitments.
- ☐ Largest expected payment is 45 days late.
- ☐ Demand doubles for 6 weeks.
- ☐ A serious defect affects an identifiable batch.
- ☐ A key contractor or employee is suddenly absent.
- ☐ A critical account or dataset becomes unavailable.
- ☐ A rule, platform term, or cost changes materially.

Precise shock	
First affected promise	
Detection signal and time	

Containment	
Minimum service	
Restoration and evidence	
Learning decision	

Fragility Map

Dependency	Share	Impact	Detection	Recovery / decision
Customer				
Offer				
Channel				
Platform				
Supplier				
Expertise				
Cash timing				
Access / data				

Founder-Absence Rehearsal

Work / decision	Stops after	Authorized owner	Missing condition
Customer communication			
Sales promise			
Delivery review			
Payments / payroll			
Supplier decision			
System access			
Incident response			

Deadline / compliance			
-----------------------	--	--	--

Day 1, week 1, and month 1 changes

Downside Cash Scenarios

Assumption	Base	Downside	Immediate stress
Available cash			
Committed inflow			
Likely inflow			
Essential obligations			
Restoration cost			
Decision time			
Action floor			

Reserve job, authority, and rebuild rule

Platform and Vendor Exit Checklist

- ☐ Record the exact jobs the platform or vendor performs.
- ☐ Confirm data ownership, export format, and export completeness.
- ☐ Preserve customer permissions and contractual records.
- ☐ Identify shared identity, region, payment, and infrastructure dependencies.
- ☐ Review notice, termination, retention, and deletion terms.
- ☐ Identify an authorized alternative and qualification requirements.
- ☐ Time an export, import, restore, or supplier trial.
- ☐ Define minimum service during migration.
- ☐ Assign customer communication and decision authority.
- ☐ Record assets, reviews, history, or functionality that cannot transfer.
- ☐ Protect confidential, personal, and regulated information.
- ☐ Set the trigger, budget, and last safe migration date.

Exit decision and remaining exposure

90-Day Resilience Plan

Window	Required result	Evidence / owner
Days 1–15	Promise, fragility map, 3 bad-week tests, priority	
Days 16–35	Minimum service, containment, access, buffer	
Days 36–60	Decision rights, handoff, backup capability	
Days 61–75	Rehearsal and measured recovery gaps	
Days 76–90	Repairs, repeat evidence, accepted exposure	

Resilience budget

Next review date and change trigger

Protect the promise.

Measure the return.