

THE GRAVITY RESTAURANT LEADERSHIP SYSTEM



The Gravity Risk & Continuity System

One coordinated operating system for anticipating disruption, protecting people, continuing critical work, and recovering with control.

OPERATING MANUAL

Published by Thomas Monroe Books
Author: Thomas Butler

Publishing and Use Notice

Copyright 2026 Thomas Monroe Books. All rights reserved. The Gravity Risk & Continuity System is the operational risk, preparedness, [incident](#), continuity, [recovery](#), and restart layer of The Gravity Restaurant Leadership System.

This product is an operational education and management resource. It is not legal, regulatory, employment, fire, building, food-safety, emergency-management, medical, cybersecurity, accounting, insurance, financial, or other professional advice. Requirements, hazards, facilities, contracts, and public instructions vary by location and change over time. Obtain [qualified review](#) and use the applicable authorities, emergency services, insurer, landlord, utilities, vendors, and regulators when required.

LIFE-SAFETY RULE Immediate danger and public-authority instructions override internal plans. Call 911 or the applicable local emergency service. Do not delay evacuation, emergency reporting, medical aid, food protection, or other required action to complete a form.

Restricted information

Do not place passwords, alarm codes, full payment-card data, protected personal data, sensitive security weaknesses, medical details, or [evidence](#) that requires restricted handling in broadly distributed forms. Reference the approved secure [record](#) instead.

Inside This Guide

Part I	Architecture, roles, risk method, activation, and decision rights
Part II	Critical operations, dependencies, emergency plans, and continuity strategies
Part III	Incident command, communications, recovery, technology, and restart
Part IV	Testing, scorecards, implementation , workbook, tools, and official references

The Management Problem This System Solves

Restaurant disruptions cross departments faster than separate binders can respond. A power failure can become a food-safety, payment, staffing, guest-communication, insurance, and restart problem at the same time. Risk records, emergency SOPs, backup leaders, technology recovery, and reopening approvals often exist in different places or only in one manager's memory.

CENTRAL PURPOSE GRV-RC creates one management path from a recognized risk to prevention, safe response, minimum operations, controlled recovery, verified restart, learning, and renewal.

The continuity loop

1. Identify and prioritize the scenario.
2. Map the critical work and dependencies it can interrupt.
3. Prepare life-safety actions, roles, contacts, workarounds, and recovery targets.
4. Activate the correct plan and maintain one decision record.
5. Recover in priority order and reopen only through defined gates.
6. Test, learn, correct, verify, and renew.

What this system consolidates

- Enterprise operational risk, continuity, emergency planning, crisis communication, backup leadership, disaster recovery, restart, exercises, and [corrective action](#).
- References to approved emergency SOPs, including power outage, severe weather, fire, utility, food-safety, facility, and technology procedures.
- The management records needed to connect the response across the complete Gravity System.

1. Architecture and Boundaries

Thirty tools are organized into six operating areas. GRV-RC coordinates the risk-to-recovery lifecycle; it does not replace task-level emergency SOPs or the source records owned by another system.

SYSTEM IDENTITY Use GRV-RC01 through GRV-RC30 as the stable tool family. GRV-R remains the customer-relationship-management family.

Six areas

- Risk Governance & Prioritization — GRV-RC01–05
- Critical Operations & Dependencies — GRV-RC06–10
- Preparedness & Emergency Response — GRV-RC11–15
- Continuity & Role Coverage — GRV-RC16–20
- Recovery & Restart — GRV-RC21–25
- Testing, Learning & Renewal — GRV-RC26–30

Boundary with GRV-I

- GRV-RC owns operational scenarios, emergency [readiness](#), continuity strategies, incident records, recovery, restart, and drills.
- GRV-I owns source [authority](#), controlled versions, evidence rules, external intelligence, formal change [control](#), and enterprise system health.
- Material cyber, vendor, privacy, accessibility, food-safety, or regulatory risk identified in GRV-I is handed to GRV-RC as an operational scenario when continuity preparation is needed.

Boundary with the SOP Library

- The SOP Library provides approved step-by-step actions for defined emergencies.
- GRV-RC identifies which SOP activates, who coordinates it, what connected systems are affected, what decisions are recorded, and how recovery is verified.
- When a procedure conflicts with official instructions, the applicable authority and qualified decision control.

2. Governance, Roles, and Incident Authority

Preparedness fails when every person is responsible in theory and nobody is authorized in practice.

MANAGER-ON-DUTY RULE When the designated incident lead is unavailable, the manager on duty protects life, calls emergency services, starts the approved location plan, and initiates the succession path.

Owner or executive sponsor

- Approves [risk appetite](#), major continuity investments, closure or reopening authority, and annual renewal.
- Secures professional, regulatory, insurance, legal, technical, or emergency-management review when needed.

General manager or continuity lead

- Maintains the program, risk register, critical operations, plans, contacts, tests, and corrective actions.
- Ensures alternates can assume authority and receive the minimum information needed.

Incident lead

- Protects life, establishes current objectives, assigns response functions, maintains a common operating picture, and schedules decision checkpoints.
- Transfers command clearly and records the handoff.

Functional leads

- Safety/operations manages immediate operating actions.
- Planning/information maintains facts, status, forecasts, and records.
- Logistics/resources obtains people, facilities, equipment, suppliers, and support.
- Finance/documentation records costs, claims, time, approvals, and retained evidence.
- Communications manages approved messages and stakeholder updates.

Decision separation

- Only trained and authorized people perform hazardous shutdown, rescue, medical, fire, electrical, gas, technology, food-disposition, or security work.

- The person who reports a signal may not have authority to close, reopen, destroy product, notify media, accept [residual risk](#), or authorize spending.

3. Risk Method and Prioritization

The system uses a consistent five-by-five management screen, then requires judgment about consequence, controls, uncertainty, speed, and authority.

RISK FORMULA Inherent score = likelihood × impact before considering the strength of current controls. Residual rating states the exposure remaining after those controls; it must be justified, not mechanically reduced.

Likelihood scale

- 1 Rare — not expected under current conditions
- 2 Unlikely — possible but limited evidence
- 3 Possible — credible and may occur
- 4 Likely — repeated signals or known exposure
- 5 Almost certain — occurring, imminent, or routinely experienced

Impact scale

- 1 Minimal — short disruption within normal management
- 2 Minor — limited service, cost, or recovery burden
- 3 Material — significant interruption, guest, people, financial, or authority involvement
- 4 Severe — extended closure, serious loss, major safety, legal, or reputation consequence
- 5 Critical — life safety, catastrophic loss, broad crisis, or viability threat

Score bands

- 1–4 Low — maintain controls and scheduled review
- 5–9 Moderate — named owner and improvement where justified
- 10–16 High — planned treatment, management review, and continuity preparation
- 17–25 Critical — immediate [escalation](#), containment or closure when required, and executive oversight

Do not average away consequence

- A low-[frequency](#) life-safety scenario can still require a plan.
- Uncertainty may justify more caution, not a lower rating.

- A score is a prioritization aid, not a prediction, guarantee, certification, or substitute for a controlling threshold.

4. Risk Appetite, Escalation, and Activation

A usable escalation matrix translates concern into observable thresholds and decisions.

Risk response choices

- Avoid — stop or do not begin the activity
- Reduce — lower likelihood, impact, or recovery time
- Transfer/share — insurance, contract, service provider, or structured partnership
- Accept — within approved appetite with an owner and review date
- Exploit/prepare — for an opportunity created by the disruption

Activation levels

- Level 0 Monitor — normal controls and observation
- Level 1 Local disruption — manager coordinates within the location
- Level 2 Significant incident — continuity lead and functional roles activate
- Level 3 Crisis — executive coordination, external authorities/support, and formal communications activate

Immediate escalators

- Actual or threatened loss of life, fire, violence, gas leak, structural danger, serious injury, uncontrolled contamination, or public emergency instruction
- Uncontrolled closure, material data or payment compromise, major utility failure, large product withdrawal, or inability to account for people
- A condition beyond local authority, competence, resources, or approved risk appetite

Deactivation

- Define who may stand down the incident structure.
- Record remaining restrictions, recovery ownership, communication duties, and monitoring.
- Deactivation is not the same as full recovery or final closure.

5. Critical Operations and Business Impact Analysis

Continuity planning starts with the minimum outcomes that must be protected or restored—not with a list of every task.

PRIORITY RULE Restore the functions that protect life, lawful operation, food safety, people, critical communications, and cash control before convenience or full capacity.

Critical-operation test

- Does failure create immediate safety or food-safety risk?
- Does failure prevent lawful operation, payment, payroll, communication, access, or required records?
- Does the impact grow rapidly with time?
- Can another location, role, system, supplier, or manual process carry the function?

Impact lenses

- Life and food safety
- Guests and service
- Employees and leadership
- Financial and cash flow
- Legal, regulatory, contract, insurance, and license
- Reputation and stakeholder trust

Time targets

- [Maximum tolerable downtime](#) states the longest disruption management believes the function can sustain before unacceptable impact.
- Recovery time [objective](#) ([RTO](#)) states the target time to restore a function or service.
- Recovery point objective ([RPO](#)) states the maximum tolerable data-loss period for a system or record.
- These are planning targets, not service guarantees; test and revise them with business and technical owners.

6. Dependencies, Suppliers, Utilities, and Single Points of Failure

A critical function is only as recoverable as the weakest resource it depends on.

Dependency categories

- People and authority
- Facility, access, equipment, refrigeration, and fire/life-safety systems
- Electricity, gas, water, wastewater, telecommunications, and fuel
- POS, payments, internet, payroll, scheduling, accounting, inventory, reservations, delivery, and communications
- Food, packaging, cleaning, repair, security, waste, transportation, and professional services
- Data, records, credentials, contracts, permits, and approved procedures

Single-point test

- Only one person knows the process or holds the authority.
- Only one supplier, route, device, circuit, file, login owner, or communication channel exists.
- A workaround exists on paper but has not been timed, supplied, trained, or tested.
- The backup depends on the same power, network, building, vendor, or person as the primary method.

Treatment

- Remove the [dependency](#) where practical.
- Create independent redundancy or alternate supply.
- Create a safe manual process with capacity and duration limits.
- Reduce restoration time through spares, contacts, contracts, access, and evidence.
- Accept only through the approved risk path.

7. Emergency Action and Life Safety

The location emergency action plan must be specific enough to act on immediately and aligned with applicable workplace, fire, building, health, and public-safety requirements.

OSHA NOTE 29 CFR 1910.38 provides federal emergency-action-plan requirements when an OSHA [standard](#) requires a plan; state plans or other authorities may add requirements. Qualified review determines applicability.

Core plan elements

- Methods for reporting fire and other emergencies
- Emergency evacuation, routes, exits, and assignments
- Critical operations that designated employees perform before evacuation, when safe and authorized
- Accountability after evacuation
- Rescue and medical duties for designated employees
- Name or job title for plan questions

Evacuation discipline

- Use approved alarms, primary and alternate routes, assembly areas, and accountability methods.
- Plan for guests, visitors, contractors, accessible evacuation, communication needs, and employees requiring assistance.
- Never direct untrained employees to fight fires, enter a danger area, perform rescue, or operate hazardous controls.
- Reentry occurs only when the applicable authority or authorized qualified person permits it.

Plan access and training

- Keep the current plan available where employees can use it.
- Train assigned roles, new employees, affected employees after a plan change, and employees whose responsibilities change.
- Walk routes and assembly areas whenever the facility or occupancy changes.

8. Severe Weather, Fire, Utility, and Facility Emergencies

Scenario plans convert official alerts and approved SOPs into coordinated management decisions.

PROCEDURE LINK GRV-RC14 coordinates the incident. The approved Power Outage, Tornado/Severe Weather, Fire, Utility, Facility, and related SOPs control task-level action.

Severe weather

- Use official National Weather Service and local emergency-management alerts.
- Define the difference between monitoring, watch, warning, shelter, closure, and all-clear actions.
- Identify protected interior locations, accessible routes, capacity, supplies, communication, and accountability.

Fire and facility danger

- Report, alarm, evacuate, account, and call emergency services according to the approved plan.
- Limit shutdown activity to trained, designated, and safe actions.
- Restrict access until the applicable authority or qualified inspector releases the area.

Power, water, gas, refrigeration, and HVAC

- Use the approved SOP Library procedures and utility contacts.
- Stop unsafe equipment and protect refrigeration without unnecessary opening.
- Set closure thresholds for lighting, ventilation, temperature control, safe water, sanitation, payment, fire protection, and occupancy.
- Verify utilities, equipment, food condition, technology, and authority [approval](#) before restart.

9. Food Safety, Contamination, and Product Withdrawal

Food emergencies require fast control, accurate traceability, approved authority contact, and protected evidence.

First controls

- Stop sale, preparation, service, or use when required.
- Isolate affected food and prevent accidental disposal or return until authorized.
- Record item, supplier, lot/date, quantity, location, service/distribution, temperature or condition, and who controlled it.
- Preserve relevant labels, records, photos, samples, and communications securely.

Authority and disposition

- Follow the applicable health department, recall notice, supplier, FDA/USDA, insurer, legal, and approved food-safety instructions.
- FDA Food Code is a model; the adopted state/local code and authority control.
- Consumer power-outage time charts are not a substitute for a restaurant's approved regulatory policy.

Reopening

- Correct the cause and complete cleaning, sanitizing, equipment, water, temperature, inventory, training, and authority requirements.
- Use the phased restart gates and document the person authorized to release the operation.

10. Continuity Strategy and Minimum Operations

Continuity is not full normal service under abnormal conditions. It is the safest approved level of essential work the restaurant can sustain.

Strategy options

- Continue through redundant resources
- Operate at reduced menu, hours, channels, volume, or locations
- Relocate work or use an alternate site
- Use a controlled manual process
- Transfer work to another location or approved provider
- Suspend and protect assets until safe recovery

Minimum-operations design

- State the exact functions and output to continue.
- Define minimum staffing, leadership, utilities, facility conditions, equipment, suppliers, technology, payment, records, and communication.
- State capacity, duration, quality, safety, data, cash, access, and approval limits.
- Define stop conditions and the handoff to recovery.

Tradeoff rule

- Do not preserve sales by accepting uncontrolled life-safety, food-safety, wage, payment, privacy, security, cash, or license risk.
- A manual process must include reconciliation, record retention, access, fraud, and error controls.

11. Backup Leadership, Staffing, and Contact Trees

Role coverage is a continuity control, not merely a phone list.

Backup leadership

- Name at least one trained alternate for each essential decision role and a second alternate where the consequence justifies it.
- State authority limits, spending, closure, communication, system access, records, contacts, and handoff expectations.
- Test the alternate in a scenario; availability alone does not prove readiness.

Emergency staffing

- Define the minimum safe roles for each continuity mode.
- Address transport, access, scheduling, timekeeping, payroll, rest, communication, and reasonable accommodation through approved processes.
- Do not pressure employees to enter unsafe conditions or disclose unnecessary medical information.

Contact tree

- Collect only permitted contact information, state the emergency purpose, protect access, and verify it regularly.
- Use more than one channel and set a time for failed-contact escalation.
- Keep public, internal, restricted, and personal-contact versions separate where needed.

12. Crisis Communication

Communication is a control when it moves verified facts, safety instructions, decisions, and next updates to the right audience.

COMMUNICATION RULE Speed matters, but an invented answer can create a second crisis. Say what is known, what action people should take, and when the next verified update will arrive.

Audience map

- Employees and backup leaders
- Guests, reservations, event contacts, loyalty members, and delivery customers
- Emergency services, regulators, health authorities, utilities, landlord, insurer, counsel, and vendors
- Suppliers, lenders, payment partners, community, media, and social channels

Message standard

- State what is verified and what is not known.
- Lead with safety action, service status, and the next update time.
- Use an approved spokesperson and channel.
- Protect privacy, investigations, security, employee information, claims, and legal review.
- Correct material errors quickly and retain the approved record.

Prepared messages

- Create short holding statements for closure, delay, severe weather, utility loss, technology/payment outage, food-safety event, and phased reopening.
- Customize them only with verified facts and current approved contacts.
- Provide accessible and language-appropriate communication when needed.

13. Incident Command and Decision Records

A scalable incident structure keeps objectives, roles, resources, facts, decisions, and handoffs visible as the event changes.

ICS BASIS The system adapts the scalable principles of FEMA's Incident Command System for restaurant management. It does not present Gravity certification or replace jurisdictional incident command.

First operational period

- Protect life and call emergency services.
- Name the incident lead and activation level.
- State the incident facts, uncertainties, current objective, affected area, restrictions, and next checkpoint.
- Assign only the functions needed; one person may hold several roles in a small incident.

Decision log

- Record date/time, verified fact or assumption, decision, authority, reason, responsible owner, communication, and next review.
- Correct the record without deleting the history.
- Reference sensitive evidence by secure location rather than copying it broadly.

Handoff

- Brief current conditions, life-safety status, objectives, risks, people, resources, external contacts, communications due, finances, and open decisions.
- The incoming lead acknowledges the transfer and the outgoing lead records the time.

14. Technology, Data, Payment, and Disaster Recovery

Technology recovery must restore a trustworthy business capability, not merely power on a device.

BACKUP RULE A backup is not verified until an authorized restore test demonstrates usable data and a documented business acceptance result.

Before disruption

- Assign business and technical owners for POS, payments, internet, reservations, delivery, payroll, scheduling, accounting, inventory, communications, access, and critical data.
- Maintain offline or otherwise resilient, protected backups appropriate to the risk.
- Record RTO, RPO, integration order, manual method, vendor contacts, access, [validation](#), and last restore test.

During disruption

- Contain suspected compromise and preserve evidence before reconnecting systems.
- Use only approved offline/payment/manual procedures and capacity limits.
- Reconcile transactions, refunds, tips, deposits, inventory, payroll, and duplicated records after restoration.

Recovery sequence

- Authorize the recovery and select a clean source.
- Restore in business priority order.
- Validate data integrity, permissions, integrations, payment, security monitoring, and reporting.
- Obtain business-owner acceptance and document exceptions.

15. Damage, Loss, Insurance, and Recovery Finance

Early documentation protects decisions, claims, cash, and accountability while avoiding unsafe entry or speculative estimates.

Initial assessment

- Enter only when emergency services, the authority having jurisdiction, and qualified facility leadership permit access.
- Record people impact, operational interruption, facility/equipment, food/inventory, technology/data, records, cash/payment, and immediate protection needs.
- Use dated photos, reports, inventories, invoices, schedules, payroll, and communications where approved.

Financial control

- Separate lost revenue, spoiled inventory, property damage, repairs, extra expense, payroll, refunds, professional services, deductibles, and recoveries.
- Assign approval, accounting, claim, and record-retention owners.
- Do not treat rough estimates as final accounting or insurance coverage determinations.

External support

- Meet required notice periods for insurers, landlords, utilities, lenders, franchises, regulators, contracts, and grants.
- Do not sign releases, authorize disposal, or commit to repairs beyond delegated authority.

16. Phased Restart and Reopening

Restart is a controlled risk decision. Passing one gate does not waive another.

REOPENING RULE A revenue target never substitutes for a passed safety, authority, food, people, facility, utility, technology, or control gate.

Restart gates

- Life safety and facility released
- Fire, building, health, utilities, insurer, landlord, or other authority requirements addressed
- Water, power, gas, ventilation, refrigeration, sanitation, and equipment verified
- Food disposition, deliveries, inventory, and supplier status controlled
- Leadership, staffing, training, communication, and access ready
- Technology, payment, data, cash, security, and reconciliation ready

Phases

- Protect and assess
- Limited internal recovery
- Controlled test or soft opening
- Reduced public operation
- Expanded operation
- Full operation with post-restart monitoring

Rollback

- Define conditions that stop or reduce the restart.
- Maintain an incident or recovery lead during the monitoring period.
- Record open restrictions, temporary controls, next checkpoints, and final close criteria.

17. Exercises, Drills, and After-Action Learning

Testing turns assumptions into evidence before a real disruption exposes them.

NO-FAULT LEARNING RULE Evaluate the system and observable decisions first. Accountability remains necessary, but blame-driven exercises hide the conditions the business needs to correct.

Progressive testing

- Contact [verification](#)
- Document and equipment walk-through
- Tabletop discussion
- Notification or evacuation drill
- Manual-workaround test
- Backup restore test
- Functional continuity or restart exercise

Exercise safety

- State objectives, [scope](#), participants, facilitator, evaluators, assumptions, and stop rules.
- Never create real hazards, confuse the public, interfere with emergency services, or test destructive actions without specialist control.
- Clearly separate exercise messages from real emergency messages.

After-action review

- Compare expected and actual decisions, time, roles, communication, workaround capacity, recovery, evidence, and outcome.
- Identify strengths, gaps, contributing conditions, and system-level causes.
- Convert approved lessons into assigned corrective actions, controlled document updates, training, and retests.

18. Readiness Scorecard and Review Cadence

The dashboard should expose weak readiness before an incident, not merely count completed forms.

SCORE DISCIPLINE A readiness score is an internal management signal, not proof of compliance, safety, insurance coverage, cybersecurity, or guaranteed recovery.

Readiness dimensions

- Risk ownership
- Life safety and emergency plans
- Critical operations and dependencies
- People and backup leadership
- Suppliers and utilities
- Technology and data
- Crisis communication
- Recovery and restart
- Testing and learning

Monthly

- Review critical/high risks, overdue reviews and actions, contact currency, backup leaders, incidents, and readiness exceptions.
- Verify at least one high-value control or dependency rather than relying only on self-report.

Quarterly

- Review critical operations, suppliers/utilities, minimum operations, communications, technology recovery, scorecard, and one exercise or test.

Annual and urgent

- Renew the full risk picture, business impact analysis, emergency action plans, role coverage, insurance/support, restart gates, exercises, and roadmap.
- Review immediately after an incident, [material change](#), new location, remodel, system/vendor change, authority notice, severe near miss, or failed test.

19. Connections to the Complete Gravity System

GRV-RC works through the existing owners and records rather than creating a second version of operating truth.

GRV-L Leadership

- Leadership accountability, delegation, communication, and manager rhythm flow into risk ownership and incident authority.
- GRV-RC owns emergency succession and backup activation records.

GRV-T Training

- GRV-T owns assigned training, completion, [competency](#), and refresher records.
- GRV-RC owns exercise objectives, scenario performance, response-role coverage, and continuity test results.

GRV-C Cost Control

- Supplies staffing and labor-continuity data; receives disruption labor, overtime, and staffing impacts.

GRV-S Service

- Supplies guest-safety, service, complaint, recovery, and communication procedures; receives continuity modes and approved guest messages.

GRV-F Food

- Supplies food-safety, temperature, traceability, disposition, waste, inventory, and supplier records; receives incident and reopening requirements.

GRV-R CRM

- Supplies permission-based guest communication channels and suppression/preferences; does not become a public emergency-alert system unless approved for that purpose.

GRV-P Performance

- Supplies financial impact, cash, margin, break-even, recovery economics, and restart performance.

GRV-I Standards & Intelligence

- Supplies controlling sources, monitored changes, versions, evidence rules, and formal change control; receives after-action and renewal changes.

20. Digital Workbook Operating Standard

The workbook is the living coordination layer for management review. It is not the official source for every operational, HR, financial, payment, security, or claim record.

Start

- Read Start Here and complete Settings.
- Enter a small, verified test set in Risk Register, Critical Operations, Dependencies, Role Coverage, Plans, Actions, and Review Calendar.
- Open Checks and correct missing dates, owners, IDs, targets, or links before relying on Dashboard.

Use

- Yellow cells with blue text are manager inputs.
- Cream or white cells with dark text contain formulas, controlled labels, or linked results.
- Use stable IDs to connect risks, functions, dependencies, plans, incidents, recovery tasks, exercises, and actions.
- Store restricted source evidence in approved systems and enter only the secure reference.

Review

- Start with critical/high risks, overdue plan reviews, missing alternates, single points, untested backups, open incidents, overdue actions, and restart restrictions.
- Open the underlying rows before deciding.
- Assign no more priorities than the operation can complete and verify.

21. Installation and 90-Day Rollout

Install the system in a sequence that protects the highest consequences first and uses existing approved procedures.

INSTALLATION GATE The system is installed when leaders can identify the current risk, activate the right plan, transfer authority, continue or stop critical work safely, recover in priority order, pass restart gates, and prove that lessons become verified change.

Days 1–30: establish control

- Assign owner, incident succession, risk appetite, activation levels, and monthly review.
- Register top risks, critical operations, essential dependencies, current emergency plans, contacts, backup leaders, insurance, and external support.
- Link the final approved SOP Library procedures and verify their location/version through GRV-I.

Days 31–60: build continuity

- Complete business impact analysis for the most critical functions.
- Approve minimum operations, role coverage, supplier/utility alternatives, crisis communication, technology recovery, and initial restart gates.
- Correct the most material life-safety, food-safety, access, contact, or single-point gaps.

Days 61–90: prove readiness

- Run one tabletop exercise, one notification/role-coverage test, and one high-value operational or technology recovery test.
- Complete the after-action review, scorecard, corrective action verification, and first management review.
- Approve the next 180-day roadmap with three priorities and defined proof.

22. Complete GRV-RC Tool Directory

Official tool IDs remain stable when approved form versions change. GRV-I controls the version and current master.

Tool	Area / owner / frequency	Tool	Area / owner / frequency
GRV-RC01 Enterprise Risk Register	Risk Governance & Prioritization Owner/GM Monthly and at change	GRV-RC16 Continuity Strategy & Minimum Operations Plan	Continuity & Role Coverage Owner/GM Quarterly
GRV-RC02 Risk Appetite & Escalation Matrix	Risk Governance & Prioritization Owner/GM Annual and at change	GRV-RC17 Backup Leadership & Role Coverage Plan	Continuity & Role Coverage Owner/GM Monthly
GRV-RC03 Risk Ownership & Accountability Map	Risk Governance & Prioritization Owner/GM Quarterly	GRV-RC18 Emergency Staffing & Contact Tree	Continuity & Role Coverage GM/People Lead Monthly and at change
GRV-RC04 Critical Incident Threshold & Activation Guide	Risk Governance & Prioritization GM/Incident Lead Quarterly and after incident	GRV-RC19 Crisis Communication & Stakeholder Plan	Continuity & Role Coverage Owner/Communications Lead Quarterly
GRV-RC05 Insurance, Contract & External Support Register	Risk Governance & Prioritization Owner/Finance Lead Quarterly	GRV-RC20 Alternate Site, Manual Workaround & Resource Plan	Continuity & Role Coverage Operations Lead Quarterly
GRV-RC06 Critical Operations Inventory	Critical Operations & Dependencies GM/Operations Lead Quarterly	GRV-RC21 Incident Command & Decision Log	Recovery & Restart Incident Lead Per incident
GRV-RC07 Business Impact Analysis	Critical Operations & Dependencies GM/Finance Lead Annual and at change	GRV-RC22 Damage, Loss & Initial Recovery Assessment	Recovery & Restart Incident/Finance Lead Per incident
GRV-RC08 Dependency & Single-Point-of-Failure Map	Critical Operations & Dependencies Operations Lead Quarterly	GRV-RC23 Technology/Data Disaster Recovery Runbook	Recovery & Restart Technology Lead Every 6 months and at incident
GRV-RC09 Critical Supplier & Utility Continuity Review	Critical Operations & Dependencies Operations/Purchasing Quarterly	GRV-RC24 Phased Restart & Reopening Plan	Recovery & Restart Owner/GM Per restart and annual drill
GRV-RC10 Technology, Data & Payment Recovery Requirements	Critical Operations & Dependencies Technology/Finance Lead Quarterly	GRV-RC25 Recovery Financial & Documentation Log	Recovery & Restart Finance Lead Per incident through closure
GRV-RC11 Emergency Action Plan	Preparedness & Emergency Response GM/Safety Lead Annual and at change	GRV-RC26 Tabletop Exercise Planner	Testing, Learning & Renewal Continuity Lead Quarterly
GRV-RC12 Life Safety & Evacuation Plan	Preparedness & Emergency Response Safety Lead Every 6 months and at change	GRV-RC27 Continuity Test & Drill Evaluation	Testing, Learning & Renewal Independent Evaluator Per exercise
GRV-RC13 Severe Weather & Shelter Plan	Preparedness & Emergency Response Manager on Duty Seasonally and after drill	GRV-RC28 After-Action Review	Testing, Learning & Renewal Incident/Exercise Lead Within 10 business days
GRV-RC14 Fire, Utility Loss & Facility Emergency Plan	Preparedness & Emergency Response Manager on Duty Every 6 months	GRV-RC29 Corrective Action & Readiness Scorecard	Testing, Learning & Renewal Owner/GM Monthly
GRV-RC15 Food Safety, Contamination & Product Withdrawal Response	Preparedness & Emergency Response Food Safety Lead Quarterly and at incident	GRV-RC30 Annual Risk & Continuity Renewal & 180-Day Roadmap	Testing, Learning & Renewal Owner/GM Annual with 180-day reset

23. Official Source References

Official sources and adopted local requirements must be rechecked because pages, editions, authorities, guidance, and effective dates change. Accessed August 10, 2026.

Reference	Official URL
Ready.gov Ready Business	https://www.ready.gov/business
Ready.gov Emergency Plans	https://www.ready.gov/business/emergency-plans
Ready.gov Business Continuity Planning	https://www.ready.gov/business/emergency-plans/continuity-planning
Ready.gov Emergency Response Plan	https://www.ready.gov/business/emergency-plans/emergency-response-plan
Ready.gov Crisis Communications Plans	https://www.ready.gov/business/emergency-plans/crisis-communications-plans
Ready.gov IT Disaster Recovery Plan	https://www.ready.gov/business/emergency-plans/recovery-plan
FEMA Continuity Resource Toolkit	https://www.fema.gov/emergency-managers/national-preparedness/continuity
FEMA Continuity Guidance Circular	https://www.fema.gov/emergency-managers/national-preparedness/continuity/documents
FEMA NIMS Components	https://www.fema.gov/emergency-managers/nims/components
FEMA Incident Command System	https://www.fema.gov/about/glossary/incident-command-system
FEMA National Disaster Recovery Framework	https://www.fema.gov/national-disaster-recovery-framework
OSHA Emergency Action Plan eTool	https://www.osha.gov/etools/evacuation-plans-procedures/eap
OSHA 29 CFR 1910.38	https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.38

Reference	Official URL
OSHA Tornado Preparedness	https://www.osha.gov/tornado/preparedness
NIST SP 800-34 Rev. 1	https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final
NIST Cybersecurity Framework 2.0	https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20
CISA Back Up Business Data	https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/back-up-business-data
CISA StopRansomware Guide	https://www.cisa.gov/stopransomware/ransomware-guide
FDA Food and Water Safety During Power Outages and Floods	https://www.fda.gov/food/buy-store-serve-safe-food/food-and-water-safety-during-power-outages-and-floods
FDA Food Code	https://www.fda.gov/food/fda-food-code
FDA Food Defense	https://www.fda.gov/food/food-defense
FoodSafety.gov Food Safety in a Disaster	https://www.foodsafety.gov/keep-food-safe/food-safety-in-disaster-or-emergency
SBA Manage and Recover Your Business	https://www.sba.gov/counseling/manage-your-business/
National Weather Service Safety	https://www.weather.gov/safety/
FINAL OPERATING STANDARD Protect life first, use the controlling authority, maintain one operating picture, continue only what can be controlled safely, recover in priority order, and do not reopen until the required gates pass.	

Linked Glossary

Select linked terms in the digital manual to move to their definitions. Definitions describe how the Gravity System uses each term; they do not replace qualified legal, regulatory, financial, safety, employment, or professional interpretation.

Accountable owner (GLOSS-001)

The person ultimately responsible for ensuring that a required result is achieved. Work may be assigned to others, but accountability remains with this person.

Action owner (GLOSS-002)

The person assigned to complete a specific action, provide the required evidence, and report its status by the due date.

Approval (GLOSS-005)

A documented decision by a person with the authority to accept, reject, release, or change a defined item.

Approved version (GLOSS-006)

The currently authorized form, standard, process, workbook, or document identified through version control.

Authority (GLOSS-009)

The legitimate right to make, approve, stop, escalate, or change a decision within defined limits.

Business continuity (GLOSS-016)

The planned ability to continue or restore critical restaurant operations during and after a disruption.

Closeout (GLOSS-018)

The documented decision that an action, issue, incident, or implementation is complete, including evidence, verification, date, and remaining follow-up.

Competency (GLOSS-020)

Demonstrated ability to perform a defined task or make a defined decision to the required standard under appropriate conditions.

Control (GLOSS-022)

A designed action, rule, approval, check, restriction, or record intended to prevent, detect, correct, or contain an unacceptable result.

Corrective action (GLOSS-026)

A documented response intended to eliminate, reduce, or control the cause of a confirmed problem, with an owner, due date, evidence, and effectiveness review.

Decision rights (GLOSS-029)

The defined boundaries identifying who may decide, approve, recommend, perform, stop, or escalate a matter.

Dependency (GLOSS-031)

A person, supplier, utility, system, facility, record, or resource required for an activity to operate successfully.

Escalation (GLOSS-034)

A controlled transfer of a decision or issue to a person with greater authority, expertise, or responsibility because a threshold, deadline, risk, or boundary has been reached.

Evidence (GLOSS-036)

Reliable information showing what occurred, what was decided, whether a requirement was met, or whether a result was achieved.

Exception (GLOSS-038)

An approved, limited, and time-bound departure from a standard, supported by authority, rationale, compensating controls, and review.

Exercise pass rate (GLOSS-039)

Exercises with overall objective Met / populated exercises.

Used primarily in: Risk & Continuity

Frequency (GLOSS-043)

The required completion rhythm for a control or tool, such as per event, daily, weekly, monthly, quarterly, annually, or when a defined change occurs.

Gravity standard (GLOSS-045)

An approved Gravity requirement or operating expectation that remains subordinate to applicable law, regulation, official authority, contract, and platform rules.

Implementation (GLOSS-047)

The controlled process of turning an approved goal or standard into configured tools, trained behavior, operating practice, evidence, verification, and sustainment.

Incident (GLOSS-048)

An event or condition that causes or could cause harm, disruption, loss, control failure, or an unacceptable operating result.

Inherent risk score (GLOSS-050)

Exposure before considering current control strength.

Used primarily in: Risk & Continuity

Material change (GLOSS-057)

A change significant enough to affect authority, risk, results, people, guests, systems, records, training, contracts, or operating controls.

Maximum tolerable downtime (GLOSS-059)

Longest interruption management believes can occur before impact becomes unacceptable.

Used primarily in: Risk & Continuity

Objective (GLOSS-063)

A specific result or condition that supports a larger goal and can be evaluated through defined evidence.

Qualified review (GLOSS-075)

Review by a person with the required professional knowledge, organizational authority, license, certification, or subject-matter responsibility.

Readiness (GLOSS-076)

Required fields and a current passing test are present according to workbook logic.

Used primarily in: Risk & Continuity

Record (GLOSS-080)

Retained information documenting an input, action, decision, approval, exception, result, or verification.

Recovery (GLOSS-081)

The controlled restoration of operations, technology, records, facilities, finances, staffing, or other capabilities after disruption.

Residual risk (GLOSS-083)

Exposure remaining after current controls.

Used primarily in: Risk & Continuity

Restart ready (GLOSS-084)

All nine restart gates Pass or Not Applicable.

Used primarily in: Risk & Continuity

Review cadence (GLOSS-086)

The approved schedule for examining a record, source, control, result, or standard and deciding whether action is required.

Risk appetite (GLOSS-087)

The amount and type of risk an authorized decision-maker is prepared to accept, reject, condition, or escalate.

RPO (GLOSS-090)

Maximum tolerable data-loss period.

Used primarily in: Risk & Continuity

RTO (GLOSS-091)

Target time to restore a function or service.

Used primarily in: Risk & Continuity

Scope (GLOSS-092)

The defined locations, roles, activities, records, time period, systems, and exclusions covered by a decision or implementation.

Single point of failure (GLOSS-094)

One dependency whose loss can stop the critical function without adequate alternative.

Used primarily in: Risk & Continuity

Standard (GLOSS-095)

An approved requirement or expectation used to guide work and evaluate conformance.

System owner (GLOSS-097)

The person accountable for the integrity, current version, controls, evidence, performance, and renewal of a defined system.

Trigger (GLOSS-100)

A defined event, condition, threshold, date, or signal that requires a tool, review, decision, action, or escalation.

Validation (GLOSS-102)

Confirmation that a design, requirement, tool, or method is appropriate for its intended purpose before or during use.

Verification (GLOSS-103)

A fact-based check confirming that a required action occurred and met the defined acceptance criteria.

Version control (GLOSS-104)

The method used to identify, approve, release, replace, archive, and trace changes to controlled materials.