THE GRAVITY RESTAURANT LEADERSHIP SYSTEM

The Gravity Standards & Intelligence Center

The control hub that keeps every Gravity standard current, connected, evidenced, and ready for change.

OPERATING MANUAL

Published by Thomas Monroe Books
Author: Thomas Butler

Publishing and Use Notice

Copyright 2026 Thomas Monroe Books. All rights reserved. The Gravity Standards & Intelligence Center is the system-wide governance and renewal layer of The Gravity Restaurant Leadership System.

This product is an operational education, governance, and management resource. It is not legal, regulatory, cybersecurity, privacy, accessibility, food-safety, accounting, insurance, human-resources, or technology advice. Laws, regulations, codes, contracts, platform rules, and official guidance change and vary by jurisdiction. Qualified professionals and the applicable government or regulatory authority must be consulted when required.

CONTROL RULE **The Center may identify a change signal and organize the response. It may not declare uncertain legal or technical requirements final without the proper authority and evidence.**

Inside This Guide

Part I	Architecture, governance, authority, documents, and version control
Part II	External intelligence, food safety, technology, law, and public signals
Part III	Cybersecurity, privacy, AI, vendors, accessibility, evidence, and audits
Part IV	System health, maturity, controlled change, renewal, workbook, and tool directory

The Management Problem This Center Solves

Restaurant standards often become outdated quietly. A vendor changes a feature, a regulator revises guidance, a new manager uses an old form, an AI tool receives data nobody approved, or a training record points to a procedure that has already changed. The operation may still appear organized while its standards, evidence, systems, and decisions drift apart.

CENTRAL PURPOSE **The Center creates one governed path from an external or internal signal to a verified decision, controlled release, trained user, retained evidence, and scheduled renewal.**

The intelligence-to-standard loop

1. Monitor trustworthy primary sources and internal signals.
2. Verify relevance, jurisdiction, status, authority, and uncertainty.
3. Assess the impact on people, guests, systems, data, contracts, documents, and training.
4. Approve, test, implement, communicate, and release the controlled change.
5. Verify the result, archive superseded versions, and schedule the next review.

What the Center does not replace

- Government agencies, regulators, legal counsel, auditors, insurers, assessors, payment-security professionals, or food-safety authorities.
- The operational records owned by GRV-L, GRV-T, GRV-C, GRV-S, GRV-F, GRV-R, GRV-P, the POS, payroll, accounting, inventory, CRM, or vendor platforms.
- Incident response, emergency action, or corrective work that must begin immediately under an approved plan.
- Human judgment, hospitality, fairness, and accountability.

1. Center Architecture

Thirty tools are organized into six control areas. The Center sits above the Gravity operating systems and governs how standards, evidence, external intelligence, and change move between them.

SYSTEM IDENTITY **Use GRV-I01 through GRV-I30 as the official tool IDs. GRV-I governs and connects the other systems; it does not duplicate their operating records.**

Governance and control

- System ownership and authority
- Controlled documents, versions, releases, archives, and replacement evidence

Change and intelligence

- Primary-source monitoring
- Regulatory, industry, technology, platform, food-safety, and public-health briefs

Risk and trust

- Cybersecurity, privacy, consent, AI, vendors, payment environment, accessibility, and inclusion

Standards verification

- Requirement records, evidence traceability, deviations, audits, and cross-system tests

System health

- Adoption, completion, training currency, incident patterns, and 90-day maturity

Decision and renewal

- Review agenda, impact assessment, implementation, post-change verification, and annual renewal

2. Governance, Roles, and Decision Rights

Every monitored subject and controlled standard needs a named owner, an approval authority, a user, and a reviewer.

DECISION RULE **The person who discovers a signal does not automatically have authority to interpret, approve, or implement it.**

Owner or executive sponsor

- Approves risk acceptance, system scope, authority, major changes, and annual renewal.
- Ensures qualified review is obtained when the Center cannot determine a legal or technical requirement.

General manager or systems lead

- Runs the recurring review, assigns system owners, resolves cross-system conflicts, and protects execution capacity.
- Limits the active change portfolio so the restaurant can implement and verify it.

Standards owner

- Maintains the controlled register, versions, effective dates, replacement evidence, and review calendar.

Intelligence owner

- Monitors approved sources, records signals, separates final requirements from proposals or commentary, and prepares decision briefs.

Subject owner

- Food safety, HR, privacy, security, AI, accessibility, payment, technology, finance, and operational owners assess their domain and supply evidence.

Independent reviewer

- Tests implementation and evidence without approving their own material exception when practical.

3. Standards Hierarchy and Authority

The Center prevents local habits, vendor advice, or Gravity materials from being treated as more authoritative than a controlling requirement.

Typical hierarchy

- Applicable law and regulation
- License, permit, health-department, fire, building, and other authority requirements
- Court order, settlement, binding contract, insurance condition, and payment or platform obligation
- Approved company policy and Gravity standard
- SOP, work instruction, checklist, form, training aid, and local practice

Conflict handling

- Record the exact conflict and affected jurisdiction.
- Pause implementation when the risk of choosing incorrectly is material.
- Obtain qualified review and document the decision source.
- Update all dependent documents rather than changing one visible copy.

Jurisdiction discipline

- FDA Food Code materials are model guidance; state and local authorities typically regulate restaurants.
- Federal resources do not replace state and local wage, leave, licensing, tax, health, alcohol, privacy, accessibility, or employment requirements.

4. Controlled Document and Version Lifecycle

A document is controlled only when its identity, owner, current version, effective date, location, distribution, review, and retirement are visible.

> **ONE-MASTER RULE** **Every active standard has one approved master. Convenience copies must identify the master and be replaced when the master changes.**

Lifecycle

- Draft
- Subject review
- Approval
- Release
- Training and distribution
- Use and evidence
- Scheduled review
- Revision, renewal, or retirement

Release minimums

- Document ID and title
- Version and effective date
- Change reason and source
- Approver
- Superseded version
- Affected users and training
- Controlled master location
- Replacement verification

Archive rule

- Archive only after the current master is available and access is verified.
- Retain records according to approved legal, contractual, insurance, tax, employment, privacy, and operational requirements.
- Do not destroy material records subject to investigation, audit, claim, incident, hold, or dispute.

5. External Intelligence Function

Intelligence is not a stream of articles. It is a governed method for deciding whether a new fact changes a standard, risk, test, or priority.

Source tiers

- Primary: official government, regulator, standards body, contract, vendor release, court, or original research owner.
- Secondary: professional association, legal or technical analysis, insurer, auditor, advisor, or respected trade publication.
- Unverified: social posts, vendor claims, summaries without a source, anecdotes, or AI-generated output.

Signal qualification

- Source and publication date
- Final, proposed, draft, advisory, enforcement, incident, research, or opinion status
- Jurisdiction and effective date
- Affected system, people, guests, data, contract, or process
- Confidence and unresolved questions
- Expiration or next-check date

Response choices

- Record only
- Monitor
- Seek qualified review
- Run a controlled test
- Implement
- Communicate urgently
- Reject or archive as not relevant

6. Regulatory, Employment, and Consumer Change Monitoring

The Center organizes legal and regulatory signals but requires the applicable authority or qualified professional to determine obligations.

Monitoring domains

- Wage, hour, tip, scheduling, leave, youth employment, posters, records, and classification
- Equal employment, accommodation, harassment, retaliation, hiring, and employee relations
- Advertising, offers, reviews, endorsements, email, text, calls, consent, and opt-out
- Health, safety, alcohol, licensing, tax, payment, accessibility, privacy, and data breach requirements

Required distinctions

- Federal versus state versus local
- Proposed versus final
- Publication date versus effective date
- Guidance versus enforceable requirement
- Applies to this employer, location, technology, transaction, or audience versus does not apply

Official starting points

- U.S. Department of Labor Restaurant Employment Toolkit and Wage and Hour guidance
- EEOC small-business and employment guidance
- OSHA restaurant and small-business safety resources
- FTC business guidance and Consumer Reviews and Testimonials Rule resources
- FCC telemarketing and TCPA materials
- ADA.gov Title III and web-accessibility guidance

7. Food Safety and Public Health Intelligence

Food-safety intelligence must move quickly without confusing a national model code with the restaurant's adopted local requirements.

Official sources

- FDA Food Code and Supplement
- State and local retail food codes and health-department alerts
- CDC, FDA, USDA, and local outbreak, recall, allergen, employee-health, and public-health information
- Approved supplier, distributor, manufacturer, and product notices

Current baseline

- FDA identifies the 2022 Food Code, including its 2024 Supplement, as the most recent edition as of this release.
- Adoption varies across states and local jurisdictions; the applicable authority must be verified.
- The Food Code is model guidance intended to support consistent retail and foodservice safety controls.

Change route

- Identify affected food, supplier, equipment, employee-health rule, process, or location.
- Apply urgent approved controls and preserve records.
- Update GRV-S SOPs, GRV-F food-control records, training, forms, and verification together.
- Close only after the local requirement and operational result are verified.

8. Industry, Consumer, Technology, and Platform Intelligence

A popular technology or trend becomes relevant only when it improves a defined restaurant outcome without creating unacceptable cost, complexity, risk, or loss of hospitality.

Industry context

- The National Restaurant Association's 2026 outlook emphasizes persistent cost pressure, uneven traffic, workforce development, digital ordering, automation, AI, data analytics, and guest connection.
- Its research supports technology as an opportunity for efficiency and experience, not as a substitute for management standards.

Technology review

- Purpose and expected outcome
- Total cost, fees, implementation load, and contract term
- Integration, data ownership, portability, access, security, privacy, and availability
- Employee and guest accessibility
- Manual fallback and exit
- Pilot, success measure, guardrail, and stop rule

Platform-change discipline

- Monitor release notes, terms, pricing, permissions, settlement rules, APIs, deprecations, support, and incident notices.
- Update dependent procedures, training, access, reports, and contracts before the effective date.

9. Cybersecurity Governance

Restaurants depend on connected POS, payment, payroll, scheduling, inventory, delivery, CRM, Wi-Fi, email, devices, and vendor platforms. Security therefore belongs in operating governance.

SECURITY RULE **Do not store passwords, full payment-card data, authentication secrets, or sensitive incident details in the Center workbook or forms.**

NIST CSF 2.0 structure

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

Restaurant baseline

- Named security owner and critical system inventory
- Unique accounts, least privilege, multifactor authentication where supported, and prompt access removal
- Supported devices, updates, vulnerability handling, network separation, and secure configuration
- Verified backups, restore testing, incident contacts, manual operations, and recovery priorities
- Vendor security and notification terms
- Employee phishing, credential, device, and reporting training

External baselines

- NIST CSF 2.0 provides voluntary outcomes for organizations of any size.
- CISA Cross-Sector Cybersecurity Performance Goals prioritize high-impact baseline actions.
- Payment systems must be handled through the applicable PCI DSS program and qualified payment partners.

10. Privacy, Consent, and Responsible Data Use

The Center applies data minimization: collect, use, share, retain, and protect only what is needed for an approved purpose.

Data review questions

- What data is collected and from whom?
- Why is it necessary?
- What notice or permission applies?
- Who can access, change, export, or delete it?
- Which vendors receive it?
- How long is it retained and how is it corrected or deleted?
- What happens if it is exposed, wrong, or used outside the purpose?

Consent and communications

- GRV-R controls guest permissions, suppression, preferences, campaigns, and relationship records.
- The Center monitors FTC, FCC, state, platform, contract, and privacy requirements and routes changes to GRV-R.
- Opt-out and revocation must be honored through approved processes and verified evidence.

Privacy framework

- NIST's Privacy Framework is a voluntary tool for identifying and managing privacy risk.
- A framework supports governance but does not determine which laws apply to a restaurant.

11. AI Governance

AI may support writing, analysis, forecasting, scheduling, training, guest communication, images, search, and administration, but each use must have a named owner and human accountability.

HUMAN-ACCOUNTABILITY RULE **AI may assist with evidence and drafts. The responsible manager remains accountable for the final fact, judgment, communication, and consequence.**

Approval minimums

- Defined purpose and decision
- Approved vendor, account, and data
- Prohibited inputs
- Human review and authority
- Accuracy, bias, privacy, security, copyright, disclosure, and record risks
- Test evidence, monitoring, incident route, and stop rule

High-risk uses

- Employment, discipline, scheduling, compensation, accommodation, food safety, allergy, health, security, legal, financial, or guest-rights decisions
- Automated decisions with no meaningful human review
- Use of confidential, sensitive, credential, payment, or regulated data
- Synthetic reviews, undisclosed endorsements, impersonation, or deceptive content

NIST basis

- NIST AI RMF provides a voluntary risk-management framework.
- The NIST Generative AI Profile identifies risks and actions specific to generative AI.
- The AI RMF and related resources are evolving; the source register must track current versions.

12. Vendor, Payment, and Dependency Risk

A vendor can be operationally critical even when it is inexpensive or easy to buy.

Criticality factors

- Service interruption stops sales, payments, scheduling, payroll, food control, access, communication, or compliance
- Vendor holds sensitive or business-critical data
- Integration failure changes numbers or decisions
- No practical manual process or replacement exists
- Contract, pricing, data, or exit terms create material exposure

Evidence to request

- Security and privacy documentation appropriate to risk
- Payment responsibility and PCI scope
- Availability, backup, recovery, support, and incident notice
- Data ownership, export, retention, deletion, and subprocessors
- Accessibility and user support
- Insurance, contract, renewal, termination, and transition terms

Payment environment

- PCI DSS v4.0.1 is the active PCI SSC version referenced by this release.
- The restaurant should confirm its merchant responsibilities, validation method, service-provider status, and evidence with its acquirer, payment processor, and qualified security resources.

13. Accessibility and Inclusion

Restaurants are public accommodations and must consider whether guests, applicants, and employees can access facilities, communication, digital tools, and services.

Review scope

- Entrances, routes, seating, counters, restrooms, parking, and alterations
- Menus, signs, notices, reservations, ordering, payment, loyalty, and websites/apps
- Effective communication and reasonable modifications
- Hiring, onboarding, training, scheduling, workplace communication, and accommodation
- Emergency information and evacuation support

Official basis

- ADA.gov states that Title III applies to businesses open to the public, including restaurants.
- DOJ guidance explains access to goods and services and provides web-accessibility and effective-communication resources.
- State and local accessibility, building, employment, and digital requirements may add obligations.

Control response

- Record the barrier and immediate access response.
- Obtain qualified review when the correction or requirement is uncertain.
- Assign a permanent correction, owner, due date, evidence, and retest.

14. Requirements, Evidence, Deviations, and Audits

A standard is dependable only when its authority, implementation, evidence, test, exception path, and correction are connected.

Requirement record

- Exact requirement and source
- Who and what it applies to
- Owner and procedure
- Training and communication
- Evidence and retention
- Test method, frequency, reviewer, and pass criteria

Evidence quality

- Specific source, exact location, version, period, as-of date, preparer, and reviewer
- Visible calculation, adjustment, limitation, and result
- Retained without unnecessary sensitive data
- Traceable to the decision, exception, audit, or change

Deviation control

- Reason and scope
- Risk and temporary control
- Approver and qualified review
- Start, expiration, monitoring, and return owner
- Closure evidence

Audit discipline

- Test a representative sample and observe execution when necessary.
- Classify findings by consequence, not by embarrassment.
- Do not close a finding when the paperwork changed but the control still fails.

15. Cross-System Control Testing

The same requirement can fail between systems even when each system looks complete by itself.

Test examples

- A food-safety change appears in the SOP, training, form, and verification record.
- A guest-consent rule appears in CRM, campaigns, vendor configuration, suppression, and audit evidence.
- A labor definition agrees across schedule, payroll, profitability, manager review, and source mapping.
- A vendor change updates contract ownership, access, data map, fallback, training, and system reports.

Six alignment checks

- Definition
- Source
- Owner
- Timing
- Transfer
- Evidence

Failure response

- Contain material risk.
- Name the system of record.
- Correct the conflict and dependent documents.
- Retest the complete path.

16. System Health, Adoption, and Training Currency

A large library is not a working system. Health depends on whether managers use the right tools, on time, and turn evidence into verified action.

NO-PADDING RULE **Retire or redesign a tool that managers repeatedly complete without producing a useful decision, control, or evidence result.**

Core health measures

- Systems with current owners
- Standards current and due
- Required tools launched and completed on time
- Records reviewed
- Evidence gaps
- Open exceptions and critical changes
- Audit pass rate
- Training current
- Actions overdue and verified closed

Adoption test

- Required
- Usable
- Completed
- Reviewed
- Acted on
- Verified
- Worth keeping

Training currency

- Train against the current version.
- Demonstrate competence where consequence matters.
- Refresh after material change, incident, failure, or required interval.
- Connect completion to the employee and the exact standard version.

17. Gravity 90-Day and 180-Day Maturity

Maturity measures whether the system can produce dependable results without repeated owner rescue.

Six maturity dimensions

- Ownership
- Standardization
- Execution
- Evidence
- Learning
- Independence

90-day assessment

- Rate the current state from observed evidence.
- Choose the highest-risk or highest-leverage gap.
- Set one 30-day action, one 60-day improvement, and one 90-day proof.
- Do not treat the score as an external benchmark or certification.

180-day roadmap

- Limit the portfolio to three system priorities.
- Name dependencies, resources, owners, review dates, and proof.
- State what will not be attempted during the cycle.
- Renew, revise, retire, or escalate at the next gate.

18. Review Cadence and Controlled Renewal

The Center stays relevant through a predictable rhythm rather than emergency cleanup.

Monthly

- Check monitored sources and vendor notices.
- Review open change signals, due standards, exceptions, audits, training gaps, incidents, and actions.
- Approve no more changes than the operation can implement and verify.

Quarterly

- Review system ownership, cybersecurity, privacy, vendors, external trends, cross-system tests, tool adoption, and the 90-day maturity assessment.

Annual

- Refresh the source register and authority matrix.
- Renew, revise, or retire controlled standards and tools.
- Complete the annual roadmap, vendor and accessibility review, and archive verification.
- Publish a change summary and schedule the next review cycle.

Urgent

- Use approved incident, food-safety, legal, security, accessibility, or emergency routes immediately.
- Do not wait for the monthly meeting when harm, law, safety, payment, privacy, or business continuity requires action.

19. Digital Workbook Operating Standard

The workbook is the living control center. It organizes decisions and evidence but is not the official record for every source system.

Start

- Read Start Here and assign the Center owner.
- Complete Settings, Source Register, System Registry, Standards Register, and Document Control.
- Enter a small verified test set before loading a full history.
- Review Checks before interpreting the dashboard.

Use

- Yellow cells with blue text are manager inputs.
- Cream or white cells with black text are formulas or controlled references.
- Use IDs to connect signals, standards, evidence, audits, exceptions, training, changes, and actions.
- Do not place passwords, payment-card data, protected health information, government identifiers, or unnecessary personal data in the workbook.

Decision

- Use the dashboard to locate due, overdue, high-risk, or weak controls.
- Open the source row and evidence before deciding.
- Assign no more than three priority changes at one review.
- Verify the result and update the controlled standard.

20. Installation and Rollout

Install the Center after the operating systems have identifiable owners and current files. It can begin small while the wider Gravity platform is completed.

INSTALLATION GATE **A Center is installed when it can prove which standard is current, why it controls, who owns it, who received it, how it is tested, and what happens when it changes.**

Days 1-30: establish control

- Register systems, owners, sources, standards, and documents.
- Identify current-versus-draft files and critical review dates.
- Create the monthly review and urgent escalation routes.

Days 31-60: verify risk and evidence

- Complete initial cybersecurity, privacy, AI, vendor, accessibility, and food-safety monitoring reviews.
- Run selected conformance audits and cross-system tests.
- Correct the most material version, evidence, access, or training gaps.

Days 61-90: renew and prove

- Complete the first system health scorecard and Gravity 90-Day Maturity Assessment.
- Implement and verify a controlled change from signal through release.
- Approve the 180-day roadmap and source-review calendar.

21. Complete GRV-I Tool Directory

The official tool IDs remain stable even when an approved form version changes.

Tool	Area / owner / frequency	Tool	Area / owner / frequency
GRV-I01 | System Registry & Ownership Map	Governance & Control | Owner/GM | Quarterly and at change	**GRV-I16 | Gravity Standard Requirement Record**	Standards Verification | Standards Owner | Per requirement
GRV-I02 | Standards Hierarchy & Authority Matrix	Governance & Control | Owner/GM | Annual and at change	**GRV-I17 | Evidence & Traceability Log**	Standards Verification | System Owner | At review
GRV-I03 | Controlled Document Master Register	Governance & Control | Standards Owner | Monthly	**GRV-I18 | Exception & Deviation Request**	Standards Verification | Owner/GM | Per exception
GRV-I04 | Version History & Release Record	Governance & Control | Standards Owner | Per release	**GRV-I19 | Standard Conformance Audit**	Standards Verification | Independent Reviewer | Quarterly
GRV-I05 | Archive & Replacement Authorization	Governance & Control | Owner/GM | Per retirement	**GRV-I20 | Cross-System Control Test**	Standards Verification | GM/Systems Lead | Quarterly
GRV-I06 | External Intelligence Source Register	Change & Intelligence | Intelligence Owner | Monthly	**GRV-I21 | System Health Scorecard**	System Health | Owner/GM | Monthly
GRV-I07 | Regulatory & Legal Change Monitor	Change & Intelligence | Owner/Compliance Lead | Monthly and at alert	**GRV-I22 | Tool Adoption & Completion Review**	System Health | GM/System Owners | Monthly
GRV-I08 | Industry & Consumer Trend Brief	Change & Intelligence | GM/Strategy Owner | Quarterly	**GRV-I23 | Training Currency & Competency Review**	System Health | Training Owner | Monthly
GRV-I09 | Technology & Platform Change Brief	Change & Intelligence | Technology Owner | Monthly and at notice	**GRV-I24 | Incident & Signal Pattern Review**	System Health | GM/Risk Owner | Monthly
GRV-I10 | Food Safety & Public Health Intelligence Brief	Change & Intelligence | Food Safety Owner | Monthly and at alert	**GRV-I25 | Gravity 90-Day Maturity Assessment**	System Health | Owner/GM | Every 90 days
GRV-I11 | Cybersecurity Baseline Assessment	Risk & Trust | Owner/Technology Lead | Quarterly	**GRV-I26 | Standards & Intelligence Review Agenda**	Decision & Renewal | Intelligence Owner | Monthly
GRV-I12 | Data Privacy & Consent Review	Risk & Trust | Privacy Owner | Quarterly and at change	**GRV-I27 | Change Impact Assessment**	Decision & Renewal | Change Owner | Per change
GRV-I13 | AI Use Case & Risk Review	Risk & Trust | Owner/AI Lead | Per use case	**GRV-I28 | Controlled Change Implementation Plan**	Decision & Renewal | Change Owner | Per approved change
GRV-I14 | Vendor & System Risk Review	Risk & Trust | Owner/Technology Lead | Annual and before contract	**GRV-I29 | Post-Implementation Verification**	Decision & Renewal | Independent Reviewer | After implementation
GRV-I15 | Accessibility & Inclusion Review	Risk & Trust | Owner/GM | Annual and at change	**GRV-I30 | Annual Standards Renewal & 180-Day Roadmap**	Decision & Renewal | Owner/GM | Annual with 180-day reset

22. Official Source References

The source register must be rechecked because editions, rules, guidance, pages, and effective dates change. Accessed August 10, 2026.

Reference	Official URL
FDA Food Code	https://www.fda.gov/food/fda-food-code
FDA Food Code 2022 and Supplement	https://www.fda.gov/food/fda-food-code/food-code-2022
FDA state retail food codes	https://www.fda.gov/food/fda-food-code/state-retail-and-food-service-codes-and-regulations-state
U.S. DOL Restaurant Employment Toolkit	https://www.dol.gov/agencies/whd/compliance-assistance/toolkits/restaurant
OSHA Restaurant Safety	https://www.osha.gov/young-workers-restaurant-safety
EEOC Small Business	https://www.eeoc.gov/employers/small-business
ADA Title III	https://www.ada.gov/topics/title-iii/
ADA Web Accessibility Guidance	https://www.ada.gov/resources/web-guidance/
FTC Business Guidance	https://www.ftc.gov/business-guidance
FTC Reviews and Testimonials Rule Q&A	https://www.ftc.gov/business-guidance/resources/consumer-reviews-testimonials-rule-questions-answers
FCC Telemarketing	https://www.fcc.gov/general/telemarketing
NIST Cybersecurity Framework 2.0	https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20
CISA Cybersecurity Performance Goals 2.0	https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0
NIST Privacy Framework	https://www.nist.gov/privacy-framework
NIST AI Resource Center	https://airc.nist.gov/

Reference	Official URL
PCI Security Standards Document Library	https://www.pcisecuritystandards.org/document_library/
National Restaurant Association 2026 State of the Industry	https://restaurant.org/research-and-media/research/research-reports/state-of-the-industry/
National Restaurant Association Technology Landscape	https://restaurant.org/research-and-media/research/research-reports/2024-technology-landscape-report/
U.S. Bureau of Labor Statistics CPI	https://www.bls.gov/cpi/

FINAL OPERATING STANDARD **Trust the best available source, disclose uncertainty, control every change, verify the installed result, and schedule the next review before the standard becomes stale.**

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.

Adoption (GLOSS-003)

Consistent use of an approved standard, process, or tool by the people and locations expected to use it.

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.

Archive (GLOSS-007)

A protected location for superseded or inactive records that must be retained but must not be mistaken for the current version.

Audit pass rate (GLOSS-008)

Passed audit records divided by all populated audit records.

Used primarily in: Standards & Intelligence Center

Authority (GLOSS-009)

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

Authority hierarchy (GLOSS-010)

Applicable law/regulation; code or regulator guidance; contract/platform rule; industry standard; Gravity standard; approved local practice.

Used primarily in: Standards & Intelligence Center

Baseline (GLOSS-012)

The documented starting condition used to compare later performance, adoption, risk, or results.

Benchmark (GLOSS-014)

A comparison point used to understand performance; it is not automatically a required target or an applicable standard.

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.

Controlled change (GLOSS-025)

Approved change with impact review, test, training, rollout, rollback, evidence, and verification.

Used primarily in: Standards & Intelligence Center

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.

Current source (GLOSS-028)

Source record has an owner, current-as-of date, review cadence, next review, and accessible evidence.

Used primarily in: Standards & Intelligence Center

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.

Due date (GLOSS-033)

The approved date by which an assigned action or decision must be completed or escalated.

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.

Evidence currency (GLOSS-037)

Current when a location exists and the valid-until date is today or later.

Used primarily in: Standards & Intelligence Center

Exception (GLOSS-038)

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

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.

Material change (GLOSS-057)

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

Maturity score (GLOSS-058)

Average of governance, currency, evidence, adoption, risk control, and closure scores, 0 to 5.

Used primarily in: Standards & Intelligence Center

Pilot (GLOSS-072)

A limited, controlled test used to identify defects, resource needs, training gaps, and evidence before wider rollout.

Qualified review (GLOSS-075)

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

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.

Review cadence (GLOSS-086)

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

Risk level (GLOSS-088)

Qualitative combination of impact and likelihood used for triage.

Used primarily in: Standards & Intelligence Center

Scope (GLOSS-092)

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

Signal (GLOSS-093)

Observed external or internal change that may require a decision.

Used primarily in: Standards & Intelligence Center

Standard (GLOSS-095)

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

System health score (GLOSS-096)

Average of standard, evidence, and adoption scores for a dimension, 0 to 5.

Used primarily in: Standards & Intelligence Center

System owner (GLOSS-097)

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

Training currency (GLOSS-099)

Current training rows divided by all populated training rows.

Used primarily in: Standards & Intelligence Center

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.