

IT GOVERNANCE | SERVICE MANAGEMENT | INFRASTRUCTURE | RISK AND RESILIENCE

# Enterprise Technology Governance & *Policy Ownership* Framework

I organized incident and service policy into accountable domains so that ownership, obligations, audit readiness, and future control needs could be managed as a single portfolio. Leadership gained a practical way to see gaps, overlaps, and evidence requirements across the full service lifecycle.

ENVIRONMENT

Multi-state retail enterprise with ~280 stores, distribution centers, and design studios supporting 3,000+ users.

MY ROLE

Designed the ownership framework, aligned accountable leaders to every domain, classified each control obligation, and used the catalog to prepare audit evidence and sequence policy work.

13

policy domains, each with one accountable function

3

control classifications that set priority

7

high-control areas held to an evidence standard

5

implementation artifacts that run the catalog

OPERATING PRINCIPLES

- ◇ Every policy domain has one named accountable function.
- ◇ Every obligation carries a classification that sets its priority.
- ◇ Every audit-ready area has a planned evidence source and review date.
- ◇ Every exception expires and carries a remediation path.

CATALOG CONTENTS

|    |                                      |   |
|----|--------------------------------------|---|
| 01 | Overview .....                       | 1 |
| 02 | Domain Ownership Architecture .....  | 2 |
| 03 | Control Classification .....         | 3 |
| 04 | Lifecycle and Register Exhibit ..... | 4 |
| 05 | Exceptions, Mapping, and Value ..... | 5 |

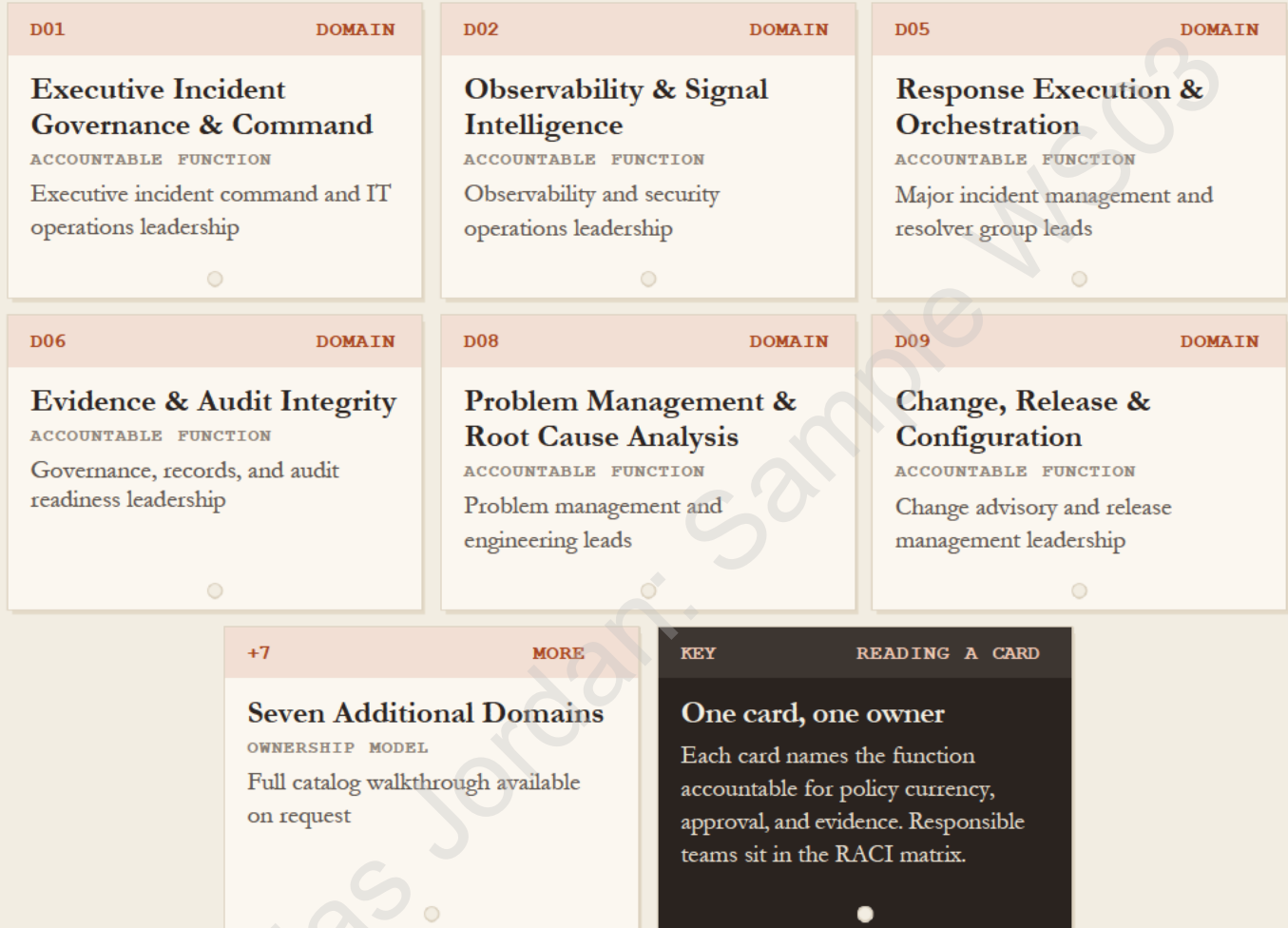
WHO USES THE CATALOG

|                                                                                                       |                                                                                                      |                                                                                                      |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <p><b>Executives</b></p> <p>See coverage, ownership, and open risk across the estate at a glance.</p> | <p><b>Control Owners</b></p> <p>Know their obligations, review dates, and evidence expectations.</p> | <p><b>Auditors</b></p> <p>Find the evidence location for every audit-ready control in one place.</p> |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|

## SECTION 02

# Domain Ownership Architecture

Thirteen domains span the full incident and service governance lifecycle; six are shown here. Accountability sits with a single function per domain, removing ownership gaps that surface during audits and incidents.



## SECTION 03

# Control Classification

Three classifications separate what the enterprise must do from what strengthens maturity, and they flag where proof matters most.

**REQUIRED**

A mandatory policy or control. A gap here is a compliance or operational risk.

**RECOMMENDED**

A practice that strengthens maturity and standardization.

**AUDIT-READY**

An area that needs defensible documentation, evidence, traceability, and review.

**PRIORITY ORDER**

1

**REQUIRED +  
AUDIT-READY**

Immediate obligation with explicit evidence expectations

2

**REQUIRED**

Mandatory control maintained on a review cycle

3

**AUDIT-READY**

Evidence discipline for areas under review

4

**RECOMMENDED**

Maturity work sequenced into the roadmap

**HIGH-CONTROL AREAS****AREA****EVIDENCE FOCUS**

Major incident declaration

Severity criteria, declaration records, and command role assignments

Incident evidence and chain of custody

Timestamped timelines and preserved artifacts

Emergency and break-glass access

Approvals, session logs, and post-use access review

Stakeholder and regulatory notification

Notification logs, approvals, and delivery times

Vendor escalation and third-party access

Escalation records, SLA evidence, and access approvals

Emergency change and configuration control

Emergency CAB approvals and baseline checks

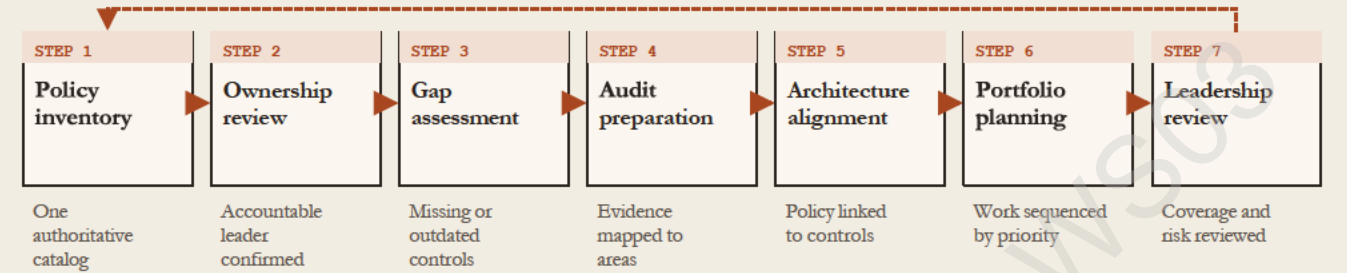
Post-incident review, root cause, and known error governance

PIR records, root cause findings, and tracked corrective actions

SECTION 04

# Lifecycle and Register Exhibit

A seven-step cycle keeps the catalog current. Leadership review feeds the next inventory, so coverage improves with every pass.



POLICY REGISTER EXCERPT

Representative entries. Identifiers, versions, and dates are illustrative.

| ID           | POLICY                                          | ACCOUNTABLE<br>FUNCTION                   | VER. | STATUS    | NEXT<br>REVIEW  | CLASS  |
|--------------|-------------------------------------------------|-------------------------------------------|------|-----------|-----------------|--------|
| POL-ITSM-004 | Major Incident Management Policy                | IT operations leadership                  | v3.2 | APPROVED  | Mar 2027        | REQAUD |
| POL-COM-002  | Incident Notification Policy                    | Communications leadership                 | v2.1 | IN REVIEW | Nov 2026        | REQAUD |
| STD-EVD-007  | Incident Evidence and Chain of Custody Standard | Governance and audit readiness leadership | v1.4 | APPROVED  | Jun 2027        | REQAUD |
| STD-DRL-003  | Major Incident Drill Standard                   | IT operations and crisis management       | v1.2 | OVERDUE   | Sep 2026        | REQAUD |
| STD-VND-005  | Vendor Escalation and SLA Standard              | Vendor management and risk                | v1.0 | DRAFT     | Set at approval | REQ    |
| GDL-AIO-001  | AI-Assisted Incident Triage Guideline           | Observability and analytics leadership    | v0.9 | DRAFT     | Set at approval | REC    |

HOW THE REGISTER DRIVES ACTION

The overdue major incident drill standard surfaces in the monthly governance review with its accountable function named. Because the standard is both required and audit-ready, it moves to the top of the remediation queue with a set completion date.

STATUS KEY

|           |                         |
|-----------|-------------------------|
| APPROVED  | Current and in force    |
| IN REVIEW | Revision underway       |
| DRAFT     | Baseline in development |
| OVERDUE   | Past its review date    |

SECTION 05

# Exceptions, Mapping, and Value

Approved deviations remain visible and temporary, and every policy requirement traces back to a working control with supporting evidence.

| EXCEPTION RECORD EXC-014                                                                                                |  | RISK ACCEPTED   EXPIRES IN 90 DAYS          |  |
|-------------------------------------------------------------------------------------------------------------------------|--|---------------------------------------------|--|
| DEVIATION                                                                                                               |  | POLICY AFFECTED                             |  |
| Legacy point-of-sale systems cannot stream alerts to central monitoring at a subset of stores                           |  | Monitoring and Alerting Standard            |  |
| COMPENSATING CONTROLS                                                                                                   |  | RISK ACCEPTANCE                             |  |
| Scheduled health checks, manual log review, and store-level escalation                                                  |  | Business owner and IT operations leadership |  |
| REMEDIATION PATH                                                                                                        |  |                                             |  |
| Platform upgrade sequenced in the next roadmap quarter, with progress reported at each governance review until closure. |  |                                             |  |

Representative record. Details are illustrative.

CONTROL-TO-POLICY MAP EXCERPT

|                              |   |                                            |   |                         |   |                                              |
|------------------------------|---|--------------------------------------------|---|-------------------------|---|----------------------------------------------|
| Incident Notification Policy | > | Approved notices sent within set windows   | > | Incident communications | > | Notification log in the GRC repository       |
| Incident Evidence Standard   | > | Evidence preserved at incident declaration | > | Governance and records  | > | Evidence index linked to incident records    |
| Major Incident Policy        | > | Closure blocked without complete evidence  | > | ITSM platform team      | > | Timestamped incident timeline and PIR record |

IMPLEMENTATION ARTIFACTS

|                                                                                                |                                                                    |                                                                               |                                                                         |                                                                              |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>Policy Register</b><br>Owner, version, status, approval, review date, and evidence location | <b>RACI Matrix</b><br>Roles below domain ownership for each policy | <b>Exception Register</b><br>Approved deviations, expiration, and remediation | <b>Control-to-Policy Map</b><br>Requirements traced to working controls | <b>Review Calendar</b><br>Coordinated review, approval, and evidence refresh |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------|

MANAGEMENT VALUE

Policy work gains the same operational discipline used for services and projects. Ownership is visible, required controls stand apart from maturity improvements, and audit readiness becomes a managed evidence practice with dates and owners. The framework fits a growing company writing its first policies and an established enterprise rationalizing hundreds of them.