**Cybersecurity Templates**

**Problem Directory Model**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Problem Directory Model** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document ID:** | GOV‑PDM‑[####] | **Owner:** | [Head of Problem Management] |
| **Approved by:** | [Operations Governance Board Chair] | **Effective date:** | [YYYY‑MM‑DD] |

Contents

[Problem Directory Model 3](#_Toc207150816)

[1. Scope & Alignment 3](#_Toc207150817)

[2. Principles 3](#_Toc207150818)

[3. Roles & RASCI 4](#_Toc207150819)

[4. Directory Structure (Logical) 5](#_Toc207150820)

[4.1 Domains (top-level) 5](#_Toc207150821)

[4.2 Standard sub‑folders per Problem 5](#_Toc207150822)

[5. Record Types & Templates 5](#_Toc207150823)

[6) Metadata Model (applies to PR/KE/WA) 6](#_Toc207150824)

[6.1 Mandatory fields 6](#_Toc207150825)

[6.2 Assessment fields 6](#_Toc207150826)

[6.3 Analysis fields (PR/KE) 6](#_Toc207150827)

[6.4 Workaround fields (KE/WA) 6](#_Toc207150828)

[6.5 Fix & Validation fields (PR/KE) 6](#_Toc207150829)

[7. Lifecycle & States 7](#_Toc207150830)

[8. Process Overview (Operating Rhythm) 7](#_Toc207150831)

[9. Governance & Controls 8](#_Toc207150832)

[10. Integrations & Data Flow 8](#_Toc207150833)

[11. KPIs, Targets & Reviews 8](#_Toc207150834)

[12. Security & Risk Considerations 9](#_Toc207150835)

[13. Training & Adoption 9](#_Toc207150836)

[14. Version Control 9](#_Toc207150837)

[Appendices — Working Templates & Registers 9](#_Toc207150838)

[Appendix A — Problem Record (PR) Template 9](#_Toc207150839)

[Appendix B — Known Error (KE) Template 10](#_Toc207150840)

[Appendix C — Workaround (WA) Template 11](#_Toc207150841)

[Appendix D — Problem Review Board (PRB) Agenda (Weekly) 11](#_Toc207150842)

[Appendix E — Data Dictionary (extract) 11](#_Toc207150843)

[Appendix F — KPI & Dashboard Definitions 12](#_Toc207150844)

[Appendix G — Records & Retention Schedule (excerpt) 12](#_Toc207150845)

# Problem Directory Model

# 1. Scope & Alignment

* **In scope:** Persistent or recurring faults impacting security or service quality; defects without immediate fix; complex misconfigurations; systemic control failures; vendor defects with interim mitigations; cross-team problems derived from incidents.
* **Out of scope:** One-off incidents resolved without underlying cause; service requests; minor tasks (handled via ticketing).
* **Framework alignment:** Problem Management, Knowledge Management, Change Management, Vulnerability Management, and Configuration Management (CMDB).
* **Systems of Record (SoR):** ITSM (problem/change), SIEM/SOAR (evidence), CMDB (CIs), DMS/ECM (decision logs/approvals), Source Repos (fix PRs).

# 2. Principles

1. **Single source of truth:** One authoritative Problem/KE entry per underlying cause; avoid duplicate shadow records.
2. **Evidence-backed:** Every claim (symptom, cause, fix) is supported by artifacts and hashes.
3. **Reusability first:** Structure captures patterns, not just events; make search and reuse effortless.
4. **Security by design:** Classification at creation; minimal personal data; access by role; audit trail on reads/changes.
5. **Lifecycle integrity:** Clear entry/exit criteria for each state; time-boxed workarounds; mandatory post-fix validation.
6. **Link everything:** Problems ↔ Incidents ↔ Changes ↔ Risks ↔ Assets/CIs ↔ Knowledge Articles.

# 3. Roles & RASCI

| **Role** | **Core Responsibilities** | **R** | **A** | **S** | **C** | **I** |
| --- | --- | --- | --- | --- | --- | --- |
| **Problem Manager** | Owns directory governance, triage, prioritization, KPIs, and quality reviews | **R** | **A** |  | Sec Gov, Change | Execs |
| **Service Owner** | Accepts impact, prioritizes fixes, funds workarounds, and permanent changes | **R** |  |  | Problem, Change | Stakeholders |
| **CIRT Lead / IR** | Provides incident linkage, evidence, ATT&CK mapping, threat context | **R** |  |  | Problem |  |
| **SMEs/Engineers** | Root‑cause analysis (RCA), develop fixes, and validate | **R** |  |  | Problem |  |
| **Change Manager/CAB** | Approves permanent fixes via RFCs; ensures non-prod testing |  |  | **S** | Problem |  |
| **Knowledge Manager** | Curates KE and workaround articles; ensures findability/KB quality | **R** |  |  | Problem |  |
| **Records Manager/Legal** | Retention, legal holds, classification and privacy review |  |  |  | Problem |  |

**RASCI Legend:** R = Responsible; A = Accountable; S = Support; C = Consulted; I = Informed.

# 4. Directory Structure (Logical)

Organize the Problem Directory as a top‑level catalogue with domain folders and standardized sub‑folders.

## 4.1 Domains (top-level)

* Identity & Access
* Network & Perimeter
* Endpoint & EDR
* Data Protection & DLP
* Application & API Security
* Platform (OS/DB/MW)
* Cloud (IaaS/PaaS/SaaS)
* Tooling & Telemetry (SIEM/SOAR/UEBA)
* Third‑Party & Supply Chain

## 4.2 Standard sub‑folders per Problem

* 00\_Admin (approvals, decision log, classification)
* 10\_Symptoms (case references, screenshots, logs, PCAPs)
* 20\_RCA (analysis notes, diagrams, ATT&CK mapping)
* 30\_Workaround (steps, risk notes, rollback)
* 40\_Fix (design, test results, RFCs, code links)
* 50\_Validation (post-fix checks, monitoring rules)
* 60\_Comms (stakeholder updates, templates)
* 70\_Metrics (SLO impact, recurrence, time to fix)
* 99\_Archive (superseded versions)

Each subfolder contains an index file that lists artifacts and includes their SHA-256 hashes.

# 5. Record Types & Templates

Three canonical record types are used. Templates appear in **Appendix A–C**.

1. **Problem Record (PR):** The authoritative container for a persistent underlying cause; includes symptoms, scope, RCA, and status.
2. **Known Error (KE):** Confirmed cause + documented workaround; may exist while a permanent fix is pending.
3. **Workaround (WA):** Actionable, risk-assessed steps to reduce impact until fix; bound by expiry criteria.

**Relationships:** A PR may have **0..n** KEs; each KE may have **1..n** WAs; a KE is closed when a permanent fix is deployed and verified.

# 6) Metadata Model (applies to PR/KE/WA)

## 6.1 Mandatory fields

* Record ID (immutable)
* Title (clear, searchable)
* Record Type (PR/KE/WA)
* Owner (role + person)
* Service/Asset (CI link)
* Environment (Prod/Pre‑Prod/DR)
* Classification (Public/Internal/Confidential/Restricted)
* Summary (≤ 5 lines; problem statement or workaround intent)
* Related Records (Incidents, Changes/RFCs, Risks, Vulnerabilities, KB)
* Attachments Index (with SHA‑256 hashes)
* Created/Updated (UTC)
* Status & State Dates (see §7)

## 6.2 Assessment fields

* Impact (Very High → Very Low)
* Urgency (Immediate → Low)
* Size/Effort (Very High → Very Low)
* Frequency/Recurrence (Frequent → Rare)
* Affected Customers/Users (counts/segments)
* Data Sensitivity (None/PII/PHI/PCI/Secrets)

## 6.3 Analysis fields (PR/KE)

* Symptoms & Indicators (IoCs, error patterns, logs)
* Scope (assets, regions, versions)
* ATT&CK Techniques (where applicable)
* RCA Method (5‑Whys/Fault Tree/Fishbone)
* Root Cause (confirmed) & Contributing Factors
* Why detection missed (coverage, tuning, process)

## 6.4 Workaround fields (KE/WA)

* Steps (reversible); Preconditions; Risk notes
* Monitoring added (detections, thresholds)
* Removal Criteria (metric/date)
* Owner of removal

## 6.5 Fix & Validation fields (PR/KE)

* Permanent Fix Design (summary + references)
* Change(s)/RFCs and test plan links
* Non‑prod results; Prod rollout plan
* Post‑Fix Validation (functional + security checks)
* Residual Risk & Acceptance (approver, expiry)

# 7. Lifecycle & States

**Problem Record (PR)**

* New ▶ Triage ▶ Analysis ▶ Known Error Issued (optional) ▶ Fix in Progress ▶ Validation ▶ Closed ▶ Archived

**Known Error (KE)**

* Draft ▶ Verified ▶ Published ▶ Superseded ▶ Closed

**Workaround (WA)**

* Proposed ▶ Approved ▶ Implemented ▶ Retired

**Entry/Exit criteria**

* Triage → Analysis: owner assigned; impact/urgency sized; evidence set started.
* Analysis → KE Issued: cause confirmed; workaround documented; risk assessed; comms sent.
* Fix in Progress → Validation: change executed; monitoring enabled.
* Validation → Closed: recurrence = 0 for [N] days; performance within ±[X]%; residual risk recorded or closed.

# 8. Process Overview (Operating Rhythm)

1. **Intake & Triage** – Create PR; deduplicate; classify; initial severity; assign owner; decide if KE/WA needed immediately.
2. **Analysis & Evidence** – Gather logs, traces, packet captures; reproduce; map ATT&CK; run RCA method; document cause & factors.
3. **Known Error + Workaround** – Publish KE/WA with rollback and monitoring; set removal criteria; notify stakeholders.
4. **Permanent Fix** – Raise RFC; build/test fix; deploy; update documentation and training; consider feature toggles/canaries.
5. **Validation** – Confirm no recurrence; validate metrics; security test; user acceptance (as needed).
6. **Closure & Learning** – Close PR/KE/WA; capture lessons learned; update detection rules; measure outcomes; archive evidence per retention.
7. **Governance** – Weekly Problem Review; monthly trend analysis; quarterly refresh of KE library.

# 9. Governance & Controls

* **Approvals:** KEs and WAs require Problem Manager + Service Owner approval; permanent fixes require CAB approval.
* **Classification & Privacy:** default **Confidential**; redact PII unless essential; apply legal holds on request.
* **Retention:** PR/KE/WA kept **Active + 3 years** (or per law); evidence packs archived; destruction certificates logged.
* **Auditing:** Quarterly sample of new PRs for metadata completeness, linkage integrity, and validation proof.
* **Exceptions:** Temporary risk acceptances tracked with expiry ≤ 90 days.

# 10. Integrations & Data Flow

* **ITSM:** Authoritative IDs for PR/KE/WA; status sync and SLA clocks.
* **CMDB:** CI linkage for impact scoping; blast radius estimation.
* **SIEM/SOAR/EDR:** Evidence ingestion and detection rule updates; case linkage.
* **Code Repos/CI‑CD:** Fix PR/MR links; pipeline results as validation evidence.
* **KB/Portal:** Auto-publish KE/WA to searchable knowledge with role-based access.
* **Dashboards:** KPIs/SLOs, heat maps by domain, aging, and recurrence.

# 11. KPIs, Targets & Reviews

|  |  |  |
| --- | --- | --- |
| **KPI** | **Definition** | **Target** |
| **Time to Issue KE** | Discovery → KE Published | ≤ 2 business days |
| **Workaround Age** | KE with WA older than threshold | < 45 days (≥90% closed) |
| **Recurrence Rate** | Incidents repeating existing KE | ≤ 5% of monthly incidents |
| **Mean Time to Permanent Fix (MTTPF)** | KE Published → Fix Validated | ≤ 30 days (median) |
| **Completeness** | PRs with mandatory metadata | ≥ 98% |
| **Linkage** | PRs with incident/change/CI links | ≥ 95% |

**Reviews:** Weekly operational review; monthly governance review; quarterly portfolio readout (top repeaters, systemic themes, vendor backlog).

# 12. Security & Risk Considerations

* **ATT&CK mapping required** where cyber‑attack techniques are present; use to prioritize detection/backlog.
* **Workaround risk:** Document adverse effects (e.g., reduced monitoring, perf impacts); time‑box and track removal.
* **Vendor engagement:** Track vendor case IDs and SLAs; mirror KEs with vendor advisories; assess supply‑chain exposure.
* **Change safety:** Canary releases, feature flags, or blue-green deployments for risky fixes; pre-approved rollback steps.
* **Evidence handling:** Sign and hash artifacts; maintain chain‑of‑custody in case of regulatory review.

# 13. Training & Adoption

* Onboarding for engineers and analysts on PR/KE/WA creation and search best practices.
* Job aids: RCA quick cards; KE authoring style guide; classification cheat‑sheet.
* Quarterly clinics reviewing best/worst KEs and outcomes.

# 14. Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Summary** |
| 1.0 | [YYYY‑MM‑DD] | [Name] | Initial release |

# Appendices — Working Templates & Registers

## Appendix A — Problem Record (PR) Template

**PR‑ID:** …  
**Title:** …  
**Service/CI:** …  
**Environment:** Prod / Pre‑Prod / DR  
**Owner:** … **Created/Updated:** …  
**Classification:** Public / Internal / Confidential / Restricted

**A1. Summary & Symptoms**

* Summary (≤ 5 lines): …
* Symptom signature(s): …
* Affected scope (services/regions/versions): …
* Frequency/Recurrence: …
* Associated incidents: [IDs]

**A2. Assessment**

* Impact: Very High / High / Medium / Low / Very Low
* Urgency: Immediate / High / Normal / Low
* Size/Effort: Very High / High / Medium / Low / Very Low
* Data Sensitivity: None / PII / PHI / PCI / Secrets
* Stakeholders: …

**A3. Analysis & Evidence**

* ATT&CK: …
* RCA Method: 5‑Whys / Fishbone / Fault Tree
* Root Cause (confirmed): …
* Contributing Factors: …
* Why detection missed: …
* Evidence index (file → SHA‑256): …

**A4. Fix Strategy**

* Options considered: …
* Selected approach & rationale: …
* RFC(s): …
* Non‑prod test results: …
* Deployment plan & rollback: …

**A5. Validation & Closure**

* Post‑fix checks (functional/security): …
* Monitoring rules/tuning applied: …
* Residual risk & acceptance: …
* Closed on: …
* Lessons learned: …

## Appendix B — Known Error (KE) Template

**KE‑ID:** … (linked PR‑ID: …)  
**Title:** …  
**Owner:** …  
**Service/CI:** …  
**Classification:** …

**B1. Confirmed Cause**

* Cause statement: …
* Evidence references: …

**B2. Workarounds (list)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| WA‑ID | Title | Preconditions | Steps (reversible) | Risk notes | Monitoring added | Removal criteria | Owner |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |

**B3. Communications & Consumers**

* Internal audiences & channels: …
* External (if any): …
* Publication date: …
* Review date: …
* Superseded by: …

## Appendix C — Workaround (WA) Template

**WA‑ID:** … (linked KE‑ID/PR‑ID: …)  
**Title:** …  
**Owner:** …  
**Risk Assessment:** …  
**Approval:** Problem Manager + Service Owner  
**Effective:** … **Expires/Removal Criteria:** …

**C1. Steps**

1. … 2) … 3) …  
   **Rollback:** …  
   **Monitoring:** …

## Appendix D — Problem Review Board (PRB) Agenda (Weekly)

1. New PRs (intake, deduplication, owners, sizing)
2. KEs pending publication; overdue WAs
3. Aging PRs and SLA breaches
4. Top repeaters and systemic themes
5. Fix progress & risks (RFCs)
6. Metrics review & actions
7. Decisions & assignments

## Appendix E — Data Dictionary (extract)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Field** | **Definition** | **Type** | **Example** | **Required** |
| Record ID | Immutable unique identifier | String | PR‑2025‑00123 | ✓ |
| Classification | Sensitivity | Enum | Confidential | ✓ |
| Impact | Business effect | Enum(5..1) | High | ✓ |
| ATT&CK | Technique IDs | List | T1190, T1059 | — |
| Evidence Hash | Integrity of artifact | String | 9f86d081… | — |

## Appendix F — KPI & Dashboard Definitions

* **Time to Issue KE:** (timestamp[KE Published] − timestamp[PR Created]) median by month.
* **Recurrence Rate:** incidents with ke\_id present ÷ all incidents (month).
* **Workaround Age:** KE with active WA age; alert at 30/45/60 days.
* **Linkage Coverage:** % PRs with ≥1 incident, ≥1 CI, and ≥1 RFC link.

## Appendix G — Records & Retention Schedule (excerpt)

| **Record Type** | **Trigger** | **Retention** | **Disposition** |
| --- | --- | --- | --- |
| PR (Problem Record) | Closed date | 3 years | Destroy w/ cert |
| KE (Known Error) | Superseded date | 3 years | Destroy |
| WA (Workaround) | Retired date | 1 year | Destroy |
| Evidence | PR/KE closed | Aligned with PR/KE | Archive then destroy |