**Cybersecurity Templates**

**Problem Record Model**

**August 2025**

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

|  |
| --- |
| **Problem Record Model** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** | GOV‑PDM‑[####] | **Prepared by:** | [Name, Title] |
| **Approved by:** | [Operations Governance Board Chair] | **Effective date:** | [YYYY‑MM‑DD] |

Contents

[Problem Record Model 2](#_Toc207221412)

[1. Executive Summary (≤ 5 lines) 2](#_Toc207221413)

[2. Problem Statement & Symptoms 2](#_Toc207221414)

[3. Scope & Impact Assessment 3](#_Toc207221415)

[4. Evidence & Timeline 3](#_Toc207221416)

[5. Analysis & Root Cause 3](#_Toc207221417)

[6. Interim Control / Workaround (WA) 4](#_Toc207221418)

[7. Known Error (KE) Publication (optional) 4](#_Toc207221419)

[8. Permanent Fix Plan (via Change) 4](#_Toc207221420)

[9. Verification & Closure Criteria 4](#_Toc207221421)

[10. Stakeholders, Communication & Escalation 5](#_Toc207221422)

[11. Compliance, Privacy & Insurance 5](#_Toc207221423)

[12. KPI Hooks (auto or manual) 5](#_Toc207221424)

[13. Records & Evidence Index 5](#_Toc207221425)

[14. Approvals & Sign‑off 5](#_Toc207221426)

[Working Aids (paste into your tools if helpful) 7](#_Toc207221427)

[A. Status Update (Internal) 7](#_Toc207221428)

[B. Investigation Question Bank (use what fits) 7](#_Toc207221429)

[C. Severity Examples (adapt to your policy) 7](#_Toc207221430)

[D. Evidence Register (quick insert) 8](#_Toc207221431)

# Problem Record Model

**Purpose**

Capture a complete, auditable picture of a **Problem**—a repeating or systemic defect with an underlying cause—so teams can investigate, mitigate the impact, deploy a permanent fix through Change, and retain the learning in Knowledge.

# 1. Executive Summary (≤ 5 lines)

* **Context:** Where/when observed; who is affected.
* **Current Risk:** Low / Medium / High / Critical (reason).
* **Interim Controls:** [e.g., throttle, blocklist, feature toggle].
* **Next Milestone:** [e.g., KE publish, RFC raised, validation window].

# 2. Problem Statement & Symptoms

* **Problem Statement:** [One clear sentence describing the recurring defect or underlying cause suspected.]
* **Symptoms & Indicators:** [Error messages, user‑visible effects, telemetry anomalies.]
* **Reproduction Steps:** [If reproducible, list precise steps and expected/actual results; else note non-repro with telemetry evidence.]
* **Detection Source(s):** SIEM alert / APM metric / User report / Vendor / Other.
* **First Seen (UTC):**
* **Frequency:** Frequent / Occasional / Rare; last **N** occurrences with timestamps.
* **Attachments/Artifacts:** [links to logs, traces, screenshots, PCAPs].

**Forensic Hygiene (if evidential):**  
Chain‑of‑custody started (Y/N) • Evidence hashed (SHA‑256) • Storage location • Access controls applied.

# 3. Scope & Impact Assessment

* **Affected Assets/Services/CIs:** [List with versions/regions/tenants].
* **User/Customer Impact:** [Counts or %; critical cohorts].
* **CIA Impact:** Confidentiality / Integrity / Availability ratings and rationale.
* **Regulatory/Contractual Exposure:** [e.g., PII/PHI/PCI, SLA/OLA at risk].
* **Business Priority:** [Narrative and stakeholder input].

**Severity Classification:**

* **Impact:** Very High / High / Medium / Low / Very Low
* **Urgency:** Immediate / High / Normal / Low
* **Size/Effort to Fix:** Very High / High / Medium / Low / Very Low

**Resulting Severity Level:** Critical / High / Medium / Low (auto-computed by your workflow or selected with justification)

# 4. Evidence & Timeline

* **Timeline (UTC):** Key events from first occurrence through triage/containment to present.
* **Logs & Metrics:** Pointers to immutable snapshots; note time windows/timezones.
* **Config/Version State:** Builds, packages, container digests, infra changes.
* **Faulting Inputs:** Sanitised payloads, repro data, hashes.
* **Screenshots & Diagrams:** Architecture/topology & sequence diagrams attached.

# 5. Analysis & Root Cause

* **Method Used:** 5‑Whys / Fishbone / Fault Tree / Comparative diff / Experimentation.
* **Hypotheses Tested & Results:** [Toggle/canary outcomes, A/B, chaos].
* **Root Cause (confirmed/suspected):** [Be precise and testable].
* **Contributing Factors:** [People / Process / Technology / External].
* **Detection Gap:** Why existing controls missed or delayed detection; proposed detection improvement.
* **Adversary Context (if applicable):** MITRE ATT&CK techniques, indicators, persistence/lateral movement notes.

# 6. Interim Control / Workaround (WA)

* **WA‑ID:**
* **Objective:** Reduce user/business risk while the fix is engineered.
* **Steps:** [Safe, reversible, and minimal blast‑radius].
* **Risk Notes:** [Residual risk, performance or security trade-offs].
* **Rollback Plan:** [Back‑out steps and trigger].
* **Monitoring Added:** [Rules, thresholds, dashboards; who reviews].
* **Removal Criteria & Expiry:** [Date/metric/event when WA must be removed].
* **Approvals:** Problem Manager + Service Owner.

# 7. Known Error (KE) Publication (optional)

* **KE‑ID / Link:**
* **KE Title (search-friendly):**
* **Cause Summary:**
* **Workarounds:** [IDs and short descriptions].
* **Preconditions / Applicability:**
* **Operational Notes:** [Monitoring, user comms, pitfalls].
* **Owner / Review Date:**
* **Removal Criteria:** [When KE should be retired].

# 8. Permanent Fix Plan (via Change)

* **Strategy Options Considered:** [A/B/C with risk, complexity, user impact].
* **Chosen Approach & Rationale:**
* **RFC / Change ID:**
* **Test Evidence (non‑prod):** Functional/regression/perf/security.
* **Rollout Plan:** Waves/canary/blue‑green; maintenance window; comms.
* **Rollback Plan:** [Trigger, steps, data restore].
* **Dependencies:** [Teams, vendors, Windows, feature flags].

# 9. Verification & Closure Criteria

* **Reproduction Test(s) Pass:** Y/N (details).
* **Telemetry Baselines Normal:** Y/N over **[X]** days/releases.
* **No Related Incidents:** Y/N over **[X]** days/releases.
* **Residual Risk:** [Accepted/Transferred/Reduced], owner, review date.
* **Runbooks/Docs Updated:** [Links].
* **Close Record:** Y/N (Approver & Date).

# 10. Stakeholders, Communication & Escalation

* **Internal:** On‑call, Engineering leads, Support, SRE, SecOps, Product.
* **External:** Customers/partners (if needed), regulators (if applicable).
* **Cadence:** [e.g., daily digest during fix, weekly PRB review, monthly exec readout].
* **Escalation Rules:** When to notify leadership; when to invoke CAB; who is the spokesperson.
* **Status Snippet (for updates):** One‑liner current state; next steps; owner; ETA; links.

# 11. Compliance, Privacy & Insurance

* **Data Classification:** [Public/Internal/Confidential/Restricted].
* **Notification Assessment:** [Jurisdictional requirements; contracts; industry bodies].
* **Insurance Clauses:** [Breach coach, notification triggers].
* **Retention:** Record & evidence retention period; legal hold if required.

# 12. KPI Hooks (auto or manual)

* **Time to Publish KE (median):**
* **Mean Time to Permanent Fix (MTTPF):**
* **Workaround Age (active > threshold):**
* **Recurrence Rate after Closure:**
* **Completeness (mandatory fields present):**

Capture these automatically where possible and display them on a Problem/KE dashboard.

# 13. Records & Evidence Index

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Artifact** | **Hash (SHA‑256)** | **Source/Collector** | **Date/Time (UTC)** | **Storage Location** | **Notes** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |

# 14. Approvals & Sign‑off

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Name** | **Signature/Approval** | **Date** |
| Problem Manager |  |  |  |
| Service Owner |  |  |  |
| Change Manager/CAB |  |  |  |
| Knowledge Manager (KE) |  |  |  |
| Legal/Privacy (if applicable) |  |  |  |

**Data Dictionary (for implementers)**

| **Field** | **Description** | **Type/Allowed Values** | **Example** |
| --- | --- | --- | --- |
| Record ID | Immutable identifier | String | PR‑2025‑00123 |
| Title | Short, action‑oriented description | String | “Recurring 500s on Checkout API under burst load” |
| Status | Lifecycle state of the problem | Enum | Analysis |
| Classification | Sensitivity of the record | Enum | Confidential |
| Owner | Accountable person for the record | Person | Jane Doe |
| Service/CI | Affected service or configuration item | Reference | svc‑checkout / ci‑db‑001 |
| Environment | Operational environment | Enum | Prod |
| Linked Records | Related Incidents/Changes/Risks/KB entries | List | INC‑4567; CHG‑8901 |
| Impact | Business effect | Enum(5..1) | High |
| Urgency | Time sensitivity | Enum | Immediate |
| Size/Effort | Estimated effort to fix | Enum(5..1) | Medium |
| Frequency | Recurrence pattern | Enum | Occasional |
| Data Sensitivity | Data at risk | Enum | PII |
| Severity | Aggregated level from Impact/Urgency/Size | Enum | High |
| Timeline | Chronological events | Text | See timeline section |
| Root Cause | Confirmed/suspected underlying cause | Text | Redis connection pool exhaustion |
| Contributing Factors | Additional influences | Text | Misconfigured pool, missing circuit‑breaker |
| Workaround | Interim control to reduce impact | Text | Rate‑limit / feature flag |
| Removal Criteria | When WA/KE must be retired | Text | Remove after fix v2.3 + 14 days clean telemetry |
| RFC | Change ticket reference | Reference | RFC‑3456 |
| Verification Window | Observation period post‑fix | Integer + unit | 14 days |
| Residual Risk | Remaining risk after fix | Enum | Accepted |
| Approvals | Formal sign‑offs | List | CAB ok 2025‑08‑20 |

# Working Aids (paste into your tools if helpful)

## Status Update (Internal)

**Subject:** [PR‑ID] — Status [State] — [Service]  
**Body:**

* *Summary:* [3–5 lines]
* *Current risk:* [why]
* *Next actions & owners:* [bullets]
* *Key dates:* [milestones]
* *Links:* [PR, KE, RFC, dashboards]

## B. Investigation Question Bank (use what fits)

* Initial intrusion/trigger?
* What post-event activity occurred? Any compromised accounts/privilege level?
* Any persistence mechanisms or lateral movement?
* Is data accessed/exfiltrated? What data/kind/volume?
* How is command and control maintained (if adversarial)?
* What vulnerabilities or misconfigurations were exploited?
* Which controls failed (prevention/detection/response)? How to improve?

## C. Severity Examples (adapt to your policy)

* **Critical:** Widespread impact on critical systems or sensitive data at risk; immediate executive visibility.
* **High:** Significant customer impact or repeated P1 incidents; urgent remediation required.
* **Medium:** Limited user impact; viable workaround exists.
* **Low:** Minimal impact; informational or housekeeping.

## D. Evidence Register (quick insert)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Details (serial/host/MAC/IP/hash)** | **Collected by (name/title)** | **Date/Time (UTC)** | **Location/Label** |
|  |  |  |  |  |