**Cybersecurity Templates**

**Knowledge & Evidence (KE) Record Model**

**August 2025**

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

|  |
| --- |
| **Knowledge & Evidence (KE) Record Model** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document ID:** | GOV‑KE‑[####] | **Owner:** | [Chief Information Security Officer] |
| **Effective Date:** | [YYYY‑MM‑DD] | **Review Cycle:** | 12 months |

Contents

[Knowledge & Evidence (KE) Record Model 4](#_Toc207138255)

[1. Purpose 4](#_Toc207138256)

[2. Scope 4](#_Toc207138257)

[3. Principles 4](#_Toc207138258)

[4. Defined Terms (selected) 5](#_Toc207138259)

[5. Governance, Roles & RACI 5](#_Toc207138260)

[6. KE Record Taxonomy (Core Catalogue) 6](#_Toc207138261)

[7. Core Metadata Model 8](#_Toc207138262)

[7.1 Mandatory fields 8](#_Toc207138263)

[7.2 Recommended fields 8](#_Toc207138264)

[7.3 Type-specific examples 9](#_Toc207138265)

[8. Classification & Handling 9](#_Toc207138266)

[9. Lifecycle Controls 9](#_Toc207138267)

[10. Systems of Record & Integrations 10](#_Toc207138268)

[11. Interfaces with Other Processes 10](#_Toc207138269)

[12. Quality & Assurance 10](#_Toc207138270)

[13. Maturity Model & Self‑Assessment 11](#_Toc207138271)

[14. KPIs & Reporting 11](#_Toc207138272)

[15. Training & Awareness 11](#_Toc207138273)

[16. Exceptions & Risk Acceptance 12](#_Toc207138274)

[17. Version Control 12](#_Toc207138275)

[Appendices (Working Templates) 12](#_Toc207138276)

[Appendix A — Meeting Minutes (Security Committee) Template 12](#_Toc207138277)

[Appendix B — Security Decision Log (GOV‑DEC) Template 12](#_Toc207138278)

[Appendix C — Incident Case File (INC‑CAS) Checklist 13](#_Toc207138279)

[Appendix D — Retention Schedule (extract; tailor to law) 13](#_Toc207138280)

[Appendix E — Metadata Dictionary (sample) 13](#_Toc207138281)

[Appendix F — System of Record Register 14](#_Toc207138282)

[Appendix G — KE Exception Register 14](#_Toc207138283)

[Appendix H — Maturity Self‑Assessment & Roadmap (abbrev.) 14](#_Toc207138284)

# Knowledge & Evidence (KE) Record Model

# 1. Purpose

Establish a unified, auditable model for creating, classifying, securing, retaining, and disposing of cybersecurity records. So evidence of decisions, actions, and outcomes is consistently captured and can be trusted in investigations, audits, litigation, and learning.

# 2. Scope

**In scope:** Security governance, risk, and operations records across:

* **Risk:** risk registers, assessments, acceptances, exceptions, third-party risk files.
* **Operations:** incident & problem records, change & release records impacting security, vulnerability management, threat intel, SOC/EDR/SIEM telemetry extracts, playbook executions.
* **Governance:** policies/standards, decision logs, committees/boards minutes, legal advice received, security architecture reviews, privacy impact assessments.
* **External:** regulator notifications, customer security questionnaires & responses, breach communications, contracts & security exhibits.

**Out of scope:** HR personnel files, financial accounting records, and generic corporate minutes (unless security-relevant). These are governed by enterprise records policies and referenced where needed.

# 3. Principles

1. **Duty to document:** Security-relevant decisions and actions must be recorded at the time of decision/action.
2. **Completeness over convenience:** A minimal, consistent core metadata set accompanies every record.
3. **Security by design:** Classification and access controls apply at creation, not retrofitted.
4. **Lifecycle integrity:** Records are retained, discoverable, and disposed of lawfully and verifiably.
5. **System‑of‑record clarity:** Exactly one authoritative repository per record type; integrations may replicate for performance but not for authority.
6. **Proportionality & privacy:** Retain no longer than required; minimize personal data; document lawful basis.

# 4. Defined Terms (selected)

* **Record:** Fixed content plus metadata providing evidence of decisions/actions.
* **Record Type:** Canonical category with defined metadata, retention, owner, and system of record (SoR).
* **System of Record (SoR):** Authoritative repository for a record type (e.g., SIEM, GRC, ticketing, DMS).
* **Custodian:** Role accountable for lifecycle controls over a record type.
* **Classification:** Sensitivity level determining handling and access (e.g., Public, Internal, Confidential, Restricted).
* **Disposition:** Final action: transfer to archive, anonymize, or destroy with proof.

# 5. Governance, Roles & RACI

| **Role** | **Responsibilities** | **Typical Tools** | **R** | **A** | **C** | **I** |
| --- | --- | --- | --- | --- | --- | --- |
| CISO | Approves model; resolves conflicts; signs exception/risk acceptances | GRC, DMS |  | **A** | C | I |
| Head of RIM | Designs metadata, retention, and taxonomy; audits compliance | DMS/ECM |  | **A** | C | I |
| Security Governance Lead | Operates KE model; coordinates record owners; training | GRC | **R** |  | C | I |
| SOC Manager | Ensures operational records (alerts/incidents) meet metadata and retention; generates evidence packs | SIEM, SOAR, EDR | **R** |  | C | I |
| Risk Manager | Maintains risk records; tracks exceptions/acceptances | GRC | **R** |  | C | I |
| Legal Counsel | Advises on privilege, discovery, and retention constraints | DMS |  |  | **C** | I |
| Data Protection Officer | Validates privacy, minimization, and cross-border rules | GRC |  |  | **C** | I |
| IT Operations Lead | Ensures change/release/backup records are captured | ITSM | **R** |  | C | I |
| Record Custodians (per type) | Enforce access, quality, retention, and disposition | SoR | **R** |  |  | I |

**RACI Legend:** R = Responsible, A = Accountable, C = Consulted, I = Informed.

# 6. KE Record Taxonomy (Core Catalogue)

Tailor the catalogue to your environment. Add rows for each record type you manage.

| **Code** | **Record** | **Purpose/**  **Evidence of** | **System of Record (SoR)** | **Custodian** | **Classification** | **Retention** | **Disposition** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| GOV‑DEC | Security Decision Log | Governance decision rationale, options, votes | DMS/GRC | SecGov Lead | Confidential | 7 yrs or per regulator | Archive |
| GOV‑MIN | Security Committee Minutes | Attendance, agenda, motions, actions | DMS | SecGov Lead | Internal | 7 yrs | Archive |
| LEG‑ADV | Legal Advice (Security) | Counsel opinion influencing security decisions | DMS | Legal | Restricted | 7 yrs (or privileged rules) | Archive/Review |
| RSK‑REG | Risk Register Item | Risk evaluation, treatment, owner | GRC | Risk Mgr | Confidential | Active + 6 yrs | Destroy w/ cert |
| RSK‑ACC | Risk Acceptance/Exception | Approved deviation from standard and expiry | GRC | CISO | Confidential | Expiry + 6 yrs | Destroy |
| CHG‑REC | Security‑Relevant Change Record | Change approvals, testing, backout | ITSM | IT Ops Lead | Internal | Active + 3 yrs | Destroy |
| VUL‑FND | Vulnerability Finding | Scanner ticket, severity, SLA, closure proof | GRC/ITSM | Risk Mgr | Internal | Finding + 3 yrs | Destroy |
| INC‑CAS | Incident Case File | Timeline, evidence, actions, lessons | SOAR/DMS | SOC Mgr | Restricted | 7 yrs (or as law) | Archive |
| THR‑RPT | Threat Intel Report | IOCs, TTPs, relevance, actions taken | TIP/DMS | SOC Mgr | Internal | 2 yrs | Destroy |
| ARC‑REV | Architecture/Security Review | Design risks, controls, sign‑off | DMS | Sec Arch Lead | Confidential | Life of system + 6 yrs | Archive |
| PIA‑DPIA | Privacy Impact Assessment | Processing risks and mitigations | GRC | DPO | Confidential (PII) | Life + 6 yrs | Archive |
| REG‑NOT | Regulator Notification | Breach/incident notifications sent/received | DMS | Legal | Restricted | 7 yrs (or per law) | Archive |

# 7. Core Metadata Model

Apply to all record types; extend via *Type‑specific fields*.

## 7.1 Mandatory fields

* Record ID (immutable)
* Record Type (from Taxonomy)
* Title (human-readable)
* Abstract/Summary (1–3 lines)
* Created On / By (system/user)
* Decision/Action Date (where applicable)
* Owner (business) & Custodian (records)
* Classification (security level)
* Legal Hold Flag (Y/N, reason, case ID)
* Retention Class (policy code)
* Source System & Link (URI)
* Related Records (IDs: e.g., change ↔ risk ↔ incident)
* Access Control List (role/group-based)

## 7.2 Recommended fields

* Jurisdiction(s)
* Personal Data Present (Y/N; categories)
* Evidence Hash / Checksum (for attachments)
* Version / Revision history
* Keywords/Tags

## 7.3 Type-specific examples

* **INC‑CAS:** severity, kill‑chain stage, regulator notice status, root cause, loss estimate.
* **RSK‑REG:** likelihood/impact before/after, control IDs, review date.
* **CHG‑REC:** CAB outcome, test results ref, backout plan ID.
* **GOV‑DEC:** options considered, vote tally, dissent note, justification link.

# 8. Classification & Handling

| **Level** | **Description** | **Examples** | **Handling Rules** |
| --- | --- | --- | --- |
| Public | Approved for anyone | Published policies | No restriction; verify publication copy |
| Internal | Business‑as‑usual info | Change records, vuln tickets | Authenticated staff; share on a need-to-know basis |
| Confidential | Sensitive operational & risk data | Risk register, DPIA | Role-based access; encrypted at rest/in transit; audit logs |
| Restricted | Highly sensitive/privileged | Incident case files, legal advice | Limited groups; multi-factor access; watermarking; DLP policies; no personal email/USB |

* **Marking:** Embed classification in header/footer and metadata.
* **PII:** Apply minimization and masking; document lawful basis before capture.
* **Encryption:** At rest and in transit for Confidential/Restricted; key mgmt via approved KMS/HSM.

# 9. Lifecycle Controls

1. **Create/Capture** – Create the record contemporaneously; ensure mandatory metadata; link to related documents.
2. **Classify** – Assign level and retention class upon creation.
3. **Store** – Save in the SoR; avoid duplicate “shadow copies.”
4. **Access/Use** – Enforce RBAC/ABAC; log every access for Restricted.
5. **Maintain** – Keep current; version control; ensure integrity hash for evidence files.
6. **Hold** – Apply legal/regulatory holds immediately; suspend disposition.
7. **Disposition** – At retention expiry: review, approve, and destroy/anonymize; produce destruction certificate and audit trail.
8. **Audit** – Periodic review of metadata completeness, access anomalies, and retention compliance.

# 10. Systems of Record & Integrations

* **GRC/IRM:** Risk, exceptions, DPIAs, policy attestations.
* **ITSM:** Changes, incidents (non‑security), service requests.
* **SIEM/SOAR/EDR/TIP:** Operational telemetry & case files; export *evidence packs* (hashed).
* **DMS/ECM:** Minutes, decisions, legal, regulator notices; versioning and retention engine.
* **Data Vault/KMS:** Keys, secrets, and cryptographic logs for proof of control.
* **Integration Rules:** Maintain unique IDs; use event/webhook sync for relationships; do not bypass SoR retention/disposition.

# 11. Interfaces with Other Processes

* **Change Management:** Security impact recorded; approvals captured in CHG‑REC; link to risks/incidents.
* **Incident Response:** Case file standard (INC‑CAS) including timeline, decisions, evidence chain‑of‑custody, and lessons learned.
* **Vendor/Third‑Party Risk:** Due diligence packages, contracts/security exhibits, assessment outcomes.
* **Compliance & Audit:** Evidence requests fulfilled from SoR with audit trail exports.
* **Information Requests:** Internally publish summaries where permitted; redact per privacy and privilege.

# 12. Quality & Assurance

* **Completeness Checks:** Mandatory metadata present; attachments legible; hashes verified.
* **Timeliness Checks:** Record created ≤ 2 business days from event; minutes issued ≤ 5 days.
* **Accuracy Checks:** Spot‑audit 10% of weekly new records; peer review for GOV‑DEC, LEG‑ADV, INC‑CAS.
* **Access Review:** Quarterly RBAC/ABAC review for Restricted records.
* **Change Control:** Updates to taxonomy/metadata follow model change request with CISO approval.

# 13. Maturity Model & Self‑Assessment

Assess your capability across **Governance**, **Creation & Capture**, **Classification & Metadata**, **Systems & Integration**, **Retention & Disposition**, **Access & Privacy**, and **Assurance**.

|  |  |  |  |
| --- | --- | --- | --- |
| **Level** | **Descriptor** | **What it looks like** | **Target Horizon** |
| Undeveloped | Ad‑hoc, incomplete records; unknown SoR | Inconsistent minutes; incident files missing decisions | 0–3 months quick wins |
| Developing | Basic taxonomy and minimal metadata | Some record types are defined; manual retention | 3–6 months |
| Acceptable | Policy‑compliant, cross-process links | Risk↔Change↔Incident linked; RBAC in place | 6–12 months |
| Managed | Automated flows; dashboards; legal holds | Workflows create records by default; audits pass | 12–18 months |
| Embedded | Enterprise-wide, analytics-driven | Predictive insights; continuous improvement loop | 18–24 months |

Use Appendix H for a scored checklist and improvement plan.

# 14. KPIs & Reporting

* **Coverage:** % of in‑scope processes with defined record types and SoR (target ≥ 95%).
* **Completeness:** % of new records with all mandatory metadata (target ≥ 98%).
* **Timeliness:** Median days from event to record capture (target ≤ 2).
* **Linkage:** % of incidents linked to risks and changes (target ≥ 90%).
* **Access Hygiene:** % of Restricted records with quarterly RBAC attestation (target 100%).
* **Disposition Compliance:** % due and completed on time (target ≥ 95%).

# 15. Training & Awareness

* Onboarding module for all security staff on record creation duties.
* Annual refresher on classification, privacy, and legal hold basics.
* Job‑aids: decision log template, minutes template, incident evidence pack checklist.

# 16. Exceptions & Risk Acceptance

* Exceptions to this model require: business justification, risk assessment, compensating controls, expiry, and approval by CISO + Legal.
* Log in the **KE Exception Register** (Appendix G) with periodic review until closure.

# 17. Version Control

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

# Appendices (Working Templates)

## Appendix A — Meeting Minutes (Security Committee) Template

* **Meeting:** [Committee/Board]
* **Date/Time (TZ):** … **Chair:** … **Secretary:** …
* **Attendees/Apologies:** …
* **Agenda Items:** 1) … 2) … 3) …
* **Discussion Summary:** Capture key points and evidence considered.
* **Motions & Decisions:** Motion text, proposer/seconder, vote, **Decision ID (GOV‑DEC‑####)**.
* **Actions:** Owner, Due Date, Dependencies.
* **Next Meeting:** …
* **Classification:** Internal/Confidential
* **Distribution:** Members only; store in DMS folder [path/ID].

## Appendix B — Security Decision Log (GOV‑DEC) Template

* **Decision Title:** …
* **Context:** What problem/opportunity is being addressed?
* **Options Considered:** A/B/C with pros/cons and evidence.
* **Decision:** … **Date:** … **Decision‑Maker(s):** …
* **Justification:** Rationale and references to risk/controls.
* **Impacts:** People, process, tech, cost.
* **Follow‑ups:** Actions, owners, due dates.
* **Related Records:** Risks, changes, incidents, legal advice IDs.
* **Classification:** … **Retention Class:** …
* **Approvals/Signatures:** …

## Appendix C — Incident Case File (INC‑CAS) Checklist

* **Summary & Timeline** (who/what/when/how)
* **Detections & Evidence** (hashes, screenshots, logs; chain‑of‑custody)
* **Classification & Legal Hold** (if applicable)
* **Containment/Eradication/Recovery actions**
* **Decision Points & Approvals** (with Decision IDs)
* **Notifications** (regulators/customers as required)
* **Post‑Incident Review** (root cause, lessons, control changes)
* **Attachments Index** (filename, checksum, description)
* **Disposition Plan** per retention rules

## Appendix D — Retention Schedule (extract; tailor to law)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Record Type** | **Trigger** | **Retention** | **Rationale** | **Final Disposition** |
| GOV‑DEC | Decision date | 7 yrs | Governance/audit needs | Archive |
| INC‑CAS | Case closure | 7 yrs (or per statute) | Legal/compliance | Archive |
| RSK‑ACC | Exception expiry | 6 yrs | Audit/contract | Destroy with cert |
| CHG‑REC | Change closure | 3 yrs | Ops audit | Destroy |
| LEG‑ADV | Advice received | 7 yrs (privilege rules apply) | Legal | Archive |

## Appendix E — Metadata Dictionary (sample)

| **Field** | **Definition** | **Type** | **Example** | **Required** |
| --- | --- | --- | --- | --- |
| Record ID | Immutable unique identifier | String | RSK‑REG‑2025‑000123 | ✓ |
| Owner | Business owner of content | Person/Role | Risk Manager | ✓ |
| Classification | Sensitivity level | Enum | Confidential | ✓ |
| Legal Hold | Active legal preservation | Boolean + Ref | Y (Case‑2025‑07) | ✓ |
| Evidence Hash | SHA‑256 hash of attachment | String | 9f86d081… | — |

## Appendix F — System of Record Register

|  |  |  |  |
| --- | --- | --- | --- |
| **Record Type** | **SoR** | **Integration(s)** | **Notes** |
| RSK‑REG | GRC/IRM | ITSM (change), DMS (reports) | Unidirectional links; nightly sync |
| INC‑CAS | SOAR/DMS | SIEM, EDR, TIP | Evidence pack export w/ hash |

## Appendix G — KE Exception Register

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Record Type** | **Exception** | **Risk** | **Compensating Controls** | **Owner** | **Expiry** | **Status** |
|  |  |  |  |  |  |  |  |

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

## Appendix H — Maturity Self‑Assessment & Roadmap (abbrev.)

Score each capability 1–5; list top 3 improvements per quarter.

| **Capability** | **Current** | **Target** | **Gap** | **Actions (Next Quarter)** | **Owner** |
| --- | --- | --- | --- | --- | --- |
| Creation & Capture | 2 | 3 | 1 | Add decision log template to GRC; train committees | SecGov Lead |
| Classification & Metadata | 2 | 4 | 2 | Enforce mandatory fields in DMS; add ACL presets | Head of RIM |
| Retention & Disposition | 1 | 3 | 2 | Configure retention in DMS; pilot destruction certs | Records Custodian |
| Access & Privacy | 3 | 4 | 1 | Quarterly RBAC attestations | DPO |
| Systems & Integration | 2 | 3 | 1 | Link ITSM↔GRC↔SOAR records | IT Ops Lead |