

CS-TPL-0002 · COMPLIANCESUITE DOCUMENTATION

# Risk Assessment.

FIT-only redaction. Effective 2026-04-28.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
<b>CS-TPL-0002</b>	<b>v1.0</b>	<b>2026-04-28</b>	<b>Validation Engineering</b>

*Public — Documentation · Review cycle: On change*

# Control block and metadata anchor.

The control block identifies the document, its current revision, the regulated process it supports, and the people accountable for its lifecycle. Every value below is the source of truth for any downstream record, audit trail entry, or signature block.

DOCUMENT ID	CS-TPL-0002
TITLE	Risk Assessment (Format Specification)
VERSION	v1.0
STATUS	FIT-CLEAN
EFFECTIVE DATE	2026-04-28
REVIEW CYCLE	On change
DOCUMENT OWNER	Validation Engineering
CLASSIFICATION	Public — Documentation
RELATED RECORDS	—
SUPERSEDES	— (initial release)

# Sign-off table, ready for ink or e-signature.

The signatures below confirm review and authorisation of this document. Approvals must be recorded in chronological order. If the document is signed electronically, the e-signature record on the ComplianceSuite platform supersedes any handwritten entry on this page and carries the same legal weight under 21 CFR Part 11 and EU GMP Annex 11.

Role	Name	Function	Date	Signature
Author		Validation Lead		
Reviewer		Quality Assurance		
Reviewer		Process / System Owner		
Approver		Head of Quality		
Approver		Regulatory Affairs		

# What's in this document.

01 — Document Control	.....	—
02 — Approvals	.....	—
03 — Contents	.....	—
01 — What this template covers	.....	—
02 — What this template does NOT cover (Roadmap)	.....	—
03 — Risk Assessment Structure	.....	—
04 — Risk Matrix (5x5 Visualization)	.....	—
05 — Code Reference	.....	—
06 — Format Tips	.....	—
Revision History	.....	—
Glossary & Abbreviations	.....	—

# What this template covers.

This Risk Assessment template defines how **risks are systematically identified, evaluated, and mitigated**:

- **FMEA Methodology**: Severity (1–5), Likelihood (1–5), Detectability (1–5)
- **Risk Priority Number (RPN)**:  $S \times L \times D$ , with Risk classification (Low / Medium / High / Critical)
- **Risk Register**: Overview of all identified risks with status (OPEN / MITIGATED / ACCEPTED / CLOSED)
- **Residual Risk**: Post-Mitigation evaluation with QA Approval
- **Risk Matrix**: 5x5 visualization of Severity  $\times$  Likelihood

# What this template does NOT cover (Roadmap).

- **Automatic Risk-Register Generation:** No auto-generation from URS items or Citation Graph
- **Citation Model:** No FK between Risk item and URS item; "From URS" is free-text reference (e.g. "URS-R-001")
- **Coverage-Gap Detection:** No validation that all High-Risk items have Mitigations
- **Residual-Risk Acceptance as Workflow:** No ApprovalChain mechanic; Approval is documentary, not procedurally enforced
- **Risk Reassessment in Periodic Review:** No automatic flagging of Risks for re-evaluation
- **Mitigation-FK to TestCase:** Mitigation references are free text (e.g. "OQ test OQ-014")

# Risk Assessment Structure.

## 1. Scope and Methodology

### 1.1 Scope

This Risk Assessment applies to:

- System: [System Name]
- Change: [Change Number]
- Change Type: Initial Validation / Upgrade / Configuration / Periodic Review

### 1.2 Methodology

FMEA per ICH Q9 (R1, 2023)

Risks are identified from:

- URS Regulatory and Performance Requirements
- System data flows and integrations
- Operational scenarios from Tenant Deviation History of similar systems

## 2. Scoring Scales

### 2.1 Severity Scale (1–5)

Score	Level	Description
5	Catastrophic	Danger to patient safety; Product recall level; Data integrity violation at Regulatory submission
4	Major	Significant impact on product quality, patient safety, or data integrity, but controlled
3	Moderate	Operational impact; user-visible impairment; reversible
2	Minor	Inconvenience; Documentation impact; practical workaround available
1	Negligible	No material impact

### 2.2 Likelihood Scale (1–5)

Score	Level	Description
5	Frequent	Expected regularly under normal operation
4	Likely	Expected occasionally
3	Possible	Could occur under foreseeable conditions
2	Unlikely	Could occur only under unusual conditions
1	Rare	Never observed; would require extraordinary combination of factors

### 2.3 Detectability Scale (1–5)

Score	Level	Description
5	Undetectable	No control would make the failure visible; detected only by consequence
4	Low	Detection requires manual review at low frequency
3	Moderate	Detection via routine procedure checks
2	High	Detection via automated Platform check with Alerting
1	Almost Certain	Detection at point of occurrence; blocking control prevents further processing

## 3. Risk Register

### 3.1 All identified risks

Each row:

- **ID:** RA-001, RA-002, ...
- **Risk:** Risk statement
- **From URS:** Reference to URS item (free text, e.g. "URS-R-001" or "—")
- **S, L, D:** Individual scores (1–5)
- **RPN:**  $S \times L \times D$
- **Class:** Computed from RPN and threshold rule

### Table: Risk Register

ID	Risk	From URS	S	L	D	RPN	Class
RA-001	Audit-trail entries could be modified retroactively without detection.	URS-R-001	5	1	1	5	Low
RA-002	Authorised user is granted a role with broader scope than intended due to manual mis-assignment.	URS-R-003	4	3	3	36	High
RA-003	Search latency degrades under sustained load.	URS-P-001	3	3	2	18	Medium
RA-...	[Add further risks]	—	—	—	—	—	—

### Risk-Class Thresholds

Standard thresholds (can be tightened per Tenant, not relaxed):

- **Low:** RPN ≤ 12
- **Medium:** 13 ≤ RPN ≤ 24
- **High:** RPN ≥ 25 OR Severity = 5
- **Critical:** (not used by default; can be defined as Tenant Override)

## 4. Mitigations and Verification

### 4.1 Mitigation Plan per Risk

Risk ID	Mitigation	Verification Reference
RA-001	Hash-chained audit trail; verification utility output reviewed at every Periodic Review.	OQ test OQ-014; Periodic Review procedure
RA-002	Quarterly Access Review by Account Compliance Lead; documented in Periodic Review record.	OQ test OQ-015; access review record

Risk ID	Mitigation	Verification Reference
RA-003	PQ test exercises search latency under target load; ongoing performance observability via Customer monitoring.	PQ test PQ-007; observability rule
RA-...	[Mitigation text]	[Test or Procedural reference]

**Note:**

- Mitigation references are **free text** (e.g. "OQ test OQ-014"); no FK to TestCase model
- Verification occurs via naming convention (IQ/OQ/PQ numbers) or procedural reference

## 5. Residual Risk and Acceptance

After completion of the Verify phase, each risk is re-evaluated.

### 5.1 Residual Risk Table

Risk ID	Pre-Mitigation RPN	Post-Mitigation RPN	Decision	Approver
RA-002	36 (High)	8 (Low)	Accepted as mitigated	[QA Name]
RA-003	18 (Medium)	12 (Low)	Accepted as mitigated	[QA Name]
RA-...	—	—	[Accepted / Carried as residual / Re-scoped]	[Name]

### 5.2 Residual Risk Carry-Forward

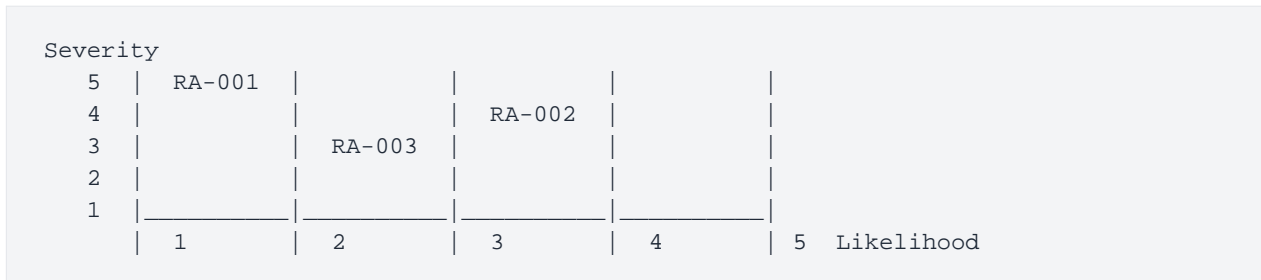
Risks with Post-Mitigation RPN in the **High Band** may be carried forward with documented justification and QA Approval.

**Validation Report Requirement:**

- **Acceptance Recommendation** must explicitly address residual risks
- **Operational Control** per residual Risk (e.g. SIEM Alert, Periodic Review Check, Routine Report)
- **Re-Trigger Condition** (when would the risk be re-evaluated?)

# Risk Matrix (5x5 Visualization).

A 5x5 matrix visualizes Severity (y-axis) vs. Likelihood (x-axis):



- **Red zones** (High Risk): Require Mitigation before Closure
- **Yellow zone** (Medium): Should be addressed; can be deferred with justification
- **Green zone** (Low): Acceptable without Mitigation

# Code Reference.

- **Risk Assessment Model:** `prisma/schema.prisma` → `RiskItem` (riskId, description, severity, likelihood, detectability, status)
- **Risk Classification:** Computed in App logic;  $RPN = S \times L \times D$ , then Mapping to Class
- **Risk Matrix:** `components/compliance/RiskMatrix.tsx` (Visualization)
- **Risk Register:** `RiskAssessment` Document Type; table management in Editor
- **Residual Risk:** `residualSeverity`, `residualProbability`, `residualDetectability` in `RiskItem` (optional)
- **Mitigation References:** Free text; no FK linkage

# Format Tips.

- **Risk Identification** is **manual**; no generation from URS
- **Scoring Discipline**: Team-based evaluation; multiple perspectives desired
- **Post-Mitigation Assessment** is performed in the Execute phase
- **Residual Risk Carry-Forward** requires documented justification + QA Approval
- **ICH Q9 (R1)** is followed conceptually, but not present as explicit Methodology enum in code

REVISION HISTORY

# Every change, tracked and signed.

Add one row for every controlled revision. Minor changes (typos, formatting) increment the patch version; substantive edits trigger a fresh review cycle and a new approver round.

Version	Date	Author	Summary of Change	Approver
1.0	2026-04-28	Documentation Team	Initial release of the Risk Assessment template.	Head of Documentation
—	—	—	Reserved for next revision. Do not delete this row.	—

GLOSSARY

# Shared language, no ambiguity.

Definitions used throughout this document. Where a term has a specific meaning inside ComplianceSuite, the platform-specific definition takes precedence over the generic regulatory term.

<b>CSV</b>	Computerized Systems Validation
<b>GAMP 5</b>	Good Automated Manufacturing Practice, Edition 5 (2nd edition, 2022)
<b>GxP</b>	Good 'x' Practice — covers GMP, GLP, GCP, GDP, GVP
<b>IQ / OQ / PQ</b>	Installation / Operational / Performance Qualification
<b>Part 11</b>	21 CFR Part 11 — US FDA rule on electronic records and electronic signatures
<b>Annex 11</b>	EU GMP Annex 11 — EU rule on computerised systems
<b>URS</b>	User Requirements Specification
<b>FRS</b>	Functional Requirements Specification
<b>RTM</b>	Requirements Traceability Matrix
<b>SOP</b>	Standard Operating Procedure
<b>ALCOA+</b>	Attributable, Legible, Contemporaneous, Original, Accurate (+ Complete, Consistent, Enduring, Available)
<b>ICH Q9</b>	International Council for Harmonisation Quality Risk Management guideline

— End of document —