CS-TPL-0002 · GXP-DESK DOCUMENTATION

Risk Assessment.

FIT-only redaction. Effective 2026-06-04.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-TPL-0002	v1.0	2026-06-04	Validation Engineering

Public — Documentation · Review cycle: On change

01 — DOCUMENT CONTROL

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	2026-06-04
REVIEW CYCLE	On change
DOCUMENT OWNER	Validation Engineering
CLASSIFICATION	Public — Documentation
RELATED RECORDS	—
SUPERSEDES	— (initial release)

02 — APPROVALS

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 GxP-Desk 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		

03 — CONTENTS

What's in this document.

01 — WHAT THIS TEMPLATE COVERS

What this template covers.

This risk-assessment template defines how **risks are systematically identified, assessed, and mitigated**:

- **FMEA methodology**: Severity (1–5), Likelihood (1–5), Detectability (1–5)
- **Risk Priority Number (RPN)**: S × L × D, with a risk classification (Low / Medium / High / Critical)
- **Risk Register**: An overview of all identified risks with status (OPEN / MITIGATED / ACCEPTED / CLOSED)
- **Residual Risk**: Post-mitigation assessment with QA approval
- **Risk Matrix**: A 5×5 visualization of Severity × Likelihood

02 — WHAT THIS TEMPLATE DOES NOT COVER (ROADMAP)

What this template does NOT cover (Roadmap).

- **Automatic risk-register generation**: No auto-generation from URS items or a citation graph
- **Citation model**: No FK between a risk item and a URS item; "From URS" is a free-text reference (e.g., "URS-R-001")
- **Coverage-gap detection**: No validation that all high-risk items have mitigations
- **Residual-risk acceptance as a workflow**: No ApprovalChain mechanism; approval is documentary, not procedurally enforced
- **Risk reassessment in periodic review**: No automatic flagging of risks for reassessment
- **Mitigation FK to TestCase**: Mitigation references are free text (e.g., "OQ test OQ-014")

Structure of the Risk Assessment.

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 the tenant deviation history of similar systems

2. Scoring Scales

2.1 Severity Scale (1–5)

Score	Level	Description
5	Catastrophic	Hazard to patient safety; product-recall level; data-integrity breach in a regulatory submission
4	Major	Significant impact on product quality, patient safety, or data integrity, but controlled
3	Moderate	Operational impact; user-visible degradation; reversible
2	Minor	Inconvenience; documentation impact; a practical workaround is 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 an exceptional combination of factors

2.3 Detectability Scale (1–5)

Score	Level	Description
5	Undetectable	No control would make the failure visible; detected only through a downstream consequence
4	Low	Detection requires manual review at low frequency
3	Moderate	Detection through routine procedural checks
2	High	Detection through an automated platform check with alerting
1	Almost Certain	Detection at the point of occurrence; a blocking control prevents further processing

3. Risk Register

3.1 All Identified Risks

Each row:

- **ID**: RA-001, RA-002, ...
- **Risk**: A statement of the risk
- **From URS**: Reference to a URS item (free text, e.g., "URS-R-001" or "—")
- **S, L, D**: Individual scores (1–5)
- **RPN**: S × L × D

- **Class**: Computed from the RPN and the 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 (may be tightened, not relaxed, per tenant):

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

Risk ID	Mitigation	Verification Reference
RA-002	Quarterly Access Review by Account Compliance Lead; documented in Periodic Review record.	OQ test OQ-015; access review record
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"); there is no FK to the TestCase model
- Verification is achieved through a naming convention (IQ/OQ/PQ numbers) or a procedural reference

5. Residual Risk and Acceptance

After the verify phase is complete, each risk is reassessed.

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 a post-mitigation RPN in the **High band** may be carried forward with a documented rationale and QA approval.

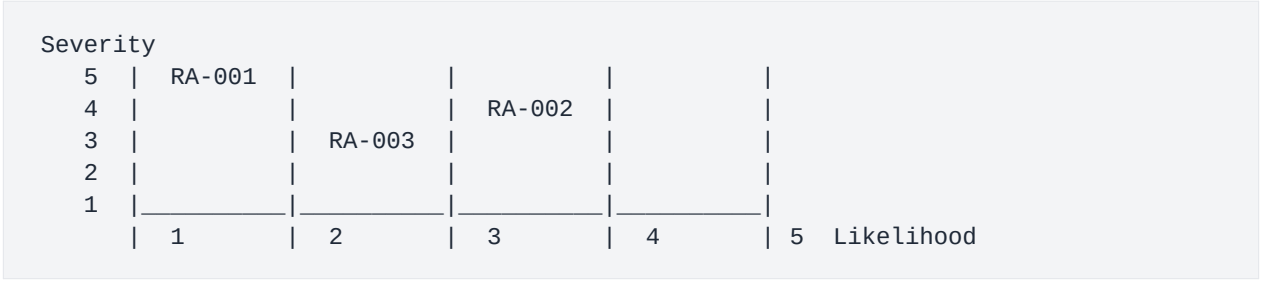
Requirements for the Validation Report:

- The **acceptance recommendation** must explicitly address residual risks
- An **operational control** per residual risk (e.g., SIEM alert, Periodic Review check, routine report)
- A **re-trigger condition** (when would the risk be reassessed?)

04 — RISK MATRIX (5×5 VISUALIZATION)

Risk Matrix (5×5 Visualization).

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



- **Red zones** (High Risk): Require mitigation before closure
- **Yellow zone** (Medium): Should be addressed; may be deferred with a rationale
- **Green zone** (Low): Acceptable even without mitigation

05 — CODE REFERENCES

Code references.

- **Risk-Assessment Model**: `prisma/schema.prisma` → `RiskItem` (riskId, description, severity, likelihood, detectability, status)
- **Risk Classification**: Computed in app logic; RPN = S × L × D, then mapped to Class
- **Risk Matrix**: `components/compliance/RiskMatrix.tsx` (visualization)
- **Risk Register**: `RiskAssessment` document type; table management in the editor
- **Residual Risk**: `residualSeverity`, `residualProbability`, `residualDetectability` in RiskItem (optional)
- **Mitigation References**: Free text; no FK linking

06 — FORMAT TIPS

Format Tips.

- **Risk identification** is **manual**; there is no generation from the URS
- **Scoring discipline**: Team-based assessment; multiple perspectives are encouraged
- **Post-mitigation assessment** is performed in the execute phase
- **Residual risk carry-forward** requires a documented justification + QA approval
- **ICH Q9 (R1)** is followed conceptually but is not present as an explicit methodology enum in the 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 GxP-Desk, the platform-specific definition takes precedence over the generic regulatory term.

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

— End of document —