Risk-Based Priority Matrix v1.0

What RBPM Combines	1. Potential Risks from RTM (Requirement Traceability Matrix) 2. Risk Impact & Likelihood analysis 3. Business Criticality (Must-Have vs Should-Have) 4. Security & E-commerce Vulnerabilities from OWASP Top 10: https://owasp.org/Top10/2025/

Priority Score Formula

Priority Score = (Impact Score) * (Likelihood Score) * MosCoW Type

Risk Factors: Impact (1-5), Likelihood (1-5)
MosCow Type: Must-have (1.20), Should-have (1.0)

The priority score is used as a guideline for relative test execution prioritization.

Risk Levels

Critical (P0)	High (P1)	Medium (P2)	Low (P3)
• Risk Score: 24 - 30 • Impact: Immediate business loss • Frequency: High • Fix urgency: ASAP	• Risk Score: 14 - 23.9 • Impact: Significant business disruption • Frequency: Medium • Fix urgency: High	• Risk Score: 7 - 13.9 • Impact: Moderate business impact • Frequency: Medium-Low • Fix urgency: Standard	• Risk Score: 1 - 6.9 • Impact: Low business impact • Frequency: Low • Fix urgency: Low

Risk Identification & Priority

REQ ID	Potential Risks	MoSCoW	MosCoW Weight	Impact	Likelihood	Risk Score	Priority
REQ-014	Authentication failure	Must-Have	1.20	5	4	24	P0
REQ-019	Payment processing failure	Must-Have	1.20	5	4	24	P0
REQ-022	Authentication failure	Must-Have	1.20	5	4	24	P0
REQ-021	Missing order records	Must-Have	1.20	5	3	18	P1
REQ-023	Unauthorized access	Must-Have	1.20	5	3	18	P1
REQ-001	Page load or routing failure	Must-Have	1.20	4	3	14.4	P1
REQ-004	Incorrect filtering logic	Must-Have	1.20	4	3	14.4	P1
REQ-008	Missing or incorrect product data	Must-Have	1.20	4	3	14.4	P1
REQ-009	Data inconsistency	Must-Have	1.20	4	3	14.4	P1
REQ-024	Invalid data creation	Must-Have	1.20	4	3	14.4	P1
REQ-025	Data inconsistency	Must-Have	1.20	4	3	14.4	P1
REQ-010	Session persistence failure	Should-Have	1.00	4	3	12	P2
REQ-020	Missing confirmation	Should-Have	1.00	4	3	12	P2
REQ-026	Residual data exposure	Must-Have	1.20	5	2	12	P2
REQ-002	Broken navigation link	Must-Have	1.20	3	3	10.8	P2
REQ-007	Broken product link	Must-Have	1.20	3	3	10.8	P2
REQ-016	Broken access flow	Must-Have	1.20	4	2	9.6	P2
REQ-017	Data persistence failure	Must-Have	1.20	4	2	9.6	P2

REQ-015	Improper error handling	Should-Have	1.00	3	3	9	P2
REQ-003	Incorrect access restriction	Should-Have	1.00	4	2	8	P2
REQ-027	Incorrect role assignment	Should-Have	1.00	4	2	8	P2
REQ-005	Filter state not reset	Must-Have	1.20	3	2	7.2	P2
REQ-006	User confusion due to empty results	Must-Have	1.20	2	3	7.2	P2
REQ-011	Session handling issues	Must-Have	1.20	3	2	7.2	P2
REQ-012	Homepage rendering issues	Must-Have	1.20	3	2	7.2	P2
REQ-013	Broken redirect	Must-Have	1.20	3	2	7.2	P2
REQ-018	Session sync issues	Should-Have	1.00	3	2	6	P3

Risk Assessment & Mitigation Strategy	Security Risks Mitigation: API testing for access control and data validation, with targeted exploratory testing.	Functional Risks Mitigation: System testing for key user flows and end-to-end scenarios	Usability Risks Mitigation: Exploratory testing to identify usability gaps and edge cases.

Test Execution Priority	API & System Testing **P0** REQ-014, REQ-019, REQ-022 **P1** REQ-001, REQ-004, REQ-008, REQ-009, REQ-021, REQ-023, REQ-024, REQ-025 **P2** REQ-002, REQ-003, REQ-005, REQ-006, REQ-007, REQ-010, REQ-011, REQ-012, REQ-013, REQ-015, REQ-016, REQ-017, REQ-020, REQ-026, REQ-027 **P3** REQ-018	UAT UAT is conducted at the user story level to validate business acceptance criteria.