CONFIDENTIAL · Distribution: Quality Engineering / Release Committee / Defect Remediation Owners / Audit & Compliance Records

Voyager V3
Inspect Defect Governance Audit Report

Defect Inspection Audit Report · Complete dossier of 178 QD defect items · Static inspection evidence · Independently reviewable

Release Blocked
FAIL

Detected **178** defects. Severity:**P0×55** / **P1×123** / **P2×0** All have been archived and handed over for remediation.

Release conclusion basis: Inspect Gate rule — any sub-specification with unaddressed P0 defects → FAIL (mandatory gate not passed).

Report No. **SO-INS-20260927-V9BF**	Inspected Object **Voyager**	Version / Baseline **V3**
Check Type **Specification Check · Inspect Four Sub-sets**	Executed Modules **QDP + QDT + QDS + CROSS**	Check Completed At **2026-09-27**
Check Duration **11m 1s**	Classification **Confidential (CONFIDENTIAL)**	Validity **Until closed-loop re-inspection passes**

B Scope & Methodology

Check Object & Version

System	Voyager
Version / Baseline	`V3`
Artifact Scope	Skill ×5 / Tool Schema ×8 / Prompt / Cross definitions
Check Level	L2 (State-changing · standard rule set)
Check Time	2026-09-27
Execution Method	Static artifact analysis + LLM rule-based checking

Sampling & Coverage

QD-P (Prompt)	40 L2 check items
QD-T (Tool)	12 L2 check items
QD-S (Skill)	20 L2 check items
ps	4 check items
pt	Skipped: Tool Schema artifacts not provided; PT check not applicable
Total Applicable	**76 items** (L2 full set, no sampling)
Skipped	4 items (PT 4)
Not Applicable	4 items (ST 4)

Preconditions

① The three artifacts (Prompt / Skill / Tool Schema) must be frozen in the same version snapshot with version numbers registered;② Check-item severity follows the inherent severity of the Agent Level (L2);③ No artifacts found for ST 4; the related modules are marked "Not Applicable", which does not affect the validity of conclusions for executed modules; in addition, PT 4 was marked "Skipped" because no cross-artifact association was matched — a coverage gap; it is recommended to supplement artifact declarations or re-check after manual review。

Method & Rule Versions

Rule Document	Version	Usage in This Report
"Inspect Prompt Sub-specification" (QD-P)	`v1.0`	Logic defects (contradiction / mismatch / scope delimitation / redundancy / implication) + explicit defects (structure / input / output / constraint boundaries / exception handling)
"Inspect Tool Sub-specification" (QD-T)	`v1.0`	Structural validity / parameter constraints / high-risk operations / semantic clarity / Schema changes
"Inspect Skill Sub-specification" (QD-S)	`v1.0`	Resource runaway / unbounded declarations / ambiguous inference / failure expansion / privilege escalation (Review Schema six dimensions)
"Inspect Cross Sub-specification" (QD-PS/PT/ST)	`v1.0`	Prompt↔Skill / Prompt↔Tool / Skill↔Tool cross-artifact consistency

Rule versions are registered together with artifact snapshots; this report references §6.2 "Release Summary Status" of the SanityOps Core Specification and §1.2 "Four-Segment Structure" of the SanityOps Linkage Mapping Specification.

Not Covered (the conclusions of this report cannot replace)

- Multi-turn dynamic attack verification — belongs to Risk Implicit (implicit risk verification), outside the scope of this report;
- Service quality and task correctness — belongs to Quality (quality assessment), outside the scope of this report;
- Runtime monitoring, online alerting, and privilege-escalation access audit logs — outside the scope of Inspect static checking.

B Scope & Methodology (cont.)

Limitations & Assumptions

- This report is a**static text audit**: it can confirm that "definition-level defects or risk expressions exist", but**cannot** alone confirm "runtime exploitability" or "impact that has already occurred";
- The "location" of defects uses version baseline`V3`as the coordinate baseline; "original evidence" is a summary of affected fragments;
- Inspect pass ≠ security pass ≠ quality pass — the three conclusions have separate boundaries and cannot substitute for one another.

C Conclusion & Determination

178	55	123	0
Defects Detected	P0 · Release Blocking	P1 · Fix in Version	P2 · Schedulable

0	68	24.3	100
QDS Score	QDT Score	QDP Score	CROSS Score

Score Calculation (recalculable layer by layer) Table 2 / Table 3 / Table 4

Table 2 QD-S Score Recalculation (Skill Sub-specification · L2)

Total Check Items (L2)	20 items (P0 6 / P1 14 / P2 0)	Total Weight	5×6 + 3×14 + 1×0 = 72
Base Score	100 / 72 = 1.3889	Per-item Deduction	Each Skill deducted independently and averaged
Failed	20 items (P0 6 / P1 14)	Total Deduction	Each Skill deducted independently and averaged → average deduction 100
QD-S Score	**0**		

Table 3 QD-T Score Recalculation (Tool Sub-specification · L2)

Total Check Items (L2)	12 items (P0 5 / P1 7 / P2 0)	Total Weight	5×5 + 3×7 + 1×0 = 46
Base Score	100 / 46 = 2.1739	Per-item Deduction	Each Skill deducted independently and averaged
Failed	6 items (P0 1 / P1 5)	Total Deduction	Each Skill deducted independently and averaged → average deduction 32.05
QD-T Score	**68**		

Table 4 QD-P Score Recalculation (Prompt Sub-specification · L2)

Total Check Items (L2)	40 items (P0 18 / P1 20 / P2 2)	Total Weight	5×18 + 3×20 + 1×2 = 152
Base Score	100 / 152 = 0.6579	Per-item Deduction	P0 3.29 / P1 1.97
Failed	29 items (P0 14 / P1 15)	Total Deduction	14×3.29 + 15×1.97 = 75.66
QD-P Score	**24.3**		

Table 5 QD-Cross Score Recalculation (Cross Sub-specification · L2)

Total Check Items (L2)	12 items (P0 9 / P1 3 / P2 0)	Total Weight	5×9 + 3×3 + 1×0 = 54
Base Score	100 / 54 = 1.8519	Per-item Deduction	—
Failed	0 items	Total Deduction	0 = 0
QD-Cross Score	**100**		

Basis: Total Weight takes the**full check-item table**of the Agent Level (not the number of failed items): W_total = P0×5 + P1×3 + P2×1; Base Score = 100 / W_total; each check-item ID is deducted only once; Score = max(100 – total deduction, 0); Score is for quality reference only, with no pass threshold.

C Conclusion & Determination (cont.)

Gate Determination Rules & Baseline Comparison

Determination Item	Rule	Result This Run
Inspect Gate	Any sub-specification with P0 → FAIL; otherwise PASS	**FAIL (P0: 55 items)**
Comparison with Previous Version	Item-by-item comparison requires the previous version's dossier (ratchet mechanism: Score must not degrade from the baseline)	No previous-version data available for comparison

Counting basis: defects are deduplicated by "check-item ID"; multiple hits on the same check-item ID deduct points only once; P0 (blocking, must fix) / P1 (significant, fix in version) / P2 (general, schedulable).

D Findings Dossier (1/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-1.1 ②P0 The Skill does not declare explicit input boundari

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** optimize_budget
⑤ **Location** `Execution Flow / Input Boundary`
⑥ **Original Evidence** **The Skill does not declare explicit input boundaries such as maximum number of cost items, maximum input characters, behavior when input exceeds limits, or safe defaults for missing/ambiguous input. The intermediate review confirms input.max_items, input.max_chars, input.if_exceeds, and input.safe_defaults are all missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add limit: "Process up to 50 items. When exceeded, process the first 50 items and notify the user."
Evidence Strength Confirmed (static)

①QDS-1.3 ②P0 The Skill does not declare explicit execution boun

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** optimize_budget
⑤ **Location** `Execution Flow / Execution Boundary`
⑥ **Original Evidence** **The Skill does not declare explicit execution boundaries such as maximum tool calls, maximum retries, task expansion policy, inference of missing data, skill chaining, allowed downstream skills, user confirmation requirements, or behavior when budget is exceeded. The intermediate review confirms these execution boundary items are missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Max retries: 3. Timeout: 60 seconds. Max tool calls per turn: 10."
Evidence Strength Confirmed (static)

①QDS-2.1 ②P0 The Skill does not declare explicit input boundari

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** optimize_budget
⑤ **Location** `Execution Flow / Input Boundary`
⑥ **Original Evidence** **The Skill does not declare explicit input boundaries for the budget optimization task. It lacks limits such as max_items, max_chars, behavior when input exceeds limits, and safe defaults. The intermediate review confirms input.max_items, input.max_chars, input.if_exceeds, and input.safe_defaults are all missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace 'all' with 'up to N items', or add explicit upper limit after unbounded words.
Evidence Strength Confirmed (static)

①QDS-2.2 ②P0 The Skill does not bound execution. It lacks max_t

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** optimize_budget
⑤ **Location** `Execution Flow`
⑥ **Original Evidence** **The Skill does not bound execution. It lacks max_tool_calls, max_retries, allow_task_expansion, allow_inference_of_missing_data, allow_skill_chaining, allowed_downstream_skills, require_user_confirmation_for, and if_budget_exceeded. Only timeout_seconds is identified, leaving execution scope effectively unbounded.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace with: "Max 3 retries. If still failing, stop and report error."
Evidence Strength Confirmed (static)

D Findings Dossier (2/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-3.4 ②P0 The Skill does not explicitly declare forbidden re

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** optimize_budget
⑤ **Location** `identity.forbidden_resources, identity.forbidden_operations`
⑥ **Original Evidence** **The Skill does not explicitly declare forbidden resources or forbidden operations, so the identity boundary is incomplete and ambiguity could allow unintended resource use or actions.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add "do not do" section: "Do not: infer from conversation history, add unprovided facts, extend to related tasks."
Evidence Strength Confirmed (static)

①QDS-4.1 ②P0 The Skill does not explicitly define failure escal

③ **Category** QD-S (Skill) · FAILURE
④ **Artifact** optimize_budget
⑤ **Location** `Execution Flow / Failure Handling`
⑥ **Original Evidence** **The Skill does not explicitly define failure escalation behavior for the FAILURE dimension. It lacks a clear requirement and boundary for how failures should be escalated, such as when to stop, retry, or hand off to a user or higher-level process.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "On execution failure, stop immediately and report error. Do not attempt alternatives."
Evidence Strength Confirmed (static)

①QDS-1.1 ②P0 The Skill does not declare explicit input boundari

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** build_itinerary
⑤ **Location** `Execution Flow / When This Skill Runs`
⑥ **Original Evidence** **The Skill does not declare explicit input boundaries such as maximum items, maximum characters, behavior when input exceeds limits, or safe defaults. The intermediate review shows input.max_items, input.max_chars, input.if_exceeds, and input.safe_defaults are all missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add limit: "Process up to 50 items. When exceeded, process the first 50 items and notify the user."
Evidence Strength Confirmed (static)

①QDS-1.3 ②P0 The Skill lacks explicit execution boundaries for

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** build_itinerary
⑤ **Location** `Execution Flow`
⑥ **Original Evidence** **The Skill lacks explicit execution boundaries for maximum tool calls, maximum retries, task expansion, inference of missing data, skill chaining, allowed downstream skills, user confirmation requirements, and budget-exceeded behavior. Only timeout_seconds is identified in the intermediate review.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Max retries: 3. Timeout: 60 seconds. Max tool calls per turn: 10."
Evidence Strength Confirmed (static)

D Findings Dossier (3/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-2.1 ②P0 The Skill does not define explicit input boundarie

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** build_itinerary
⑤ **Location** `INPUT (Input Boundary)`
⑥ **Original Evidence** **The Skill does not define explicit input boundaries. It lacks limits such as max_items, max_chars, behavior when input exceeds limits, and safe defaults. The intermediate review confirms input.max_items, input.max_chars, input.if_exceeds, and input.safe_defaults are all missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace 'all' with 'up to N items', or add explicit upper limit after unbounded words.
Evidence Strength Confirmed (static)

①QDS-2.2 ②P0 The Skill does not define explicit execution bound

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** build_itinerary
⑤ **Location** `EXECUTION (Execution Boundary)`
⑥ **Original Evidence** **The Skill does not define explicit execution boundaries. It lacks limits such as max_tool_calls, max_retries, allow_task_expansion, allow_inference_of_missing_data, allow_skill_chaining, allowed_downstream_skills, require_user_confirmation_for, and if_budget_exceeded. The intermediate review confirms these execution boundary items are missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace with: "Max 3 retries. If still failing, stop and report error."
Evidence Strength Confirmed (static)

①QDS-3.4 ②P0 The Skill does not explicitly declare identity bou

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** build_itinerary
⑤ **Location** `Skill metadata and Execution Flow`
⑥ **Original Evidence** **The Skill does not explicitly declare identity boundaries for non-goals, allowed/forbidden resources, or allowed/forbidden operations. Without these explicit boundaries, the agent may infer permissible scope and resources, enabling ambiguity-induced inference.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add "do not do" section: "Do not: infer from conversation history, add unprovided facts, extend to related tasks."
Evidence Strength Confirmed (static)

①QDS-4.1 ②P0 The Skill does not explicitly define failure escal

③ **Category** QD-S (Skill) · FAILURE
④ **Artifact** build_itinerary
⑤ **Location** `Execution Flow / Failure Handling`
⑥ **Original Evidence** **The Skill does not explicitly define failure escalation behavior for the FAILURE dimension. Although it mentions surfacing a travel blocker and proposing alternatives, it lacks an explicit escalation requirement and boundary for failures such as tool errors, infeasible plans, or unresolved blockers.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "On execution failure, stop immediately and report error. Do not attempt alternatives."
Evidence Strength Confirmed (static)

D Findings Dossier (4/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-1.1 **②P0** No explicit input boundary is declared. The Skill

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** prep_travel_documents
⑤ **Location** `Execution Flow / When This Skill Runs`
⑥ **Original Evidence** **No explicit input boundary is declared. The Skill does not specify max_items, max_chars, behavior when input exceeds limits, or safe defaults for missing/ambiguous traveler data such as nationality, passport expiry, destination, transit countries, or dates.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add limit: "Process up to 50 items. When exceeded, process the first 50 items and notify the user."
Evidence Strength Confirmed (static)

①QDS-1.3 **②P0** Execution boundaries are largely absent. Although

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** prep_travel_documents
⑤ **Location** `Execution Flow`
⑥ **Original Evidence** **Execution boundaries are largely absent. Although timeout_seconds is identified, the Skill does not declare max_tool_calls, max_retries, allow_task_expansion, allow_inference_of_missing_data, allow_skill_chaining, allowed_downstream_skills, require_user_confirmation_for, or if_budget_exceeded.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Max retries: 3. Timeout: 60 seconds. Max tool calls per turn: 10."
Evidence Strength Confirmed (static)

①QDS-2.1 **②P0** The Skill does not declare explicit input boundari

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** prep_travel_documents
⑤ **Location** `Execution Flow steps 1-3; When This Skill Runs`
⑥ **Original Evidence** **The Skill does not declare explicit input boundaries. The intermediate review shows input.max_items, input.max_chars, input.if_exceeds, and input.safe_defaults are all missing. The Skill accepts traveler nationality, destination countries, transit countries, dates, passport expiry, prior trips, and itinerary details without limits or overflow handling, leaving the input scope unbounded.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace 'all' with 'up to N items', or add explicit upper limit after unbounded words.
Evidence Strength Confirmed (static)

①QDS-2.2 **②P0** The Skill does not declare explicit execution boun

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** prep_travel_documents
⑤ **Location** `Execution Flow steps 1-6; Error Handling`
⑥ **Original Evidence** **The Skill does not declare explicit execution boundaries. The intermediate review shows execution.max_tool_calls, execution.max_retries, execution.allow_task_expansion, execution.allow_inference_of_missing_data, execution.allow_skill_chaining, execution.allowed_downstream_skills, execution.require_user_confirmation_for, and execution.if_budget_exceeded are all missing. Only timeout_seconds is identified. The flow can call tools, infer missing data, and persist results without declared limits or confirmation gates.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace with: "Max 3 retries. If still failing, stop and report error."
Evidence Strength Confirmed (static)

D Findings Dossier (5/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-3.4 ②P0 The Skill does not explicitly declare identity bou

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** prep_travel_documents
⑤ **Location** `Skill metadata / Execution Flow`
⑥ **Original Evidence** **The Skill does not explicitly declare identity boundaries for ambiguity handling: no non-goals, allowed/forbidden resources, or allowed/forbidden operations are stated. This leaves the agent free to infer scope and resources when requirements are ambiguous.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add "do not do" section: "Do not: infer from conversation history, add unprovided facts, extend to related tasks."
Evidence Strength Confirmed (static)

①QDS-4.1 ②P0 The Skill does not explicitly define a failure esc

③ **Category** QD-S (Skill) · FAILURE
④ **Artifact** prep_travel_documents
⑤ **Location** `Error Handling`
⑥ **Original Evidence** **The Skill does not explicitly define a failure escalation requirement or boundary. The Error Handling section is truncated and only partially addresses one failure case ('Visa window already blown'); it does not establish an explicit escalation path, escalation triggers, or escalation target for failures.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "On execution failure, stop immediately and report error. Do not attempt alternatives."
Evidence Strength Confirmed (static)

①QDS-1.1 ②P0 No explicit input boundary is declared: the Skill

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** replan_disruption
⑤ **Location** `Execution Flow / When This Skill Runs`
⑥ **Original Evidence** **No explicit input boundary is declared: the Skill does not state max_items, max_chars, behavior when input exceeds limits, or safe defaults for missing/empty input. The intermediate review confirms input.max_items, input.max_chars, input.if_exceeds, and input.safe_defaults are all missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add limit: "Process up to 50 items. When exceeded, process the first 50 items and notify the user."
Evidence Strength Confirmed (static)

①QDS-1.3 ②P0 Execution boundaries are largely undeclared: no ma

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** replan_disruption
⑤ **Location** `Execution Flow`
⑥ **Original Evidence** **Execution boundaries are largely undeclared: no max_tool_calls, max_retries, allow_task_expansion, allow_inference_of_missing_data, allow_skill_chaining, allowed_downstream_skills, require_user_confirmation_for, or if_budget_exceeded. Only timeout_seconds is identified, which is insufficient for the P0 execution boundary requirement.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Max retries: 3. Timeout: 60 seconds. Max tool calls per turn: 10."
Evidence Strength Confirmed (static)

D Findings Dossier (6/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-2.1 ②P0 The Skill does not declare any input boundary for

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** replan_disruption
⑤ **Location** `Execution Flow step 1 (Take stock) / When This Skill Runs`
⑥ **Original Evidence** **The Skill does not declare any input boundary for the disruption report or itinerary data it consumes. There is no max_items, max_chars, if_exceeds, or safe_defaults declaration, so an unbounded or malformed input could be processed without a defined limit or fallback.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace 'all' with 'up to N items', or add explicit upper limit after unbounded words.
Evidence Strength Confirmed (static)

①QDS-2.2 ②P0 The Skill does not bound its execution. It declare

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** replan_disruption
⑤ **Location** `Execution Flow steps 1-7`
⑥ **Original Evidence** **The Skill does not bound its execution. It declares no max_tool_calls, max_retries, allow_task_expansion, allow_inference_of_missing_data, allow_skill_chaining, allowed_downstream_skills, require_user_confirmation_for, or if_budget_exceeded. Only timeout_seconds is identified in the intermediate review, leaving the directive effectively unbounded.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace with: "Max 3 retries. If still failing, stop and report error."
Evidence Strength Confirmed (static)

①QDS-3.4 ②P0 The Skill does not explicitly declare identity bou

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** replan_disruption
⑤ **Location** `Skill content / frontmatter and Execution Flow`
⑥ **Original Evidence** **The Skill does not explicitly declare identity boundaries for ambiguity handling: non-goals, allowed/forbidden resources, and allowed/forbidden operations are missing, so the agent may infer scope and permissions when disruption details are ambiguous.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add "do not do" section: "Do not: infer from conversation history, add unprovided facts, extend to related tasks."
Evidence Strength Confirmed (static)

①QDS-4.1 ②P0 The Skill does not explicitly define failure escal

③ **Category** QD-S (Skill) · FAILURE
④ **Artifact** replan_disruption
⑤ **Location** `Execution Flow / FAILURE section`
⑥ **Original Evidence** **The Skill does not explicitly define failure escalation behavior for the FAILURE dimension. It lacks a declared escalation path or boundary for when disruption replanning fails (e.g., no viable replacement transport/lodging, rebooking tools fail, or the traveler rejects the rebuilt plan). The intermediate review confirms failure.on_empty_input, failure.on_insufficient_input, failure.on_user_dissatisfied, and failure.forbidden_behaviors are all missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "On execution failure, stop immediately and report error. Do not attempt alternatives."
Evidence Strength Confirmed (static)

D Findings Dossier (7/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-1.1 ②P0 The Skill does not declare explicit input boundari

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** monitor_travel_alerts
⑤ **Location** `Execution Flow / Skill content`
⑥ **Original Evidence** **The Skill does not declare explicit input boundaries. It lacks limits such as max_items, max_chars, behavior when input exceeds limits, and safe defaults for missing or malformed itinerary/alert inputs.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add limit: "Process up to 50 items. When exceeded, process the first 50 items and notify the user."
Evidence Strength Confirmed (static)

①QDS-1.3 ②P0 The Skill does not declare explicit execution boun

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** monitor_travel_alerts
⑤ **Location** `Execution Flow`
⑥ **Original Evidence** **The Skill does not declare explicit execution boundaries. It lacks max_tool_calls, max_retries, allow_task_expansion, allow_inference_of_missing_data, allow_skill_chaining, allowed_downstream_skills, require_user_confirmation_for, and if_budget_exceeded controls.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Max retries: 3. Timeout: 60 seconds. Max tool calls per turn: 10."
Evidence Strength Confirmed (static)

①QDS-2.1 ②P0 The Skill does not declare explicit input boundari

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** monitor_travel_alerts
⑤ **Location** `Execution Flow step 2; Severity Matrix`
⑥ **Original Evidence** **The Skill does not declare explicit input boundaries for the alert sweep. It lacks limits such as max destinations, max date-window span, max alerts processed, or behavior when input exceeds those limits. The intermediate review confirms input.max_items, input.max_chars, input.if_exceeds, and input.safe_defaults are all missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace 'all' with 'up to N items', or add explicit upper limit after unbounded words.
Evidence Strength Confirmed (static)

①QDS-2.2 ②P0 The Skill does not bound execution. It allows per-

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** monitor_travel_alerts
⑤ **Location** `Execution Flow steps 2-5`
⑥ **Original Evidence** **The Skill does not bound execution. It allows per-destination and transit-corridor sweeps, weather checks, severity classification, and possible immediate replanning, but declares no max tool calls, max retries, task-expansion policy, inference policy, skill-chaining policy, allowed downstream skills, user-confirmation requirements, or budget-exceeded behavior. The intermediate review confirms these execution boundary fields are missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace with: "Max 3 retries. If still failing, stop and report error."
Evidence Strength Confirmed (static)

D Findings Dossier (8/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-3.4 **②P0** The Skill does not explicitly declare identity bou

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** monitor_travel_alerts
⑤ **Location** `Skill content / frontmatter and body`
⑥ **Original Evidence** **The Skill does not explicitly declare identity boundaries for ambiguity-induced inference: no non-goals, allowed/forbidden resources, or allowed/forbidden operations are stated. This leaves the agent free to infer scope and act beyond the intended travel-alert monitoring purpose.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add "do not do" section: "Do not: infer from conversation history, add unprovided facts, extend to related tasks."
Evidence Strength Confirmed (static)

①QDS-4.1 **②P0** The Skill does not explicitly define failure escal

③ **Category** QD-S (Skill) · FAILURE
④ **Artifact** monitor_travel_alerts
⑤ **Location** `FAILURE (Failure Handling) / Execution Flow`
⑥ **Original Evidence** **The Skill does not explicitly define failure escalation behavior for empty input. The intermediate review shows failure.on_empty_input as missing, and the Skill content contains no requirement or boundary for handling an empty itinerary or empty alert sweep result.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "On execution failure, stop immediately and report error. Do not attempt alternatives."
Evidence Strength Confirmed (static)

①QD-T-1.4 **②P0** additionalProperties not controlled

③ **Category** QD-T (Tool) · Structure
④ **Artifact** search_flights
⑤ **Location** `$.function.parameters`
⑥ **Original Evidence** **The parameters object does not declare additionalProperties: false, allowing arbitrary extra fields.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-1.4
⑧ **Impact** Uncontrolled extra fields may cause backend errors or injection risks.
⑨ **Remediation** Explicitly declare additionalProperties: false to prevent LLM from passing unexpected fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-1.4 **②P0** additionalProperties not controlled

③ **Category** QD-T (Tool) · Structure
④ **Artifact** search_accommodations
⑤ **Location** `$.function.parameters`
⑥ **Original Evidence** **The parameters object does not declare additionalProperties: false, allowing arbitrary extra fields.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-1.4
⑧ **Impact** Uncontrolled extra fields may cause backend errors or injection risks.
⑨ **Remediation** Explicitly declare additionalProperties: false to prevent LLM from passing unexpected fields
Evidence Strength Confirmed (static) · Check method: Automated

D Findings Dossier (9/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QD-T-1.4 ②P0 additionalProperties not controlled

③ **Category** QD-T (Tool) · Structure
④ **Artifact** search_activities
⑤ **Location** `$.function.parameters`
⑥ **Original Evidence** **The parameters object does not declare additionalProperties: false, allowing arbitrary extra fields.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-1.4
⑧ **Impact** Uncontrolled extra fields may cause backend errors or injection risks.
⑨ **Remediation** Explicitly declare additionalProperties: false to prevent LLM from passing unexpected fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-1.4 ②P0 additionalProperties not controlled

③ **Category** QD-T (Tool) · Structure
④ **Artifact** get_weather_forecast
⑤ **Location** `$.function.parameters`
⑥ **Original Evidence** **The parameters object does not declare additionalProperties: false, allowing arbitrary extra fields.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-1.4
⑧ **Impact** Uncontrolled extra fields may cause backend errors or injection risks.
⑨ **Remediation** Explicitly declare additionalProperties: false to prevent LLM from passing unexpected fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-1.4 ②P0 additionalProperties not controlled

③ **Category** QD-T (Tool) · Structure
④ **Artifact** convert_currency
⑤ **Location** `$.function.parameters`
⑥ **Original Evidence** **The parameters object does not declare additionalProperties: false, allowing arbitrary extra fields.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-1.4
⑧ **Impact** Uncontrolled extra fields may cause backend errors or injection risks.
⑨ **Remediation** Explicitly declare additionalProperties: false to prevent LLM from passing unexpected fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-1.4 ②P0 additionalProperties not controlled

③ **Category** QD-T (Tool) · Structure
④ **Artifact** check_travel_requirements
⑤ **Location** `$.function.parameters`
⑥ **Original Evidence** **The parameters object does not declare additionalProperties:false, allowing arbitrary extra fields.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-1.4
⑧ **Impact** Uncontrolled extra fields may cause backend errors or injection risks.
⑨ **Remediation** Explicitly declare additionalProperties: false to prevent LLM from passing unexpected fields
Evidence Strength Confirmed (static) · Check method: Automated

D Findings Dossier (10/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QD-T-1.4 **②P0** additionalProperties not controlled

③ **Category** QD-T (Tool) · Structure
④ **Artifact** check_travel_requirements
⑤ **Location** `$.function.returns`
⑥ **Original Evidence** **The returns object does not declare additionalProperties:false, allowing arbitrary extra fields.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-1.4
⑧ **Impact** Uncontrolled extra fields may cause backend errors or injection risks.
⑨ **Remediation** Explicitly declare additionalProperties: false to prevent LLM from passing unexpected fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-1.4 **②P0** additionalProperties not controlled

③ **Category** QD-T (Tool) · Structure
④ **Artifact** get_travel_alerts
⑤ **Location** `$.function.parameters`
⑥ **Original Evidence** **The parameters object does not declare additionalProperties:false, allowing arbitrary extra fields.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-1.4
⑧ **Impact** Uncontrolled extra fields may cause backend errors or injection risks.
⑨ **Remediation** Explicitly declare additionalProperties: false to prevent LLM from passing unexpected fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-1.4 **②P0** additionalProperties not controlled

③ **Category** QD-T (Tool) · Structure
④ **Artifact** get_travel_alerts
⑤ **Location** `$.function.returns`
⑥ **Original Evidence** **The returns object does not declare additionalProperties:false, allowing arbitrary extra fields.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-1.4
⑧ **Impact** Uncontrolled extra fields may cause backend errors or injection risks.
⑨ **Remediation** Explicitly declare additionalProperties: false to prevent LLM from passing unexpected fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-1.4 **②P0** additionalProperties not controlled

③ **Category** QD-T (Tool) · Structure
④ **Artifact** save_itinerary
⑤ **Location** `$.function.parameters`
⑥ **Original Evidence** **The parameters object does not declare additionalProperties:false, allowing arbitrary extra fields.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-1.4
⑧ **Impact** Uncontrolled extra fields may cause backend errors or injection risks.
⑨ **Remediation** Explicitly declare additionalProperties: false to prevent LLM from passing unexpected fields
Evidence Strength Confirmed (static) · Check method: Automated

D Findings Dossier (11/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QD-T-1.4 ②P0 additionalProperties not controlled

③ **Category** QD-T (Tool) · Structure
④ **Artifact** save_itinerary
⑤ **Location** `$.function.returns`
⑥ **Original Evidence** **The returns object does not declare additionalProperties:false, allowing arbitrary extra fields.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-1.4
⑧ **Impact** Uncontrolled extra fields may cause backend errors or injection risks.
⑨ **Remediation** Explicitly declare additionalProperties: false to prevent LLM from passing unexpected fields
Evidence Strength Confirmed (static) · Check method: Automated

①QDP-1.2.1 ②P0 Role/responsibility mismatch

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Section 3 prep_travel_documents; Boundaries`
⑥ **Original Evidence** **Voyager is defined as a leisure travel planner that 'does not give legal or medical advice (including vaccination decisions)', yet prep_travel_documents is required to produce vaccination requirements and apply-by deadlines, which is effectively medical/legal guidance; the role scope and the assigned responsibility conflict.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Logic Defect · QDP-1.2.1
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Review role definition, ensure responsibilities match role capabilities, remove unreasonable responsibility assignments
Evidence Strength Confirmed (static)

①QDP-1.3.3 ②P0 Boundary not defined

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Boundaries`
⑥ **Original Evidence** **The prompt does not define the boundary for handling non-leisure or out-of-scope requests (e.g., business travel, medical questions, visa legal disputes) beyond a one-line disclaimer, nor how to respond when a user insists; the agent cannot tell whether to refuse, redirect, or partially help.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Logic Defect · QDP-1.3.3
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Clearly declare task scope boundaries: only process ..., do not process ...
Evidence Strength Confirmed (static)

①QDP-1.5.2 ②P0 Resources do not support workflow

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Payments stay with the user; section 4 monitor_travel_alerts`
⑥ **Original Evidence** **The workflow requires booking-summary generation, confirmation-number capture, and monitoring between booking and return, but no tool or resource is declared for producing booking summaries, storing confirmation numbers, or scheduling/polling alerts over time.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Logic Defect · QDP-1.5.2
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Declare all resources and tools required by the workflow, ensure accessibility
Evidence Strength Confirmed (static)

D Findings Dossier (12/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDP-1.6.1 ②P0 Ambiguous key decision word

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Section 4 monitor_travel_alerts`
⑥ **Original Evidence** **Severity classification for alerts uses 'low / medium / high' per a 'severity matrix' that is not provided, and 'high means invoke the replan capability immediately' is a key decision made on an undefined threshold.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Logic Defect · QDP-1.6.1
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Provide clear judgment conditions and decision rules for key decision points
Evidence Strength Confirmed (static)

①QDP-2.2.1 ②P0 Input source not declared

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Sections 1–5`
⑥ **Original Evidence** **The prompt names tools (search_flights, get_weather_forecast, etc.) but does not declare the input sources, API keys, or data providers behind them, nor the source of user inputs such as budget, dates, and accessibility needs.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.2.1
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Clearly declare the input source: input comes from the ... part of the user message, in the format of ...
Evidence Strength Confirmed (static)

①QDP-2.2.2 ②P0 Input format not constrained

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Who Voyager Serves; Payments stay with the user`
⑥ **Original Evidence** **No input types, formats, ranges, or length limits are defined for user inputs such as dates, budget, destination, or pasted confirmation numbers.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.2.2
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Declare input format constraints: input must be UTF-8 encoded, no more than 1000 characters
Evidence Strength Confirmed (static)

①QDP-2.2.3 ②P0 Required/optional status not distinguished

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Section 1 build_itinerary`
⑥ **Original Evidence** **It is not stated which trip inputs are required (destinations, dates, budget, interests, accessibility needs) versus optional, nor what defaults apply.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.2.3
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Clearly label: required inputs: ...; optional inputs: ...
Evidence Strength Confirmed (static)

D Findings Dossier (13/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDP-2.2.4 ②P0 Missing-input handling not defined

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Section 1 build_itinerary`
⑥ **Original Evidence** **There is no defined behavior for missing required inputs (e.g., user gives no budget or no dates); the prompt does not say whether to ask, assume, or degrade gracefully.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.2.4
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Declare: when required input is missing, ask the user instead of assuming on its own
Evidence Strength Confirmed (static)

①QDP-2.3.1 ②P0 Output format not defined

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Sections 1–5; Payments stay with the user`
⑥ **Original Evidence** **The prompt describes content (itinerary, cost table, checklist, booking summary) but never defines the output structure, formatting, or length constraints for any deliverable.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.3.1
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Declare output format: output is in JSON format, containing fields: title, content, summary
Evidence Strength Confirmed (static)

①QDP-2.3.2 ②P0 Incomplete output schema

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Sections 3 and 5`
⑥ **Original Evidence** **Referenced fields such as documents_needed, itinerary versions, and change logs are named but their schema, types, and required constraints are not defined.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.3.2
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Improve the output Schema, define all necessary fields and types
Evidence Strength Confirmed (static)

①QDP-2.3.4 ②P0 Missing security/privacy filtering

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Payments stay with the user; section 3`
⑥ **Original Evidence** **The prompt allows users to paste confirmation numbers and holds passport/visa data, but defines no sensitive-data masking, storage, or output-filtering rules.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.3.4
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Add filtering rules: output must not contain sensitive information such as passwords, ID numbers, or internal system addresses
Evidence Strength Confirmed (static)

D Findings Dossier (14/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDP-2.4.2 ②P0 Resources/tools not declared

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Sections 1–5`
⑥ **Original Evidence** **Tools are named but not declared with their providers, endpoints, or availability; several required resources (booking-summary generator, confirmation store, alert scheduler) are entirely absent.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.4.2
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Declare all resources and tools used and their access methods
Evidence Strength Confirmed (static)

①QDP-2.4.3 ②P0 Missing tool-call convention

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Sections 1–5`
⑥ **Original Evidence** **No tool parameter types, return structures, error handling, or permissions are defined for any of the named tools (search_flights, convert_currency, save_itinerary, etc.).**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.4.3
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Declare the tool invocation specification: pass ... parameters when invoking, extract ... fields from returned results
Evidence Strength Confirmed (static)

①QDP-2.5.2 ②P0 Missing security-boundary constraint

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Payments stay with the user; Boundaries`
⑥ **Original Evidence** **Prohibited operations and data boundaries are only partially stated ('never takes payment or holds card details'); other boundaries such as storing passport data or sharing user data with providers are undefined.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.5.2
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Add safety boundaries: forbid delete/modify/send-out operations, high-risk operations require user confirmation before execution
Evidence Strength Confirmed (static)

①QDS-1.2 ②P1 The Skill does not declare explicit output boundar

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** optimize_budget
⑤ **Location** `Example Output Frame / Output Boundary`
⑥ **Original Evidence** **The Skill does not declare explicit output boundaries such as maximum total characters, maximum items per section, whether additional sections are allowed, whether partial results are allowed, or behavior when input is insufficient for a section. The intermediate review confirms these output boundary items are missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Keep output within 1500 Chinese characters / 1000 English words."
Evidence Strength Confirmed (static)

D Findings Dossier (15/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-1.4 ②P1 The Skill does not declare explicit identity bound

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** optimize_budget
⑤ **Location** `Skill metadata / Identity Boundary`
⑥ **Original Evidence** **The Skill does not declare explicit identity boundaries such as non-goals, allowed resources, forbidden resources, allowed operations, or forbidden operations. The intermediate review confirms these identity boundary items are missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Explicitly list: "Allowed: read, list. Forbidden: write, delete, update, overwrite."
Evidence Strength Confirmed (static)

①QDS-1.5 ②P1 The Skill does not declare explicit trigger bounda

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** optimize_budget
⑤ **Location** `When This Skill Runs / Trigger Boundary`
⑥ **Original Evidence** **The Skill does not declare explicit trigger boundaries such as forbidden_when conditions or ambiguity policy for missing content and scope expansion. The intermediate review confirms trigger.forbidden_when, trigger.ambiguity_policy.if_content_missing, and trigger.ambiguity_policy.may_expand_scope are missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.5
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Declare: "Only use data explicitly provided in the current request. Do not access conversation history or external systems."
Evidence Strength Confirmed (static)

①QDS-2.3 ②P1 The Skill defines an output format but does not bo

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** optimize_budget
⑤ **Location** `Example Output Frame / Output Boundary`
⑥ **Original Evidence** **The Skill defines an output format but does not bound output size or completeness. It lacks max_total_chars, max_items_per_section, allow_additional_sections, partial_result_allowed, and if_input_insufficient_for_section, so output can expand without explicit limits.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Use closed enumeration: "Only includes the following: A, B, C. Do not add extra parts."
Evidence Strength Confirmed (static)

①QDS-2.4 ②P1 The Skill identifies a purpose but does not declar

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** optimize_budget
⑤ **Location** `Skill metadata / Identity`
⑥ **Original Evidence** **The Skill identifies a purpose but does not declare identity boundaries. It lacks non_goals, allowed_resources, forbidden_resources, allowed_operations, and forbidden_operations, so the directive scope is not explicitly constrained.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace "manage" with specific actions: "list database tables", "view table structure", "query data (read-only)"
Evidence Strength Confirmed (static)

D Findings Dossier (16/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-3.1 ②P1 The Skill describes when it runs but does not expl

③ **Category** QD-S (Skill) · TRIGGER
④ **Artifact** optimize_budget
⑤ **Location** `trigger.forbidden_when`
⑥ **Original Evidence** **The Skill describes when it runs but does not explicitly declare forbidden trigger conditions, leaving ambiguity about when it must not run.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Specify: "Only use when user explicitly requests: weekly report, work summary, progress report."
Evidence Strength Confirmed (static)

①QDS-3.2 ②P1 The Skill lacks an explicit ambiguity policy for m

③ **Category** QD-S (Skill) · TRIGGER
④ **Artifact** optimize_budget
⑤ **Location** `trigger.ambiguity_policy.if_content_missing, trigger.ambiguity_policy.may_expand_scope`
⑥ **Original Evidence** **The Skill lacks an explicit ambiguity policy for missing trigger content and does not state whether scope may be expanded, so ambiguous trigger inputs could lead to unintended inference.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Do not activate for: debugging, code review, system administration requests."
Evidence Strength Confirmed (static)

①QDS-3.3 ②P1 The Skill does not declare input limits such as ma

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** optimize_budget
⑤ **Location** `input.max_items, input.max_chars, input.if_exceeds, input.safe_defaults`
⑥ **Original Evidence** **The Skill does not declare input limits such as max items, max chars, behavior when input exceeds limits, or safe defaults, leaving input boundaries ambiguous.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "When input is incomplete or ambiguous, ask the user instead of guessing."
Evidence Strength Confirmed (static)

①QDS-3.6 ②P1 The Skill does not explicitly declare allowed reso

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** optimize_budget
⑤ **Location** `identity.non_goals, identity.allowed_resources, identity.allowed_operations`
⑥ **Original Evidence** **The Skill does not explicitly declare allowed resources, allowed operations, or non-goals, so its identity and purpose boundaries are incomplete.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.6
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Rename to accurate description: e.g., "readonly-database-diagnostic" instead of "database-maintenance-assistant".
Evidence Strength Confirmed (static)

D Findings Dossier (17/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-4.2 ②P1 The Skill does not explicitly define the output bo

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** optimize_budget
⑤ **Location** `Example Output Frame`
⑥ **Original Evidence** **The Skill does not explicitly define the output boundary required by QDS-4.2. The example output frame is truncated and there is no explicit requirement for output format limits, partial-result handling, or behavior when input is insufficient for a section.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Partial results are acceptable. When some parts lack information, skip or mark as insufficient."
Evidence Strength Confirmed (static)

①QDS-4.3 ②P1 The Skill does not explicitly define the failure h

③ **Category** QD-S (Skill) · FAILURE
④ **Artifact** optimize_budget
⑤ **Location** `Execution Flow / Failure Handling`
⑥ **Original Evidence** **The Skill does not explicitly define the failure handling requirement and boundary represented by QDS-4.3. It lacks declarations for on_empty_input, on_insufficient_input, on_user_dissatisfied, and forbidden_behaviors, so failure escalation is not controlled.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "After failure, prohibit: extending task scope, generating fake data to fill gaps, lowering quality standards."
Evidence Strength Confirmed (static)

①QDS-5.1 ②P1 The Skill does not explicitly declare identity bou

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** optimize_budget
⑤ **Location** `Skill metadata and Execution Flow`
⑥ **Original Evidence** **The Skill does not explicitly declare identity boundaries for Permission Overflow: allowed/forbidden resources and allowed/forbidden operations are missing, so it is unclear what the Skill may access or perform.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Explicitly list: "Allowed: read, list, query. Forbidden: write, update, delete, insert, DROP."
Evidence Strength Confirmed (static)

①QDS-5.3 ②P1 Execution boundaries are not explicitly controlled

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** optimize_budget
⑤ **Location** `Execution Flow`
⑥ **Original Evidence** **Execution boundaries are not explicitly controlled: max_tool_calls, max_retries, allow_task_expansion, allow_inference_of_missing_data, allow_skill_chaining, allowed_downstream_skills, require_user_confirmation_for, and if_budget_exceeded are missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Do not access production database, production API, online systems, or unauthorized external services. Only use local/test/sandbox environments."
Evidence Strength Confirmed (static)

D Findings Dossier (18/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-5.4 ②P1 The Skill lacks explicit permission-overflow safeg

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** optimize_budget
⑤ **Location** `Execution Flow steps 6-7`
⑥ **Original Evidence** **The Skill lacks explicit permission-overflow safeguards for execution scope, including confirmation requirements before applying changes and limits on downstream skill use or task expansion.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Can only call: skill-A, skill-B. Forbidden to call: skill-C (has admin privileges)."
Evidence Strength Confirmed (static)

①QDS-1.2 ②P1 The Skill does not declare output boundaries such

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** build_itinerary
⑤ **Location** `Execution Flow / Assemble`
⑥ **Original Evidence** **The Skill does not declare output boundaries such as output format, maximum total characters, maximum items per section, whether additional sections are allowed, whether partial results are allowed, or behavior when input is insufficient for a section. All output review items are missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Keep output within 1500 Chinese characters / 1000 English words."
Evidence Strength Confirmed (static)

①QDS-1.4 ②P1 The Skill does not declare identity boundaries for

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** build_itinerary
⑤ **Location** `Skill metadata / When This Skill Runs`
⑥ **Original Evidence** **The Skill does not declare identity boundaries for non-goals, allowed resources, forbidden resources, allowed operations, or forbidden operations. Only identity.purpose is identified in the intermediate review.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Explicitly list: "Allowed: read, list. Forbidden: write, delete, update, overwrite."
Evidence Strength Confirmed (static)

①QDS-1.5 ②P1 The Skill lacks explicit trigger boundaries for fo

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** build_itinerary
⑤ **Location** `When This Skill Runs`
⑥ **Original Evidence** **The Skill lacks explicit trigger boundaries for forbidden_when conditions and ambiguity policy, including behavior when content is missing and whether scope may expand. Only trigger.allowed_when is identified.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.5
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Declare: "Only use data explicitly provided in the current request. Do not access conversation history or external systems."
Evidence Strength Confirmed (static)

D Findings Dossier (19/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-2.3 ②P1 The Skill does not define explicit output boundari

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** build_itinerary
⑤ **Location** `OUTPUT (Output Boundary)`
⑥ **Original Evidence** **The Skill does not define explicit output boundaries. It lacks output.format, output.max_total_chars, output.max_items_per_section, output.allow_additional_sections, output.partial_result_allowed, and output.if_input_insufficient_for_section. The intermediate review confirms these output boundary items are missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Use closed enumeration: "Only includes the following: A, B, C. Do not add extra parts."
Evidence Strength Confirmed (static)

①QDS-2.4 ②P1 The Skill does not define explicit identity bounda

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** build_itinerary
⑤ **Location** `IDENTITY (Identity & Purpose)`
⑥ **Original Evidence** **The Skill does not define explicit identity boundaries. It lacks identity.non_goals, identity.allowed_resources, identity.forbidden_resources, identity.allowed_operations, and identity.forbidden_operations. The intermediate review confirms these identity boundary items are missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace "manage" with specific actions: "list database tables", "view table structure", "query data (read-only)"
Evidence Strength Confirmed (static)

①QDS-3.1 ②P1 The Skill states when it runs but does not explici

③ **Category** QD-S (Skill) · TRIGGER
④ **Artifact** build_itinerary
⑤ **Location** `When This Skill Runs`
⑥ **Original Evidence** **The Skill states when it runs but does not explicitly declare forbidden trigger conditions. Missing forbidden_when allows the agent to infer that ambiguous or out-of-scope requests may still trigger execution.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Specify: "Only use when user explicitly requests: weekly report, work summary, progress report."
Evidence Strength Confirmed (static)

①QDS-3.2 ②P1 The Skill lacks an explicit ambiguity policy for m

③ **Category** QD-S (Skill) · TRIGGER
④ **Artifact** build_itinerary
⑤ **Location** `When This Skill Runs`
⑥ **Original Evidence** **The Skill lacks an explicit ambiguity policy for missing trigger content and does not state whether scope may be expanded. This permits inference about whether to proceed, ask, or expand scope when trigger details are incomplete.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Do not activate for: debugging, code review, system administration requests."
Evidence Strength Confirmed (static)

D Findings Dossier (20/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-3.3 ②P1 The Skill does not declare input limits such as ma

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** build_itinerary
⑤ **Location** `When This Skill Runs and Execution Flow`
⑥ **Original Evidence** **The Skill does not declare input limits such as max_items, max_chars, behavior when input exceeds limits, or safe defaults. Missing input boundaries allow the agent to infer how much input to accept and how to handle incomplete or excessive input.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "When input is incomplete or ambiguous, ask the user instead of guessing."
Evidence Strength Confirmed (static)

①QDS-3.6 ②P1 The Skill does not explicitly forbid inference of

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** build_itinerary
⑤ **Location** `When This Skill Runs and Execution Flow`
⑥ **Original Evidence** **The Skill does not explicitly forbid inference of missing data or task expansion. Although it says missing preferences are asked about rather than guessed, it lacks a formal identity boundary covering allowed/forbidden operations and inference limits.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.6
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Rename to accurate description: e.g., "readonly-database-diagnostic" instead of "database-maintenance-assistant".
Evidence Strength Confirmed (static)

①QDS-4.2 ②P1 The Skill does not explicitly define the output bo

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** build_itinerary
⑤ **Location** `Execution Flow step 7 / Output Boundary`
⑥ **Original Evidence** **The Skill does not explicitly define the output boundary required by QDS-4.2. It describes assembling a daily_plan and save_itinerary payload, but does not specify output format, maximum output size, partial-result behavior, or handling when input is insufficient for a section.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Partial results are acceptable. When some parts lack information, skip or mark as insufficient."
Evidence Strength Confirmed (static)

①QDS-4.3 ②P1 The Skill does not explicitly define the failure h

③ **Category** QD-S (Skill) · FAILURE
④ **Artifact** build_itinerary
⑤ **Location** `Failure Handling`
⑥ **Original Evidence** **The Skill does not explicitly define the failure handling requirement and boundary represented by QDS-4.3. It lacks declarations for on_empty_input, on_insufficient_input, on_user_dissatisfied, and forbidden failure behaviors.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "After failure, prohibit: extending task scope, generating fake data to fill gaps, lowering quality standards."
Evidence Strength Confirmed (static)

D Findings Dossier (21/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-5.1 ②P1 The Skill does not explicitly declare identity bou

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** build_itinerary
⑤ **Location** `IDENTITY section / frontmatter`
⑥ **Original Evidence** **The Skill does not explicitly declare identity boundaries for Permission Overflow: allowed/forbidden resources and allowed/forbidden operations are missing, so the agent's permitted scope is not bounded.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Explicitly list: "Allowed: read, list, query. Forbidden: write, update, delete, insert, DROP."
Evidence Strength Confirmed (static)

①QDS-5.3 ②P1 Execution boundaries are not explicitly controlled

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** build_itinerary
⑤ **Location** `Execution Flow`
⑥ **Original Evidence** **Execution boundaries are not explicitly controlled: max_tool_calls, max_retries, allow_task_expansion, allow_inference_of_missing_data, allow_skill_chaining, allowed_downstream_skills, require_user_confirmation_for, and if_budget_exceeded are all missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Do not access production database, production API, online systems, or unauthorized external services. Only use local/test/sandbox environments."
Evidence Strength Confirmed (static)

①QDS-5.4 ②P1 The Skill lacks explicit execution limits and over

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** build_itinerary
⑤ **Location** `Execution Flow`
⑥ **Original Evidence** **The Skill lacks explicit execution limits and overflow handling for tool use, retries, task expansion, inference, chaining, confirmation, and budget exceedance, allowing permission overflow beyond declared boundaries.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Can only call: skill-A, skill-B. Forbidden to call: skill-C (has admin privileges)."
Evidence Strength Confirmed (static)

①QDS-1.2 ②P1 Output boundaries are missing. The Skill provides

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** prep_travel_documents
⑤ **Location** `Example Response Frame`
⑥ **Original Evidence** **Output boundaries are missing. The Skill provides an example response frame but does not declare output.format, max_total_chars, max_items_per_section, allow_additional_sections, partial_result_allowed, or if_input_insufficient_for_section.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Keep output within 1500 Chinese characters / 1000 English words."
Evidence Strength Confirmed (static)

D Findings Dossier (22/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-1.4 ②P1 Identity boundaries are incomplete. The Skill iden

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** prep_travel_documents
⑤ **Location** `Skill metadata / When This Skill Runs`
⑥ **Original Evidence** **Identity boundaries are incomplete. The Skill identifies a purpose and trigger context, but does not declare non_goals, allowed_resources, forbidden_resources, allowed_operations, or forbidden_operations.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Explicitly list: "Allowed: read, list. Forbidden: write, delete, update, overwrite."
Evidence Strength Confirmed (static)

①QDS-1.5 ②P1 Identity boundary controls are missing for resourc

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** prep_travel_documents
⑤ **Location** `Skill metadata / Execution Flow`
⑥ **Original Evidence** **Identity boundary controls are missing for resource and operation scope. The Skill does not explicitly state which resources may be accessed, which are forbidden, which operations are allowed, or which operations are forbidden.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.5
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Declare: "Only use data explicitly provided in the current request. Do not access conversation history or external systems."
Evidence Strength Confirmed (static)

①QDS-2.3 ②P1 The Skill does not declare explicit output boundar

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** prep_travel_documents
⑤ **Location** `Example Response Frame`
⑥ **Original Evidence** **The Skill does not declare explicit output boundaries. The intermediate review shows output.format, output.max_total_chars, output.max_items_per_section, output.allow_additional_sections, output.partial_result_allowed, and output.if_input_insufficient_for_section are all missing. The example response frame is illustrative but does not define enforceable output limits or handling for insufficient input.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Use closed enumeration: "Only includes the following: A, B, C. Do not add extra parts."
Evidence Strength Confirmed (static)

①QDS-2.4 ②P1 The Skill does not declare explicit identity bound

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** prep_travel_documents
⑤ **Location** `Skill metadata; Execution Flow`
⑥ **Original Evidence** **The Skill does not declare explicit identity boundaries. The intermediate review shows identity.non_goals, identity.allowed_resources, identity.forbidden_resources, identity.allowed_operations, and identity.forbidden_operations are all missing. Only identity.purpose is identified, leaving the Skill's operational scope and resource permissions unbounded.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace "manage" with specific actions: "list database tables", "view table structure", "query data (read-only)"
Evidence Strength Confirmed (static)

D Findings Dossier (23/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-3.1 **②P1** Trigger conditions are only partially specified. '

③ **Category** QD-S (Skill) · TRIGGER
④ **Artifact** prep_travel_documents
⑤ **Location** `When This Skill Runs`
⑥ **Original Evidence** **Trigger conditions are only partially specified. 'When This Skill Runs' lists allowed triggers, but there is no explicit forbidden_when boundary or ambiguity policy for missing trigger content, so the agent may infer activation in ambiguous cases.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Specify: "Only use when user explicitly requests: weekly report, work summary, progress report."
Evidence Strength Confirmed (static)

①QDS-3.2 **②P1** No trigger ambiguity policy is declared. The Skill

③ **Category** QD-S (Skill) · TRIGGER
④ **Artifact** prep_travel_documents
⑤ **Location** `When This Skill Runs`
⑥ **Original Evidence** **No trigger ambiguity policy is declared. The Skill lacks rules for what to do when trigger content is missing or whether scope may be expanded, allowing ambiguity-induced inference about when the Skill applies.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Do not activate for: debugging, code review, system administration requests."
Evidence Strength Confirmed (static)

①QDS-3.3 **②P1** Input boundaries are not declared: no max_items, m

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** prep_travel_documents
⑤ **Location** `Execution Flow steps 1-3`
⑥ **Original Evidence** **Input boundaries are not declared: no max_items, max_chars, if_exceeds behavior, or safe_defaults. The Skill accepts nationality, destinations, transit countries, dates, passport expiry, and prior trips without limits or defaults, so missing or ambiguous input may be inferred.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "When input is incomplete or ambiguous, ask the user instead of guessing."
Evidence Strength Confirmed (static)

①QDS-3.6 **②P1** Identity boundaries for inference are missing. The

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** prep_travel_documents
⑤ **Location** `Execution Flow / Error Handling`
⑥ **Original Evidence** **Identity boundaries for inference are missing. The Skill does not state whether it may infer missing data, expand tasks, or chain skills, nor does it define forbidden behaviors, leaving ambiguity-induced inference uncontrolled.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.6
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Rename to accurate description: e.g., "readonly-database-diagnostic" instead of "database-maintenance-assistant".
Evidence Strength Confirmed (static)

D Findings Dossier (24/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-4.2 ②P1 The Skill does not explicitly define the output bo

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** prep_travel_documents
⑤ **Location** `Example Response Frame / Output`
⑥ **Original Evidence** **The Skill does not explicitly define the output boundary required by QDS-4.2. The intermediate review shows output.format, output.max_total_chars, output.max_items_per_section, output.allow_additional_sections, output.partial_result_allowed, and output.if_input_insufficient_for_section are all missing, so the required output requirement and boundary are not declared.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Partial results are acceptable. When some parts lack information, skip or mark as insufficient."
Evidence Strength Confirmed (static)

①QDS-4.3 ②P1 The Skill does not explicitly define the failure h

③ **Category** QD-S (Skill) · FAILURE
④ **Artifact** prep_travel_documents
⑤ **Location** `Error Handling`
⑥ **Original Evidence** **The Skill does not explicitly define the failure handling requirement and boundary represented by QDS-4.3. The intermediate review shows failure.on_empty_input, failure.on_insufficient_input, failure.on_user_dissatisfied, and failure.forbidden_behaviors are all missing; the Error Handling table is incomplete and does not cover these failure conditions.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "After failure, prohibit: extending task scope, generating fake data to fill gaps, lowering quality standards."
Evidence Strength Confirmed (static)

①QDS-5.1 ②P1 The Skill does not explicitly declare identity bou

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** prep_travel_documents
⑤ **Location** `Skill metadata / identity declarations`
⑥ **Original Evidence** **The Skill does not explicitly declare identity boundaries for Permission Overflow: no non-goals, allowed/forbidden resources, or allowed/forbidden operations are defined. The intermediate review confirms identity.non_goals, identity.allowed_resources, identity.forbidden_resources, identity.allowed_operations, and identity.forbidden_operations are all missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Explicitly list: "Allowed: read, list, query. Forbidden: write, update, delete, insert, DROP."
Evidence Strength Confirmed (static)

D Findings Dossier (25/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-5.3 **②P1** Execution boundaries are largely undeclared. The S

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** prep_travel_documents
⑤ **Location** `Execution Flow / Error Handling`
⑥ **Original Evidence** **Execution boundaries are largely undeclared. The Skill lacks explicit limits for max_tool_calls, max_retries, allow_task_expansion, allow_inference_of_missing_data, allow_skill_chaining, allowed_downstream_skills, require_user_confirmation_for, and if_budget_exceeded. Only timeout_seconds is identified, which is insufficient to control Permission Overflow.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Do not access production database, production API, online systems, or unauthorized external services. Only use local/test/sandbox environments."
Evidence Strength Confirmed (static)

①QDS-5.4 **②P1** The Skill does not define required execution safeg

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** prep_travel_documents
⑤ **Location** `Execution Flow / Error Handling`
⑥ **Original Evidence** **The Skill does not define required execution safeguards for Permission Overflow, including user confirmation requirements, downstream skill restrictions, task expansion limits, or budget-exceeded behavior. The intermediate review marks these execution controls as missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Can only call: skill-A, skill-B. Forbidden to call: skill-C (has admin privileges)."
Evidence Strength Confirmed (static)

①QDS-1.2 **②P1** Output boundary is not explicitly controlled: outp

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** replan_disruption
⑤ **Location** `Execution Flow step 6 / Persist as a new version`
⑥ **Original Evidence** **Output boundary is not explicitly controlled: output.format, max_total_chars, max_items_per_section, allow_additional_sections, partial_result_allowed, and if_input_insufficient_for_section are all missing per the intermediate review. The Skill describes presenting old vs. new but does not declare output limits or fallback behavior.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Keep output within 1500 Chinese characters / 1000 English words."
Evidence Strength Confirmed (static)

①QDS-1.4 **②P1** Identity boundary is incomplete: identity.non_goal

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** replan_disruption
⑤ **Location** `Skill metadata / Execution Flow`
⑥ **Original Evidence** **Identity boundary is incomplete: identity.non_goals, allowed_resources, forbidden_resources, allowed_operations, and forbidden_operations are missing. The Skill names tools in flow but does not explicitly declare allowed/forbidden resources or operations.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Explicitly list: "Allowed: read, list. Forbidden: write, delete, update, overwrite."
Evidence Strength Confirmed (static)

D Findings Dossier (26/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-1.5 ②P1 Identity boundary remains insufficient: no explici

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** replan_disruption
⑤ **Location** `Skill metadata / Execution Flow`
⑥ **Original Evidence** **Identity boundary remains insufficient: no explicit forbidden operations or non-goals are declared, and the Skill does not state what Voyager must not do beyond a single consent note. The intermediate review shows identity.non_goals, forbidden_resources, and forbidden_operations missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.5
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Declare: "Only use data explicitly provided in the current request. Do not access conversation history or external systems."
Evidence Strength Confirmed (static)

①QDS-2.3 ②P1 The Skill does not declare an output boundary. The

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** replan_disruption
⑤ **Location** `Execution Flow step 6 (Present the rebuilt plan)`
⑥ **Original Evidence** **The Skill does not declare an output boundary. There is no output.format, max_total_chars, max_items_per_section, allow_additional_sections, partial_result_allowed, or if_input_insufficient_for_section, so the rebuilt plan presentation is unbounded and has no defined behavior when input is insufficient.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Use closed enumeration: "Only includes the following: A, B, C. Do not add extra parts."
Evidence Strength Confirmed (static)

①QDS-2.4 ②P1 The Skill does not declare identity boundaries. It

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** replan_disruption
⑤ **Location** `Skill metadata / Execution Flow`
⑥ **Original Evidence** **The Skill does not declare identity boundaries. It lacks non_goals, allowed_resources, forbidden_resources, allowed_operations, and forbidden_operations, so the scope of what the agent may do or access during replanning is not explicitly controlled.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace "manage" with specific actions: "list database tables", "view table structure", "query data (read-only)"
Evidence Strength Confirmed (static)

①QDS-3.1 ②P1 Trigger conditions are only partially specified. T

③ **Category** QD-S (Skill) · TRIGGER
④ **Artifact** replan_disruption
⑤ **Location** `When This Skill Runs`
⑥ **Original Evidence** **Trigger conditions are only partially specified. The Skill states when it runs but does not define forbidden_when conditions or an ambiguity policy for missing trigger content, allowing inference about whether to invoke the Skill.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Specify: "Only use when user explicitly requests: weekly report, work summary, progress report."
Evidence Strength Confirmed (static)

D Findings Dossier (27/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-3.2 ②P1 The trigger ambiguity policy is missing: there is

③ **Category** QD-S (Skill) · TRIGGER
④ **Artifact** replan_disruption
⑤ **Location** `When This Skill Runs`
⑥ **Original Evidence** **The trigger ambiguity policy is missing: there is no explicit rule for if_content_missing or whether the Skill may expand scope when the disruption report is incomplete or ambiguous.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Do not activate for: debugging, code review, system administration requests."
Evidence Strength Confirmed (static)

①QDS-3.3 ②P1 Input boundaries are not declared. The Skill does

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** replan_disruption
⑤ **Location** `Execution Flow / Take stock`
⑥ **Original Evidence** **Input boundaries are not declared. The Skill does not specify max_items, max_chars, behavior if input exceeds limits, or safe defaults, so the agent may infer missing itinerary or disruption data.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "When input is incomplete or ambiguous, ask the user instead of guessing."
Evidence Strength Confirmed (static)

①QDS-3.6 ②P1 Identity and purpose boundaries are incomplete. Th

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** replan_disruption
⑤ **Location** `Skill content / Execution Flow`
⑥ **Original Evidence** **Identity and purpose boundaries are incomplete. The Skill describes its job but does not explicitly forbid inference of missing data, task expansion, or skill chaining, leaving ambiguity about what the agent is allowed to do.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.6
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Rename to accurate description: e.g., "readonly-database-diagnostic" instead of "database-maintenance-assistant".
Evidence Strength Confirmed (static)

①QDS-4.2 ②P1 The Skill does not explicitly define the output bo

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** replan_disruption
⑤ **Location** `Present the rebuilt plan / OUTPUT section`
⑥ **Original Evidence** **The Skill does not explicitly define the output boundary required by QDS-4.2. The intermediate review shows output.format, output.max_total_chars, output.max_items_per_section, output.allow_additional_sections, output.partial_result_allowed, and output.if_input_insufficient_for_section are all missing, so the required output constraints and escalation behavior for insufficient output are not declared.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Partial results are acceptable. When some parts lack information, skip or mark as insufficient."
Evidence Strength Confirmed (static)

D Findings Dossier (28/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-4.3 **②P1** The Skill does not explicitly define the failure e

③ **Category** QD-S (Skill) · FAILURE
④ **Artifact** replan_disruption
⑤ **Location** `Preservation Priority / FAILURE section`
⑥ **Original Evidence** **The Skill does not explicitly define the failure escalation requirement and boundary represented by QDS-4.3. It describes normal replanning steps but does not specify what happens when the disruption cannot be resolved, when committed costs cannot be preserved, or when the traveler is dissatisfied; the intermediate review confirms failure.on_user_dissatisfied and failure.forbidden_behaviors are missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "After failure, prohibit: extending task scope, generating fake data to fill gaps, lowering quality standards."
Evidence Strength Confirmed (static)

①QDS-5.1 **②P1** The Skill does not explicitly declare identity bou

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** replan_disruption
⑤ **Location** `Skill content: frontmatter and Execution Flow`
⑥ **Original Evidence** **The Skill does not explicitly declare identity boundaries for allowed/forbidden resources or operations. It describes rebooking, searching, saving, and monitoring actions but does not state which resources or operations are permitted or forbidden, leaving permission overflow risk unaddressed.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Explicitly list: "Allowed: read, list, query. Forbidden: write, update, delete, insert, DROP."
Evidence Strength Confirmed (static)

①QDS-5.3 **②P1** Execution boundaries are missing: no explicit max_

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** replan_disruption
⑤ **Location** `Skill content: Execution Flow steps 4-7`
⑥ **Original Evidence** **Execution boundaries are missing: no explicit max_tool_calls, max_retries, allow_task_expansion, allow_inference_of_missing_data, allow_skill_chaining, allowed_downstream_skills, require_user_confirmation_for, or if_budget_exceeded declarations. The Skill can call multiple tools and rebook replacements without explicit execution limits.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Do not access production database, production API, online systems, or unauthorized external services. Only use local/test/sandbox environments."
Evidence Strength Confirmed (static)

D Findings Dossier (29/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-5.4 ②P1 The Skill lacks explicit execution boundary contro

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** replan_disruption
⑤ **Location** `Skill content: Execution Flow and Preservation Priority`
⑥ **Original Evidence** **The Skill lacks explicit execution boundary controls for tool-call budgets, retries, task expansion, inference of missing data, skill chaining, downstream skill allowlists, user confirmation triggers, and budget-exceeded behavior. This permits uncontrolled execution expansion during disruption replanning.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Can only call: skill-A, skill-B. Forbidden to call: skill-C (has admin privileges)."
Evidence Strength Confirmed (static)

①QDS-1.2 ②P1 The Skill does not declare explicit output boundar

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** monitor_travel_alerts
⑤ **Location** `Notification Discipline / Skill content`
⑥ **Original Evidence** **The Skill does not declare explicit output boundaries. It lacks output.format, max_total_chars, max_items_per_section, allow_additional_sections, partial_result_allowed, and if_input_insufficient_for_section declarations.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Keep output within 1500 Chinese characters / 1000 English words."
Evidence Strength Confirmed (static)

①QDS-1.4 ②P1 The Skill does not declare identity boundaries. It

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** monitor_travel_alerts
⑤ **Location** `Skill metadata / Skill content`
⑥ **Original Evidence** **The Skill does not declare identity boundaries. It lacks non_goals, allowed_resources, forbidden_resources, allowed_operations, and forbidden_operations declarations.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Explicitly list: "Allowed: read, list. Forbidden: write, delete, update, overwrite."
Evidence Strength Confirmed (static)

①QDS-1.5 ②P1 The Skill does not declare trigger and failure bou

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** monitor_travel_alerts
⑤ **Location** `When This Skill Runs / Skill content`
⑥ **Original Evidence** **The Skill does not declare trigger and failure boundaries. It lacks forbidden_when, ambiguity policy, on_empty_input, on_insufficient_input, on_user_dissatisfied, and forbidden_behaviors declarations.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-1 Missing Boundary · QDS-1.5
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Declare: "Only use data explicitly provided in the current request. Do not access conversation history or external systems."
Evidence Strength Confirmed (static)

D Findings Dossier (30/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-2.3 ②P1 The Skill does not define output boundaries. It me

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** monitor_travel_alerts
⑤ **Location** `Notification Discipline; Execution Flow step 6`
⑥ **Original Evidence** **The Skill does not define output boundaries. It mentions session summaries and itinerary notes but does not specify output format, max total chars, max items per section, whether additional sections are allowed, partial-result behavior, or what to do when input is insufficient for a section. The intermediate review confirms output boundary fields are missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Use closed enumeration: "Only includes the following: A, B, C. Do not add extra parts."
Evidence Strength Confirmed (static)

①QDS-2.4 ②P1 The Skill does not fully bound identity and purpos

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** monitor_travel_alerts
⑤ **Location** `Frontmatter; When This Skill Runs`
⑥ **Original Evidence** **The Skill does not fully bound identity and purpose. It identifies the purpose and trigger cadence, but does not declare non-goals, allowed resources, forbidden resources, allowed operations, or forbidden operations. The intermediate review confirms identity.non_goals, identity.allowed_resources, identity.forbidden_resources, identity.allowed_operations, and identity.forbidden_operations are missing.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-2 Unbounded Declaration · QDS-2.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Replace "manage" with specific actions: "list database tables", "view table structure", "query data (read-only)"
Evidence Strength Confirmed (static)

①QDS-3.1 ②P1 Trigger conditions are only partially specified. T

③ **Category** QD-S (Skill) · TRIGGER
④ **Artifact** monitor_travel_alerts
⑤ **Location** `When This Skill Runs`
⑥ **Original Evidence** **Trigger conditions are only partially specified. The Skill states when it runs (cadence and manual trigger) but does not declare forbidden_when conditions, so ambiguous or out-of-scope triggers may still invoke the Skill.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Specify: "Only use when user explicitly requests: weekly report, work summary, progress report."
Evidence Strength Confirmed (static)

①QDS-3.2 ②P1 The trigger ambiguity policy is missing. There is

③ **Category** QD-S (Skill) · TRIGGER
④ **Artifact** monitor_travel_alerts
⑤ **Location** `When This Skill Runs`
⑥ **Original Evidence** **The trigger ambiguity policy is missing. There is no rule for what to do if trigger content is missing or ambiguous, and no explicit prohibition on expanding scope when trigger details are unclear.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Do not activate for: debugging, code review, system administration requests."
Evidence Strength Confirmed (static)

D Findings Dossier (31/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-3.3 ②P1 Input boundaries are not declared. The Skill does

③ **Category** QD-S (Skill) · INPUT
④ **Artifact** monitor_travel_alerts
⑤ **Location** `Execution Flow / Load the current itinerary`
⑥ **Original Evidence** **Input boundaries are not declared. The Skill does not specify max items, max chars, behavior when input exceeds limits, or safe defaults, allowing inference from incomplete or oversized itinerary/alert inputs.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "When input is incomplete or ambiguous, ask the user instead of guessing."
Evidence Strength Confirmed (static)

①QDS-3.6 ②P1 Identity boundaries for inference are not controll

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** monitor_travel_alerts
⑤ **Location** `Execution Flow / Act on the classification`
⑥ **Original Evidence** **Identity boundaries for inference are not controlled. The Skill does not state whether it may infer missing data, expand tasks, chain skills, or which downstream skills are allowed, so ambiguity can lead to unauthorized inference or action.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-3 Ambiguous Inference · QDS-3.6
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Rename to accurate description: e.g., "readonly-database-diagnostic" instead of "database-maintenance-assistant".
Evidence Strength Confirmed (static)

①QDS-4.2 ②P1 The Skill does not explicitly define output bounda

③ **Category** QD-S (Skill) · OUTPUT
④ **Artifact** monitor_travel_alerts
⑤ **Location** `OUTPUT (Output Boundary) / Notification Discipline`
⑥ **Original Evidence** **The Skill does not explicitly define output boundary requirements. The intermediate review shows output.format, output.max_total_chars, output.max_items_per_section, output.allow_additional_sections, output.partial_result_allowed, and output.if_input_insufficient_for_section as missing, and the Skill content does not specify these output constraints.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.2
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Partial results are acceptable. When some parts lack information, skip or mark as insufficient."
Evidence Strength Confirmed (static)

①QDS-4.3 ②P1 The Skill does not explicitly define failure escal

③ **Category** QD-S (Skill) · FAILURE
④ **Artifact** monitor_travel_alerts
⑤ **Location** `FAILURE (Failure Handling) / Notification Discipline`
⑥ **Original Evidence** **The Skill does not explicitly define failure escalation behavior for insufficient input, user dissatisfaction, or forbidden behaviors. The intermediate review shows failure.on_insufficient_input, failure.on_user_dissatisfied, and failure.forbidden_behaviors as missing, and the Skill content does not specify these failure handling requirements.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-4 Failure Expansion · QDS-4.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "After failure, prohibit: extending task scope, generating fake data to fill gaps, lowering quality standards."
Evidence Strength Confirmed (static)

D Findings Dossier (32/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDS-5.1 ②P1 The Skill does not explicitly declare identity bou

③ **Category** QD-S (Skill) · IDENTITY
④ **Artifact** monitor_travel_alerts
⑤ **Location** `IDENTITY review items: identity.allowed_resources, identity.forbidden_resources, identity.allowed_operations, identity.forbidden_operations`
⑥ **Original Evidence** **The Skill does not explicitly declare identity boundaries for Permission Overflow: allowed/forbidden resources and allowed/forbidden operations are missing, so it is unclear what the Skill is permitted to access or perform.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.1
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Explicitly list: "Allowed: read, list, query. Forbidden: write, update, delete, insert, DROP."
Evidence Strength Confirmed (static)

①QDS-5.3 ②P1 Execution boundaries are not explicitly controlled

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** monitor_travel_alerts
⑤ **Location** `EXECUTION review items and Execution Flow steps 2-5`
⑥ **Original Evidence** **Execution boundaries are not explicitly controlled: max_tool_calls, max_retries, allow_task_expansion, allow_inference_of_missing_data, allow_skill_chaining, allowed_downstream_skills, require_user_confirmation_for, and if_budget_exceeded are missing. The Skill can invoke replan_disruption and call multiple tools without declared limits or confirmation boundaries.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.3
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Do not access production database, production API, online systems, or unauthorized external services. Only use local/test/sandbox environments."
Evidence Strength Confirmed (static)

①QDS-5.4 ②P1 The Skill lacks explicit execution boundary contro

③ **Category** QD-S (Skill) · EXECUTION
④ **Artifact** monitor_travel_alerts
⑤ **Location** `EXECUTION review items: execution.max_tool_calls, execution.max_retries, execution.allow_task_expansion, execution.allow_inference_of_missing_data, execution.allow_skill_chaining, execution.allowed_downstream_skills, execution.require_user_confirmation_for, execution.if_budget_exceeded`
⑥ **Original Evidence** **The Skill lacks explicit execution boundary controls for Permission Overflow, including no declared limits on tool calls, retries, task expansion, inference of missing data, skill chaining, downstream skills, user confirmation requirements, or behavior when execution budget is exceeded.**
⑦ **Criterion** QD-S · Skill Sub-specification · QDS-5 Permission Boundary Violation · QDS-5.4
⑧ **Impact** This issue may allow the Skill to operate beyond its intended scope.
⑨ **Remediation** Add: "Can only call: skill-A, skill-B. Forbidden to call: skill-C (has admin privileges)."
Evidence Strength Confirmed (static)

D Findings Dossier (33/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** search_flights
⑤ **Location** `$.function.parameters.properties.origin`
⑥ **Original Evidence** **The origin string parameter has no minLength or maxLength constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** search_flights
⑤ **Location** `$.function.parameters.properties.destinations`
⑥ **Original Evidence** **Destination strings within the array have no length constraints.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.3 ②P1 Number without boundary constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** search_flights
⑤ **Location** `$.function.parameters.properties.max_price`
⑥ **Original Evidence** **max_price has no minimum or maximum boundary defined.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.3
⑧ **Impact** Extreme numeric values may cause calculation errors or resource exhaustion.
⑨ **Remediation** Set reasonable minimum and maximum boundaries for numeric fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.4 ②P1 Array without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** search_flights
⑤ **Location** `$.function.parameters.properties.destinations`
⑥ **Original Evidence** **The destinations array has no minItems or maxItems constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.4
⑧ **Impact** Unbounded arrays may cause excessive batch processing or memory use.
⑨ **Remediation** Set reasonable maxItems and minItems for array fields
Evidence Strength Confirmed (static) · Check method: Automated

D Findings Dossier (34/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QD-T-4.1 ②P1 Insufficient description quality

③ **Category** QD-T (Tool) · Description quality
④ **Artifact** search_flights
⑤ **Location** `$.function.parameters.properties.return_date`
⑥ **Original Evidence** **return_date uses format 'iso-date' which is not a standard JSON Schema format (should be 'date'), making the expected format ambiguous.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-4.1
⑧ **Impact** An unclear description can lead to incorrect Tool calls.
⑨ **Remediation** Add trigger conditions, exclusion scenarios, and necessary input descriptions
Evidence Strength Confirmed (static) · Check method: Semi-automated

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** search_accommodations
⑤ **Location** `$.function.parameters.properties.location`
⑥ **Original Evidence** **The location string parameter has no minLength or maxLength constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.3 ②P1 Number without boundary constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** search_accommodations
⑤ **Location** `$.function.parameters.properties.max_price_per_night`
⑥ **Original Evidence** **max_price_per_night has no minimum or maximum boundary defined.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.3
⑧ **Impact** Extreme numeric values may cause calculation errors or resource exhaustion.
⑨ **Remediation** Set reasonable minimum and maximum boundaries for numeric fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.4 ②P1 Array without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** search_accommodations
⑤ **Location** `$.function.parameters.properties.amenities`
⑥ **Original Evidence** **The amenities array has no minItems or maxItems constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.4
⑧ **Impact** Unbounded arrays may cause excessive batch processing or memory use.
⑨ **Remediation** Set reasonable maxItems and minItems for array fields
Evidence Strength Confirmed (static) · Check method: Automated

D Findings Dossier (35/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QD-T-4.1 ②P1 Insufficient description quality

③ **Category** QD-T (Tool) · Description quality
④ **Artifact** search_accommodations
⑤ **Location** `$.function.parameters.properties.check_in`
⑥ **Original Evidence** **check_in/check_out use format 'iso-date' which is not a standard JSON Schema format (should be 'date').**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-4.1
⑧ **Impact** An unclear description can lead to incorrect Tool calls.
⑨ **Remediation** Add trigger conditions, exclusion scenarios, and necessary input descriptions
Evidence Strength Confirmed (static) · Check method: Semi-automated

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** search_activities
⑤ **Location** `$.function.parameters.properties.location`
⑥ **Original Evidence** **The location string parameter has no minLength or maxLength constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.3 ②P1 Number without boundary constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** search_activities
⑤ **Location** `$.function.parameters.properties.max_price`
⑥ **Original Evidence** **max_price has no minimum or maximum boundary defined.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.3
⑧ **Impact** Extreme numeric values may cause calculation errors or resource exhaustion.
⑨ **Remediation** Set reasonable minimum and maximum boundaries for numeric fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.3 ②P1 Number without boundary constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** search_activities
⑤ **Location** `$.function.parameters.properties.duration_max_hours`
⑥ **Original Evidence** **duration_max_hours has no minimum or maximum boundary defined.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.3
⑧ **Impact** Extreme numeric values may cause calculation errors or resource exhaustion.
⑨ **Remediation** Set reasonable minimum and maximum boundaries for numeric fields
Evidence Strength Confirmed (static) · Check method: Automated

D Findings Dossier (36/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QD-T-2.4 ②P1 Array without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** search_activities
⑤ **Location** `$.function.parameters.properties.interests`
⑥ **Original Evidence** **The interests array has no minItems or maxItems constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.4
⑧ **Impact** Unbounded arrays may cause excessive batch processing or memory use.
⑨ **Remediation** Set reasonable maxItems and minItems for array fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** get_weather_forecast
⑤ **Location** `$.function.parameters.properties.location`
⑥ **Original Evidence** **The location string parameter has no minLength or maxLength constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.2 ②P1 String without format constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** get_weather_forecast
⑤ **Location** `$.function.parameters.properties.start_date`
⑥ **Original Evidence** **start_date/end_date use format 'iso-date' which is not a standard JSON Schema format (should be 'date').**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.2
⑧ **Impact** Unvalidated formats may cause parsing failures or inconsistent behavior.
⑨ **Remediation** Set pattern or format constraints for fields requiring specific formats
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-4.1 ②P1 Insufficient description quality

③ **Category** QD-T (Tool) · Description quality
④ **Artifact** get_weather_forecast
⑤ **Location** `$.function.parameters.properties.end_date`
⑥ **Original Evidence** **The 14-day range constraint is only stated in the description text, not enforced by any schema boundary.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-4.1
⑧ **Impact** An unclear description can lead to incorrect Tool calls.
⑨ **Remediation** Add trigger conditions, exclusion scenarios, and necessary input descriptions
Evidence Strength Confirmed (static) · Check method: Semi-automated

D Findings Dossier (37/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** convert_currency
⑤ **Location** `$.function.parameters.properties.from_currency`
⑥ **Original Evidence** **from_currency/to_currency strings have no minLength or maxLength constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.2 ②P1 String without format constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** convert_currency
⑤ **Location** `$.function.parameters.properties.to_currency`
⑥ **Original Evidence** **Currency code parameters do not define a pattern (e.g., ^[A-Z]{3}$) to enforce ISO 4217 format.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.2
⑧ **Impact** Unvalidated formats may cause parsing failures or inconsistent behavior.
⑨ **Remediation** Set pattern or format constraints for fields requiring specific formats
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.3 ②P1 Number without boundary constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** convert_currency
⑤ **Location** `$.function.parameters.properties.amount`
⑥ **Original Evidence** **amount has no minimum or maximum boundary defined.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.3
⑧ **Impact** Extreme numeric values may cause calculation errors or resource exhaustion.
⑨ **Remediation** Set reasonable minimum and maximum boundaries for numeric fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** check_travel_requirements
⑤ **Location** `$.function.parameters.properties.nationality`
⑥ **Original Evidence** **String parameter 'nationality' has no maxLength/minLength constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

D Findings Dossier (38/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** check_travel_requirements
⑤ **Location** `$.function.parameters.properties.destination`
⑥ **Original Evidence** **String parameter 'destination' has no maxLength/minLength constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.4 ②P1 Array without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** check_travel_requirements
⑤ **Location** `$.function.parameters.properties.transit_countries`
⑥ **Original Evidence** **Array parameter 'transit_countries' has no maxItems/minItems constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.4
⑧ **Impact** Unbounded arrays may cause excessive batch processing or memory use.
⑨ **Remediation** Set reasonable maxItems and minItems for array fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** check_travel_requirements
⑤ **Location** `$.function.returns.properties.visa_type`
⑥ **Original Evidence** **Return string 'visa_type' has no length constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** check_travel_requirements
⑤ **Location** `$.function.returns.properties.official_source_url`
⑥ **Original Evidence** **Return string 'official_source_url' has no length constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

D Findings Dossier (39/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QD-T-4.1 ②P1 Insufficient description quality

③ **Category** QD-T (Tool) · Description quality
④ **Artifact** check_travel_requirements
⑤ **Location** `$.function.returns.properties.error`
⑥ **Original Evidence** **The error object lacks a description and its code enum values are not explained.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-4.1
⑧ **Impact** An unclear description can lead to incorrect Tool calls.
⑨ **Remediation** Add trigger conditions, exclusion scenarios, and necessary input descriptions
Evidence Strength Confirmed (static) · Check method: Semi-automated

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** get_travel_alerts
⑤ **Location** `$.function.parameters.properties.location`
⑥ **Original Evidence** **String parameter 'location' has no maxLength/minLength constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.4 ②P1 Array without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** get_travel_alerts
⑤ **Location** `$.function.parameters.properties.alert_types`
⑥ **Original Evidence** **Array parameter 'alert_types' has no maxItems/minItems constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.4
⑧ **Impact** Unbounded arrays may cause excessive batch processing or memory use.
⑨ **Remediation** Set reasonable maxItems and minItems for array fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** get_travel_alerts
⑤ **Location** `$.function.returns.properties.alerts.items.properties.type`
⑥ **Original Evidence** **Return string 'type' has no length constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

D Findings Dossier (40/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** get_travel_alerts
⑤ **Location** `$.function.returns.properties.alerts.items.properties.source_url`
⑥ **Original Evidence** **Return string 'source_url' has no length constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-4.1 ②P1 Insufficient description quality

③ **Category** QD-T (Tool) · Description quality
④ **Artifact** get_travel_alerts
⑤ **Location** `$.function.returns.properties.error`
⑥ **Original Evidence** **The error object lacks a description and its code enum values are not explained.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-4.1
⑧ **Impact** An unclear description can lead to incorrect Tool calls.
⑨ **Remediation** Add trigger conditions, exclusion scenarios, and necessary input descriptions
Evidence Strength Confirmed (static) · Check method: Semi-automated

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** save_itinerary
⑤ **Location** `$.function.parameters.properties.trip_name`
⑥ **Original Evidence** **String parameter 'trip_name' has no maxLength/minLength constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.1 ②P1 String without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** save_itinerary
⑤ **Location** `$.function.parameters.properties.notes`
⑥ **Original Evidence** **String parameter 'notes' has no maxLength/minLength constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.1
⑧ **Impact** Unbounded strings may increase memory use or degrade performance.
⑨ **Remediation** Set reasonable maxLength and minLength for String type parameters
Evidence Strength Confirmed (static) · Check method: Automated

D Findings Dossier (41/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QD-T-2.4 **②P1** Array without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** save_itinerary
⑤ **Location** `$.function.parameters.properties.traveler_names`
⑥ **Original Evidence** **Array parameter 'traveler_names' has no maxItems/minItems constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.4
⑧ **Impact** Unbounded arrays may cause excessive batch processing or memory use.
⑨ **Remediation** Set reasonable maxItems and minItems for array fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.4 **②P1** Array without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** save_itinerary
⑤ **Location** `$.function.parameters.properties.documents_needed`
⑥ **Original Evidence** **Array parameter 'documents_needed' has no maxItems/minItems constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.4
⑧ **Impact** Unbounded arrays may cause excessive batch processing or memory use.
⑨ **Remediation** Set reasonable maxItems and minItems for array fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.4 **②P1** Array without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** save_itinerary
⑤ **Location** `$.function.parameters.properties.flights`
⑥ **Original Evidence** **Array parameter 'flights' has no maxItems/minItems constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.4
⑧ **Impact** Unbounded arrays may cause excessive batch processing or memory use.
⑨ **Remediation** Set reasonable maxItems and minItems for array fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-2.4 **②P1** Array without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** save_itinerary
⑤ **Location** `$.function.parameters.properties.accommodations`
⑥ **Original Evidence** **Array parameter 'accommodations' has no maxItems/minItems constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.4
⑧ **Impact** Unbounded arrays may cause excessive batch processing or memory use.
⑨ **Remediation** Set reasonable maxItems and minItems for array fields
Evidence Strength Confirmed (static) · Check method: Automated

D Findings Dossier (42/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QD-T-2.4 ②P1 Array without length constraint

③ **Category** QD-T (Tool) · Parameter constraints
④ **Artifact** save_itinerary
⑤ **Location** `$.function.parameters.properties.daily_plan`
⑥ **Original Evidence** **Array parameter 'daily_plan' has no maxItems/minItems constraint.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-2.4
⑧ **Impact** Unbounded arrays may cause excessive batch processing or memory use.
⑨ **Remediation** Set reasonable maxItems and minItems for array fields
Evidence Strength Confirmed (static) · Check method: Automated

①QD-T-4.1 ②P1 Insufficient description quality

③ **Category** QD-T (Tool) · Description quality
④ **Artifact** save_itinerary
⑤ **Location** `$.function.returns.properties.error`
⑥ **Original Evidence** **The error object lacks a description and its code enum values are not explained.**
⑦ **Criterion** QD-T · Tool Sub-specification · QD-T-4.1
⑧ **Impact** An unclear description can lead to incorrect Tool calls.
⑨ **Remediation** Add trigger conditions, exclusion scenarios, and necessary input descriptions
Evidence Strength Confirmed (static) · Check method: Semi-automated

①QDP-1.1.2 ②P1 Priority conflict

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Operating Rules / Decision priorities; section 5 replan_disruption; Boundaries`
⑥ **Original Evidence** **The 'Decision priorities' list orders Safety > Budget > Preferences > Convenience, but the capability descriptions and Boundaries section introduce conflicting obligations (e.g., 'prioritizing non-refundable bookings, then hard-to-rebook experiences, then must-do' in replan_disruption, and 'does not plan trips for travelers whose entry requirements cannot be met') without mapping them onto the stated priority order, so it is unclear which rule wins when, e.g., a must-do preference conflicts with a non-refundable booking or a safety advisory.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Logic Defect · QDP-1.1.2
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Declare a priority number for each rule, or use if-else structure to clarify execution order
Evidence Strength Confirmed (static)

①QDP-1.3.2 ②P1 Ambiguous qualifier

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Operating Rules item 2; section 3; section 1`
⑥ **Original Evidence** **Key decisions rely on vague qualifiers such as 'meaningfully better', 'tight windows', 'realistic transit time', and 'at least one flexible block' without thresholds, so the agent cannot consistently decide when to flag an overage or escalate a document deadline.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Logic Defect · QDP-1.3.2
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Replace vague qualifiers with quantifiable standards, e.g., 'no more than 500 words', 'within 30 seconds'
Evidence Strength Confirmed (static)

D Findings Dossier (43/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDP-1.4.3 ②P1 Invalid Skill definition

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Sections 1-5`
⑥ **Original Evidence** **Skills are referenced by name (build_itinerary skill, optimize_budget skill, prep_travel_documents skill, monitor_travel_alerts skill, replan_disruption skill) but their trigger conditions, inputs, and outputs are not defined, so it is unclear when each skill should be invoked versus the named tools.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Logic Defect · QDP-1.4.3
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Improve Skill definition, ensure all required parameters and invocation flow are complete
Evidence Strength Confirmed (static)

①QDP-1.6.3 ②P1 Interleaved soft rules without arbitration

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Section 1 build_itinerary`
⑥ **Original Evidence** **Multiple soft rules interact without arbitration: 'no more than two must-book anchors per day', 'at least one flexible block', 'jet-lag day ones stay light', and 'activities clustered geographically' can conflict on a short trip, and no rule states which yields.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Logic Defect · QDP-1.6.3
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Set priorities for soft rules or merge them into a unified rule
Evidence Strength Confirmed (static)

①QDP-1.6.6 ②P1 Implicit-assumption dependency

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Section 2 optimize_budget; Payments stay with the user`
⑥ **Original Evidence** **The prompt assumes the user's stated budget is in the user's currency and that 'the user's currency' is known, and assumes tool availability for flights/accommodations/activities, without declaring these assumptions or how to proceed when they fail.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Logic Defect · QDP-1.6.6
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Explicitly declare hidden assumptions as preconditions
Evidence Strength Confirmed (static)

①QDP-1.6.7 ②P1 Non-monotonic reasoning defect

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Section 3 prep_travel_documents`
⑥ **Original Evidence** **Rules based on static knowledge (e.g., 'Schengen 90/180', 'six-month rule', visa processing times) become invalid when requirements change, but the prompt provides no mechanism to re-verify or invalidate prior conclusions when new information arrives.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Logic Defect · QDP-1.6.7
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Add a clear conclusion retraction mechanism: when new information X is obtained, retract previous conclusion Y
Evidence Strength Confirmed (static)

D Findings Dossier (44/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDP-2.3.3 ②P1 Missing output-stability guarantee

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Sections 1–5`
⑥ **Original Evidence** **No determinism, template, or format-stability requirement is defined, so the same trip request could yield differently structured itineraries or cost tables across sessions.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.3.3
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Add stability constraint: same input must produce the same output structure
Evidence Strength Confirmed (static)

①QDP-2.4.1 ②P1 Incomplete workflow steps

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `How a Trip Moves Through Voyager`
⑥ **Original Evidence** **The five capabilities are described but the overall workflow order, dependencies, and handoffs between them (e.g., when monitoring triggers replanning, when documents prep begins) are not fully specified.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.4.1
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Add the missing workflow steps, ensure a complete loop from input to output
Evidence Strength Confirmed (static)

①QDP-2.5.1 ②P1 Missing termination constraint

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Sections 4 and 5`
⑥ **Original Evidence** **No maximum retries, timeouts, or exit conditions are defined for tool calls, replanning loops, or monitoring polls.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.5.1
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Add termination conditions: stop after all input items are processed, or stop after processing at most N items
Evidence Strength Confirmed (static)

①QDP-2.5.3 ②P1 Missing permission-control boundary

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Sections 1–5`
⑥ **Original Evidence** **Tool and resource permissions are not limited; it is not stated which tools may write to the itinerary or which may only read.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.5.3
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Declare permission boundaries: only read operations allowed, write/delete/modify operations forbidden
Evidence Strength Confirmed (static)

D Findings Dossier (45/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①QDP-2.5.4 ②P1 Constraint priority not defined

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Operating Rules / Decision priorities`
⑥ **Original Evidence** **Although a priority list exists, it does not cover conflicts among the many soft constraints (pacing, clustering, budget substitutions, must-do preservation), leaving arbitration undefined for those cases.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.5.4
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Declare constraint priorities: safety constraints > format constraints > style constraints
Evidence Strength Confirmed (static)

①QDP-2.5.5 ②P1 Missing resource call-frequency limit

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Section 4 monitor_travel_alerts`
⑥ **Original Evidence** **No per-conversation call limit or frequency limit is defined for tools such as get_travel_alerts or get_weather_forecast, which are described as polled.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.5.5
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Add frequency limits: invoke tools at most 5 times, stop and report when exceeded
Evidence Strength Confirmed (static)

①QDP-2.7.1 ②P1 Insufficient positive-example coverage

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Who Voyager Serves; section 5`
⑥ **Original Evidence** **Only brief scenario sketches are given; there is no complete worked positive example showing a full itinerary, cost table, or document checklist output.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.7.1
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Increase the number of positive examples, ensure coverage of main usage scenarios and edge cases
Evidence Strength Confirmed (static)

①QDP-2.7.2 ②P1 Insufficient negative-example coverage

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Operating Rules; Transparency about what's real`
⑥ **Original Evidence** **No negative examples are provided showing what Voyager must not do (e.g., presenting an over-budget option as fine, inventing flight numbers, reporting 'all clear' without data).**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.7.2
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Add negative examples covering common error patterns, marked with 'do not do this'
Evidence Strength Confirmed (static)

D Findings Dossier (46/46)

Each dossier entry contains: ①ID ②Severity ③Category ④Artifact ⑤Location ⑥Original Evidence ⑦Criterion Clause ⑧Impact ⑨Remediation

①`QDP-2.7.3` **②P1** Missing boundary-case examples

③ **Category** QD-P (Prompt)
④ **Artifact** Prompt: System Prompt
⑤ **Location** `Who Voyager Serves`
⑥ **Original Evidence** **No boundary-case examples are provided for empty, overlong, or malformed inputs such as missing budget, invalid dates, or unparseable confirmation numbers.**
⑦ **Criterion** QD-P · Prompt Sub-specification · Structure Integrity · QDP-2.7.3
⑧ **Impact** This issue may reduce the prompt's reliability or consistency.
⑨ **Remediation** Add boundary case examples: return a prompt message on empty input; truncate and notify on overly long input
Evidence Strength Confirmed (static)

E Localization & Linkage

Table 6 Localization Three-Layer Positioning

Layer	Definition	Corresponding QD ID
Relationship Layer	Cross-artifact relationship defects — consistency issues between Prompt and Tool definitions	`QD-PS / QD-PT / QD-ST-x.y`
Artifact Layer	Defects within a single artifact, located in the Prompt template / Skill definition / Tool Schema itself	`QD-P-x.y.z / QD-S-x.y / QD-T-x.y`
Field Layer	Defects located to specific file lines and fields (see D section "⑤ Location")	— (location coordinates)

Table 7 Four-Segment Relationship Structure (SanityOps Linkage Mapping Specification §1.2)

Layer	Content (taking QDS-1.1 as an example)
Defect	`QDS-1.1 The Skill does not declare explicit input boundari`
Impact	This issue may allow the Skill to operate beyond its intended scope.
Validation	Re-inspect the QD determination + boundary parameter testing / exceptional-input regression
Evidence	Artifact snapshots, original fragments, re-inspection reports, quality regression results

F Re-inspection & Regression

Re-inspection Scope & Criteria

①**Scope**：Full re-run of 76 applicable check items + item-by-item regression of 178 failed items；②**Criteria**：P0 re-verification with 0 failures, Gate = PASS, and each sub-specification Score not worse than this baseline (quality ratchet)；③**Rule Version**：Sub-specification versions consistent with this run (v1.0); if rules are upgraded, record and re-determine (SanityOps Core Specification §8.5 "Rule or Evaluator Changes")。

Table 8　Regression Comparison (this baseline → re-inspection target)

Metric	This run V3	Re-inspection Target	Criteria
QD-S Score	0	≥ 0	Quality ratchet, not worse than baseline
QD-T Score	68	≥ 68	Quality ratchet, not worse than baseline
QD-P Score	24.3	≥ 24.3	Quality ratchet, not worse than baseline
QD-Cross Score	100	≥ 100	Quality ratchet, not worse than baseline
P0 Defect Count	55	= 0	Release condition
Inspect Gate	**FAIL**	PASS	P0 existence (Inspect Tool Sub-specification §5.1 "Scoring Principles")

Closure Determination (SanityOps Linkage Mapping Specification §5.6.3 "Closure Determination")

1. Original static defects have been fixed, or formally accepted as exceptions;
2. Similar variants and adjacent attack paths have been regression-tested;
3. High-risk Tools and the backend still retain hard safeguards;
4. Quality regression has not introduced task failures or boundary behavior degradation;
5. Artifact, test, environment, and evidence versions are all traceable.

Note: closure**must not**be judged solely on "attack payloads no longer succeeding" (SanityOps Linkage Mapping Specification §5.6.3).

Exceptions & Risk Acceptance

No exceptions applied for in this run (`exceptions: []`) . The release conclusion is `FAIL`, not `PASS_WITH_EXCEPTION`.

If exceptions are applied for later, all of the following must be satisfied: a unique `EXC-*` identifier; traceable Finding / artifact version / residual risk / business justification; compensating controls assessed and recorded; approver, expiry date, and review triggers clearly defined; mandatory verification gaps must not be converted directly into exceptions to bypass remediation.

G Appendix I · Terms / Criteria / Referenced Documents

Table 9 Glossary

Term	Description
Inspect (Defect Inspection)	The module that performs systematic static scanning, localization, and grading of Prompt / Skill / Tool / Cross of AI systems; not dynamic testing.
QD-P / QD-S / QD-T / QD-PT	Inspect check-item IDs: QD-P (Prompt), QD-S (Skill), QD-T (Tool), QD-PS/PT/ST (cross-artifact Cross).
P0 / P1 / P2 (severity)	By inherent check-item severity: P0 (blocking, must fix), P1 (significant, fix in version), P2 (general, schedulable); Inspect Gate considers P0 only.
Inspect Gate (release gate)	Any sub-specification with P0 → FAIL, otherwise PASS; Score is for reference only and does not replace the gate.
Score (sub-specification score)	Score = max(100 − total deduction, 0); QD-P/S/T/PT are computed separately and not merged.
W_total / base	Intermediate parameters: W_total = 5·N_P0 + 3·N_P1 + 1·N_P2; base = 100 / W_total.
Localization (defect localization)	Three-layer positioning: relationship layer / artifact layer / field layer.
Finding / State Machine	Finding records and their state values`open / confirmed / mitigated / accepted / closed / invalid`。
Review Schema	The six-dimension intermediate analysis framework for Skill checking: IDENTITY / TRIGGER / INPUT / EXECUTION / OUTPUT / FAILURE.
Skill / N/A	In this run, no artifacts found; ST 4, 4 items in total, are judged Not Applicable (N/A)。

Table 10 Determination Criteria (scoring parameters & gate rules)

Item	Rule
Total Weight	W_total = 5·N_P0 + 3·N_P1 + 1·N_P2; N takes the full check-item table of the Agent Level
Base Score	base = 100 / W_total
Per-item deduction	P0 = base×5； P1 = base×3； P2 = base×1
Each check-item ID is deducted only once, regardless of the number of hits	Each check-item ID is deducted only once, regardless of the number of hits
Score	Score = max(100 − total deduction, 0)
Gate	Any sub-specification with P0 → FAIL; otherwise PASS (Score is still output)
Release summary status	One of the five states in SanityOps Core Specification §6.2; this run: FAIL

G Appendix I · Terms / Criteria / Referenced Documents (cont.)

Table 11 Referenced Documents

Referenced in This Report	Document	Usage
§1.2 "Four-Segment Structure", §1.5 "Defect Chain Mapping", §5.5.1 "Report Wording Requirements", §5.6.2 "Minimal Evidence Package", §5.6.3 "Closure Determination"	SanityOps Linkage Mapping Specification	Localization linkage, defect chains, wording, evidence packages, and closure determination
§5.3 "Finding States", §6.2 "Release Summary Status", §6.4 "PASS_WITH_EXCEPTION Constraints"	SanityOps Core Specification	Finding state machine, five release states, exception constraints
§1.x Logic defects, §2.2.3 "Output Definition Defects", §2.2.5 "Constraint & Boundary Defects", §4.2 "Calculation Steps", §4.3 "Check Item Distribution Table"	Inspect Prompt Sub-specification	Prompt check items, score calculation, and distribution table
§1.2.2 "Required Field Inconsistency", §2.2.2 "High-Risk Operation Defects", §5.1 "Scoring Principles", §5.2.1 "Check Item Distribution Table"	Inspect Tool Sub-specification	Tool check items, scoring principles, and distribution table
§1.x Five major defect categories, §3.2 "Check Item Details", §8.2 "Calculation Steps"	Inspect Skill Sub-specification	Skill check items (Review Schema), score calculation
§3.2 "QD-PT Six Check Item Details", §8.2 "Calculation Steps", §8.3 "Check Item Distribution Table"	Inspect Cross Sub-specification	Cross check items, score calculation, and distribution table

G Appendix II · Release Status / Change History / Signatures

Table 12 Five States of Release Summary Status (SanityOps Core Specification §6.2)

Status	Meaning
`PASS`	All applicable mandatory gates passed; no unaddressed blocking defects.
`PASS_WITH_EXCEPTION`	Approved, traceable, unexpired exceptions exist; residual risks, compensating controls, and owners are clear.
`FAIL`	Unaddressed, unacceptable blocking conclusions exist, or a mandatory gate was not passed.
`NEEDS_REVIEW`	Unresolved conflicts exist in applicability, evidence, conclusions, or responsibility; release cannot be reliably determined.
`ERROR`	Artifacts, version, environment, dependencies, evaluator, or input are incomplete; the assessment cannot be executed effectively.

This report uses **`FAIL`** and uses no state name beyond the five states; this status does not replace the original conclusions of the sub-specifications.

Table 13 Change History

Rev	Date	Description
v1.0	2026-09-27	First issue: rebuilt on the 8-section skeleton of §7 "Audit Report" of the SanityOps Report Template; conclusion FAIL; 178 defects detected (P0 55 / P1 123 / P2 0).
v1.1	(To be filled)	To be backfilled after re-inspection: static re-inspection conclusion, dynamic verification and quality regression evidence, closure conclusion.

Signature Block

Prepared by	Reviewed by	Approved by
Signature / Date	Signature / Date	Signature / Date

Reader's note: Decision makers read pages 1–3 (dossier header / scope & methodology / conclusion & determination); remediation executors read pages 4–6 (findings dossier); reviewers and audit-record keepers read pages 52–53 (localization & linkage / re-inspection & regression); terms and specification fields are on pages 54–56.