M13-03 · GIBALJA VISUAL MANUAL

공공·기업 운영 조건 정의하기

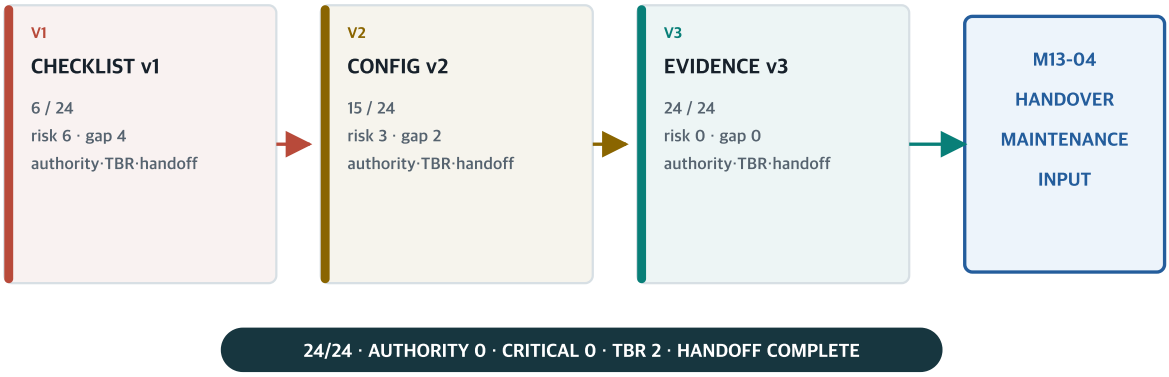
한 문장 목표: `M12·M13 source → 조직 profile·authority → applicability·current state → ID·망·접근성·데이터·보안·연계·운영 조건 → rehearsal·exception·rollout → Organization Readiness Gate → M13-04` 인수인계·유지보수 를 한 evidence trace로 연결합니다.

학습·법률·승인 경계: 이 장의 기관·회사·사용자·tenant·수치·정책 적용·pilot은 모두 합성입니다. `organization_readiness_package_ready` 는 실제 법률 자문·규제 적합 판정·보안/개인정보/접근성 인증·cloud eligibility·조달/예산 승인·production acceptance·public pilot·release·가용성 보장이 아닙니다. 국내 공공 규칙은 각 적용 범위와 효력일을 다시 확인하고, 실제 판단은 조직 policy와 자격 있는 법무·개인정보·보안·접근성·조달·재무·운영 전문가가 수행해야 합니다.

M13-03 · 15

Organization Readiness Gate를 닫고 M13-04로 넘깁니다

6/24→15/24→24/24로 개선해 source·condition·rehearsal·exception·residual risk와 handoff를 보존합니다.



24/24 · AUTHORITY 0 · CRITICAL 0 · TBR 2 · HANDOFF COMPLETE

Gate 통과는 교육용 package 준비 상태이며 실제 규제 적합·인증·조달·pilot·release 승인이 아닙니다.

한눈에 보기. 정책 이름 체크 6/24에서 evidence 24/24로 개선하고 authority·critical risk·gap·TBR·handoff를 닫습니다.

Organization Readiness Gate를 단

6/24→15/24→24/24로 개선해 source·condition·rehearsal·exception·re

V1

CHECKLIST v1

6 / 24

risk 6 · gap 4

authority·TBR·handoff

V2

CONFIG v2

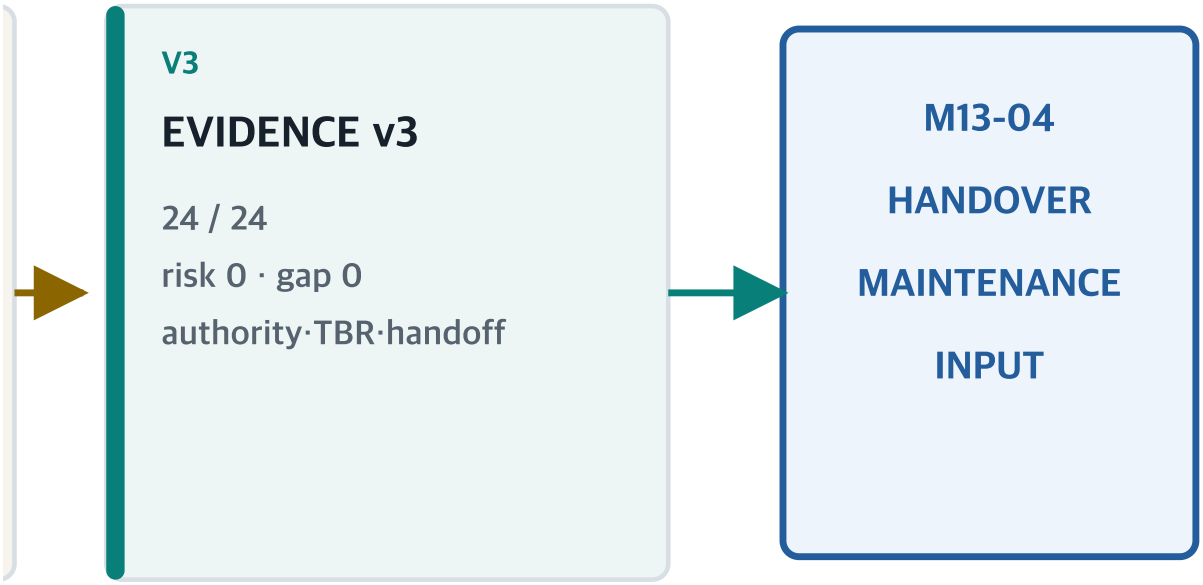
15 / 24

risk 3 · gap 2

authority·TBR·handoff

24/24 · AUTHORITY 0 · CRITICAL

sidual risk와 handoff를 보존합니다.



0 · TBR 2 · HANDOFF COMPLETE

1. 이 장에서 완성할 것

산출물	핵심 내용	합성 완료 신호
Readiness input	M12·M13 source·scope·authority	34 linked·orphan0·conflict0
Organization context	4 profile·stakeholder·current state	owner·version·TBR
Adoption conditions	ID·망·접근성·data·integration·ops	8/8 testable
Evidence package	12 controls·24 scenarios·12 evidence	coverage 100%
Gate	authority·critical risk/gap·TBR	0·0·0·2
M13-04 handoff	runbook·SLO·risk·dependency·owner	not real approval

2. 그림부터 읽는 5분 지도

그림 묶음	먼저 볼 질문	설명할 수 있어야 할 것
01~03	무엇을 어느 조직 경계에서 도입하나	evidence journey·authority·profiles
04~06	무슨 근거와 owner로 현재 조건을 정하나	applicability·RACI·inventory
07~09	사람과 단말이 실제로 접근할 수 있나	identity lifecycle·network path·accessibility
10~12	데이터와 연계가 실패 뒤에도 설명 가능한가	lifecycle·crosswalk·rehearsal
13~15	어떻게 복구·확대·예외·인계하나	SLO·rollout·Gate·M13-04

3. 합성 사례 카드

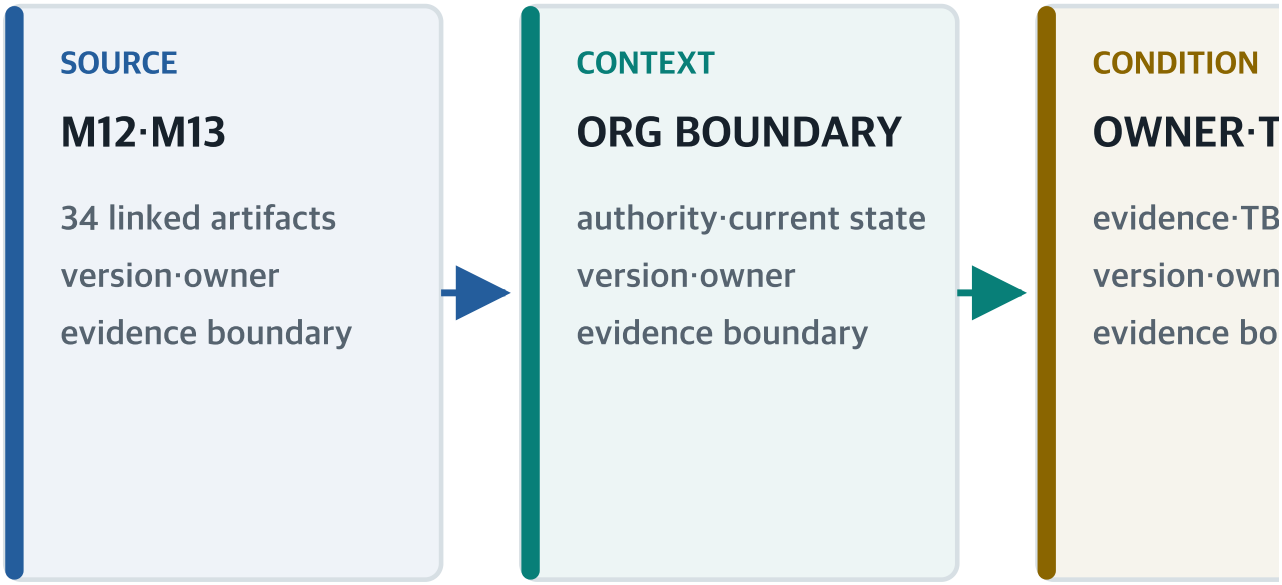
항목	합성 값	경계
Product	회의 후 실행 기록 서비스의 공공·기업 도입 조건 정의	실제 서비스·기관 아님

항목	합성 값	경계
Source	M12-04 + M13-01 + M13-02 = 34 linked	실제 정책·계약 자료 아님
Organization	240명 workforce + 1,200명 public user signal	실제 인원·부하 아님
Profile	ORG-C hybrid learning candidate	기관 유형 판정 아님
Quality	p95 800ms·RTO4h·RPO1h·response30m	SLA·가용성 보장 아님
Rollout	3 synthetic waves	public pilot·release 아님
Readiness	8 conditions·12 evidence·24 scenarios	compliance·certification 아님
Target	M13-04 handover and maintenance input	production acceptance 아님

4. 조직 조건을 하나의 evidence 흐름으로 잇기

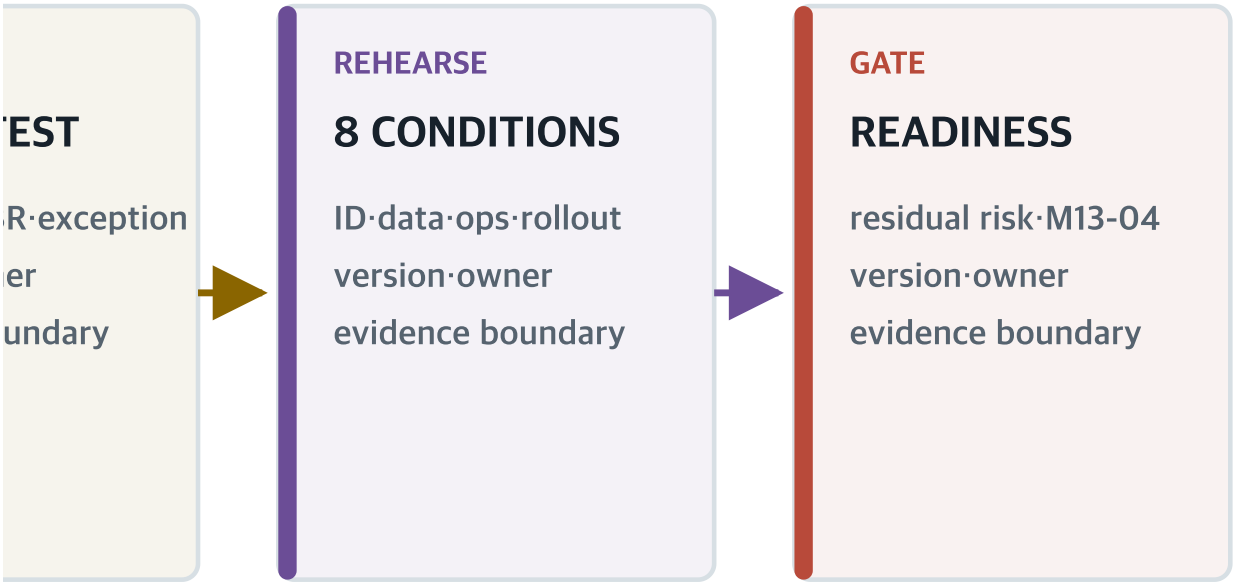
그림 1. Source→context→condition→rehearsal→Gate→M13-04를 같은 ID와 owner로 잇습니다.

제품·architecture·vendor evidence를 조직 맥락과 owner·test·exceptio



SOURCE → CONDITION → REHEARS

n이 있는 운영 조건으로 바꿉니다.



SAL → RESIDUAL RISK → HANDOFF

핵심 원칙: 운영 조건은 체크리스트가 아니라 source·owner·test·evidence·예외가 이어지는 추적 가능한 약속입니다.

좋아 보이는 architecture나 vendor package도 조직의 identity·network·data·support 환경에 맞지 않으면 실제로 도입할 수 없습니다. 합성 사례는 이전 세 장의 34개 artifact를 받아 8개 adoption condition과 12개 readiness evidence로 바꿉니다.

관점	합성 사례	확인할 evidence
Source	34 linked artifacts	version·orphan0·conflict0
Context	조직·서비스·데이터 경계	applicability owner
Condition	8 adoption conditions	owner·test·evidence
Rehearsal	24 scenarios	expected↔actual
Handoff	M13-04 input	risk·TBR·maintenance

흔한 오답: 법령과 인증 이름을 모아 표에 체크하고 도입 준비 완료라고 선언합니다.

고친 예: 각 조건에 source·scope·owner·test·evidence·exception·effective date를 붙이고 재현된 결과만 Gate로 보냅니다.

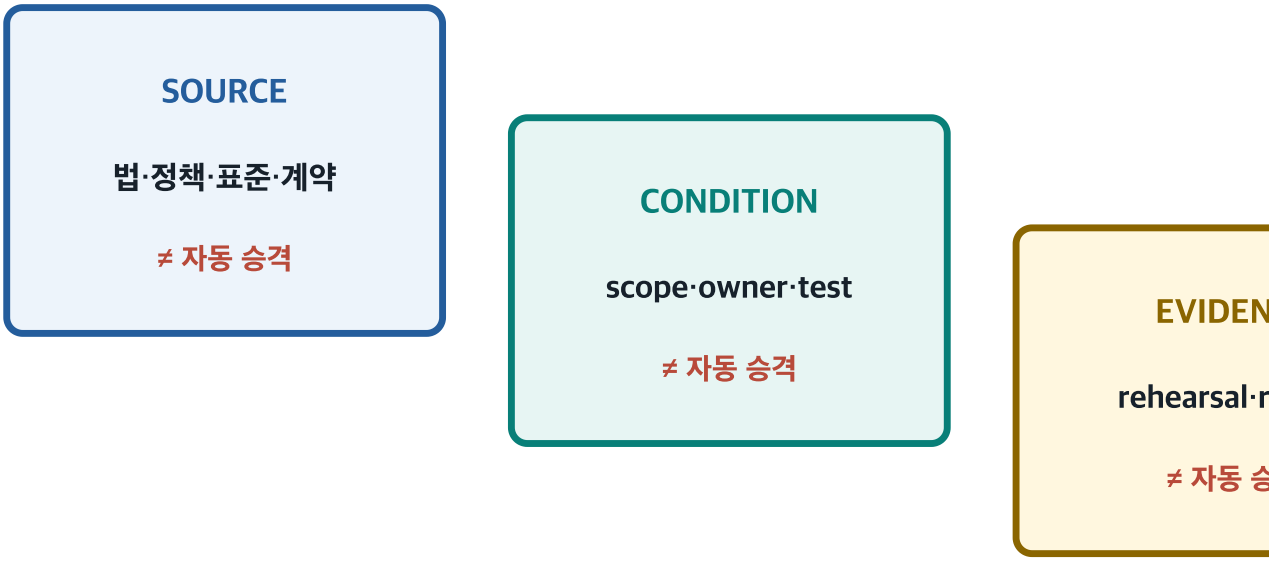
그림을 보며 4단계 연습

1. Source version과 authority를 확인합니다.
2. 조직 경계와 adoption condition을 씁니다.
3. 조건별 rehearsal과 evidence를 연결합니다.
4. Residual risk·TBR·handoff를 기록합니다.

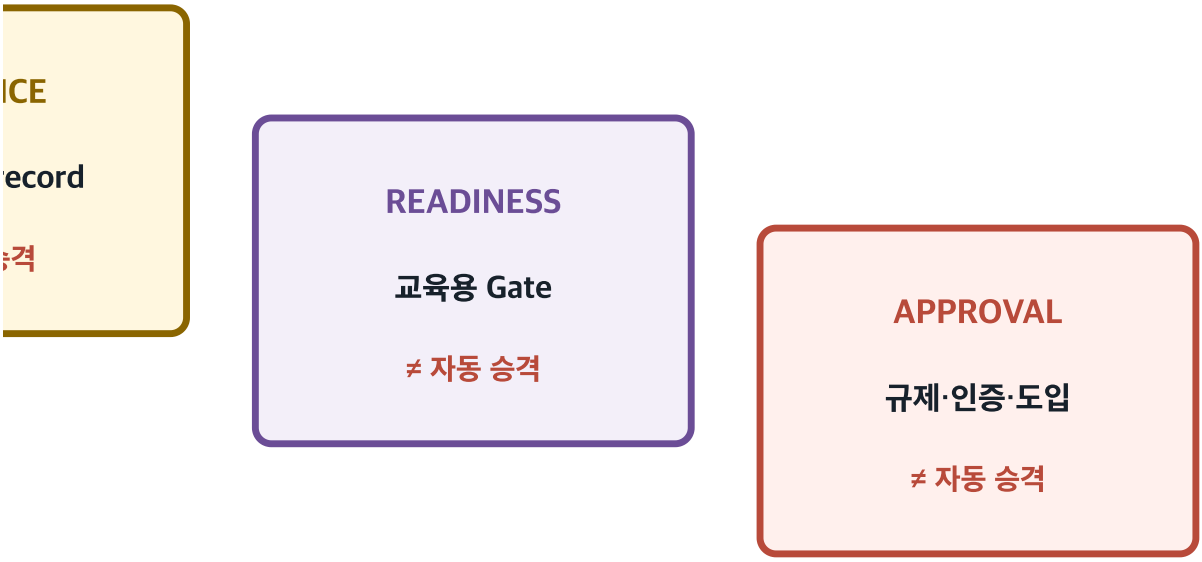
5. 근거·조건·증거와 실제 승인 권한 분리하기

그림 2. Source가 있어도 적용 판정·증거 준비·실제 도입 승인은 서로 다른 단계입니다.

각 층의 질문과 authority를 나눠 교육용 준비 상태를 실제 규제 적합이나 ㄷ



도입 승인으로 오해하지 않습니다.



핵심 원칙: 교육용 readiness는 decision input이지 규제 적합·인증·조달·배포 승인이 아닙니다.

법령·고시·표준은 적용 범위와 효력일이 다르고, 인증은 정해진 심사 범위를 가집니다. 이 장의 package는 질문과 evidence를 정리하지만 실제 판단은 조직 policy와 개인정보·보안·법무·조달·재무·운영 authority가 수행해야 합니다.

관점	합성 사례	확인할 evidence
Source	공식 원문·current edition	authority·date
Condition	scope·owner·test	organization context
Evidence	rehearsal record	version·coverage
Readiness	gap·risk·TBR	learning Gate
Approval	실제 도입·예산·release	qualified authority

흔한 오답: CSAP나 ISO 인증 이름이 보이면 해당 서비스와 기관의 cloud 사용이 자동 승인됐다고 씁니다.

고친 예: 인증 범위·등급·service·location·effective date와 조직의 cloud eligibility·보안·조달 authority를 별도 행으로 둡니다.

그림을 보며 4단계 연습

1. 현재 문서가 답하는 질문을 씁니다.
2. 답하지 않는 실제 결정을 나열합니다.
3. 각 결정의 source와 authority를 연결합니다.
4. 오해 가능한 '준비 완료'를 경계 문장으로 고칩니다.

6. 같은 서비스도 조직 profile별 조건 다르게 보기

그림 3. 같은 제품이라도 사용자·identity·data·운영 경계에 따라 우선 조건이 달라집니다.

[illegible]

대국민·기업 workforce·hybrid·소규모 profile을 비교해 context를 requir

ORG-A

대국민 서비스형

public user edge
accessibility·audit
민원 flow
synthetic only

ORG-B

기업 workforce형

SSO·SCIM·device
internal integration
account lifecycle
synthetic only

SAME PRODUCT · DIFFERENT CO

ement보다 먼저 확인합니다.

ORG-C

공공·기업 hybrid형

public+workforce
regulated data
learning candidate
synthetic only

LEARNING PROFILE

ORG-D

소규모 baseline형

simple SaaS
small integration
growth trigger
synthetic only

NTEXT · DIFFERENT CONDITIONS

핵심 원칙: 조직 유형은 정답 label이 아니라 놓치기 쉬운 조건을 드러내는 비교 lens입니다.

대국민 서비스는 접근성과 공개 edge가 중요하고, 기업 workforce는 SSO·SCIM·managed device가 중요합니다. Hybrid는 두 경계를 동시에 다뤄 복잡도가 높고, 작은 조직도 성장·규제·복구 trigger가 생기면 조건을 다시 확장해야 합니다.

관점	합성 사례	확인할 evidence
ORG-A	대국민 서비스형	accessibility·public edge
ORG-B	기업 workforce형	SSO·SCIM·device
ORG-C	공공·기업 hybrid형	두 경계 trade-off
ORG-D	소규모 baseline형	growth trigger
Selected	ORG-C learning candidate	실제 기관 판정 아님

흔한 오답: 공공기관이면 모든 기준과 최고 수준 통제를 동일하게 적용한다고 가정합니다.

고친 예: 기관·업무·사용자·data·technology scope를 먼저 쓰고 profile별 조건과 적용 source를 비교합니다.

그림을 보며 4단계 연습

1. 우리 사례의 사용자 집단을 나눕니다.
2. 네 profile과 닮은 점·다른 점을 씁니다.
3. 각 profile의 우선 조건을 세 개 고릅니다.
4. 재검토 trigger와 owner를 정합니다.

7. 적용 가능성을 근거 이름보다 범위와 authority로 판정하기

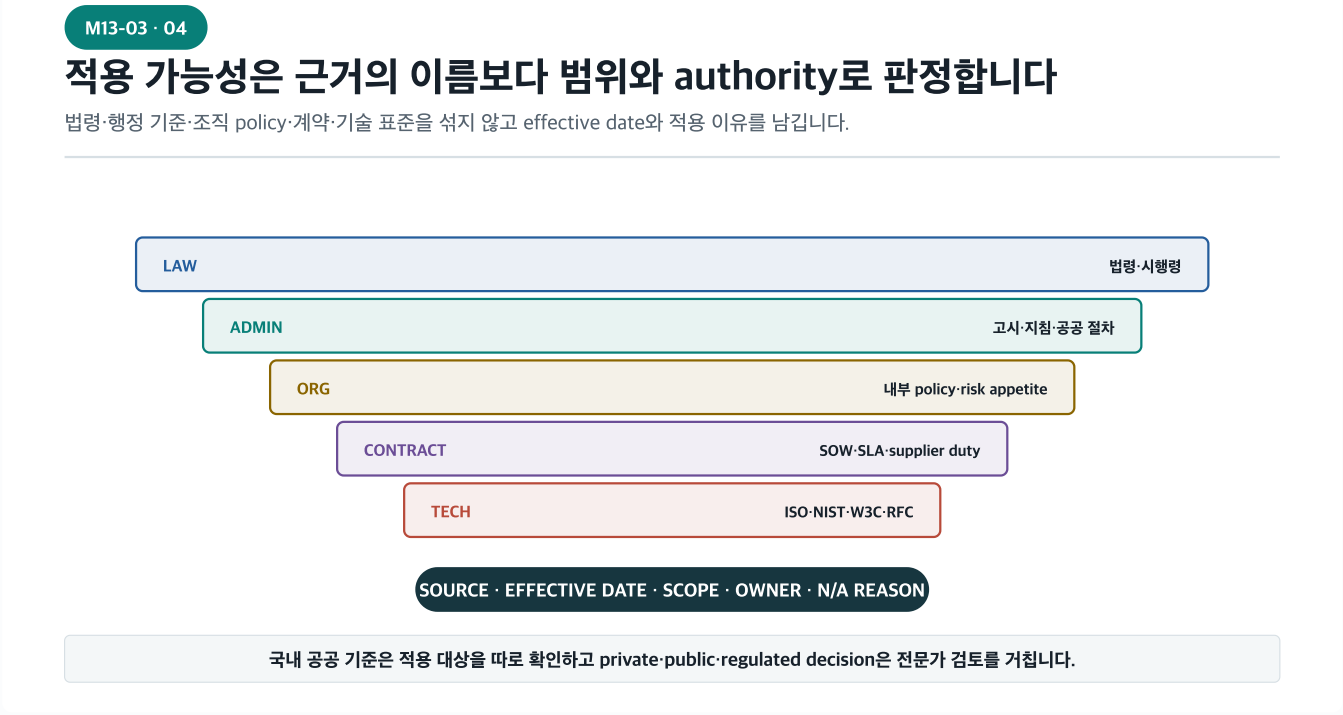
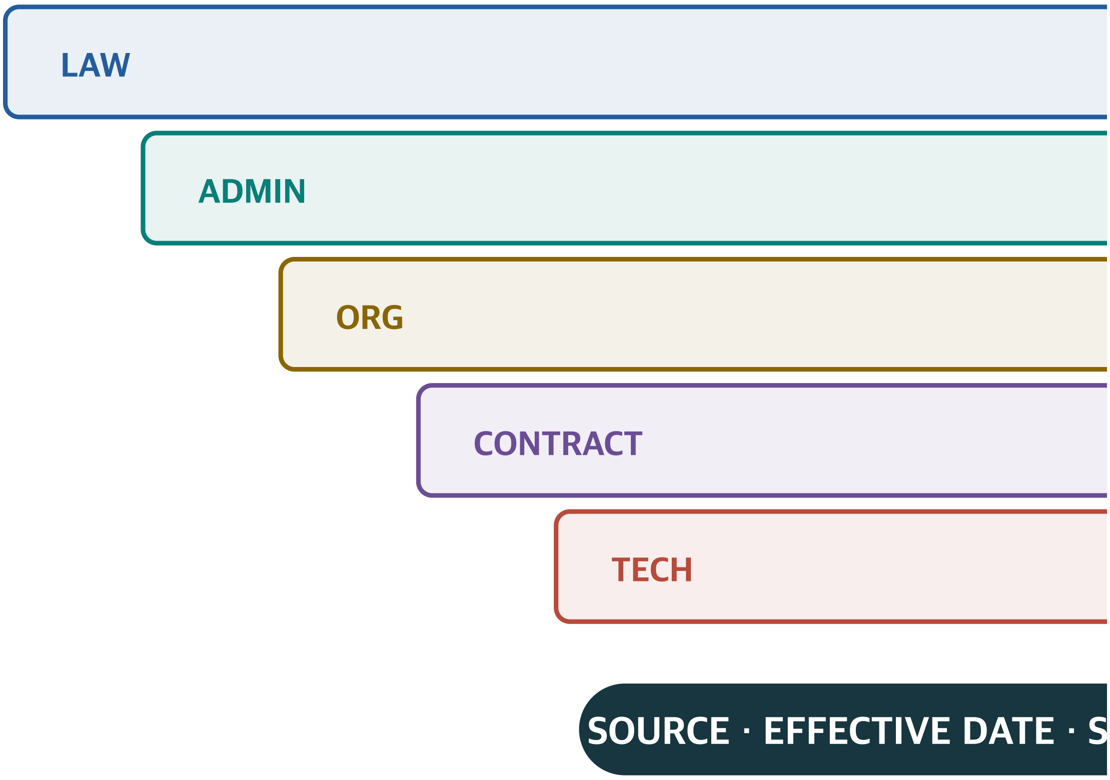
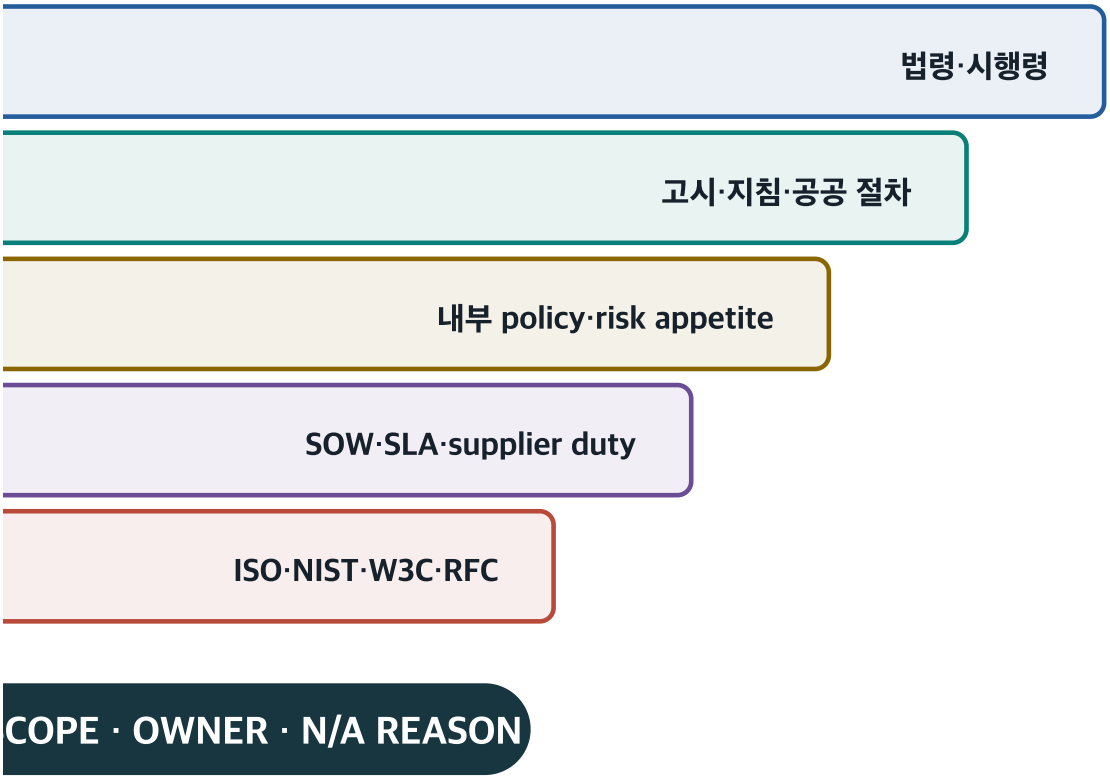


그림 4. Source hierarchy보다 해당 조직·업무·데이터에 적용되는 범위와 결정 권한을 기록합니다.

법령·행정 기준·조직 policy·계약·기술 표준을 섞지 않고 effective date와



적용 이유를 남깁니다.


법령·시행령
고시·지침·공공 절차
내부 policy·risk appetite
SOW·SLA·supplier duty
ISO·NIST·W3C·RFC
COPE · OWNER · N/A REASON

핵심 원칙: '유명한 기준'과 '우리 서비스에 적용되는 기준'은 같은 말이 아닙니다.

국내 공공 지침은 기관과 사업 범위가 정해져 있고, 국제 표준은 자발적 적용 또는 계약 조건일 수 있습니다. 최신 source를 확인한 뒤 적용·비적용·TBR을 근거와 함께 기록하고 모호한 법적 해석은 자격 있는 전문가에게 올립니다.

관점	합성 사례	확인할 evidence
Law	법률·시행령	jurisdiction·effective date
Admin	고시·지침	기관·사업 scope
Organization	내부 policy	owner·precedence
Contract	서비스·공급자 의무	binding scope
Standard	ISO·NIST·WCAG	tailoring·evidence

흔한 오답: 검색 결과의 요약 문장만 복사하고 적용 범위와 시행일을 확인하지 않습니다.

고친 예: 공식 원문 URL·edition·효력일·scope test·interpretation owner·next review date를 register에 남깁니다.

그림을 보며 4단계 연습

1. 후보 source의 공식 원문을 찾습니다.
2. 기관·service·data scope test를 씁니다.
3. 적용/비적용/TBR과 근거를 기록합니다.
4. 해석·예외·승인 authority를 연결합니다.

8. 도입 조건에 accountable owner와 예외 권한 붙이기

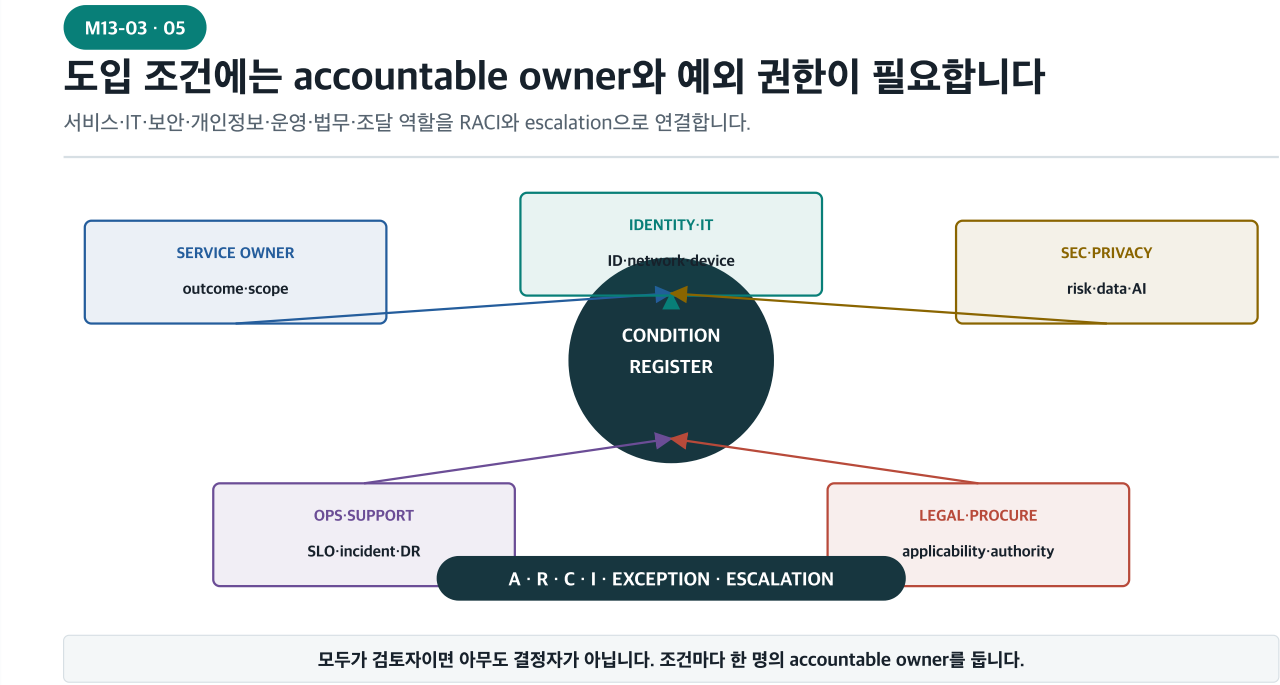
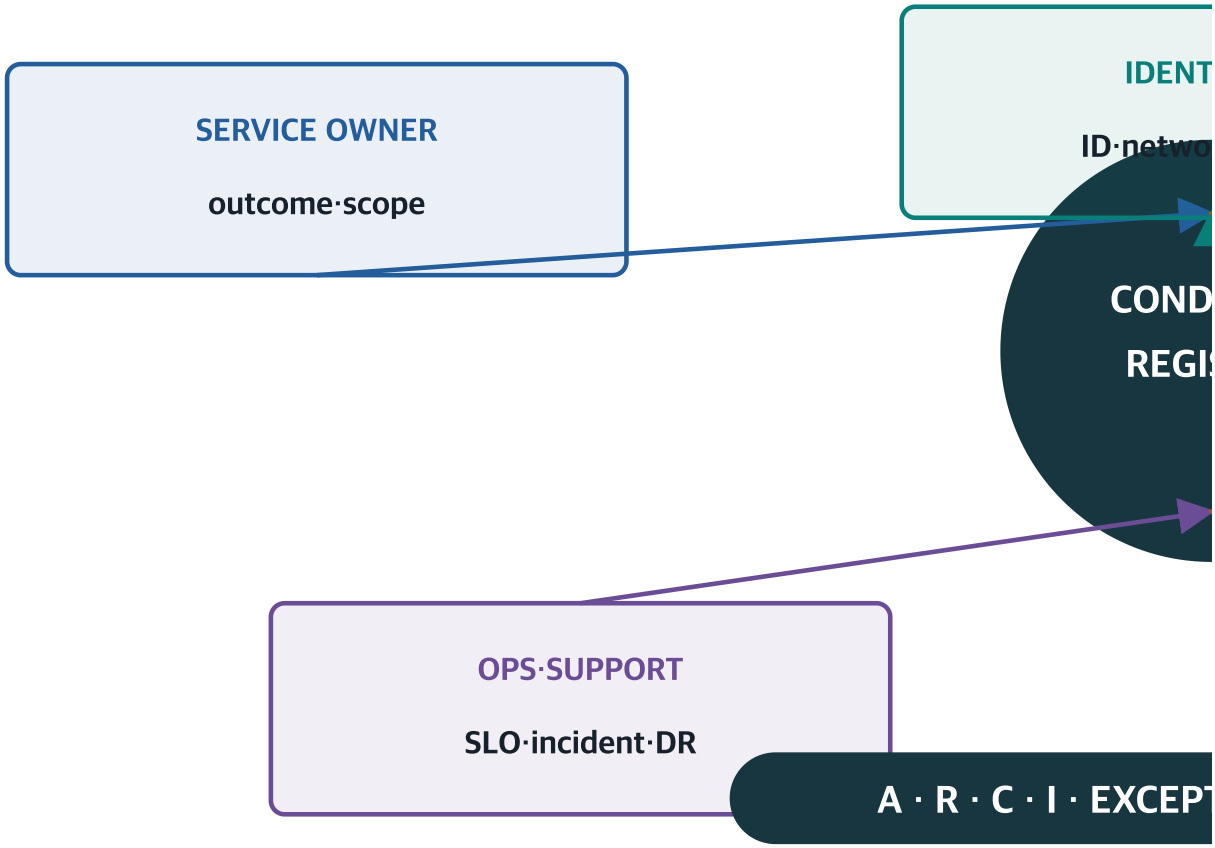


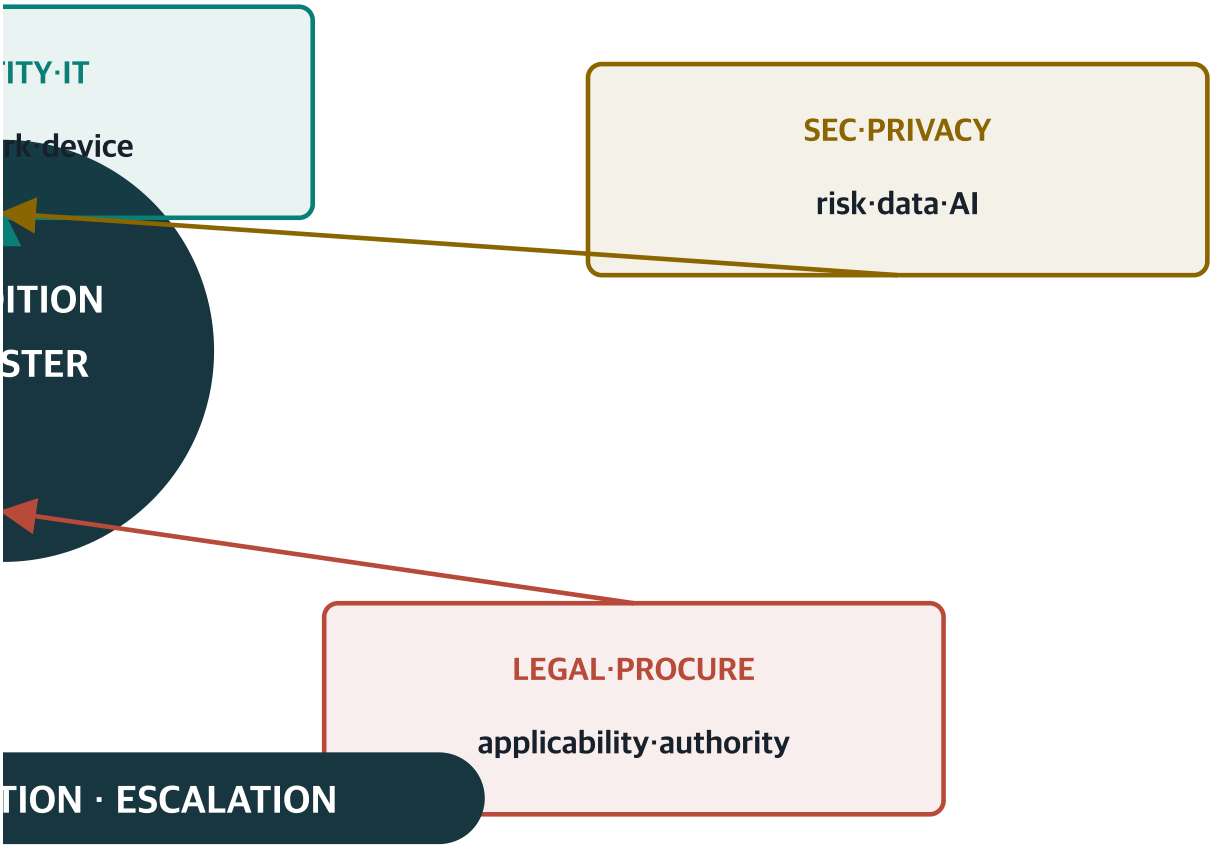
그림 5. 조건마다 accountable owner 한 명과 실제 예외·escalation authority를 분리합니다.

그림 로컬에는 accountable owner가

서비스·IT·보안·개인정보·운영·법무·조달 역할을 RACI와 escalation으로 연



결합니다.


ITY·IT
k·device
ITION
STER
SEC·PRIVACY
risk·data·AI
LEGAL·PROCURE
applicability·authority
TION · ESCALATION

> **핵심 원칙:** 모두가 검토하는 조건도 최종 설명 책임과 예외 승인은 명확해야 합니다.

Identity·security·privacy·accessibility·operations는 서로 의존하지만 책임을 공동이라고만 쓰면 실패 때 결정이 멈춥니다. RACI와 decision right를 condition별로 작성하고, 문서상 owner와 실제 조직 권한의 충돌을 0으로 닫습니다.

관점	합성 사례	확인할 evidence
Service owner	outcome·scope	accountable
Identity/IT	SSO·device·network	responsible
Security/privacy	risk·data·exception	consulted/authority
Operations	SLO·incident·restore	receiving owner
Legal/procurement	applicability·contract	qualified review

> **흔한 오답:** 보안·개인정보·법무팀을 모두 승인자로 적고 최종 결정 경로는 비워 둡니다.

> **고친 예:** 조건마다 A는 한 명, R은 실행 역할, C/I는 협의·통보로 나누고 예외·release 권한을 별도 열에 씁니다.

그림을 보며 4단계 연습

1. Stakeholder와 관심사를 그립니다.
2. 조건별 RACI를 작성합니다.
3. 예외·risk acceptance·release authority를 확인합니다.
4. Authority conflict와 escalation을 rehearsal합니다.

9. 현행 환경을 모르면 좋은 requirement도 연결되지 않음을 이해하기

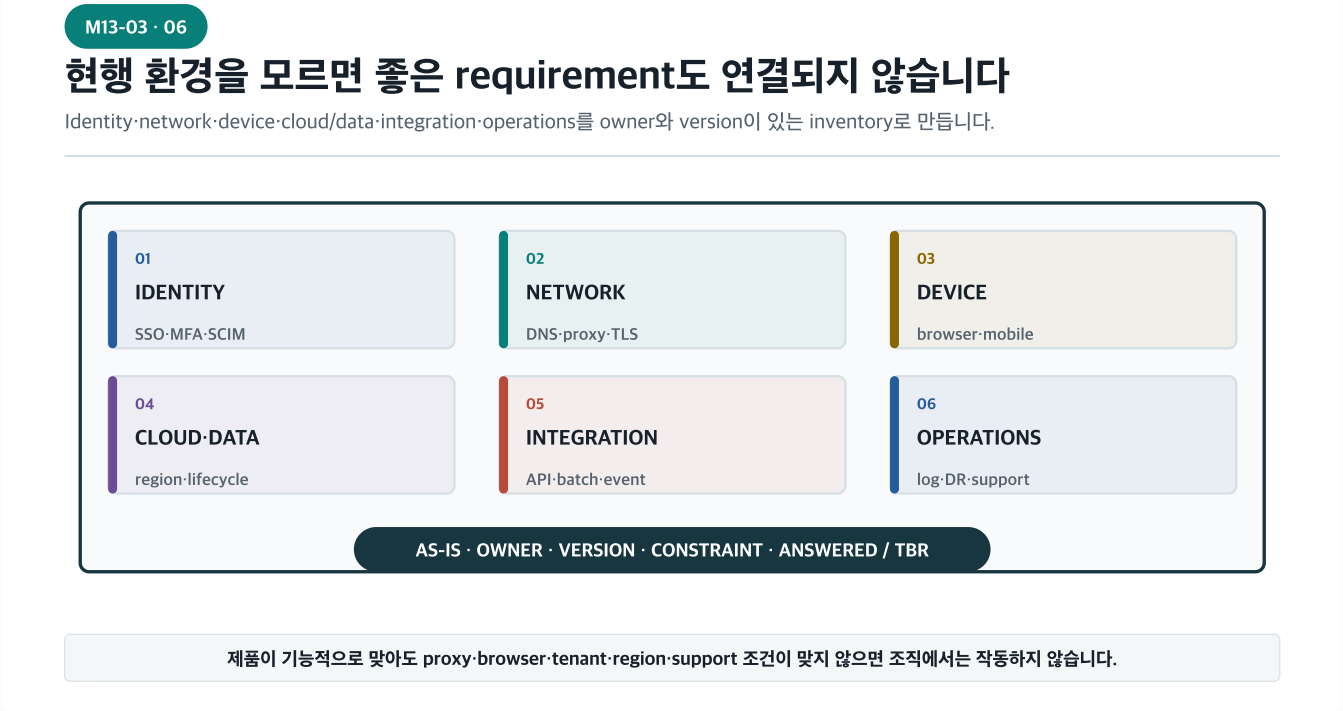
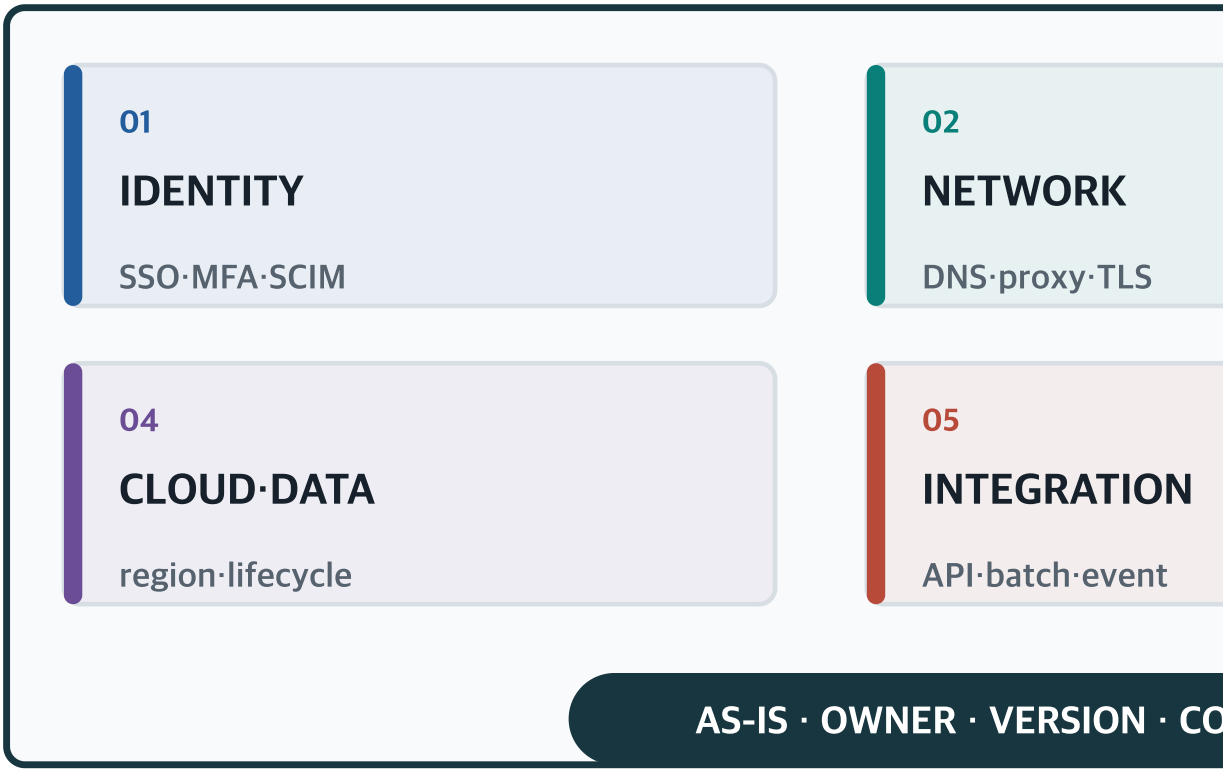


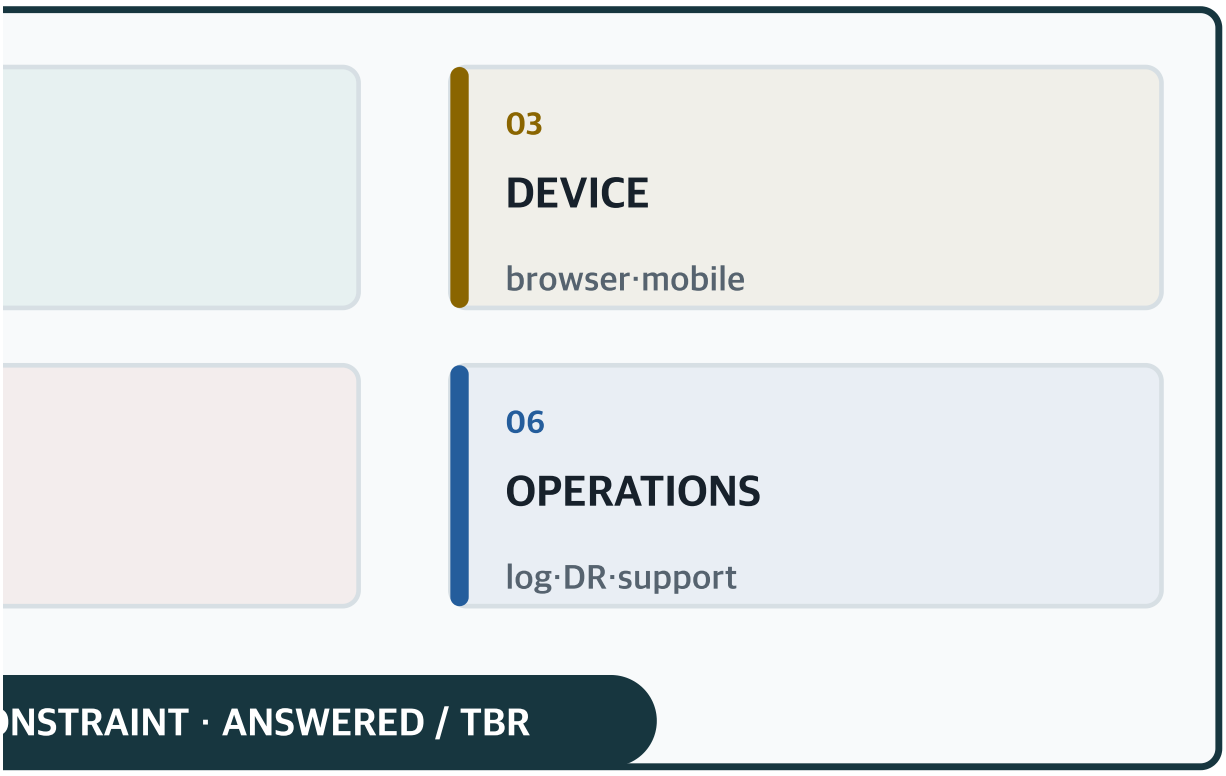
그림 6. 목표 설계 전에 실제 identity·network·device·cloud·data·integration·operations를 inventory로 고정합니다.

[illegible]

Identity·network·device·cloud/data·integration·operations를 owner와



· version이 있는 inventory로 만듭니다.



핵심 원칙: 도입 조건은 목표만 쓰지 않고 현재 환경과 gap·owner·TBR을 함께 보여 줘야 합니다.

SSO가 필요하다는 문장만으로는 IdP·protocol·group source·계정 회수 시간을 알 수 없습니다. Proxy·browser·mobile·data location·API·log·support window도 현재 version과 owner를 조사해야 testable requirement가 됩니다.

관점	합성 사례	확인할 evidence
Identity	IdP·SSO·MFA·SCIM	owner·protocol
Network	DNS·proxy·TLS·egress	path·failure
Device	managed·browser·mobile	support baseline
Cloud/data	region·copy·backup	location·retention
Integration/ops	API·log·support	SLO·version

흔한 오답: 제안 architecture 그림을 current state로 간주하고 실제 환경 조사를 생략합니다.

고친 예: 각 inventory item에 current version·owner·constraint·evidence·freshness·answered/TBR을 붙입니다.

그림을 보며 4단계 연습

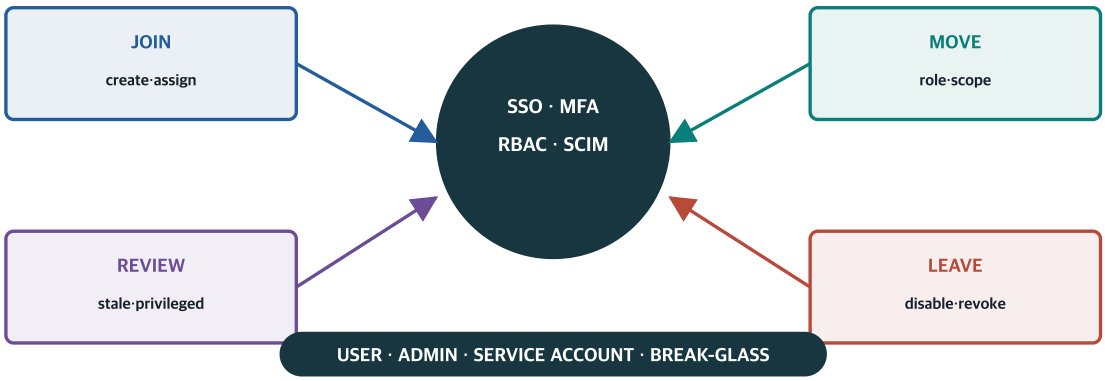
1. 7개 환경 영역의 source를 찾습니다.
2. 현재값·owner·version을 기록합니다.
3. Target과 gap·dependency를 비교합니다.
4. 미확인은 TBR과 due로 보냅니다.

10. 로그인 성공보다 계정 생애주기 전체 검증하기

M13-03 · 07

로그인 성공보다 계정 생애주기 전체를 검증합니다

SSO·MFA·RBAC·SCIM을 joiner·mover·leaver·review와 privileged·service account까지 연결합니다.

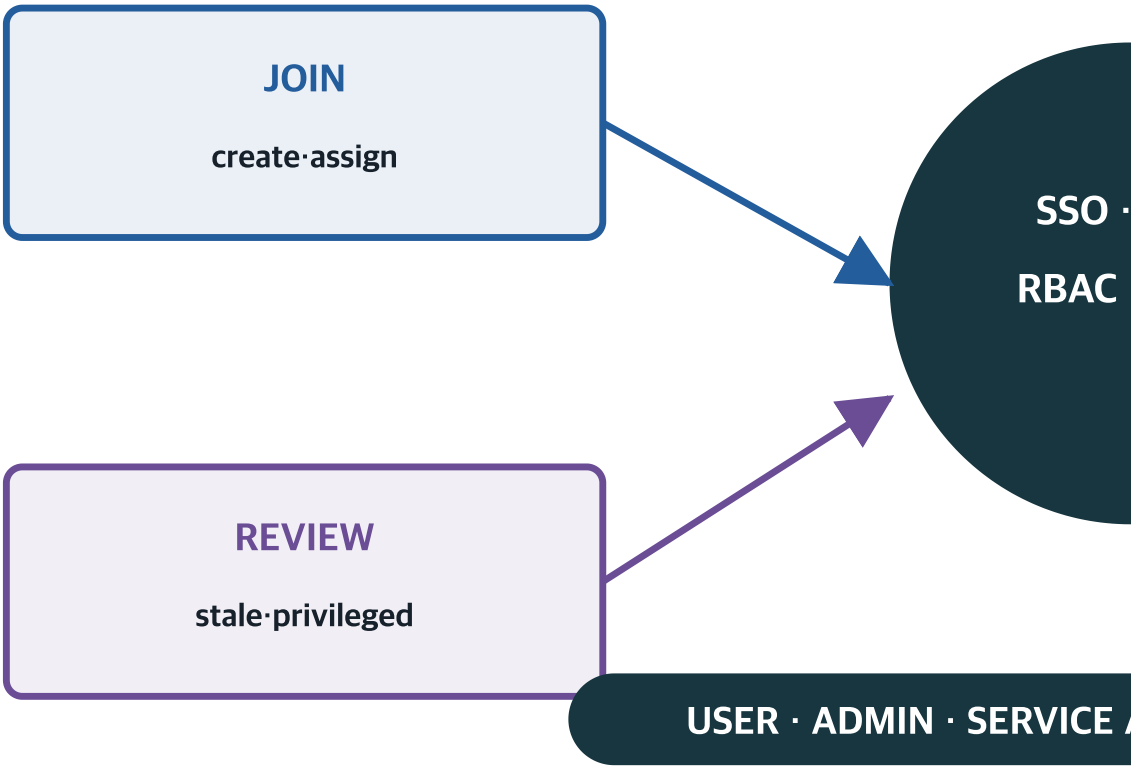


퇴사 계정과 service credential이 실제로 revoke되는 시간을 재현해야 access lifecycle evidence가 됩니다.

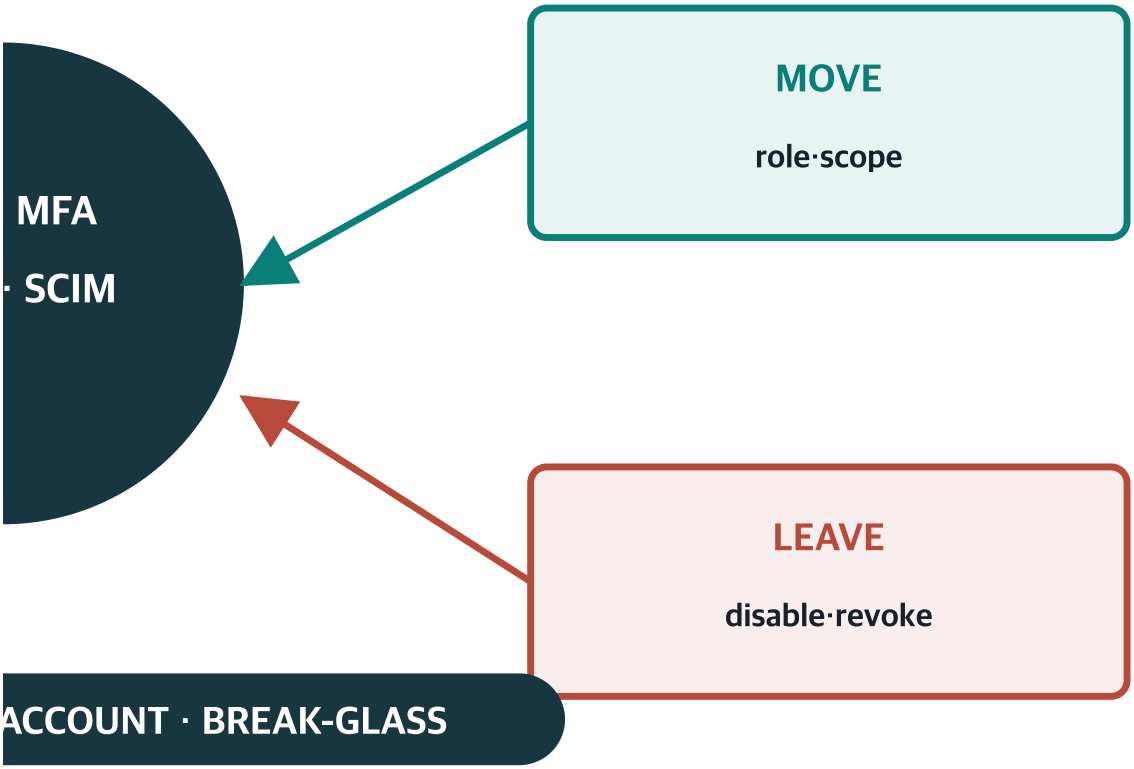
그림 7. Join·move·review·leave와 service account·break-glass까지 권한 부여와 회수를 rehearsal합니다.

로그인 성공 후 세션 생성까지 흐름

SSO·MFA·RBAC·SCIM을 joiner·mover·leaver·review와 privileged·servi



ce account까지 연결합니다.



핵심 원칙: 인증 화면이 열리는 것보다 올바른 권한이 생기고 바뀌고 사라지는지가 중요합니다.

SSO·MFA·RBAC를 설정해도 mover의 과거 권한, 퇴사자의 session, owner 없는 service account가 남을 수 있습니다. 합성 tenant에서 join·move·leave·revoke를 실행하고 stale access 0, revocation 시간, privileged review를 evidence로 남깁니다.

관점	합성 사례	확인할 evidence
Join	proof→account→role	approved provision
Move	role change	old access revoke
Review	recertification	owner decision
Leave	disable·session revoke	stale access0
Special	service·break-glass	alert·rotation·expiry

흔한 오답: MFA 로그인 screenshot 하나로 identity와 access control을 모두 통과시킵니다.

고친 예: Subject·role·resource·condition별 expected access와 actual을 비교하고 모든 lifecycle event의 evidence를 보존합니다.

그림을 보며 4단계 연습

1. Subject와 role·resource를 나눕니다.
2. Join·move·leave expected를 씁니다.
3. Privileged·service·break-glass rule을 추가합니다.
4. Revoke·review·audit를 rehearsal합니다.

11. 망 조건을 end-to-end 허용·차단 경로로 검증하기

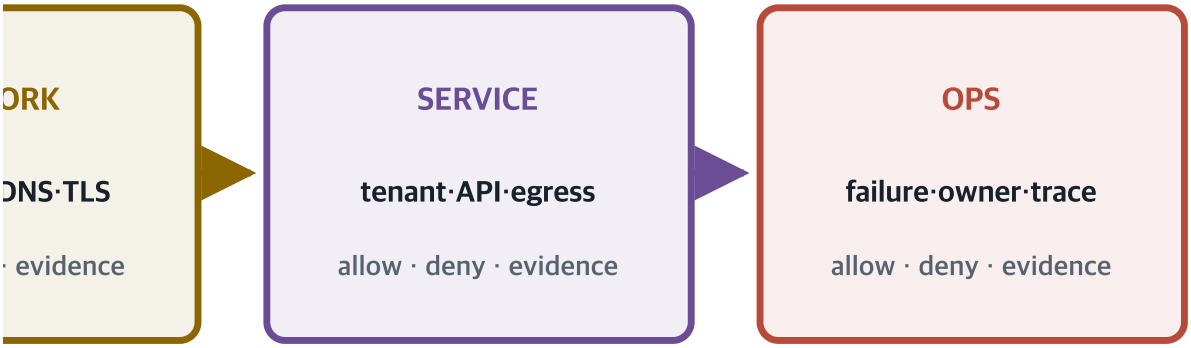
그림 8. 사용자 단말부터 service·operations까지 DNS·proxy·firewall·TLS·egress와 실패 owner를 잇습니다.

Device·identity·proxy/firewall·DNS/TLS·service egress와 실패 owner를

APPROVED PATH 100% · UNDEC

[illegible]

[illegible] 같은 connectivity matrix에서 검증합니다.



CLARED EGRESS 0 · FAIL CLOSED

핵심 원칙: 망 연계는 URL 목록이 아니라 승인된 path와 차단된 path를 모두 재현하는 계약입니다.

기관 proxy·private route·DNS filtering·certificate inspection·managed device가 서로 영향을 줍니다. 허용 경로 100%, undeclared egress 0, 차단 경로 fail-closed, 모든 실패의 owner를 합격 조건으로 둡니다.

관점	합성 사례	확인할 evidence
Device	managed/unmanaged	posture·browser
Identity	SSO·MFA	redirect·certificate
Network	DNS·proxy·firewall	allow/deny
Service	API·storage	TLS·endpoint
Operations	monitor·support	failure owner

흔한 오답: 방화벽에 443을 열면 연결 조건이 완료됐다고 기록합니다.

고친 예: Source→destination→protocol→DNS→proxy→TLS→egress→expected result→owner를 path matrix로 시험합니다.

그림을 보며 4단계 연습

1. 다섯 trust zone을 그립니다.
2. 허용·차단 path를 함께 씁니다.
3. Device·browser·remote access 조건을 붙입니다.
4. Failure와 recovery owner를 rehearsal합니다.

12. 접근성을 자동 검사 한 번이 아닌 사용자 여정 품질로 검증하기

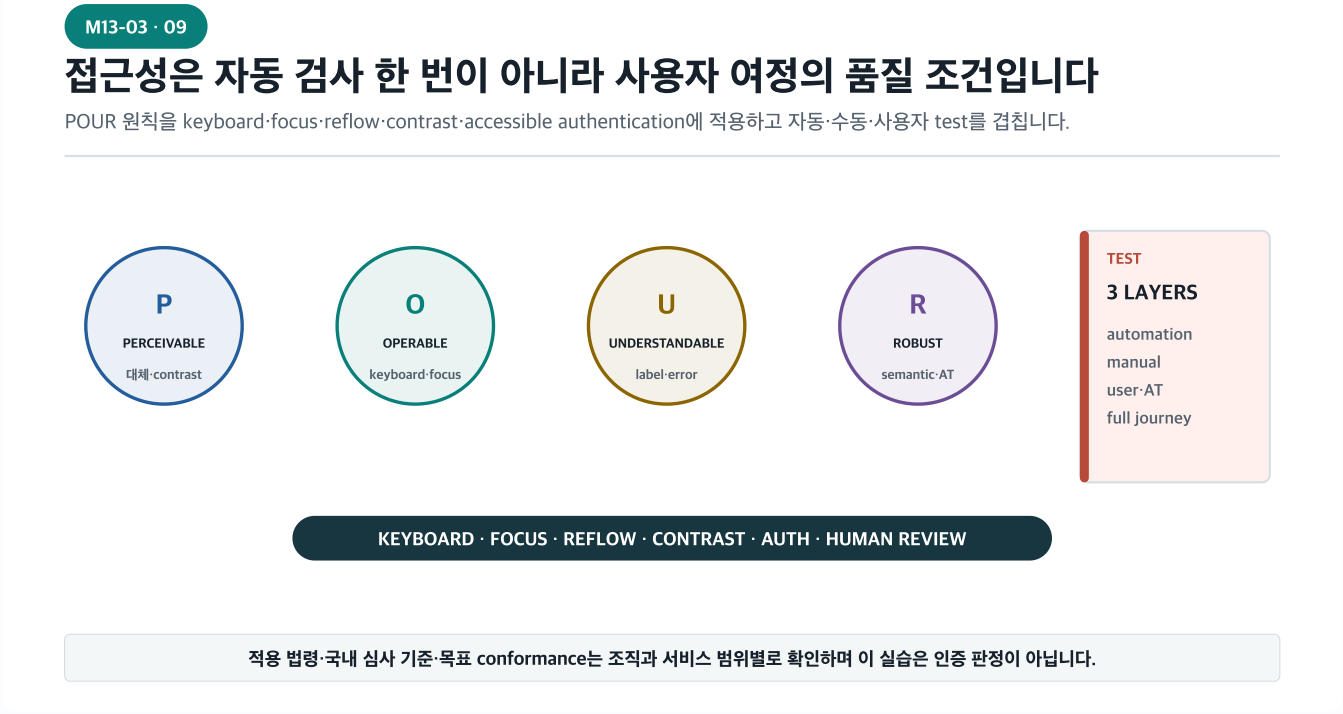


그림 9. 적용 기준과 scope를 정한 뒤 자동·수동·보조기술·사용자 test를 겹쳐 검증합니다.

접근성 체크리스트 [illegible]

POUR 원칙을 keyboard·focus·reflow·contrast·accessible authenticatio

KEYBOARD · FOCUS · REFLOW · CO

n에 적용하고 자동·수동·사용자 test를 겹칩니다.

ANDABLE
error

R
ROBUST
semantic·AT

TEST
3 LAYERS
automation
manual
user·AT
full journey

ONTRAST · AUTH · HUMAN REVIEW

핵심 원칙: 접근성은 보고서 점수가 아니라 핵심 task를 인식·조작·이해·완료할 수 있는 품질입니다.

자동 도구는 일부 규칙을 빠르게 찾지만 focus order·keyboard trap·screen reader 의미·오류 회복은 사람이 확인해야 합니다. 목표 기준과 scope, 대표 journey, known exception, remediation owner를 함께 기록합니다.

관점	합성 사례	확인할 evidence
Perceivable	alt·contrast·reflow	visual/semantic
Operable	keyboard·focus	full journey
Understandable	label·error·help	recovery
Robust	semantic·AT	browser/reader
Test layers	auto→manual→user	evidence·owner

흔한 오답: 자동 검사 오류가 0이므로 접근성 인증을 받았다고 표현합니다.

고친 예: 적용 기준·target·page/task scope·자동 결과·manual journey·보조기술·사용자 review·known gap을 분리합니다.

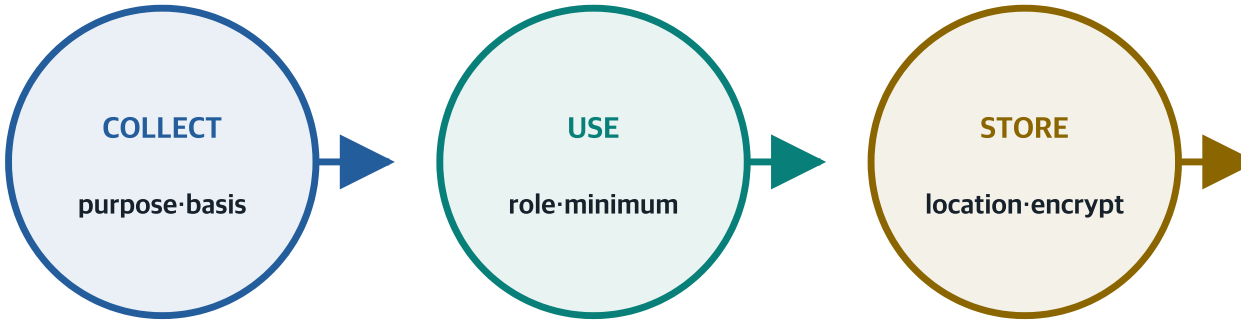
그림을 보며 4단계 연습

1. 적용 후보 기준과 목표 level을 확인합니다.
2. P0 user journey를 고릅니다.
3. Keyboard·focus·reflow·auth를 test합니다.
4. 사람 review와 remediation evidence를 남깁니다.

13. 데이터를 수집부터 삭제·반출까지 위치와 책임으로 추적하기

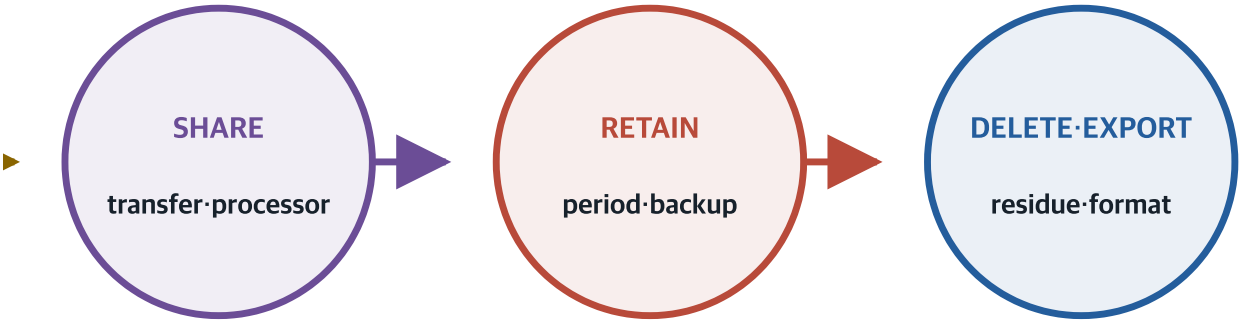
그림 10. Field마다 목적·owner·classification·location·retention·deletion·export를 연결합니다.

필드별 purpose·classification·residency·transfer·retention·backup resi



FIELD · OWNER · CLASS · LOCA

due·export를 하나의 map으로 잇습니다.



TION · RETENTION · EVIDENCE

핵심 원칙: 데이터 조건은 DB region 한 줄이 아니라 원본·복제·log·backup·integration의 생애주기입니다.

업무 DB를 지워도 audit log·검색 index·analytics·backup·subprocessor copy에 data가 남을 수 있습니다. Field와 목적에서 시작해 모든 처리 위치·transfer·보존·삭제·잔존 결정·export format을 trace합니다.

관점	합성 사례	확인할 evidence
Collect/use	purpose·basis·minimum	field owner
Store	DB·cache·index	location·encryption
Share	API·processor	transfer·contract
Retain/delete	schedule·backup residue	verification
Export/exit	format·checksum	receiving owner

흔한 오답: 주 database가 국내 region이라는 정보만으로 data residency와 lifecycle을 완료합니다.

고친 예: Field→purpose→system/copy→country/region→owner→retention→delete method→residue/exception→export를 map으로 씁니다.

그림을 보며 4단계 연습

1. 대표 field와 classification을 고릅니다.
2. 모든 copy와 location을 그립니다.
3. Retention·deletion·backup residue를 연결합니다.
4. Export·exit와 authority를 rehearsal합니다.

14. Privacy·security·AI 근거를 조직 control과 evidence에 crosswalk하기

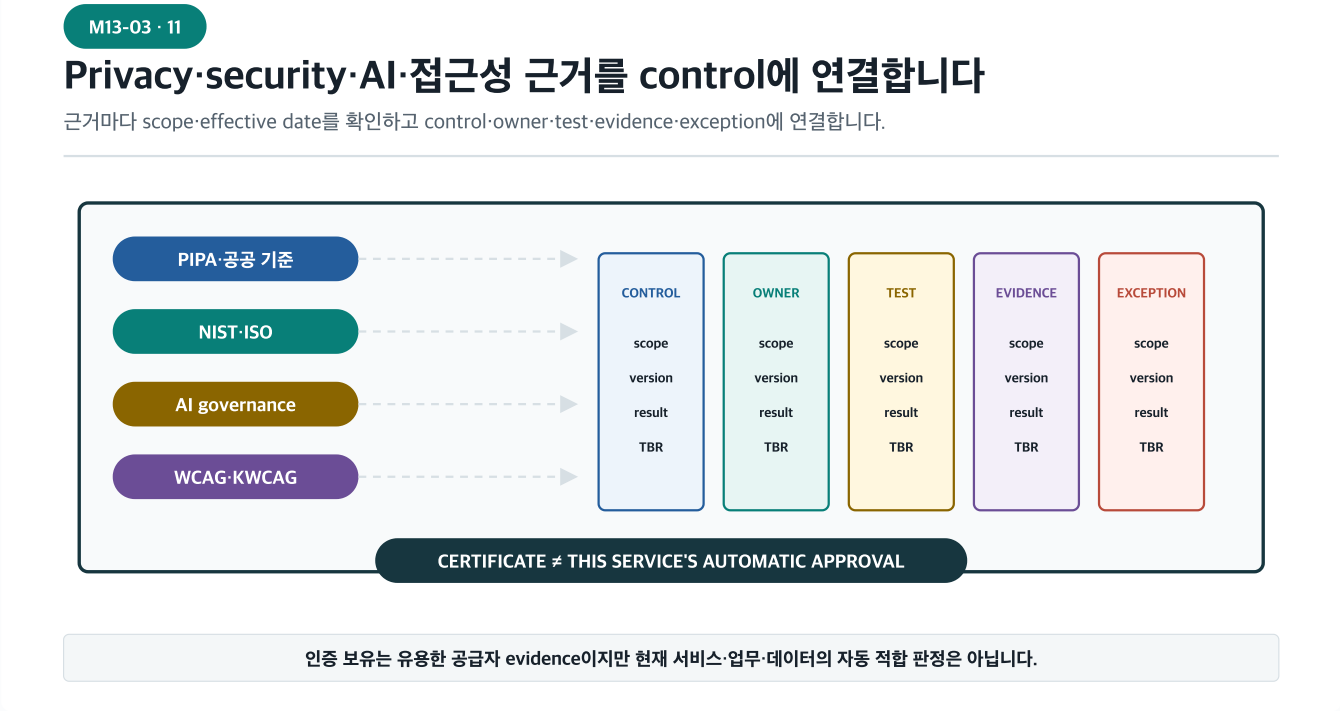
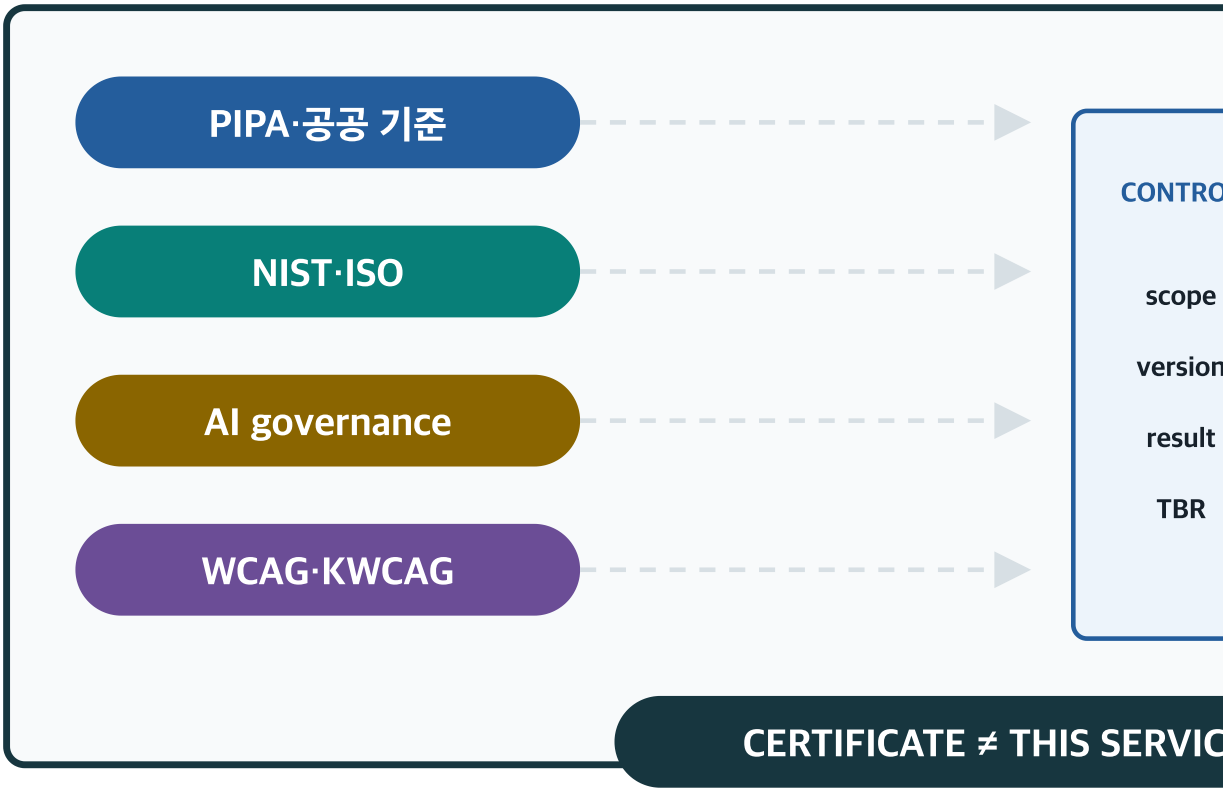


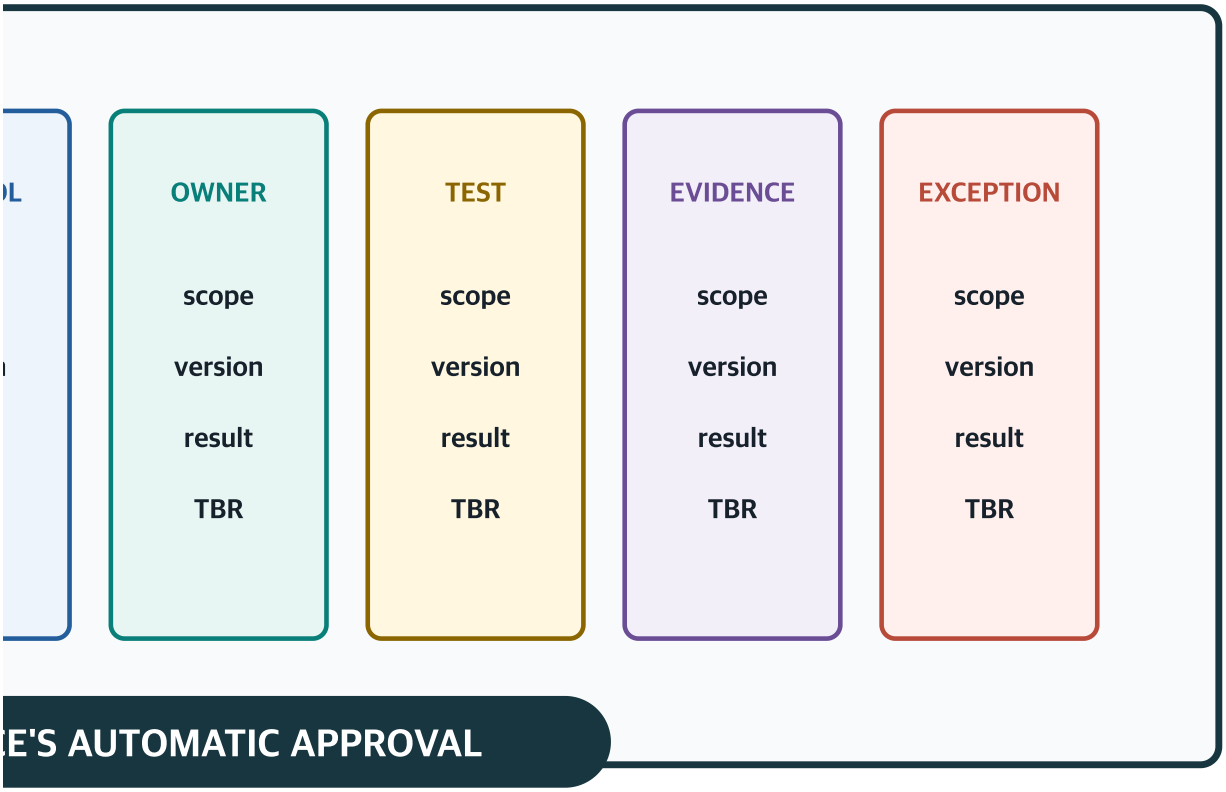
그림 11. 서로 다른 기준의 문장을 공통 control·owner·test·evidence·exception 구조로 번역합니다.

Privacy·Security·AI 검증 근거별 c

근거마다 scope·effective date를 확인하고 control·owner·test·evidence



·exception에 연결합니다.



핵심 원칙: 인증 logo와 policy 이름보다 현재 서비스에 적용되는 control outcome과 evidence가 중요합니다.

Privacy·information security·AI governance·accessibility 기준은 목적과 적용 범위가 다릅니다. Source를 섞어 하나의 '준수' check로 만들지 말고 각 범위를 확인한 뒤 공통 control language에 연결합니다.

관점	합성 사례	확인할 evidence
Privacy	purpose·rights·lifecycle	PIPA/ISO27701 context
Security	risk·access·incident	ISMS-P/CSAP/27001/NIST
AI	map·measure·human oversight	AI Act/RMF/42001
Accessibility	POUR·journey	WCAG/KWCAG
Crosswalk	control·owner·test·evidence	exception·version

흔한 오답: ISO 27001 인증이 있으므로 privacy·AI·accessibility 조건까지 모두 충족했다고 간주합니다.

고친 예: 각 source의 scope와 edition을 적고 서비스 control·owner·test·actual evidence·gap을 한 행씩 연결합니다.

그림을 보며 4단계 연습

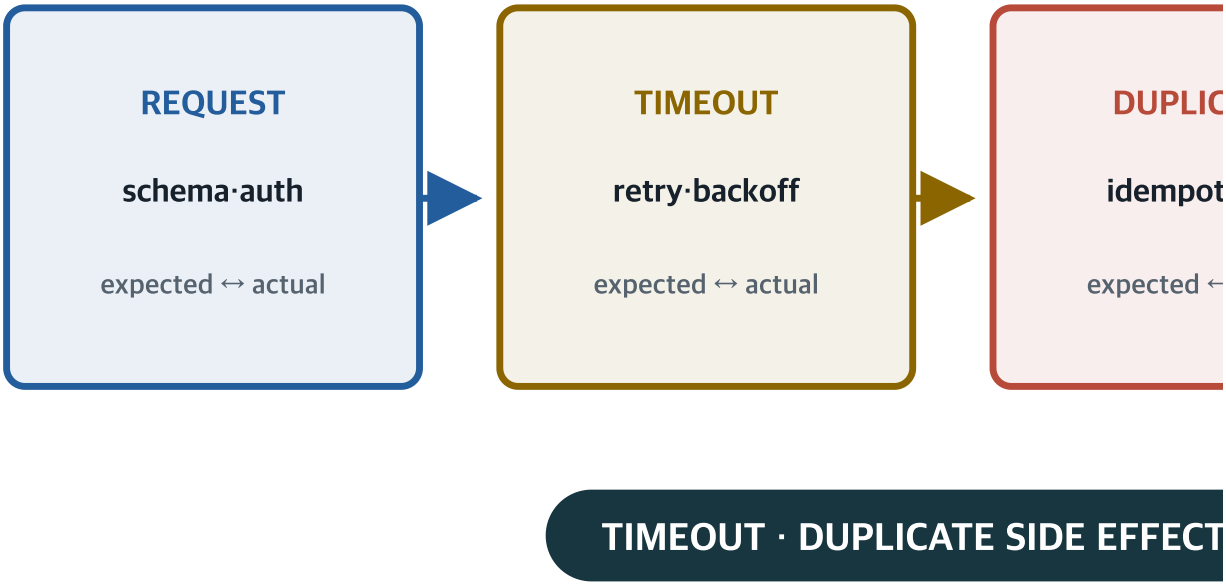
1. 후보 source의 scope를 확인합니다.
2. 중복 outcome과 고유 requirement를 구분합니다.
3. Control·owner·test·evidence를 연결합니다.
4. Gap·exception·qualified review를 기록합니다.

15. 연계 조건을 정상 API보다 실패·중복·재처리 감사로 검증하기

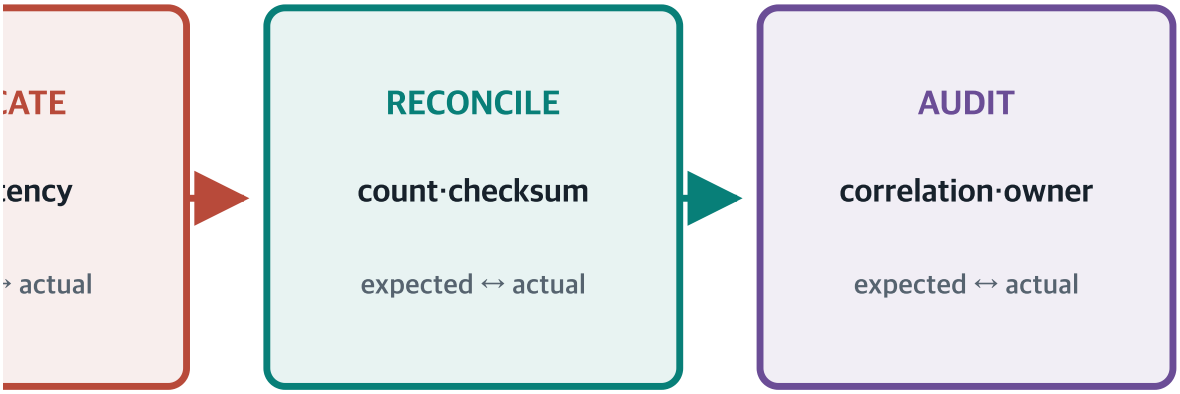
그림 12. Timeout·retry·duplicate·reconciliation·correlation을 주입해 연계 실패를 재현합니다.

통합 설계 실패 패턴

API·batch·event·file contract에 timeout·retry·idempotency·reconciliat



tion·correlation·owner를 넣고 리허설합니다.



0 · RECONCILE 100% · CORRELATE

핵심 원칙: 연계는 happy path 호출 성공이 아니라 실패 뒤 data와 책임이 일치하는 능력입니다.

API·batch·event·file은 응답 유실·중복·순서 변경·schema version 차이로 업무 side effect를 만들 수 있습니다. Contract에 auth·timeout·retry·idempotency·reconciliation·correlation·deprecation·exit를 함께 둡니다.

관점	합성 사례	확인할 evidence
Contract	schema·auth·version	provider/consumer
Timeout	deadline·state	retry rule
Duplicate	idempotency	side effect0
Reconcile	record·total·status	100% account
Audit	correlation·owner	incident evidence

흔한 오답: API documentation과 성공 response screenshot만 제출합니다.

고친 예: Timeout·duplicate·reject·late event를 주입하고 expected state·retry·reconcile·audit·owner ack를 검증합니다.

그림을 보며 4단계 연습

1. 네 interface와 owner를 inventory합니다.
2. Schema·auth·timeout·version을 씁니다.
3. 실패 세 가지를 주입합니다.
4. Reconcile·correlation·exit evidence를 닫습니다.

16. 가용성 문구를 측정·복구·지원·변경 rehearsal로 바꾸기

그림 13. SLI·SLO→incident→backup/restore→DR→support/change를 하나의 rehearsal로 묶습니다.

SLI/SLO·incident·backup/restore·RTO/RPO·DR/BCP·support·release/r

01

SLI·SLO

measure·target

error budget

business impact

02

INCIDENT

severity·response

escalate·communicate

post review

DETECT → ESCALATE → RESTOR

ollback을 한 service model로 묶습니다.

03

BACKUP·DR

restore drill
RTO 4h·RPO 1h
workaround

04

SUPPORT·CHANGE

response 30m
maintenance
release·rollback

E → COMMUNICATE → IMPROVE

핵심 원칙: 가용성 숫자는 측정 source·error budget·복구·소통·owner가 있을 때 운영 조건이 됩니다.

99.9%라는 숫자만으로는 측정 구간·제외·support 시간·RTO/RPO·rollback을 알 수 없습니다. 합성 사례는 p95 800ms, RTO 4h, RPO 1h, first response 30m를 실제 보장이 아닌 학습 threshold로 rehearsal합니다.

관점	합성 사례	확인할 evidence
SLI/SLO	latency·error·availability	window·source
Incident	severity·escalation	communication
Backup/DR	restore·RTO/RPO	drill evidence
Support	tier·response·handoff	receiving operator
Change	release·rollback	post review

흔한 오답: 공급자 SLA 문구를 복사하고 실제 monitoring·restore·support 경로는 확인하지 않습니다.

고친 예: 사용자 outcome별 SLI·target·window·owner를 쓰고 failure를 탐지·escalate·restore·communicate·improve합니다.

그림을 보며 4단계 연습

1. 핵심 user outcome의 SLI를 정합니다.
2. SLO·error budget·severity를 씁니다.
3. Backup·restore·DR·support를 rehearsal합니다.
4. Change·rollback·post-review evidence를 남깁니다.

17. 도입을 한 번의 launch가 아닌 wave·예외·종료 결정으로 설계하기

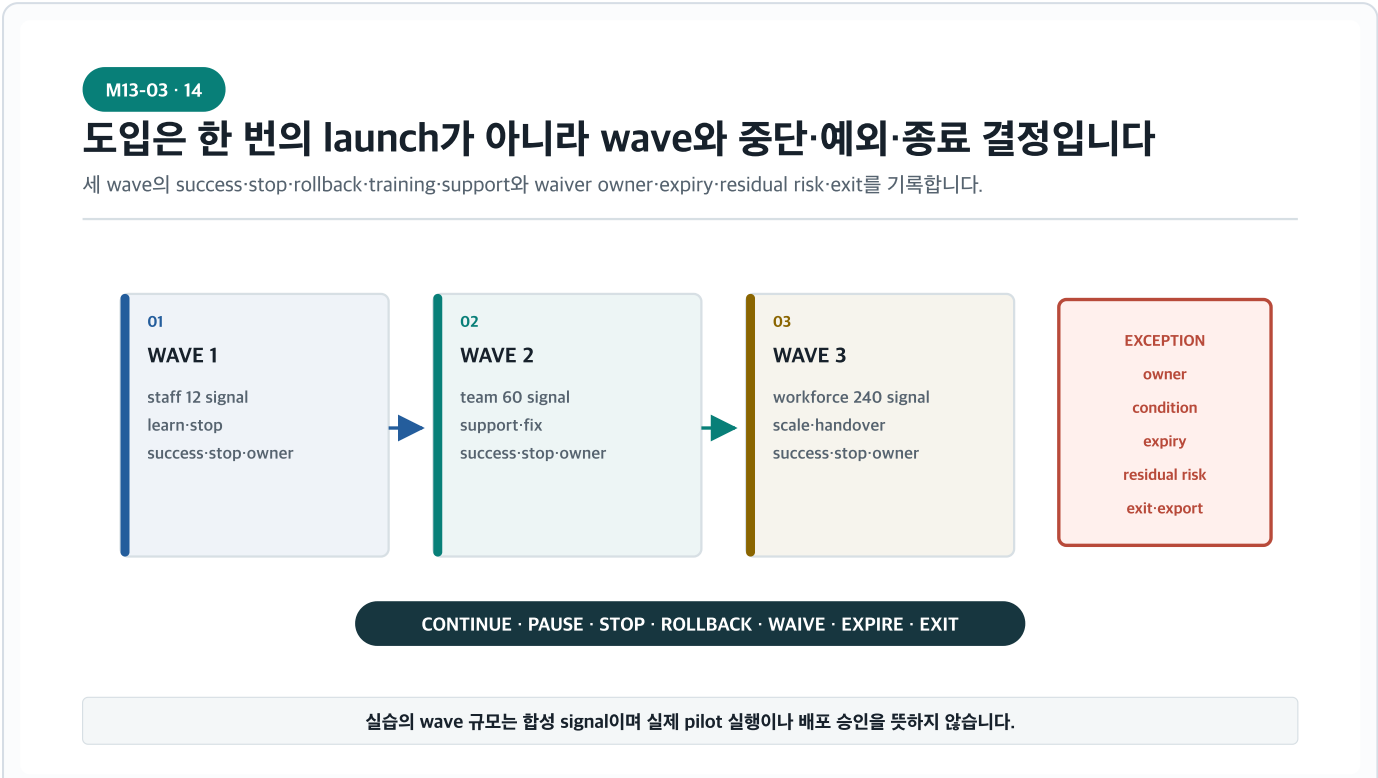


그림 14. Wave마다 success·stop·rollback을 판정하고 예외의 만료와 exit를 함께 rehearsal합니다.

세 wave의 success·stop·rollback·training·support와 waiver owner·exp

01

WAVE 1

staff 12 signal

learn·stop

success·stop·owner

02

WAVE 2

team 60 signal

support·fix

success·stop·owner

CONTINUE · PAUSE · STOP · ROL

iry·residual risk·exit를 기록합니다.

03

WAVE 3

workforce 240 signal

scale·handover

success·stop·owner

EXCEPTION

owner

condition

expiry

residual risk

exit·export

LBACK · WAIVE · EXPIRE · EXIT

핵심 원칙: Pilot과 rollout은 규모를 키우는 일정이 아니라 학습 evidence로 계속·중지·되돌림을 결정하는 과정입니다.

교육·support·accessibility feedback·incident·adoption을 보지 않고 전체 launch하면 사용 장벽과 운영 부하가 한꺼번에 커집니다. 예외는 owner·risk·compensating control·expiry가 있어야 하며 종료 때 data export와 계정 폐기도 검증합니다.

관점	합성 사례	확인할 evidence
Wave1	대표 12명 signal	learn·stop
Wave2	60명 signal	support·fix
Wave3	240명 signal	scale·handoff
Exception	owner·risk·expiry	review·close
Exit	export·revoke·decommission	receiving proof

흔한 오답: pilot 시작일과 전체 배포일만 적고 중지 기준·접근성 feedback·rollback owner를 비웁니다.

고친 예: Wave별 entry·success·stop·support·training·accessibility·rollback·exit evidence와 decision authority를 씁니다.

그림을 보며 4단계 연습

1. 세 wave의 대상과 가설을 정합니다.
2. Success·stop·rollback metric을 씁니다.
3. 예외 owner·expiry·compensating control을 붙입니다.
4. Export·revoke·handoff를 rehearsal합니다.

18. Organization Readiness Gate를 닫고 M13-04로 넘기기

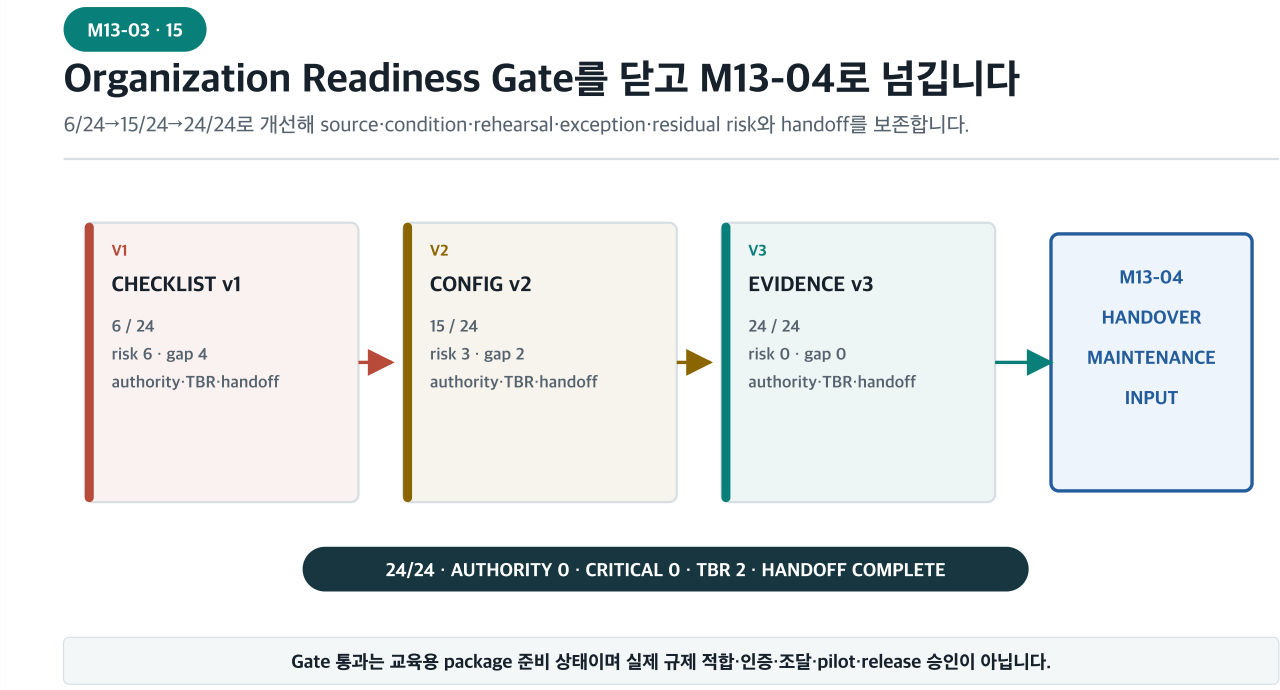


그림 15. 6/24→15/24→24/24로 개선해 authority conflict·critical risk·gap을 0으로 닫습니다.

Organization Readiness Gate로 단

6/24→15/24→24/24로 개선해 source·condition·rehearsal·exception·re

V1

CHECKLIST v1

6 / 24

risk 6 · gap 4

authority·TBR·handoff

V2

CONFIG v2

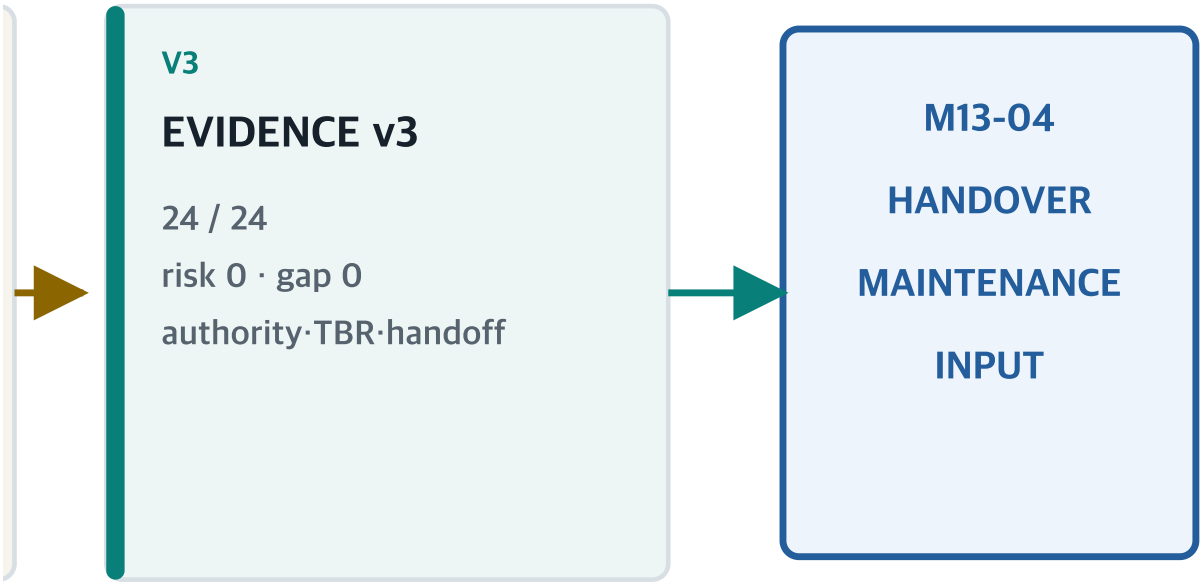
15 / 24

risk 3 · gap 2

authority·TBR·handoff

24/24 · AUTHORITY 0 · CRITICAL

sidual risk와 handoff를 보존합니다.



0 · TBR 2 · HANDOFF COMPLETE

핵심 원칙: Gate는 policy check를 재현된 조직 조건·residual risk·owner·인계 package로 바꿉니다.

최종 합성안은 24 scenario, 12 control, 네 lane 각 6개, 12 coverage domain 100%, authority conflict 0, critical risk 0, critical gap 0, TBR 2와 M13-04 handoff를 요구합니다. Ready는 교육 package 상태일 뿐 실제 승인과 보장이 아닙니다.

관점	합성 사례	확인할 evidence
Checklist v1	6/24	risk6·gap4·TBR8
Configured v2	15/24	risk3·gap2·TBR4
Evidence v3	24/24	risk0·gap0·TBR2
Gate	12 controls·4 lanes	authority0
Handoff	M13-04	maintenance input

흔한 오답: organization_readiness_package_ready이므로 public pilot과 production release를 승인합니다.

고친 예: 교육용 ready 상태·남은 TBR·실제 authority boundary·12 evidence·receiving owner를 함께 M13-04에 넘깁니다.

그림을 보며 4단계 연습

1. 세 variant를 실행합니다.
2. Fixed·regressed·risk·gap·TBR을 비교합니다.
3. 12 coverage와 Gate를 확인합니다.
4. M13-04 owner·maintenance input·authority boundary를 씁니다.

19. 12개 Organization Readiness Control

ID	통제	최소 evidence
CTRL-01	M12·M13 source·scope·authority handoff	Readiness input manifest
CTRL-02	Organization context·stakeholder·RACI	Context and authority map
CTRL-03	Current environment·constraint inventory	Current environment inventory
CTRL-04	Identity·authentication·authorization lifecycle	Identity and access matrix
CTRL-05	Network·device·connectivity boundary	Connectivity and device pack
CTRL-06	Accessibility·usability·user enablement	Accessibility validation pack
CTRL-07	Data classification·residency·lifecycle	Data lifecycle and location map
CTRL-08	Privacy·security·AI governance crosswalk	Assurance applicability crosswalk
CTRL-09	Integration·interoperability·failure contract	Integration contract and rehearsal
CTRL-10	Logging·audit·observability evidence	Audit and observability evidence
CTRL-11	SLO·resilience·DR·support·change	Resilience and service rehearsal
CTRL-12	Pilot·rollout·exception·Organization Readiness Gate	Organization Readiness Gate

20. 24개 합성 시나리오 포트폴리오

ID	Lane	시나리오	위험	Source → Evidence	Controls
SC-01	organization-context-governance	M12·M13 34개 source를 readiness input으로 인수	authority-ambiguity	product architecture vendor package → readiness input manifest	CTRL-01, CTRL-02
SC-02	organization-context-governance	교육 후보와 실제 규제·인증·도입 권한 분리	authority-ambiguity	readiness question → authority boundary	CTRL-01, CTRL-02, CTRL-12

ID	Lane	시나리오	위험	Source → Evidence	Controls
SC-03	organization-context-governance	공공·민간·규제 맥락과 적용 source 식별	authority-ambiguity	organization and service context → applicability register	CTRL-02, CTRL-08
SC-04	organization-context-governance	Stakeholder·RACI·예외 권한과 escalation 정의	authority-ambiguity	stakeholder interviews → authority and RACI map	CTRL-02, CTRL-12
SC-05	organization-context-governance	현행 ID·망·기기·cloud·data·연계·운영 inventory	integration-audit-blindspot	current environment sources → current environment inventory	CTRL-03
SC-06	organization-context-governance	Requirement를 owner·test·evidence·TBR 조건으로 정규화	authority-ambiguity	policy and environment claims → condition register	CTRL-01, CTRL-02, CTRL-03
SC-07	identity-network-accessibility	SSO·MFA·RBAC와 세션·break-glass 조건 검증	access-lifecycle-gap	identity policy and role model → identity access matrix	CTRL-04
SC-08	identity-network-accessibility	Joiner·mover·leaver·SCIM·revocation 리허설	access-lifecycle-gap	synthetic identity events → lifecycle rehearsal evidence	CTRL-04, CTRL-10
SC-09	identity-network-accessibility	Privileged·service account·access review evidence	access-lifecycle-gap	admin and workload identities → privileged access record	CTRL-04, CTRL-10
SC-10	identity-network-accessibility	Proxy·firewall·DNS·TLS·egress·private path 검증	integration-audit-blindspot	connectivity matrix → network path rehearsal	CTRL-05, CTRL-09
SC-11	identity-network-accessibility	Managed device·browser·mobile·remote access 조건	access-lifecycle-gap	device and client inventory → client compatibility record	CTRL-05
SC-12	identity-network-accessibility	Keyboard·focus·reflow·contrast·accessible auth 검증	adoption-exit-lockin	P0 user journeys → accessibility validation pack	CTRL-06
SC-13	data-security-integration	데이터 owner·purpose·분류·처리 위치 map	data-lifecycle-gap	field and flow inventory → data classification map	CTRL-07, CTRL-08
SC-14	data-security-integration	Residency·transfer·subprocessor·export 조건	data-lifecycle-gap	service and supplier topology → location and transfer schedule	CTRL-07, CTRL-08

ID	Lane	시나리오	위험	Source → Evidence	Controls
SC-15	data-security-integration	Retention·deletion·backup residue 리허설	data-lifecycle-gap	synthetic lifecycle event → deletion and residue evidence	CTRL-07, CTRL-10, CTRL-11
SC-16	data-security-integration	Privacy·security·AI source를 control evidence에 crosswalk	authority-ambiguity	applicability register → assurance crosswalk	CTRL-08
SC-17	data-security-integration	API·batch·event schema·auth·version contract	integration-audit-blindspot	integration inventory → versioned integration contract	CTRL-09
SC-18	data-security-integration	Timeout·duplicate·reconciliation·correlation 리허설	integration-audit-blindspot	synthetic integration faults → integration rehearsal evidence	CTRL-09, CTRL-10
SC-19	operations-rollout-handover	Security·privacy·admin·business audit event 정의	integration-audit-blindspot	event and decision inventory → audit event catalog	CTRL-10
SC-20	operations-rollout-handover	SLI·SLO·support severity·incident communication	resilience-support-gap	service objectives and support model → service level evidence	CTRL-10, CTRL-11
SC-21	operations-rollout-handover	Backup·restore·RTO·RPO·DR·BCP rehearsal	resilience-support-gap	synthetic disruption → restore and continuity evidence	CTRL-11
SC-22	operations-rollout-handover	Release·change·rollback·configuration ownership	resilience-support-gap	synthetic change request → change and rollback evidence	CTRL-03, CTRL-11
SC-23	operations-rollout-handover	3-wave pilot·교육·지원·adoption·stop 조건	adoption-exit-lockin	synthetic rollout plan → wave readiness record	CTRL-06, CTRL-12
SC-24	operations-rollout-handover	Exception·expiry·residual risk·exit·M13-04 Gate	adoption-exit-lockin	all readiness evidence → Organization Readiness Gate	CTRL-01, CTRL-12

네 lane은 각각 6개 scenario를 가집니다: `organization-context-governance`, `identity-network-accessibility`, `data-security-integration`, `operations-rollout-handover`.

21. 4개 합성 조직 Profile 한눈표

ID	Profile	형태	강점	위험	상태
ORG-A	대국민 서비스형	외부 사용자·민원 흐름·접근성·감사 중심	공개 서비스와 사용자 다양성 조건이 선명함	identity federation과 내부 업무 조건이 약할 수 있음	reference-profile
ORG-B	기업 workforce형	SSO·SCIM·managed device·내부 연계 중심	계정 lifecycle과 업무 integration 조건이 선명함	대국민 접근성·공공 cloud 적용 범위를 놓칠 수 있음	reference-profile
ORG-C	공공·기업 hybrid형	public edge+enterprise identity+regulated data+audit	두 경계의 trade-off와 handoff를 함께 학습	실제 적용은 기관·업무·데이터별 전문가 확인 필요	synthetic-learning-candidate
ORG-D	소규모 baseline형	작은 팀·단순 SaaS·최소 integration	낮은 복잡도와 빠른 학습	성장·규제·공급망·복구 조건이 뒤늦게 드러날 수 있음	deferred-trigger-profile

22. 8개 Adoption Condition 한눈표

ID	속성	Source·stimulus	Environment·artifact	Response measure
COND-01	authority	accountable owner · reviews one proposed condition	versioned applicability register · law·policy·standard·contract source	100% P0 condition has source·owner·authority; 0 implied approval
COND-02	identity lifecycle	identity administrator · joins, moves, disables and revokes a synthetic user	synthetic tenant adapter · SSO·MFA·RBAC·SCIM mapping	4/4 lifecycle steps pass; privileged access reviewed; stale access 0
COND-03	connectivity	network operator · tests approved and blocked paths	synthetic proxy·firewall matrix · DNS·TLS·egress·private route	approved paths 100%; undeclared egress 0; owner for every failure
COND-04	accessibility	keyboard and assistive-technology reviewer · completes the P0 journey	desktop·mobile·zoom·reflow · UI and accessible authentication	keyboard journey pass; focus visible; no critical blocker; human review present
COND-05	data lifecycle	data and privacy owner · traces one record from collect to delete and export	synthetic classified dataset · app·DB·log·backup·integration	100% selected fields traced; unexplained copy 0; backup residue decision present

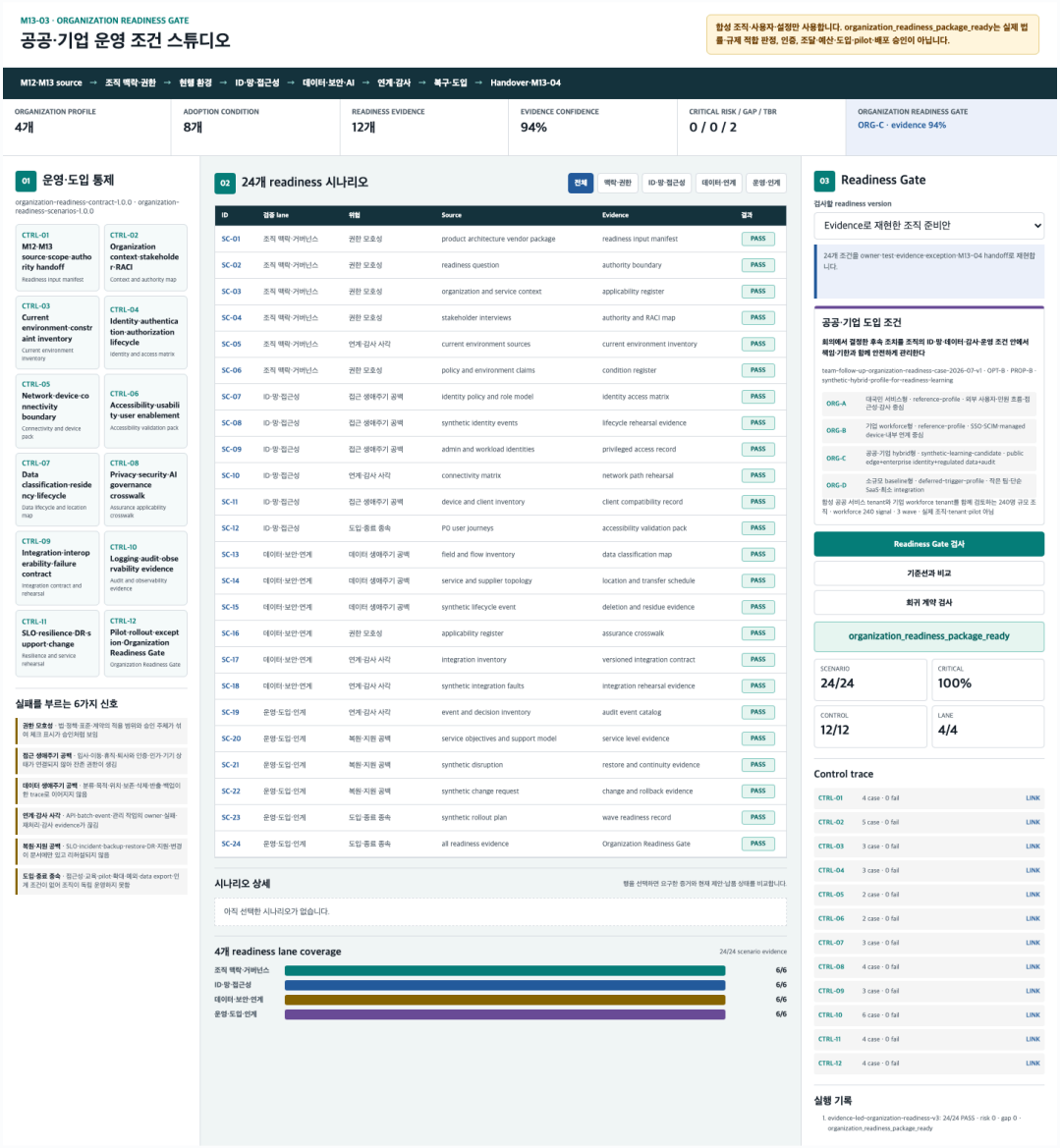
ID	속성	Source·stimulus	Environment·artifact	Response measure
CON D-06	integration and audit	integration operator · injects timeout, duplicate and rejected request	versioned synthetic contract · API·batch·event and audit plane	duplicate side effect 0; reconciliation 100%; correlation present
CON D-07	resilience and support	receiving operator · declares failure and restores service	documented tabletop and restore drill · monitoring·backup·runbook·support	RTO ≤4h; RPO ≤1h; first response ≤30m; rollback proven
CON D-08	rollout and handover	change and adoption owner · runs synthetic wave review and exit rehearsal	three-wave adoption plan · training·support·exception·export·handoff	success·stop owner present; waiver expiry present; export readable; M13-04 linked

23. 12개 Readiness Evidence 검수표

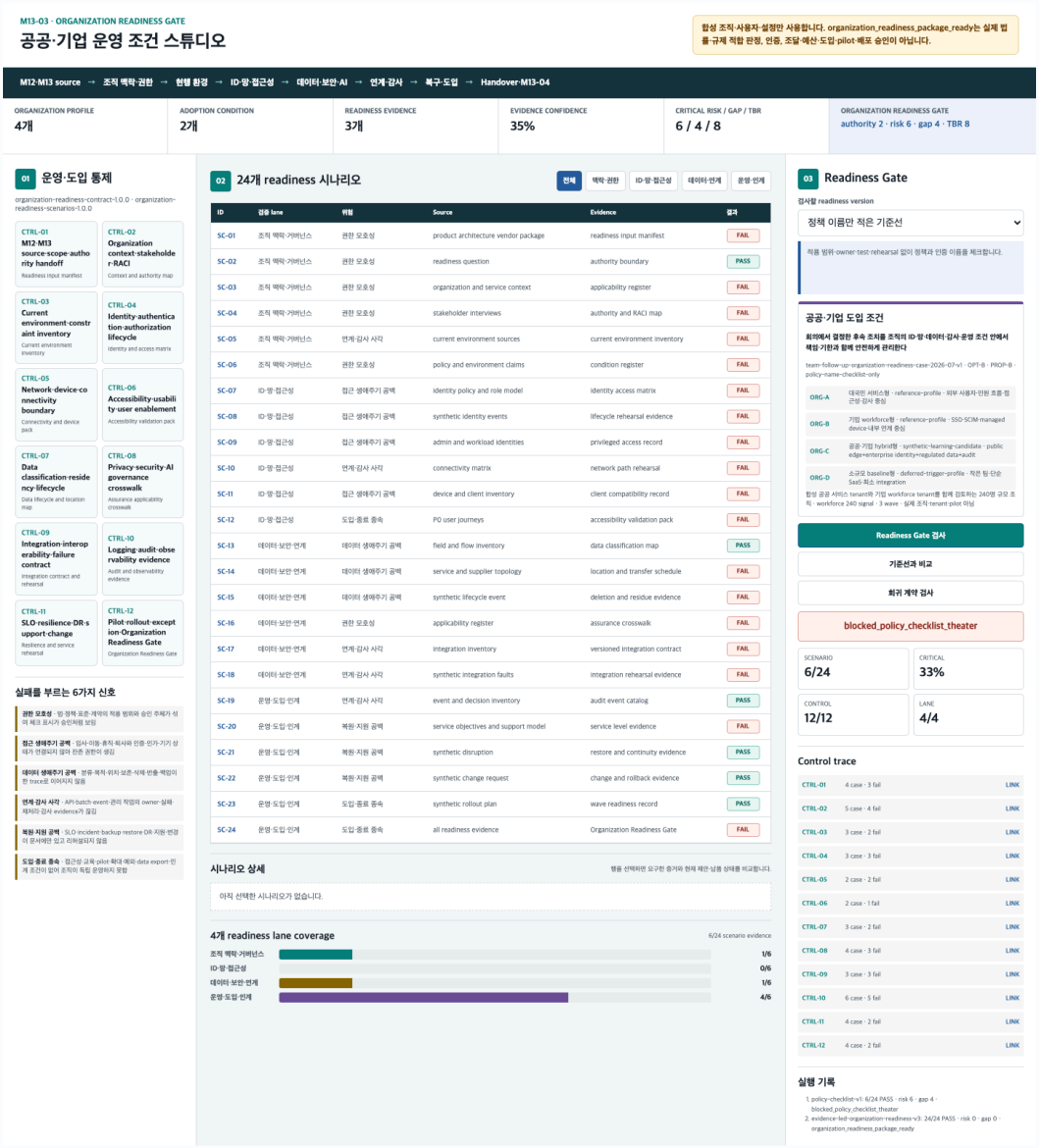
ID	Evidence	최소 proof
EVD-01	Readiness input manifest	M12·M13 version·scope·orphan·conflict·TBR
EVD-02	Context and authority map	applicability·stakeholder·RACI·decision·exception
EVD-03	Current environment inventory	identity·network·device·cloud·data·integration·operations
EVD-04	Identity and access matrix	SSO·MFA·RBAC·SCIM·JML·privileged·revoke rehearsal
EVD-05	Connectivity and device pack	DNS·proxy·firewall·TLS·egress·browser·mobile·failure
EVD-06	Accessibility validation pack	target·keyboard·focus·reflow·contrast·screen reader·user test
EVD-07	Data lifecycle and location map	purpose·classification·residency·transfer·retention·deletion·export
EVD-08	Assurance applicability crosswalk	source·scope·control·owner·test·evidence·exception
EVD-09	Integration contract and rehearsal	schema·auth·timeout·retry·reconcile·version·exit
EVD-10	Audit and observability evidence	event·correlation·retention·access·alert·review·redaction
EVD-11	Resilience and service rehearsal	SLI·SLO·incident·restore·DR·support·change·rollback
EVD-12	Rollout exception and handoff record	wave·success·stop·training·waiver·expiry·exit·M13-04

24. 실습 스튜디오: 세 readiness version 실행

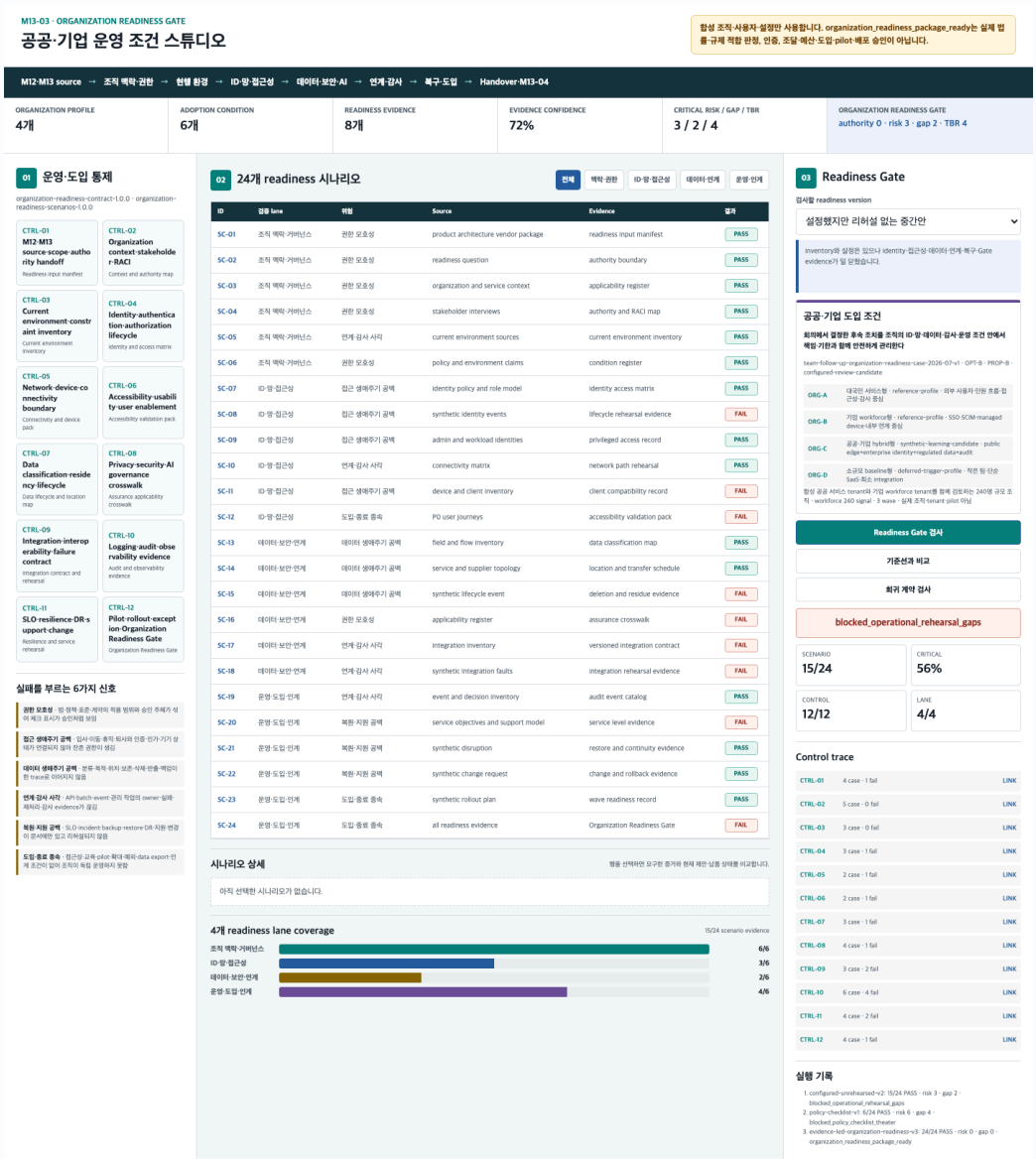
실습은 loopback-only·standard-library-only이며 실제 기관·회사·개인정보·identity tenant·정책 원문·cloud·외부 network·production resource를 사용하지 않습니다. 같은 24 scenario에서 policy check, configured state, rehearsed evidence의 expected/actual 차이를 비교합니다.



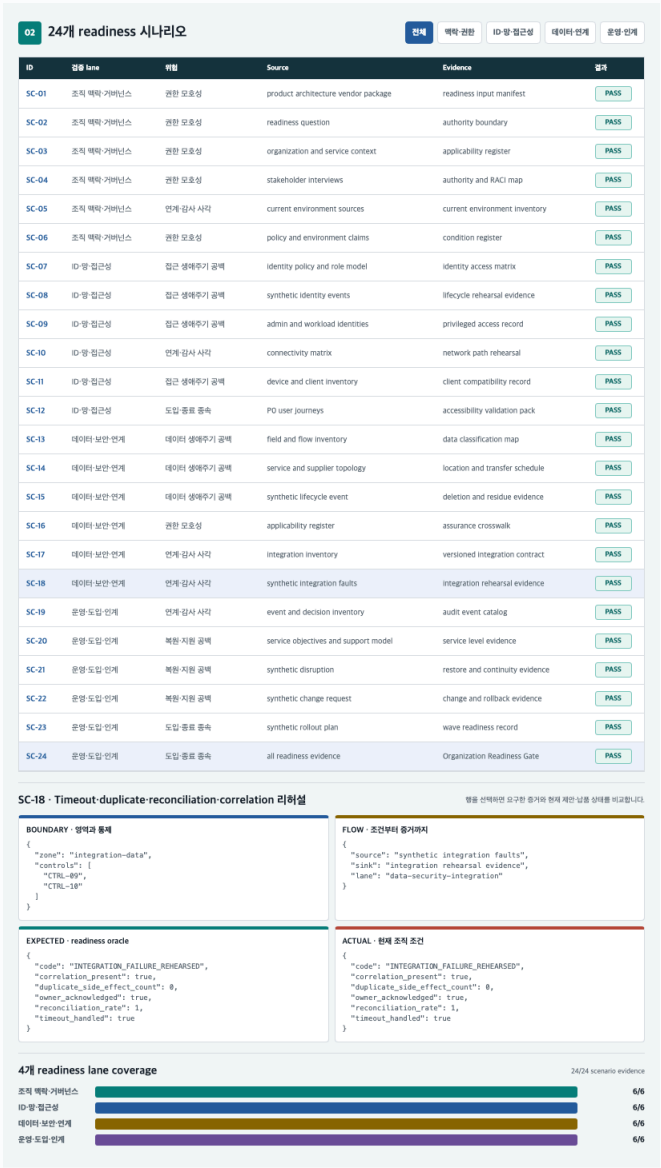
실습 화면 1. Candidate는 24/24, critical 100%, 8 conditions, 12 evidence, authority0·risk0·gap0·TBR2를 표시합니다.



실습 화면 2. Baseline은 6/24, condition2·evidence3·confidence35%로 checklist theater의 공백을 드러냅니다.



실습 화면 3. 중간안은 15/24이며 identity·접근성·data·integration·restore·Gate evidence가 덜 닫혔습니다.



실습 화면 4. SC-18에서 timeout·duplicate·reconciliation·correlation의 expected와 actual을 나란히 봅니다.

실습 화면 5. 모바일에서도 authority boundary와 profile·condition·evidence·risk/gap/TBR가 먼저 보입니다.

실습 화면 6. 좁은 화면에서도 네 lane과 24 scenario를 순서대로 검토합니다.

Version	Pass	Fail	주요 상태	판정
policy-checklist-v1	6	18	condition2·evidence3·confidence35%·risk6·gap4·TBR8	blocked_policy_checklist_theater
configured-unrehearsed-v2	15	9	condition6·evidence8·confidence72%·risk3·gap2·TBR4	blocked_operational_rehearsal_gaps
evidence-led-organization-readiness-v3	24	0	condition8·evidence12·confidence94%·risk0·gap0·TBR2	organization_readiness_package_ready

25. 90분 실습 워크북

시간	행동	남길 evidence	통과 질문
0~10분	Source·profile·authority boundary	input manifest	실제 승인과 학습 준비를 구분했나
10~20분	Applicability·stakeholder·RACI	source register·authority map	범위·효력일·owner가 있나
20~30분	Current environment inventory	identity/network/data/ops map	현재 사실과 TBR이 갈렸나
30~40분	Identity·access lifecycle	access matrix·revoke record	권한이 생기고 사라지는가
40~50분	Network·device·accessibility	path matrix·journey test	허용·차단·사용 완료가 재현되나
50~60분	Data·privacy·security·AI	lifecycle·crosswalk	모든 copy와 적용 범위가 보이나
60~70분	Integration·audit	contract·failure rehearsal	중복0·reconcile100%·correlation인가
70~80분	SLO·restore·support·change	resilience rehearsal	탐지·복구·소통·rollback이 되나
80~90분	Rollout·exception·Gate·M13-04	wave decision·handoff	멈춤·만료·exit·receiving owner가 있나

```
Source IDs·versions + applicability + effective dates:
Organization profile + service/data/user boundary:
Stakeholder RACI + exception/release authority:
Current identity/network/device/cloud/data/integration/ops inventory:
Identity lifecycle + network paths + accessibility journey:
Data location/lifecycle + privacy/security/AI crosswalk:
Integration failure + audit/observability evidence:
SLI/SLO + incident + restore/DR + support/change rehearsal:
Rollout waves + adoption + stop/rollback + exception/expiry/exit:
Gate result + residual risk + TBR + M13-04 handoff + authority boundary:
```

26. Organization Readiness Package 템플릿

별도 템플릿 `03_Templates/T13-03_organization-readiness-package.md`를 사용합니다. 15개 section은 metadata/authority·source/context/applicability·stakeholder/RACI·current environment·identity/access·network/device·accessibility·data lifecycle/location·privacy/security/AI·integration·audit/observability·SLO/resilience/support/change·pilot/rollout/adoption·exception/exit·Gate/M13-04입니다.

27. 셀프 테스트 30

1. 공공·기업 운영 조건을 기능 요구와 따로 정의해야 하는 이유는 무엇인가요?

정답 보기
정답: 같은 기능도 조직의 권한·ID·망·기기·접근성·데이터·감사·복구·지원 조건에 따라 도입 가능성과 검증 evidence가 달라지기 때문입니다.

2. organization_readiness_package_ready가 뜻하지 않는 것을 세 가지 쓰세요.

정답 보기
정답: 실제 법률·규제 적합 판정, 인증·cloud eligibility, 조달·예산·production acceptance·public pilot·release 승인을 뜻하지 않습니다.

3. 합성 사례가 이전 장에서 인수한 source는 몇 개인가요?

정답 보기
정답: M12-04·M13-01·M13-02에서 이어진 34개 linked artifact이며 orphan과 conflict는 각각 0입니다.

4. 네 조직 profile은 무엇이며 왜 하나만 정답이 아닌가요?

정답 보기
정답: ORG-A 대국민 서비스형, ORG-B 기업 workforce형, ORG-C 공공·기업 hybrid형, ORG-D 소규모 baseline형입니다. 적용 조건은 기관·업무·데이터·사용자·기술 경계에 따라 달라집니다.

5. 적용 가능성 register에 최소 무엇을 기록하나요?

정답 보기
정답: 공식 source, 적용 후보 이유, 조직·서비스·데이터 범위, 효력일, 적용·비적용·TBR 판정, 근거, 해석·승인 owner를 기록합니다.

6. 법령이나 인증 이름을 체크하면 왜 readiness가 되지 않나요?

정답 보기

정답: 적용 범위·owner·test·evidence·예외·효력일을 연결하지 않으면 서비스가 실제 조건을 충족하는지 재검토하거나 운영할 수 없기 때문입니다.

7. RACI에서 accountable owner를 한 명으로 명확히 하는 이유는 무엇인가요?

정답 보기

정답: 결정과 결과의 최종 설명 책임이 분산되거나 서로 미뤄지는 것을 막기 위해서입니다.

8. authority conflict의 예를 하나 드세요.

정답 보기

정답: 보안팀과 서비스 owner가 같은 예외의 최종 승인자로 기록되었지만 조직 규정상 실제 권한은 별도 risk committee에 있는 경우입니다.

9. 현행 환경 inventory가 목표 architecture만큼 중요한 이유는 무엇인가요?

정답 보기

정답: 실제 IdP·proxy·browser·기기·data location·integration·support 제약을 모르면 설계가 배포 환경과 연결되지 않고 숨은 TBR이 생깁니다.

10. inventory item에 owner·version·constraint·answered/TBR을 붙이는 이유는 무엇인가요?

정답 보기

정답: 현재 사실과 추측을 구분하고 변경 책임·최신성·미결정을 추적하기 위해서입니다.

11. 인증과 인가의 차이는 무엇인가요?

정답 보기
정답: 인증은 subject가 누구인지 확인하는 과정이고, 인가는 인증된 subject가 어떤 resource와 action에 접근할 수 있는지 결정하는 과정입니다.

12. Joiner·mover·leaver rehearsal의 합격 신호를 쓰세요.

정답 보기
정답: 계정 생성·역할 변경·퇴사 차단·권한 회수가 모두 통과하고, stale access 0이며 고권한 접근 review evidence가 남아야 합니다.

13. Break-glass account에 필요한 운영 조건은 무엇인가요?

정답 보기
정답: 제한된 발급·보관·사용 사유·강한 인증·즉시 alert·사후 review·credential rotation·만료와 owner가 필요합니다.

14. 망 조건을 주소 목록이 아니라 end-to-end 경로로 써야 하는 이유는 무엇인가요?

정답 보기
정답: 사용자 기기부터 identity·network·service·operations까지 DNS·proxy·firewall·TLS·egress·실패 owner가 이어져야 실제 허용·차단을 재현할 수 있기 때문입니다.

15. Zero Trust가 단순 VPN 제품명이 아닌 이유는 무엇인가요?

정답 보기
정답: network 위치를 자동 신뢰하지 않고 subject·device·resource·context를 계속 확인해 최소 권한을 적용하는 architecture 원칙이기 때문입니다.

16. 접근성 자동 검사만으로 충분하지 않은 이유는 무엇인가요?

정답 보기

정답: keyboard journey·focus order·screen reader 의미·오류 회복·실제 사용자 task처럼 자동 도구가 판정하기 어려운 품질이 있기 때문입니다.

17. WCAG/KWCAG 이름을 적는 것과 conformance 판정의 차이는 무엇인가요?

정답 보기

정답: 이름은 후보 기준이고, conformance는 적용 범위·목표 level·page/task sample·자동·수동·사용자 test와 알려진 예외를 evidence로 판정합니다.

18. 데이터 위치 map에 원본 DB 외에 무엇을 포함해야 하나요?

정답 보기

정답: log·cache·search index·integration copy·analytics·backup·export와 subprocessor 위치까지 포함해야 합니다.

19. Retention과 deletion을 함께 rehearsal해야 하는 이유는 무엇인가요?

정답 보기

정답: 업무 DB에서 지워져도 log·backup·export·연계 시스템에 잔존할 수 있어 목적·기간·예외·복구 copy의 종료를 함께 확인해야 합니다.

20. 인증서 보유가 이 서비스의 적합성을 자동 보장하지 않는 이유는 무엇인가요?

정답 보기

정답: 인증의 조직·service·location·control 범위와 현재 구성·데이터·운영 조건이 다를 수 있으므로 applicability와 service evidence를 별도로 확인해야 합니다.

21. Privacy·security·AI crosswalk의 공통 열을 쓰세요.

정답 보기

정답: Source·scope·control·owner·test·evidence·exception·version·effective date입니다.

22. Integration contract에 timeout·retry·idempotency가 함께 필요한 이유는 무엇인가요?

정답 보기

정답: 응답이 불확실한 실패에서 재시도가 중복 side effect를 만들지 않도록 시간 제한·재시도 정책·중복 안전성을 한 contract로 정의해야 합니다.

23. Reconciliation과 correlation ID가 각각 답하는 질문은 무엇인가요?

정답 보기

정답: Reconciliation은 두 시스템의 결과가 결국 일치했는지, correlation ID는 한 업무 흐름의 요청·event·log를 함께 추적할 수 있는지를 답합니다.

24. Audit event에 actor·action·target·time·result가 필요한 이유는 무엇인가요?

정답 보기

정답: 누가 무엇을 어떤 대상에 언제 시도했고 결과가 어땠는지 조사·책임·재현이 가능해야 하기 때문입니다.

25. SLA·SLI·SLO의 차이를 쓰세요.

정답 보기

정답: SLI는 실제 측정값, SLO는 달성할 내부·운영 목표, SLA는 당사자 간 service 수준과 책임을 합의한 문서입니다.

26. RTO와 RPO는 무엇을 재야 하나요?

정답 보기

정답: RTO는 중단 뒤 복구까지 허용 시간, RPO는 복구 시 허용 가능한 data 손실 시점을 재며 실제 restore rehearsal로 확인해야 합니다.

27. 세 wave rollout에서 계속·중지·rollback을 무엇으로 결정하나요?

정답 보기

정답: 각 wave의 entry·success·stop metric, 접근성·사용자 feedback, incident·support load, training 완료, rollback owner와 evidence로 결정합니다.

28. 예외 기록에 반드시 필요한 다섯 요소를 쓰세요.

정답 보기

정답: 예외 범위·이유, residual risk, compensating control, accountable/approval authority, expiry·review·exit 조건입니다.

29. 세 readiness version의 pass 수와 판정을 쓰세요.

정답 보기

정답: policy-checklist-v1은 6/24·blocked_policy_checklist_theater, configured-unrehearsed-v2는 15/24·blocked_operational_rehearsal_gaps, evidence-led-organization-readiness-v3는 24/24·organization_readiness_package_ready입니다.

30. Organization Readiness Gate가 M13-04에 넘기는 핵심은 무엇인가요?

정답 보기

정답: 12개 readiness evidence, owner·authority, identity/network/data/integration/operations 조건, rehearsal 결과, exception·residual risk·TBR, rollout·exit와 유지보수 입력을 넘깁니다.

28. 공식 자료와 적용 경계

아래 자료는 **적용 가능성 확인을 위한 일차 자료**입니다. 목록에 있다는 이유만으로 특정 조직·서비스에 자동 적용되거나 적합·인증·승인되는 것은 아닙니다. 국내 공공 규칙은 각 기관·사업·데이터 범위와 효력일을 다시 확인하고, 실제 법률·개인정보·보안·접근성·AI·cloud·조달 판단은 조직 policy와 자격 있는 전문가가 수행해야 합니다. 확인 기준일은 2026-07-16입니다.

공식 자료	이 장에서 확인할 원리	현재판·적용 경계
개인정보의 안전성 확보조치 기준	개인정보 처리의 관리·기술·물리적 안전조치	개인정보보호위원회고시 제2026-9호, 2026-07-01 시행; 처리자·업무 scope 확인
행정기관 및 공공기관 정보시스템 구축·운영 지침	공공 정보시스템 구축·운영 조건	2025-01-02 시행판; 적용 기관·사업과 최신 개정 재확인
행정·공공기관 cloud 이용 기준 및 안전성 확보 고시	공공 cloud 이용의 적용·안전성 판단 입력	2025-12-29 시행판; 자동 cloud eligibility 결정 아님
KISA 2025 CSAP 안내서	cloud service 보안인증 제도·범위 확인	인증 범위와 기관 이용 승인·service 적합성은 별도
KISA ISMS-P 자료실	정보보호·개인정보보호 관리체계 control language	2023.11 안내서 표시; 최신 공지·심사 범위 재확인
지능정보화 기본법	지능정보사회·공공 정보화의 법적 맥락	2026-01-02 시행판; 해당 조문·기관 범위 전문가 확인
인공지능 발전과 신뢰 기반 조성 등에 관한 기본법	AI 사용의 적용 범위·투명성·책임 후보	2026-01-22 시행; 실제 AI 범주·의무 법률 검토 필요
개인정보 보호법 시행령	개인정보 처리·권리·안전조치의 시행 조건	current text와 해당 조문·효력일 재확인
전자정부법 시행령	공공 정보시스템 감리·운영 맥락	기관·사업·규모별 적용 여부 별도 판단
클라우드컴퓨팅법 시행령	cloud service와 이용·보호의 법적 맥락	2026-01-02 시행판; 공공 이용 승인과 동일하지 않음
모바일 전자정부서비스 관리 지침	공공 mobile service의 관리 조건 후보	2026-05-12 시행; mobile service 적용 범위 확인
한국 웹 접근성 관련 공식 자료	국내 웹 접근성 기준·시험 자료 확인	적용 법령·표준·대상·level과 최신판을 별도 확인
NIST CSF 2.0	Govern·Identify·Protect·Detect·Respond·Recover 위험 관리	자발적 framework; certification이나 법적 적합 판정 아님

공식 자료	이 장에서 확인할 원리	현재판·적용 경계
NIST SP 800-53 Release 5.2.0	조직·시스템 보안·privacy control catalog	2025 release 5.2.0; 조직 context에 tailoring 필요
NIST SP 800-207 Zero Trust Architecture	위치 자동 신뢰 없이 subject·device·resource 접근 검증	architecture guidance; 특정 제품·배포 승인 아님
NIST AI RMF	AI 위험의 Govern·Map·Measure·Manage	AI RMF 1.0은 revision 진행 중; current page 재확인
NIST AI 600-1 GenAI Profile	생성형 AI 고유 위험과 action profile	AI RMF 보완 profile; 법적 의무·인증 아님
ISO/IEC 27001:2022	정보보호 관리체계 요구사항	인증 scope와 service 실제 구성·control evidence 분리
ISO/IEC 27701:2025	privacy information management system	2025판; 개인정보 법률 의견을 대체하지 않음
ISO/IEC 42001:2023	AI management system 요구사항	AI system·조직 scope와 인증 범위 별도
ISO/IEC 20000-1:2018	service management system 요구사항	2018판이 current이고 2023 confirm; 특정 SLA 보장 아님
ISO 22301:2019	business continuity management system	2019판이 current이나 2026년 revision 개발 중; 최신 상태 재확인
WCAG 2.2	POUR 기반 웹 접근성 success criteria	목표 level·scope·국내 적용과 human test 별도
OpenID Connect Core 1.0	OAuth 2.0 기반 identity federation contract	profile·claim·session·security setting을 조직별 검증
IETF RFC 7644 SCIM	사용자·group provisioning protocol	JML owner·mapping·deprovision evidence 별도
IETF RFC 5424 Syslog	구조화된 event message와 logging vocabulary	전체 audit·retention·privacy 요구를 자동 충족하지 않음

29. 용어집 300 학습 순서

`04_Glossary/GLOSSARY_organization_readiness.md`에는 15개 묶음·300개 unique term이 있습니다.

묶음	핵심 질문
01~03	조직 맥락·authority·current environment를 설명하는가

묶음	핵심 질문
04~07	Identity·access·network·accessibility journey를 재현하는가
08~10	Data·privacy·security·AI scope와 lifecycle을 구분하는가
11~13	Integration·audit·SLO·resilience를 evidence로 연결하는가
14~15	Support·rollout·exception·exit·Gate·M13-04를 구분하는가

30. 다음 단계 · M13-04 인수인계·유지보수 handoff

M13-04에서는 이 readiness package를 실제 receiving team이 읽고 유지할 수 있는 인수인계서로 바꿉니다. 조건의 이름보다 누가 어떤 runbook과 계정·SLO·dependency·known risk·exception·지원 경로를 이어받고, 어떤 rehearsal로 독립 운영을 증명하는지가 중요합니다.

```
M12-04 product·requirement·document package
→ M13-01 architecture context·quality scenarios·ADR
→ M13-02 vendor·acceptance·delivery evidence
→ M13-03 organization profile·applicability·conditions·rehearsals
→ owner·runbook·SLO·dependency·risk·exception·rollout·exit
→ M13-04 handover and maintenance package
```

Handoff item	M13-03 source	M13-04 use
Authority/context	profile·RACI·applicability	ownership·decision/escalation
Current environment	identity·network·device·cloud inventory	access·configuration baseline
User access	JML·privileged·accessibility	operator/user procedures
Data/assurance	lifecycle·location·crosswalk	retention·deletion·review calendar
Integration/audit	contract·failure rehearsal·events	runbook·diagnosis·reconciliation
Service resilience	SLI/SLO·incident·restore·DR	support·maintenance·drill schedule
Rollout/exit	wave·exception·export·TBR	transition·decommission·receiving proof

마지막 확인: 좋은 운영 조건 자료는 규정 이름을 많이 적은 문서가 아닙니다. 우리 조직의 어떤 경계에서 누가 무엇을 근거로 판단하고, 어떤 실패를 어떻게 재현·복구하며, 무엇을 아직 모르는지 다음 운영자에게 설명할 수 있는 자료입니다.