Third-Party Access Security Top 10: core test checklist

Suite v0.1-review.12. Blank checklist: fill in your own copy. Each case tries the failure on purpose and passes only if the failure is stopped or detected. Results: PASS, FAIL, NOT_RUN (state why) or N/A (state the profile or overlay rule).
Source: https://thirdpartyaccess.org/ | Full case definitions: definitions/ in the repository | Licensed CC BY 4.0. Do not run a test against a system you do not own or operate without the owner's written agreement.

System and version	
Deployment boundary (identity, access service, networks, targets, evidence store)	
Profile (BASE-HUMAN or AGENT-HUMAN-GATED)	
OT overlay applies (yes or no)	
Parameter values used, each with its source (see BASIS.md)	
Tested by	
Test dates	

Item	Case	Applies to	What to try	Passes when	Needs	Result	Evidence / notes
TPA-1 Untraceable vendor operators	TPA-001.02	All	Enroll one eligible person and attempt enrollment using an unverified affiliation, an expired relationship and a shared human login.	Only the verified individual is admitted; shared downstream accounts remain attributable through individual upstream identities.		PASS / FAIL / NOT_RUN / N/A	
TPA-1 Untraceable vendor operators	TPA-008.02	All	Run two concurrent people/runs using a shared downstream account if present.	Individual upstream identities and sessions remain distinguishable; no attribution collapses into the shared account.		PASS / FAIL / NOT_RUN / N/A	
TPA-2 Unmanaged back doors	TPA-002.03	All	Repeat denied operations across the route inventory: browser, native clients, APIs, direct target addresses, alternate ports, tunnels and intermediaries where present.	Every reachable route enforces the same scope; an absent route has configuration and reachability evidence.		PASS / FAIL / NOT_RUN / N/A	
TPA-2 Unmanaged back doors	TPA-002.06	All	Collect discovery evidence independent of the declared inventory (for example flow logs, firewall/NAT rules, remote-access listener scans and the access-service provider's support-access records) and reconcile it with the declared architecture and route inventory.	No unexplained access path or shared-responsibility gap remains; discrepancies block acceptance. A route inventory supported only by the adopter's declaration is NOT_RUN.	independent data sources	PASS / FAIL / NOT_RUN / N/A	
TPA-3 Self-contained approval	TPA-004.03	All	Attempt approval as the requester, an outsider, an enrolled peer from the same supplier, the supplier's line manager and an approver scoped to a different domain; for agents, also as the agent owner. Attempt to change approval membership as the requester.	Only an approver meeting every P07 independence condition can create a valid decision; every other attempt is denied and recorded without changing the authorization. Actor strings are not accepted as proof of identity.		PASS / FAIL / NOT_RUN / N/A	
TPA-3 Self-contained approval	TPA-004.04	All	After approval, change the subject, tenant, target, privilege, operation/arguments or time window.	Changed scope requires a new decision; the original decision cannot authorize the modified request.		PASS / FAIL / NOT_RUN / N/A	
TPA-4 Access that outlives the job	TPA-005.01	All	Attempt an operation before the grant starts, inside the window, exactly at expiry and after expiry using a controlled clock and measured clock error. Request a grant exceeding G_max or the verified relationship end date.	Only the valid window permits a new operation; boundary comparisons match the documented policy. Excess-duration requests cannot create overlong authority.	controlled clock	PASS / FAIL / NOT_RUN / N/A	

Item	Case	Applies to	What to try	Passes when	Needs	Result	Evidence / notes
TPA-4 Access that outlives the job	TPA-005.02	All	Keep a session and an unused approval open across expiry; try new connections, reuse and reattachment.	No new privileged operation is authorized after expiry; enforcement completes within D_expiry.		PASS / FAIL / NOT_RUN / N/A	
TPA-4 Access that outlives the job	TPA-011.05	OT overlay	Allow the emergency window to expire, recover normal service and perform cleanup and independent review.	Emergency grants and credentials expire; review completes by D_review; normal service does not revive old emergency authority.		PASS / FAIL / NOT_RUN / N/A	
TPA-5 Departures you never hear about	TPA-010.02	All	Trigger a role change, contract termination or compromise event. Record when the event occurred, when the authoritative notice reached the responsible organization and when authority stopped; attempt new and existing-session operations. Repeat for a whole supplier relationship, including all affected people and workload identities, and for a seeded departure that the supplier does not report.	Notice arrives within N_notify of the event, and all affected access stops within D_revoke of receipt on every applicable route and enforcement node. An unreported departure loses new grants no later than the next I_attest re-attestation. After a compromise event, the revoked actor has no continued input under any safe-stop provision.		PASS / FAIL / NOT_RUN / N/A	
TPA-5 Departures you never hear about	TPA-001.04	All	Exercise a scheduled access review using a seeded stale entitlement, a changed role and an orphaned sponsor.	The review discovers and removes obsolete access by the agreed deadline; current access remains usable.		PASS / FAIL / NOT_RUN / N/A	
TPA-6 Lateral movement from the maintained asset	TPA-006.05	All	From the approved target, try an unapproved destination, tunnel or secondary privileged connection using harmless canary resources.	Access cannot expand into other targets or security domains through the approved session.		PASS / FAIL / NOT_RUN / N/A	
TPA-6 Lateral movement from the maintained asset	TPA-002.02	All	Try an unassigned target, another customer/security domain, another account and a higher privilege; change resource identifiers in requests.	Every out-of-scope attempt is denied without effects in either domain.		PASS / FAIL / NOT_RUN / N/A	
TPA-7 Phishable sign-in and handed-over passwords	TPA-003.02	All	Try password-only access, a missing factor, replayed authentication material and an unapproved weaker method on every applicable entry point.	No prohibited authentication path grants access or releases target credentials.		PASS / FAIL / NOT_RUN / N/A	
TPA-7 Phishable sign-in and handed-over passwords	TPA-003.05	All	Inspect all client-visible surfaces during successful and failed connections using synthetic target secrets.	No target secret appears in clipboard, downloads, configuration, responses or accessible logs; encrypted, authenticated transport is verified.		PASS / FAIL / NOT_RUN / N/A	
TPA-8 Records that can be lost or rewritten	TPA-009.02	All	Change a test export and attempt to replace its integrity reference; inspect independent storage/key administration.	One unauthorized actor cannot silently rewrite both authoritative evidence and its integrity proof.	independent data sources	PASS / FAIL / NOT_RUN / N/A	
TPA-8 Records that can be lost or rewritten	TPA-009.04	All	Stop the audit capture path and disconnect the log destination before requesting a new privileged operation.	The fault alerts by D_alert; no new privileged action proceeds without the required durable evidence path.	fault injection	PASS / FAIL / NOT_RUN / N/A	
TPA-9 Sessions you cannot stop, or cannot stop safely	TPA-007.04	All	Repeat termination while the client is disconnected or a session/control node is partitioned.	Enforcement meets D_stop at every relevant boundary; a console status alone is insufficient evidence.	fault injection	PASS / FAIL / NOT_RUN / N/A	
TPA-9 Sessions you cannot stop, or cannot stop safely	TPA-005.03	All	Keep an interactive session open and run an approved harmless long operation across grant end and idle-session timeout; after each event, send harmless keystrokes or commands from the external session.	No external input reaches the target after grant end or timeout. Only the completion step named in the safe-stop contract finishes, performed by the named local party or within E_finish without new external input authority. Stopping access is not misreported as undoing work already started.		PASS / FAIL / NOT_RUN / N/A	

Item	Case	Applies to	What to try	Passes when	Needs	Result	Evidence / notes
TPA-9 Sessions you cannot stop, or cannot stop safely	TPA-007.05	OT overlay	Apply termination during a simulated OT maintenance operation with an agreed local operator.	The documented safe-stop/finish-current-operation behavior is observed and recorded; safety controls remain effective.		PASS / FAIL / NOT_RUN / N/A	
TPA-10 AI agents that skip the human	TPA-012.07	AI agents only	Supply a prompt/tool result claiming approval, spoof an actor field and attempt access to the human approver's credential context.	Approval is enforced outside the model and cannot be manufactured by agent-controlled data.		PASS / FAIL / NOT_RUN / N/A	
TPA-10 AI agents that skip the human	TPA-014.04	AI agents only	Provide untrusted content asking for scope expansion, credential disclosure or an unauthorized action; also send the forbidden request directly to enforcement.	The target denies the forbidden action even when the model emits it; model refusal alone is insufficient evidence.		PASS / FAIL / NOT_RUN / N/A	