Vendor and contractor access checklist

Many withdrawal paths run partly on someone else's systems: wallet software, signing infrastructure, instruction servers, operator screens, cloud hosting, outsourced engineering and support. If a third party can reach the path, an attacker who compromises that third party can reach it too. These thirty-one yes / no / unknown questions are about those parties. Answer them from contracts, access lists and logs, not from the vendor's brochure.

– How to use it

1. Have the owner of the vendor relationship, a security engineer and someone who can read the contracts answer together.
2. Answer from evidence: an access list, a contract clause, a log, a test. If you cannot show it, answer "unknown".
3. Do it per vendor for the vendors that touch the path, not once for the whole estate. Start with the one with the deepest access.
4. Repeat when a vendor, a contract or a vendor's access changes.
5. If you cannot change a contract, the questions still tell you what to compensate for with your own controls.

– What this is not

It is not an audit, a certification, a regulatory submission or legal advice. It does not tell you whether your vendor is secure; it tells you what you know and can show about how they reach your path.

01 Inventory and ownership

1.1 Do you have a current list of every third party that can read, queue, alter, approve or sign a withdrawal, directly or through a tool they run?

□ Yes □ No □ Unknown

1.2 Does the list include sub-contractors and "fourth parties" that the vendor relies on for the part that touches your path?

□ Yes □ No □ Unknown

1.3 Is a named person in your organisation responsible for each vendor's security, separate from the person who owns the contract or the budget?

□ Yes □ No □ Unknown

1.4 Is the list reviewed on a schedule, and when a new tool or integration is added to the path?

□ Yes □ No □ Unknown

1.5 Do you know which of these vendors also serve your competitors, and have you thought through what that means for incident handling?

□ Yes □ No □ Unknown

---

02 What their access reaches

2.1 For each vendor, can you state in one sentence what they can reach: the request queue, the signing environment, both, or neither?

□ Yes □ No □ Unknown

2.2 Can vendor staff view, create, change or approve a withdrawal request? Which actions, in which environments?

□ Yes □ No □ Unknown

2.3 Can vendor staff reach production systems, secrets or keys directly, and if so through what route (VPN, bastion, shared account, vendor-held credentials)?

□ Yes □ No □ Unknown

2.4 Is vendor access individual, named and time-limited, or shared, standing and permanent?

□ Yes □ No □ Unknown

2.5 Is vendor access logged in a place the vendor cannot edit, and does someone on your side read it?

□ Yes □ No □ Unknown

2.6 Is multi-factor authentication required for every vendor account that reaches the path, and is it phishing-resistant for the highest-access ones?

□ Yes □ No □ Unknown

---

03 What a compromised vendor could do

3.1 If the vendor's production environment were compromised, what is the worst a withdrawal request could be changed into?

□ Yes □ No □ Unknown

3.2 Does anything on your side check, independently of the vendor, that what was signed equals what you approved?

□ Yes □ No □ Unknown

3.3 Would you notice a change in a request that the vendor's software made before it was broadcast?

□ Yes □ No □ Unknown

3.4 If one vendor employee's workstation were compromised, what could the attacker reach in your path?

□ Yes □ No □ Unknown

3.5 Has anyone tested a vendor-compromise scenario against your path, even on paper, in the last twelve months?

□ Yes □ No □ Unknown

04 Changes the vendor makes

4.1 Are you told in advance about vendor releases or configuration changes that touch the path?

□ Yes □ No □ Unknown

4.2 Can the vendor push a change to software or configuration that runs inside your signing or approval environment without your approval?

□ Yes □ No □ Unknown

4.3 Do you verify what you run (version, hash or signature) against what the vendor says they shipped?

□ Yes □ No □ Unknown

4.4 Is there a freeze or approval process for vendor changes during sensitive periods?

□ Yes □ No □ Unknown

05 Incidents and evidence

5.1 Does the contract set a time limit for the vendor to tell you about a security incident that could touch your path?

□ Yes □ No □ Unknown

5.2 Do you have the right to evidence of the vendor's controls (independent reports, test results, access reviews), and have you ever asked for it?

□ Yes □ No □ Unknown

5.3 Do you have the right to audit or have a third party review the part of the vendor's service that touches your path?

□ Yes □ No □ Unknown

5.4 If the vendor reported an incident tomorrow, do you know who on your side decides whether to stop withdrawals, and how fast?

□ Yes □ No □ Unknown

5.5 Do you hold enough logs yourself to reconstruct what the vendor's service did to a request, without relying on the vendor's own account?

□ Yes □ No □ Unknown

5.6 Are the vendor's own insider-risk controls (background checks, access reviews, separation of duties) described in the contract or in evidence you have seen?

□ Yes □ No □ Unknown

06 Resilience and exit

6.1 If the vendor were unavailable for a day, could you still process an emergency withdrawal, safely and with the same approval rules?

□ Yes □ No □ Unknown

6.2 Is there a written, tested way to move away from the vendor, including your keys, key shares and data?

□ Yes □ No □ Unknown

6.3 Do you know who legally holds the keys, key shares and recovery material, and under which agreement they are returned?

□ Yes □ No □ Unknown

6.4 Does one vendor sit on more than one critical step (for example both request queue and signing), and have you decided that on purpose?

□ Yes □ No □ Unknown

6.5 Can a vendor suspend, throttle or delay your withdrawals without your agreement?

□ Yes □ No □ Unknown

– Reading your answers

- Section 3 matters most. A "no" or "unknown" there means you do not know what a compromised vendor could do to a request.
- An "unknown" counts as a "no" until evidence exists.
- There is no score on purpose.

---

deebug.io — security engineering & assurance · operated by 株式会社eMoment Japan KK

research@deebug.io · security.txt · privacy · LinkedIn