Supplier risk: which suppliers could hurt you most, and how fast could you cut them off?

This quarter, list every supplier that holds admin access, tokens or a copy of your critical data, and make sure you can cut off each one's access within an hour. Then focus on that top tier: read their audit reports instead of sending questionnaires, fix the contract at renewal and plan for a week without them.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.1**	**IT, security, procurement and compliance leads in EU organizations, especially in Germany**

Latest version
sheets.einblick.dev/third-party-risk/

If you only do five things

1. **List the suppliers that can reach your systems or data.** Record each supplier with admin rights, remote access, API or OAuth tokens, or a copy of critical data, with an owner and a contact. Verizon found third-party involvement, including exploited vendor flaws, in 48% of breaches in its 2026 report, up from 30%[1].
2. **Be able to cut any supplier off within an hour.** For each top-tier supplier, write down how to disable its accounts, revoke its tokens and stop its remote access tool, and test it. Attackers used compromised Salesloft Drift tokens to export Salesforce data from 8 to at least 18 August 2025[2].
3. **Ask the top tier for audit reports, not questionnaires.** Request the current SOC 2 Type 2 or BSI C5 report and read its scope, period and exceptions. Type 2 tests whether controls worked over time; Type 1 only checks their design[3].
4. **Add five clauses at each renewal.** Incident notice, vulnerability handling, audit rights, subcontractor rules, and exit with data return. NIS2's implementing rules make cloud providers and MSPs demand all five from their suppliers, where appropriate[4].
5. **Plan for a week without each critical supplier.** Decide how the business keeps running and keep your data exportable. In October 2025, a DynamoDB fault in one AWS region caused 14.5 hours of disruption that spread to EC2 and Lambda[5].

Decide a supplier's tier

1. **Can it act inside your systems?** Admin accounts, an RMM agent, a VPN account or an app with broad API scopes put a supplier in the top tier, whatever the contract is worth. An attacker who compromises an MSP can reach many of its customers' networks and data[6].
2. **Does it hold data you must protect?** Count personal, financial and confidential data, and the secrets hidden in it: the Drift attackers searched stolen Salesforce records for AWS keys, passwords and Snowflake tokens[2].
3. **What stops if it is down for a week?** If a critical process stops, the supplier is top tier even without any access to your systems.
4. **How hard is it to replace?** A supplier you can't swap within weeks needs an exit plan and a tested data export. DORA makes financial entities weigh providers that are not easily substitutable as concentration risk[7].
5. **Record the tier and review it.** One yes answer makes a supplier top tier. Review tiers at least yearly and after significant changes, as ENISA advises[8].

What to ask for and what to sign

- **Read the audit report, not the logo.** Check that it covers your service, is current and tests whether key controls operate, as DORA requires for critical or important functions[9]. Get every later C5 report and run the customer controls it assigns you[3].
- **Ask about the product, not just the company.** CISA and the FBI suggest asking whether SSO and MFA come at no extra cost and whether SaaS security logs are kept for at least six months at no additional charge[10].
- **Incident notice within hours.** Require notice of incidents that put your systems at risk[4] within a fixed time, such as 24 hours, or sooner if your own reporting clock is shorter. The GDPR sets processors no fixed deadline, so the EDPB suggests contracts require early notice[12].
- **Vulnerabilities and audits.** Require vulnerability handling and audits or audit reports[4], and patches within the patching sheet's deadlines.
- **Subcontractors.** Require the same security terms for subcontractors[4] and notice of material changes with a right to object, as DORA requires for critical functions[13].
- **Exit and data return.** Require your data back in an easily accessible format on termination or insolvency, a transition period and incident help at a preset cost[7]. Remove supplier accounts and data flows at exit[8].

Limit what suppliers can reach

- **Give MSP staff named accounts with MFA.** Keep them out of internal admin groups, limit them to the systems the MSP manages and disable them when not in use[14]. No admin credential should serve several customers[6].
- **Allow one remote access tool.** Allowlist the approved RMM tool, block the ports of others and keep log deletion out of its reach[6]. In 2025, ransomware actors exploited unpatched SimpleHelp RMM to compromise a billing software provider's customers[15].
- **Take Global Administrator away from Microsoft partners.** Under **Settings** > **Partner relationships**, remove partner roles you don't need and ask for least-privilege GDAP roles[16]. Review them quarterly.
- **Limit OAuth consent.** In Entra ID, let users consent only to verified publishers' apps for low-impact permissions, and send other requests to the admin consent workflow[17]. Give integrations the narrowest scopes and avoid Salesforce's `full`[2].
- **Watch supplier activity.** Alert on sign-ins by supplier accounts, new app consents and new RMM agents, and keep those logs for 12 months, as the logging sheet recommends.

When a supplier is breached

1. **Cut its access, then rotate.**
   Using your supplier list, disable its accounts and apps, revoke its tokens[2] and isolate its remote access server[15]. Replace keys and secrets tied to it or found in data it held[2].
2. **Hunt in your own logs.**
   Review sign-ins, API calls and queries by its accounts and apps from before the disclosure[2].
3. **Which clocks have started?**
   For personal data it processed for you, the GDPR's 72 hours generally start when it tells you[12]. The EU security laws sheet has the other clocks.

What you can skip

- **Your own 300-question questionnaire.** Send low tiers a one-page form, or take the supplier's completed SIG or CAIQ, which ENISA names as evidence[8].
- **Custom terms with hyperscalers.** Compare their standard terms and audit reports with your clauses and record the gaps. ENISA suggests negotiating jointly[8]; DORA allows pooled audits[9].
- **Mapping every fourth party.** NIS2 and the BSIG address direct suppliers[21]; DORA adds subcontractors behind critical or important functions[13]. Ask the top tier which subcontractors touch your data.
- **A security rating feed before a supplier list.** No outside score tells you who holds admin rights in your tenant.

What changed in 2026

- **Manufacturers must now warn you about exploited flaws.** Since 11 September 2026, the CRA requires makers of software and connected devices, but not of standalone SaaS, to tell impacted users about actively exploited vulnerabilities and severe incidents, also for products already on the market[19]. Give key vendors a monitored security contact.
- **Integration token theft hit another SaaS vendor.** In June 2026, an attacker used a stolen GitHub token to plant code in Klue's integration service and collect customers' Salesforce OAuth tokens[20].
- **The BSI published C5:2026.** Final since March 2026[18], it has 168 criteria instead of 121 and applies to attestations from 1 June 2027[3]. Ask cloud suppliers when their first report is due.

Mistakes that cost the most

- **Assuming outsourcing moves the duty.** The BSI says NIS-2 entities that outsource all IT remain responsible and that contracts alone aren't enough[21]. DORA keeps financial entities fully responsible too[7].
- **Leaving access behind when a contract ends.** CISA and partners note that disabling MSP accounts can be overlooked then[14]. Revoke its tokens too.
- **Tightening consent without cleanup.** New Entra consent settings leave existing grants in place[17]. Revoke the ones you don't need.
- **Letting your MSP hold your only backups.** One breach of its accounts then reaches both. Keep a copy it can't delete.

What this looks like at your size

Small team, no security staff

- Require least privilege and 2-step verification on your IT provider's accounts[11], and get a list of them.
- Remove Global Administrator from Microsoft partners under **Settings** > **Partner relationships**[16].
- Agree how fast your provider reports incidents and ask for regular health reports[11].

Growing, with IT or security staff

- Keep the supplier list with tier, owner, access, data, contacts and contract dates, and review it yearly[8].
- Turn on the Entra admin consent workflow[17] and review app permissions every quarter.
- Write a one-page cut-off runbook per top-tier supplier and rehearse one each quarter.

Enterprise or regulated

- Under DORA, keep the register of information and test exit plans for critical or important functions[7].
- Join pooled audits[9] and include key suppliers in crisis exercises[8].
- Map which top-tier suppliers share a cloud region or subcontractor, and plan for that failure.

Version history

5 Nov 2026, version 1.1 Reviewed for company readers: clarified that low-tier suppliers can send their own completed SIG or CAIQ.

Sources

1. 2026 Data Breach Investigations Report. Verizon, 19 May 2026. verizon.com
2. Widespread data theft targets Salesforce instances via Salesloft Drift. Google Threat Intelligence Group, updated 28 Aug 2025. cloud.google.com
3. Kriterienkatalog C5: FAQ. BSI, checked 4 Nov 2026. bsi.bund.de
4. Implementing Regulation (EU) 2024/2690, Article 1 and Annex points 5.1.4 and 5.2. EUR-Lex, 17 Oct 2024. eur-lex.europa.eu
5. Summary of the Amazon DynamoDB service disruption in the Northern Virginia (US-EAST-1) Region. AWS, Oct 2025. aws.amazon.com
6. Guide to Securing Remote Access Software. CISA, NSA, FBI, MS-ISAC and INCD, 6 Jun 2023. cisa.gov
7. Regulation (EU) 2022/2554 (DORA), Articles 28 to 30. EUR-Lex, 2022. eur-lex.europa.eu
8. NIS2 Technical Implementation Guidance, version 1.0. ENISA, 26 Jun 2025. enisa.europa.eu
9. Delegated Regulation (EU) 2024/1773 (DORA contract policy), Article 8. EUR-Lex, 13 Mar 2024. eur-lex.europa.eu
10. Secure by Demand Guide. CISA and FBI, Aug 2024. cisa.gov
11. Choosing a managed service provider. NCSC (UK), 24 Nov 2025. ncsc.gov.uk
12. Guidelines 9/2022 on personal data breach notification, version 2.0. EDPB, 28 Mar 2023. edpb.europa.eu
13. Delegated Regulation (EU) 2025/532 (DORA subcontracting), Articles 4 to 6. EUR-Lex, 24 Mar 2025. eur-lex.europa.eu
14. Protecting against cyber threats to MSPs and their customers (AA22-131A). CISA, NCSC (UK) and partners, 11 May 2022. cisa.gov
15. Ransomware actors exploit unpatched SimpleHelp RMM (AA25-163A). CISA, 12 Jun 2025. cisa.gov
16. Manage Microsoft-certified solution provider partner relationships. Microsoft Learn, 30 Mar 2026. learn.microsoft.com
17. Configure how users consent to applications. Microsoft Learn, 15 Jun 2025. learn.microsoft.com
18. C5:2026. BSI, checked 4 Nov 2026. bsi.bund.de
19. Regulation (EU) 2024/2847 (Cyber Resilience Act), Articles 14, 69 and 71. EUR-Lex, 2024. eur-lex.europa.eu
20. CrowdStrike investigation summary and security improvements. Klue, 1 Jul 2026. klue.com
21. Fragen und Antworten zu NIS-2. BSI, checked 4 Nov 2026. bsi.bund.de