

Suppliers and dependencies

Templates for procurement, IT and business owners. Start with one important supplier, review their access and agree reporting routes. Verify the details together; a completed worksheet does not grant approval.

Organisation / owner / date: _____

Review area	Details or restricted reference
Supplier and specific service	_____ _____
Internal owner and deputy	_____ _____
Affected business activity Impact of outage or data loss	_____ _____
Data and system access Categories or internal references only	_____ _____
Important subcontractors Where relevant to this service	_____ _____
Fallback and ability to switch What is tested and what is only planned?	_____ _____

Set the review scope

Priority and reason: _____

Required security evidence / scope / reviewed on: _____

Open issues / owner / due date: _____

Base the review on the service, data and possible impact. A certificate alone does not establish that the specific service meets every requirement. Do not record credentials or full customer data in this template.

Review and end supplier access

IT and the business owner review access before it starts, when it changes and at the agreed review date. Explicitly assign responsibility for revocation at contract end.

Supplier / approval owner: _____

Account or system	Purpose and required permissions	Owner and end date
_____ _____	_____ _____	_____ _____
_____ _____	_____ _____	_____ _____
_____ _____	_____ _____	_____ _____

Identity and assignment

Confirm requests through a known contact; unusual urgency does not replace review.

Permissions and protection

Agree named accounts, necessary permissions, suitable MFA and approved remote access with IT. Justify and time-limit exceptions.

Accountability

Assign logging and review responsibilities. Exchange secrets only through approved procedures.

Changes and subcontractors

Review new people, purposes or additional suppliers before granting extra access. Update the affected data and systems.

Contract end and handover

Revoke accounts and tokens, close connections and obtain evidence of agreed data return or deletion. Rotate shared secrets where needed.

Decision / conditions / next review: _____

Revocation completed by / date / evidence: _____

Reporting routes and a joint rehearsal

Agree reachable contacts and responsibilities for an incident at a supplier. Keep these details protected and accessible if normal systems are unavailable.

Contact or arrangement	Verified detail or reference
Internal coordinator and deputy	
Supplier contact and fallback channel	
Reporting triggers and agreed response times	
Next status update and communication route	

What the first report should contain

Observation and time with timezone, affected service, known impact, actions taken and a reachable contact. Label assumptions and follow up missing details. IT coordinates necessary action. Responsible specialists separately assess legal or contractual reporting duties.

Fictional practice case

Your IT provider reports a possible account compromise. Remote support is interrupted; the impact on your systems is still unclear. Who verifies the report through a known channel? Who decides with IT about access and fallback operations? When and how will the next update arrive?

Observed gap / action / owner / due date:

Use and sources

Original Paragamix GmbH templates. Free to use internally, adapt and share with clients; a source link is welcome but not required. Review internally before use. Not a complete supplier assessment or confirmation of compliance.

[NCSC Supply chain security](#) | [BSI Anforderungen an Lieferanten \(DE\)](#)

[Current version](#)