



Critical Supplier Dependency Sheet

What you depend on, and how long you can do without

Version 1.0 · NIS2 · IEC 62443 · AI

A cyber incident does not have to enter your network to stop your operation. **Your firewall works, your backups are good, and your production is down anyway.**

This sheet makes that dependency concrete, per supplier, in hours and in names.

What this sheet is for

One sheet per critical supplier. At the end there is a decision on paper: how long you can do without them, what you are going to do, who carries it and when you review it.

How to fill it in

- **Split out the kind of dependency.** A licence server that stops is not the same as an engineer who cannot come, and they call for different measures.
- **Fill in the tolerable interruption first.** While that field is empty, every fallback is good enough and nothing happens.
- **Do not forget documentation and knowledge.** Those two are almost never counted as supplier risk and are the hardest to solve. You can stock a spare part; you cannot stock knowledge.
- **A fallback that has not been rehearsed is an assumption.** Note when it was last actually done.

Supplier name, and who your contact there is	
Kind of dependency support / licence server / spare parts / data feed / documentation / knowledge	
What you need from them concretely, not "support"	
What stops at your end which process, and after how long	
Tolerable interruption hours or days, and where that number comes from	
Fallback what you do without them, and whether it has been done once	
Decision accept / arrange a fallback / second source / change the contract	
Owner a name, not procurement as a department	
Evidence	

contract, a test of the fallback, or a recorded agreement	
Review date, and what would make you look sooner	

How to fill in the list

- Tick a box when it is genuinely arranged **and** you can show it: a contract, a report, an agreement on paper.
- Not arranged yet? No tick. That is not a failure, that is your starting point.
- Does a line not apply here? Strike it out. It then drops out of your maximum as well.
- Each line shows how many points it is worth. Not every line weighs the same.
- Add up what you have at the end. Below the list you can read what that number means.

NIS2 and national implementation

- | | |
|--|------|
| ☐ This supplier is in the supply chain overview with the other critical parties. (art. 21(2)) | 2 pt |
| ☐ The dependency appears in the risk analysis, not only in the contract. (art. 21) | 2 pt |
| ☐ You tested whether an outage at their end would be reportable at yours. (art. 23) | 2 pt |
| ☐ Agreements on notifying you of an incident on their side are on paper. | 1 pt |
| ☐ Management knows the five suppliers without whom things stop. (art. 20) | 2 pt |

Continuity

- | | |
|--|------|
| ☐ The tolerable interruption comes from an analysis and not from a feeling. (ISO 22301) | 3 pt |
| ☐ The fallback has been genuinely executed at least once, with a date. | 3 pt |
| ☐ There is a scenario for them being out longer than your threshold. | 2 pt |
| ☐ The contact details work even when your own systems are down. | 2 pt |
| ☐ A second source has been considered, even if it costs more. | 1 pt |

Where it touches OT or AI

- | | |
|---|------|
| ☐ Remote access by this supplier runs through a conduit with its own target level. (IEC 62443-3-2) | 2 pt |
| ☐ Their access is per identity, time bound, and traceable afterwards. (IEC 62443-2-4) | 2 pt |
| ☐ If they supply an AI function, it is in your AI inventory. (ISO/IEC 42001) | 1 pt |
| ☐ For a third party model, what happens when they replace it is recorded. | 1 pt |

Generic, what a CISO checks anyway

- | | |
|---|------|
| ☐ The contract names availability and recovery, not only delivery. | 2 pt |
| ☐ The documentation they maintain also sits with you, up to date. | 1 pt |
| ☐ More than one person at your end knows how this system works. | 2 pt |
| ☐ The exit is described: what do you take with you if you stop. | 1 pt |
| ☐ This dependency features in the crisis exercise. | 1 pt |
| ☐ The review date is in somebody's calendar. | 1 pt |

What your result means

Add up your points. Everything together is 34. That puts this supplier here:

0 – 16 po	This supplier can stop you without anyone seeing it coming. Start with the tolerable interruption and the fallback; the rest follows from those.
17 – 26 po	You know what you depend on, but during an incident you would still be working it out. Make sure the fallback has been done once for real and that the contact details work when your own systems are down.
27 – 34 po	This dependency is under control and can be explained to your board, a regulator or your insurer. Put the review date in a calendar; this expires quietly when the supplier changes.

Struck out any lines? Take those off the maximum. The thresholds sit at half and at four fifths of what remains.

Five mistakes this sheet is meant to prevent

- **Supplier risk as one thing.** Six kinds, six measures. Lumped together it produces one generic clause that solves nothing.
- **No tolerable interruption.** Without that number every fallback is good enough and there is no reason to arrange anything.
- **A fallback on paper.** Never executed means unknown, not present.
- **Looking only at the big names.** The party that stops you is often small and supplies one thing you cannot get elsewhere.
- **Filling it in without deciding.** Pick one of the four, with a name and a date next to it.

NIS2 names supply chain security as part of the measures and does not prescribe a method; the directive does not apply to every organisation. ISO 22301 covers business continuity and is not an obligation under NIS2. This sheet is an aid, not a standard. More at cyber-busters.com/en/blog.