Questions for the people who develop your software

The questions below help to assess whether the systems developed and run by a supplier would remain usable in its absence. They require no technical knowledge. Under each one, a short note states what makes a good answer; the space on the right is for writing down the answer received. An incomplete answer is not a judgement on the supplier: it marks a point to be clarified and, where necessary, written into the contract.

Company _____ Supplier _____

System _____ Date of the meeting _____

	QUESTION	SUPPLIER'S ANSWER
1	**Where is the documentation of the system, and when was it last updated?** **A good answer:** a place the company can also access and a recent date; the documentation states where each part of the system is installed, which external services it uses and how it is restored.	
2	**Who holds the access keys, and where are they kept?** **A good answer:** an encrypted store (a vault), the people who have access to it, a list of the keys by name. Files on one person's computer, spreadsheets or email messages are not adequate safekeeping.	
3	**In whose name are the domain, the servers and the accounts of external services registered?** **A good answer:** a list, service by service, with the holder of each one; for services registered to the supplier, how they would be transferred to the company.	
4	**What happens if the supplier is unavailable for a few weeks, or no longer available at all?** **A good answer:** a written procedure, with whom to contact and how soon to expect a reply, and a document with the essential information on each system that can be consulted even when the supplier does not respond.	

QUESTION	SUPPLIER'S ANSWER
5 Who would take over, and has the company approved that person? **A good answer:** a named person with contact details, outside the supplier's organisation, known to and approved by the company, who receives personal, time-limited access rather than the supplier's passwords.	
6 Can the company obtain its emergency keys, and how long would it take? **A good answer:** yes, through a procedure and within a period set out in the contract, in a manner similar to the transfer of a domain; the supplier can suspend the release only for a stated reason.	
7 Can the backups actually be restored, and when was this last tested? **A good answer:** the date and outcome of the last restore test actually carried out, and how often the test is repeated. "We back up every night", on its own, is not an answer.	
8 Who has had access to the systems, and is there a record of it? **A good answer:** a log with people and dates, not a list from memory; when a team member leaves the supplier, their access is revoked and the keys they knew are replaced.	
9 What happens at the end of the contract? **A good answer:** a list of what is handed over (documentation readable without the supplier's software, keys, code, service accounts), with the timing and the form, written into the contract.	

NIS2 directive. Companies within the scope of Directive (EU) 2022/2555 are required, among their risk-management measures, to address supply chain security, including their relationships with direct suppliers (Article 21). The answers to these questions can help with that, but they do not replace the assessments the legislation requires, which should be carried out with the company's own advisers.

Annotated version. Each question is explained more fully, together with how a software house that uses Symbiont answers it, at getsymbiont.com/for-clients.html. This document may be printed and handed on freely.