Acht Fragen vor dem Kauf von Software

Vor der Ausschreibung zu stellen und nicht nach der Übernahme des Anbieters: was das System mit der Information des Hauses tut.

Kategorie: Checkliste. Bezug im Buch: Abschnitt 2.8 (Leitfrage, Tabellen 2, 3, 4 und 5); Norm: Klausel 6.3 sowie Maßnahmen A 5.8, 5.23, 8.26, 8.31, 8.32 und 8.33 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Buches. Rechtsstand des Bandes: 27. September 2026.

Haus / Standort		**Ausgefüllt von**	
System / Vorhaben		**Datum dieses Blattes**	

So nutzen Sie diese Vorlage

1. Legen Sie die acht Fragen der Anforderungsliste bei, bevor ausgeschrieben wird. Jeder Anbieter beantwortet sie; die Antworten werden neben den Funktionen bewertet (2.8, Prinzip).
2. Die Verantwortliche des Informationssicherheitssystems sitzt im Auswahlausschuss. Die Antworten werden im Vertrag zu Pflichten, mit Fristen und Kosten (Direktion).
3. Die Fragen sind dieselben für ein Verwaltungssystem, eine Buchungsplattform für das Spa, ein Reservierungswerkzeug für das Restaurant oder einen Nachrichtendienst für Gäste. Sie zu stellen, dauert einen Nachmittag.

Zeilen mit Sicherheit, Speicherort oder Ausstieg:

Lautet die Antwort null, wurde das System für das ausgewählt, was es tut (2.8, Leitfrage).

1 Die acht Fragen, in ihrer Reihenfolge

Nr.	Frage	Grund (aus dem Band)	Im Buch
1	**Speicherort.** In welchem Land und bei welchem Hostinganbieter werden die Daten des Hauses gespeichert, und darf der Anbieter sie verlegen?	Der Anbieter konnte ohne Nachprüfung nicht sagen, in welchem Land die Daten lagen; jede Verlegung verändert das Risiko, das das Haus trägt.	**Methode** dieses Bandes. Verlangt: Sicherheitsanforderungen bei der Beschaffung ermitteln (A 8.26). Recht: Art. 44 ff. DSGVO (DE, AT); revDSG Art. 16 (CH).
2	**Unterauftragnehmer.** Welche anderen Unternehmen setzt der Anbieter für Hosting und Betreuung ein?	Der Vertrag sagte nicht, welche anderen Unternehmen der Anbieter einsetzte; das System war im Vorjahr zu einem anderen Hostinganbieter gewechselt.	**Methode** dieses Bandes. Recht: Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO); CH: Auftragsbearbeitung (revDSG Art. 9), Unterauftragnehmer nur mit vorgängiger Genehmigung.
3	**Zugriff.** Wer beim Anbieter kann die Daten des Hauses erreichen, und wie werden sie geschützt?	Keine Anforderung beschrieb, wie die Information geschützt würde und wer beim Anbieter sie erreichen könnte.	**Methode** dieses Bandes. Verlangt: Sicherheitsanforderungen bei der Beschaffung (A 8.26).
4	**Vorfälle.** Wie erfährt das Haus von einem Vorfall beim Anbieter?	Keine Anforderung beschrieb, wie das Haus von einem Vorfall erführe.	**Methode** dieses Bandes. Verlangt: Sicherheitsanforderungen bei der Beschaffung (A 8.26).
5	**Nachweise.** Welche Nachweise zur Sicherheit seiner Dienste kann der Anbieter vorlegen?	Anforderungen formen alles, was folgt; Informationssicherheit, die in ihnen fehlt, fehlt in der Auswahl.	**Methode** dieses Bandes. Eine vollständige Sicherheitsprüfung jedes Anbieters ist nicht verlangt.
6	**Export.** Kann das Haus am Ende der Beziehung seine Daten in brauchbarer Form mitnehmen, in welchem Format und zu welchen Kosten?	Der Vertrag sagte nichts zum Export; der Anbieter verlangte achtzehntausend Franken für ein Format, das kein anderes System ohne weitere Arbeit lesen konnte.	**verlangt:** Abläufe für Beschaffung, Nutzung, Verwaltung und Ausstieg aus Clouddiensten (A 5.23). Recht: Data Act seit 12. September 2025 (DE, AT); CH: vertraglich vereinbaren.
7	**Löschung.** Löscht der Anbieter die Kopie des Hauses nach dem Ende der Beziehung und bestätigt er die Löschung?	Der Vertrag verpflichtete ihn nicht, die Daten nach dem Ende der Beziehung zu löschen oder die Löschung zu bestätigen.	**verlangt:** Ausstieg aus Clouddiensten (A 5.23). Recht: Data Act (DE, AT): Abruffrist, dann Löschung, gesetzliche Ausnahmen beachten; CH: vertraglich vereinbaren.
8	**Eigentümerwechsel.** Wie und wie früh informiert der Anbieter das Haus über einen Wechsel des Eigentümers?	Das Haus erfuhr vom Ende des Produkts aus einer fröhlichen E-Mail der Gruppe, die den Anbieter übernommen hatte.	**Methode** dieses Bandes. Das Gesetz sagt nicht, wie früh ein Eigentümerwechsel angekündigt wird; nur der Vertrag sagt es.

Kosten der Fragen: Sie kosten vor der Unterschrift nichts und nach ihr viel. Vor der Unterschrift will der Anbieter den Vertrag, beantwortet sie und stimmt vernünftigen Bedingungen meist zu (2.8).

2 Die Antworten der Anbieter, neben den Funktionen bewertet

Frage	Anbieter 1:	Anbieter 2:	Anbieter 3:	Anbieter 4:	Im Vertrag als Pflicht (Frist, Kosten)
1					☐
2					☐
3					☐
4					☐
5					☐
6					☐
7					☐
8					☐

3 Wohin die Antworten gehören (Tabelle 2)

Stelle	Was dort hingehört	Wer	Erledigt (Datum)
Anforderungsliste	die acht Fragen	Betriebsleitung mit der Verantwortlichen des Systems	
Auswahlausschuss	eine Person, die nach der Information fragt	Verantwortliche des Informationssicherheitssystems	
Vertrag	die Antworten als Pflichten, mit Fristen und Kosten	Direktion	
Umzugsplan	welche Daten umziehen, welche Testdaten, wann das alte System endet	Betriebsleitung mit Integrator	
Erstes Jahr	ein Probeexport	IT	

verlangt: Informationssicherheit im Projektmanagement (A 5.8); geplante Änderung am Informationssicherheitssystem (6.3, A 8.32); Testinformation ausgewählt und geschützt, Testumgebung vom Betrieb getrennt (A 8.31, 8.33). **Methode** dieses Bandes: die Seite mit Fragen, der Probeexport im ersten Jahr; nicht verlangt sind eine förmliche Projektmethodik, eine Sicherheitsfreigabe in jeder Projektphase, eine Cloudstrategie oder eine Plattform für Testdaten.

Was diese Vorlage nicht ist

Dieses Blatt ersetzt weder die Norm noch eine Rechtsberatung, weder die Prüfung eines Vertrags noch das Urteil einer Zertifizierungsstelle. Ein ausgefülltes Blatt ist kein Nachweis: Es hält fest, was gefragt und was geantwortet wurde, und ersetzt nicht den Vertrag, in dem die Antworten Pflichten werden. Die Rechtshinweise geben den Stand des Bandes wieder (Rechtsstand des Bandes: 27. September 2026); verbindlich ist die jeweils gültige Fassung von Gesetz und Norm.