7 Questions Every CFO Should Ask Before Signing the Next Enterprise Software Deal - Practical, expert-driven IT audit and compliance services that add real value.

7 Questions Every CFO Should Ask Before Signing the Next Enterprise Software Deal

Posted by:
William
|
On:
March 31, 2026
|
Guides & Best Practices, Risk Management, Third-Party Vendor Management
audit ready vendor contracts, breach notification requirements SaaS, CFO risk management strategy, CFO software decision checklist, CMMC vendor requirements, data migration costs SaaS, data ownership SaaS contracts, duplicate software risk, enterprise risk management software vendors, enterprise SaaS agreements, enterprise software contracts, enterprise software risk management, enterprise software ROI analysis, GDPR SaaS compliance, governance risk and compliance SaaS, HIPAA SaaS requirements, IT procurement strategy, PCI DSS vendor risk, SaaS audit rights, SaaS compliance risk, SaaS contract best practices 2026, SaaS contract negotiation, SaaS exit strategy, SaaS indemnification clauses, SaaS license optimization, SaaS M&A risk, SaaS performance risk, SaaS pricing increases negotiation, SaaS

pricing negotiation, SaaS renewal risk, SaaS risk assessment, SaaS security due diligence, SaaS total cost of ownership, SaaS usage optimization, service level agreement penalties, shadow IT risk management, SLA negotiation SaaS, SOC 2 vendor evaluation, software contract exit clauses, software contract hidden costs, software contract termination fees, software deal negotiation checklist, software procurement best practices, SOX vendor compliance, subprocessor risk management, subscription management SaaS, technology risk management, third-party risk software vendors, vendor contract risk analysis, vendor control environment assessment, vendor due diligence checklist, vendor liability clauses, vendor lock-in risk, vendor monitoring and oversight, vendor performance SLAs, vendor risk management SaaS

7 Questions Every CFO Should Ask Before Signing the Next Enterprise Software Deal

Enterprise software deals promise efficiency, innovation, and growth. But a poorly vetted contract can lock your organization into hidden costs, compliance gaps, security weaknesses, and limited exit options for years.

CFOs increasingly sit at the center of these decisions—not just for budget approval, but because the financial, operational, and regulatory risks flow straight to the bottom line. Before you sign the next SaaS, cloud, or enterprise agreement, ask these **5 critical questions**.

1. What Are the True Total Cost Implications—Including Price Increases, Exit Fees, and Data Migration?
Many contracts include automatic renewal clauses with 5–10%+ annual increases or significant early termination fees. Ask: What triggers price hikes? How easy (and expensive) is it to exit or migrate data? Factor in potential costs for data extraction, transition support, and retraining.

A strong negotiation point: Cap annual increases and require clear, itemized exit assistance.

Tip: **"Negotiate before you need leverage."** Your strongest position is before signature—not at renewal.

2. Does the Vendor's Control Environment Align with Our Compliance and Risk Requirements?
A SOC 2 logo isn't enough (see our post on SOC 2 red flags). Probe: How do your controls address our specific needs (SOX, HIPAA, PCI, CMMC, GDPR)? What Complementary User Entity Controls (CUECs) will we be responsible for? Can you provide recent evidence of effective operation?

If the vendor pushes back on sharing details or the scope doesn't match the services you're buying, that's a major warning sign.

Tip: **"Assume audits will happen."** Structure terms so you'll be comfortable defending them to auditors later.

3. How Does the Agreement Handle Data Ownership, Breach Notification, and Liability?
Who owns the data you input or generate? What are the vendor's breach notification timelines (aim for under 72 hours)? Are liability caps reasonable, or do they leave your organization exposed to disproportionate risk?

Demand strong indemnity for breaches caused by the vendor's negligence and clear data return/destruction obligations upon termination.

Tip: "If it's not in writing, it doesn't exist." Verbal commitments from sales won't survive procurement or legal review.

4. What Ongoing Due Diligence and Monitoring Rights Do We Have?
Will the vendor allow periodic reviews of their security posture, SOC reports, or sub-processors? How transparent will they be about ownership changes, funding rounds, or M&A activity that could affect service stability?

Build in rights to request updated evidence and audit clauses that support your third-party risk program.

5. How Does This Solution Fit into Our Broader Technology Landscape and Risk Appetite?
Does this new tool create shadow IT risks or duplicate existing capabilities? How will it impact our business continuity and incident response plans? What's the strategic exit strategy if the vendor's direction shifts?

Involve IT audit and compliance early to evaluate integration risks and ensure alignment with your policy framework.

6. What Happens If the Vendor Underperforms?
Most contracts are strong on what *you* owe the vendor—but weak on what happens if they fall short.
Ask:

- Are SLAs tied to meaningful service credits—or just nominal penalties?
- Can we terminate for repeated SLA failures?
- Is there a clear escalation path for chronic issues?

Tip: Tie performance failures to real financial consequences or termination rights—not just "best effort" language.

7. Are We Solving a New Problem—or Duplicating Existing Capabilities?
Before adding another SaaS solution, take a step back and ask, "*Do we already have tools that can meet this need?"* (or *"Is another business department already using the same solution?"*)
Many organizations accumulate overlapping applications across departments—driving up costs, increasing integration complexity, and expanding the risk surface.
Ask:

- Do we already own tools with similar functionality that are underutilized?
- Has IT or procurement validated that this isn't duplicative?
- Will this create new data silos or shadow IT risks?

Tip: Conduct a quick capability and usage review of your current tech stack before approving a new vendor. In many cases, optimizing what you already have delivers faster ROI with less risk.

BONUS: Are We Locked into SaaS Subscriptions That Don't Reflect Actual Usage?
SaaS agreements often look flexible—but many lock you into fixed subscription tiers, user minimums, or auto-renewals that outpace actual needs.
Ask:

- *Can subscriptions **scale down** as easily as they **scale up**?*
- ***Are we locked into minimum user counts** or multi-year commitments?*
- ***How are renewals structured**—and can we adjust quantities before renewal?*

Tip: Negotiate flexible subscription terms, including the ability to right-size licenses at renewal and avoid paying for unused capacity.

Protect Your Organization Before the Ink Dries
Signing a suboptimal enterprise software deal can create years of downstream pain: higher costs, audit findings, insurance complications, and increased breach exposure. The best time to mitigate these risks is before signature—not during the first audit or incident.

At **Ward Tech Audit & Compliance**, we help CFOs, procurement teams, and compliance leaders review enterprise software agreements, evaluate vendor controls, and build robust due diligence processes that protect the organization without slowing the business.

Ready to strengthen your software procurement process? Contact Ward Tech Audit & Compliance for a no-obligation consultation on vendor contract reviews or third-party risk support.
——-

Back to Blogs
Posted by
William
in
Guides & Best Practices, Risk Management, Third-Party Vendor Management