Adopting software in the cloud: Questions for your vendor

IFS

enterprise
Consulting, Inc.

Make an informed choice when considering a move to the cloud

As we take the first steps into the fourth industrial revolution, people's technology concerns tend to now center on robotics, AI, quantum computing and other "fourth era tech." Beginning its rise in the nineties, Software as a Service (SaaS) adoption has become widespread. For many, concerns over adopting enterprise software in the cloud have died down considerably–it's a proven and well-established model (in contrast to AI, for example) they've now fully embraced. But some organizations have concluded the SaaS model isn't suitable for them, others are still mulling the decision over.

This whitepaper is for the latter group. If that's you, read on to learn about:

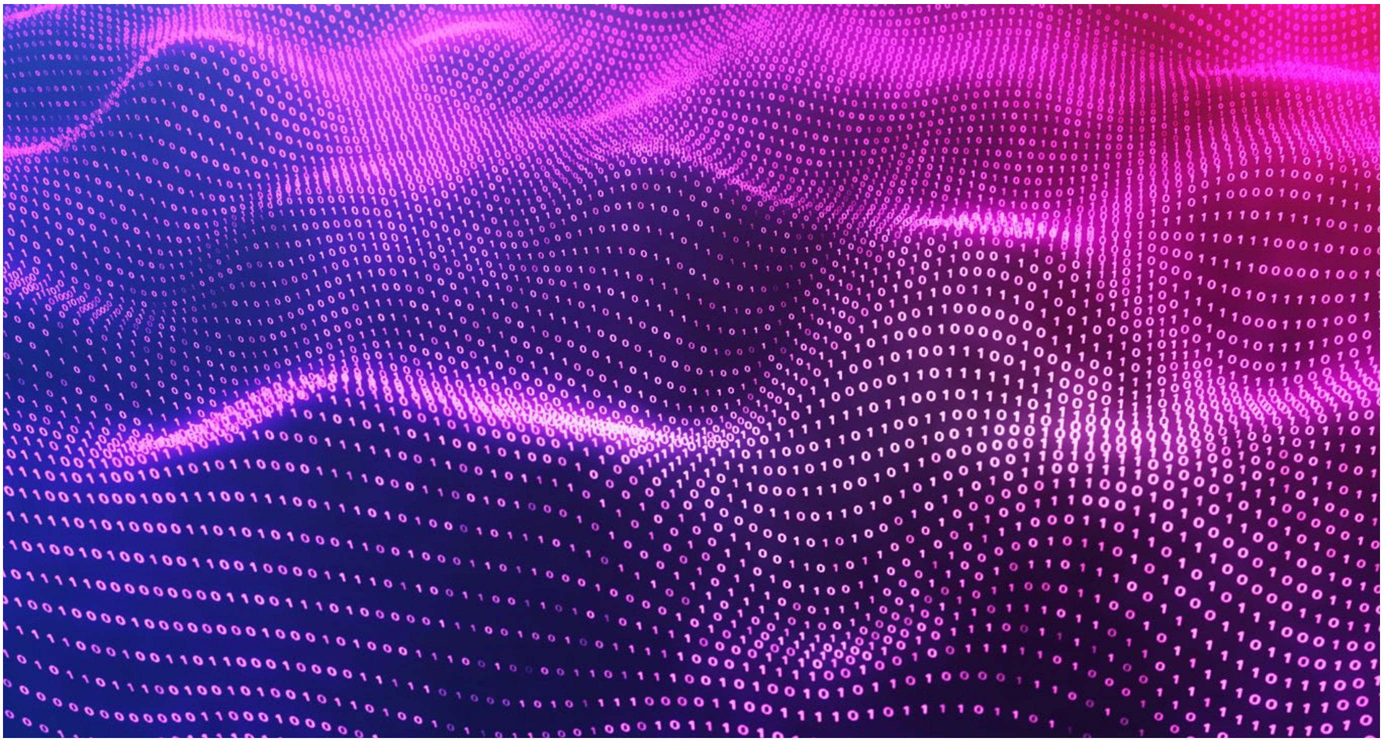
Security:
Is on-premise more secure?
What are the principle security threats?

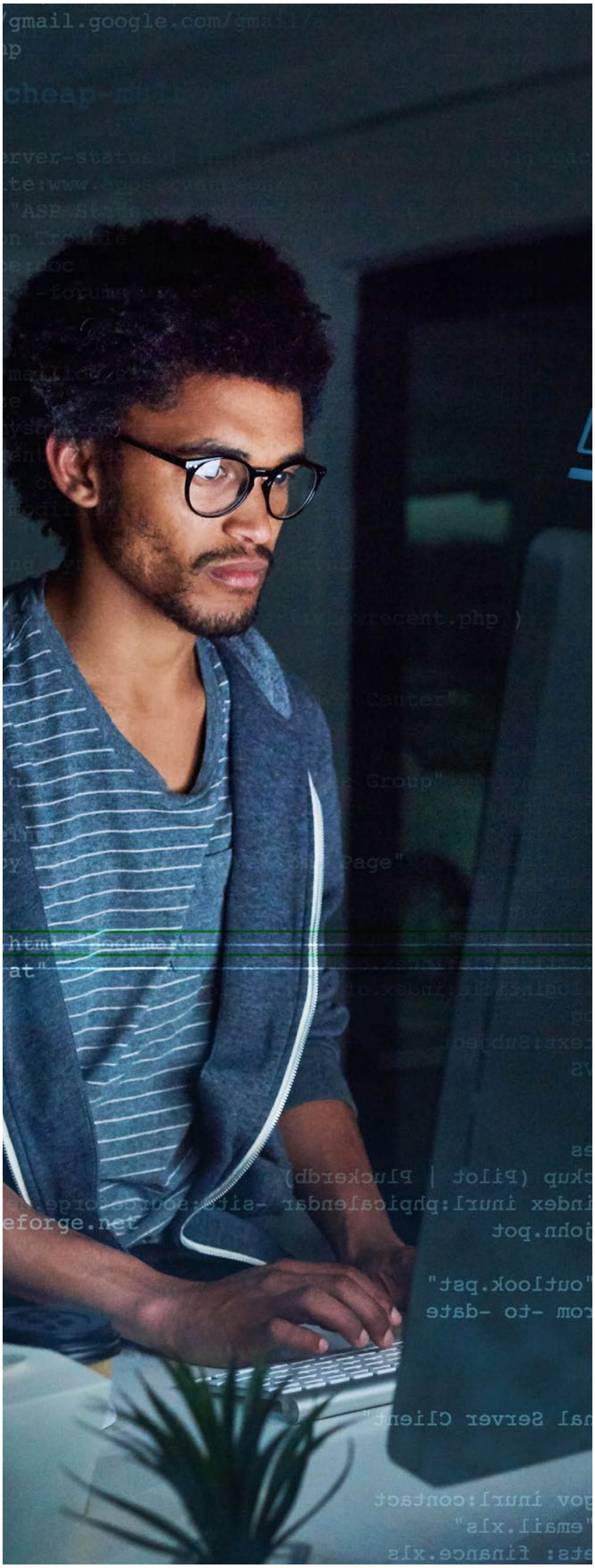
Vendor lock in:
This is a common concern for organizations considering the cloud–is it well-grounded?

Forced or unplanned updates:
What's the best balance to strike regarding mandatory and optional updates?

Uptime and availability:
What sort of availability levels does a business need?

The adoption of enterprise software can be a weighty decision, and in many ways, each case will be unique. But this whitepaper will help you to both make an informed choice and know the pertinent questions to ask prospective vendors.





66% of IT professionals report security as their most significant concern in adopting an enterprise cloud computing strategy.

1. Security

When considering a move to the cloud, security is typically towards the top of an organization's agenda. This is understandable, since the impact of a breach can be dramatic.

There are several reasons why on-premise might seem more secure:

- It's run over a local network rather than an internet connection
- A business might feel "safer" because the information is physically closer to their location
- There have been some high-profile cases of cloud security breaches to make the news in the past few years

These points might go a reasonable way to explain the perceptions some people have of security. But none of them settle the important question: is the cloud more or less secure?

To examine this, you need to consider three key areas:

1. **Access and location:**
   A hacker would likely gain access to a cloud system over the public internet. Sometimes on-premise systems will be accessible via the internet too–either deliberately or inadvertently because of flaws in the customer's network security. But it's quite likely that for an on-premise security breach, the method of access would be different–through a phishing email or unpatched security hole, for example.

   However, there's no reason to say on-premise is any less vulnerable because of this difference. And because on-premise data centers are usually located within or close to the organization itself, the network is at risk of physical access by unauthorized users, particularly insider threats who work for the business. Meanwhile, the top cloud vendors safeguard servers (physically located anywhere in the world) with protections such as biometric devices, fences, guards, security cameras, and have contingencies in place for natural disasters.

The stark truth:

Most security breaches are a result of a hacker exploiting a human vulnerability or mistake.

2. **Technical expertise:**
   Public cloud providers have a deeply vested interest in keeping their customers' data secure: their reputation and profitability depend on it. If the enterprise software you adopted were hosted on Microsoft Azure, for example, you would automatically capitalize on the expertise of more than 3,500 global cybersecurity experts.[1] Unless your organization is already in the business of IT security, it will be hard to match this level of knowledge.

3. **Root cause of security failures:**
   Whether your data is housed on-premise or in the cloud, the stark truth is this: most security breaches are a result of a hacker exploiting a human vulnerability or mistake. Your network infrastructure might be sitting in a distant data center in Northern Virginia or just a few feet away in the office server room. Either way, history has shown most security breaches are caused by a mistake the customer has made rather than the vendor. Gartner expresses this rather more bluntly, reporting "through 2025, 99% of cloud security failures will be the customer's fault." [2]

To sum up, our earlier question "is the cloud more or less secure?" perhaps isn't the right one to ask. Experts can't agree on a conclusive answer because there most likely isn't one. A better approach–regardless of the environment you choose – is to instead ask yourself: how do I use it securely?

[1] Microsoft, Strengthen your security posture with Azure
[2] Gartner, Is the Cloud Secure?

Questions for your vendor

Question	What you’re looking for
What protection do you provide for my applications and data?	Your vendor should be able to tell you precisely where your data is housed and how it’s shielded. It should also encrypt your data at all times, both in transit or at rest.
What sort of identity and access management do you provide?	This is crucial to protecting your company data as it lets you manage who has access to what information. Look for features such as role-based access, two factor authentication, custom password polices and single sign-on (SSO).
What is your disaster recovery plan?	Ideally, a vendor should start by telling you how unlikely disaster recovery would ever be. Ascertain how many single points of failure there are–i.e. the more redundant connections and geographically separate data centers there are, the less likely it is disaster recovery will ever be needed. Once you have that information, act as if disaster recovery will be needed and ask where the vendor stores backups. As with data centers, there should be some spread, as it means a complete backup could still be performed if a natural disaster destroyed all data centers in a particular area.

Breaking the myth.

Having data nearby doesn't automatically make it any more accessible than storing it remotely.

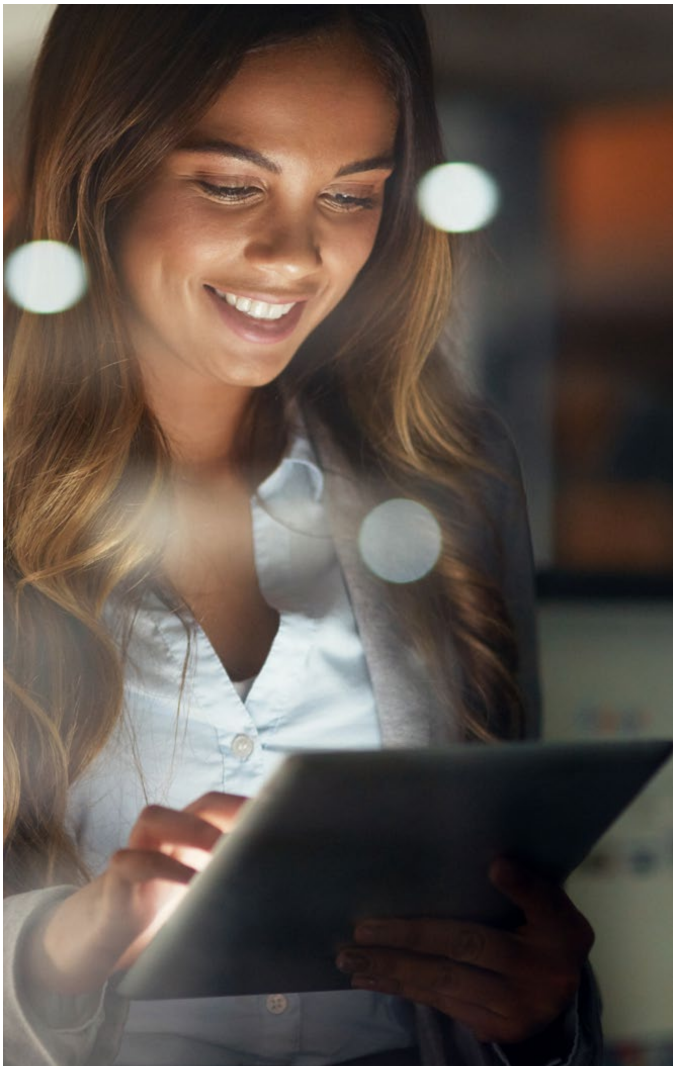
2. Vendor Lock In

Along with security, vendor lock in is usually the most frequently cited concern when enterprises are considering a move to the cloud.

But are these fears well-grounded?

The short answer: yes and no. The dangers of vendor lock in, for any product or service in general shouldn't be dismissed. For business leaders, the thought of paying for something that doesn't meet their needs, knowing there's a better alternative on the market (but not being able to do anything about it) is a scenario keeping them up at night for good reason.

But the idea that vendor lock in is symptomatic of the cloud per se, is in fact a myth; having data nearby doesn't automatically make it any more accessible than storing it remotely. Much like money in a vault, it's "locked up"–the location of the vault is irrelevant.



Here are three more key reasons why vendor lock in shouldn't be more of a concern in the cloud than for other deployment options:

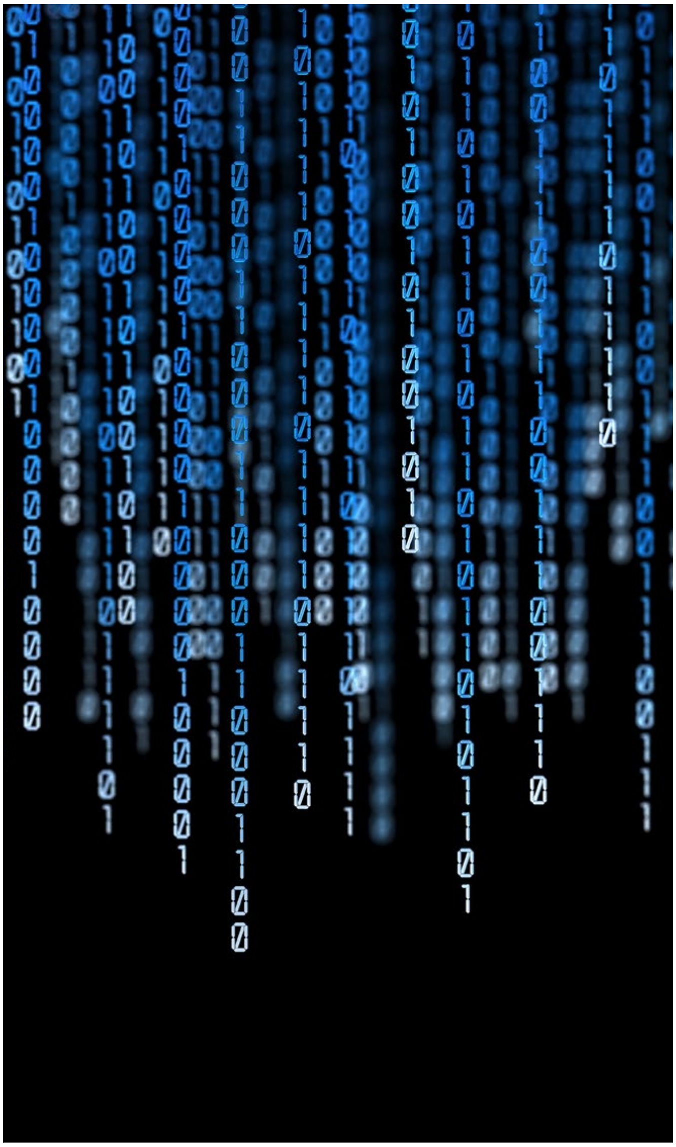
1. **Customer choice:**
   The best providers offer reasonably short commitment periods for a cloud service. However, since on-premise is licensed perpetually, a customer essentially commits for a longer time in order to recoup or pay off their investment.

2. **The human link:**
   Whether it's your CTO–who was responsible for the cloud migration project–or the System Administrator that diligently built up and now manages an on-premise environment, both have an emotional attachment that present its own form of lock in. Arguably, IT staff will be more attached to on-site infrastructure–it's a tangible system to tinker with. But cloud doesn't need to be perceived by IT staff as a threat. The outsourcing of the technology stack presents opportunity as time is freed up for teams to focus on other more high-level or business growth focused activities.

3. **Migration is migration:**
   To move data from one enterprise application to another often requires reformatting. This work would need to be done regardless of the hosting environment–an on-premise environment isn't any less "locked in." In fact, on-premise often becomes harder to migrate, since the system is typically in a less defined and well-structured state than a cloud solution. An on-premise solution is more likely to evolve over a period of time without comprehensive documentation and consideration.

Questions for your vendor

Question	What you're looking for
If I decided to end my agreement, would you provide data migration tools or services?	The task of moving data from a unique custom-built system will be made infinitely easier if the vendor provides tools or services to help you. After all, they know their own system best.
What are the details of the exit strategy if we part ways?	This should be made clear in the contract–what the processes will be for abandoning the application. For example, how the data comes out and how much time you will have after service nonrenewal.
Which industry standards do you comply with?	Standards such as ISO 27001 provide added assurance when it comes to a 3rd party handling your data.



3. Forced or unplanned updates

A common concern is that updates will be "shoved" at the customer, who will have little/no say over when they get scheduled. The worst-case scenario being an incomprehensible new user experience or business process landing at their feet overnight without any warning. Or an update landing in the middle of the busiest season, when the customer has other IT priorities.

It's easy to draw parallels with Microsoft Windows updates here. For example, you might well remember the days of Windows XP and Vista, when sometimes a hapless colleague would go for a coffee break, only to return and find their computer had rebooted itself to install updates and all their unsaved work had been lost.

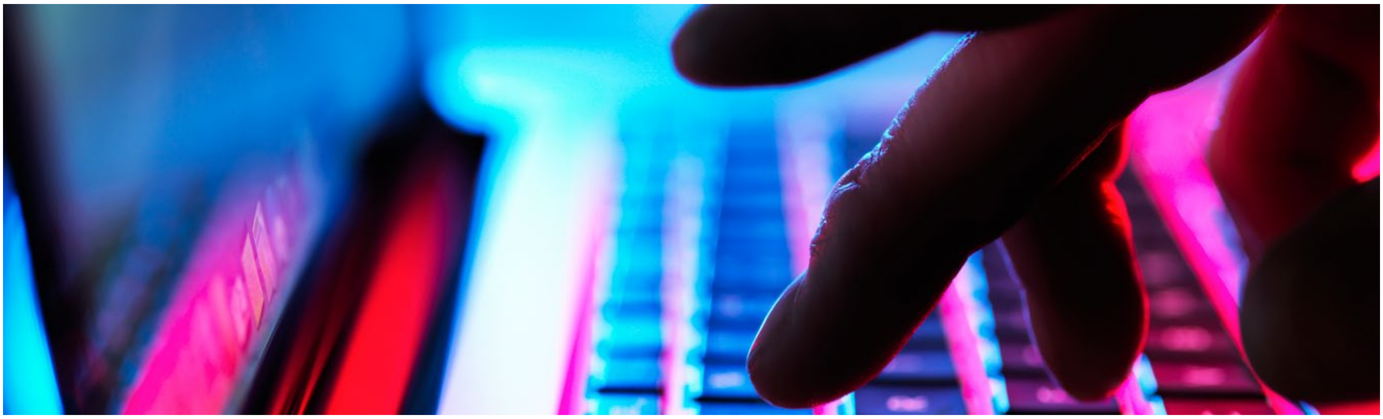
But how did Microsoft respond to this?

They improved Windows Updates significantly by putting the user first and offering choice. Later versions of Windows let you install updates at more convenient times, such as when you shut down/reboot your PC or at a time you choose. It makes sense for the patching of critical security vulnerabilities to be mandatory and automatic. Quite simply, the risk of the security vulnerabilities outweighs the risk of possible disruption to workloads. However, the same can't be said for non-critical updates, so a choice of when to deploy these updates is one that pays. And any disruption to workloads that does occur is likely to be minor; security patches seldom introduce invasive changes to business processes or user experience.

In summary, look for providers that offer choice when it comes to cloud software updates.

Questions for your vendor

Question	What you're looking for
When will planned maintenance occur and what prior notice will be given?	The task of moving data from a unique custom-built system will be made infinitely easier if the vendor provides tools or services to help you. After all, they know their own system best.
What support will you offer to internal IT teams after updates have been deployed?	Even though your provider will be handling the updates, you will still need to conduct some testing internally. Your IT teams may be able to do this with confidence or may at times benefit from some guidance.
Will there be a choice of updates and patches?	Some SaaS vendors will be inflexible, uniformly deploying updates to all their customers. They may also simply apply updates at a time to suit them and not even tell customers they have happened. If that's the case, try to evaluate what the potential impact of certain mandatory (and potentially unwanted) updates on business continuity and staff training might be.



Top Tip:

When evaluating vendors and their uptime and availability levels, try to assess ownership and commitment. There's a world of difference between a SaaS service that provides an SLA on the outcome (i.e. that users can access the software), and more fragmented solutions where there is no end-to-end commitment.

A typical example is a vendor that's essentially only providing outsourced IT management but makes bold claims about availability levels (e.g. 99.9% or higher). Such vendors often don't make any actual commitments, provide any SLAs, or demonstrate how they will achieve the numbers they state.

4. Uptime and availability

For most enterprises, availability and performance will increase in the cloud when compared to on-premise instances of software, particularly for multi-location businesses and for users outside the four walls of the business. While affordable 100 percent data center availability is still a long way away for many organizations, you can reasonably expect a contractual commitment of 99 percent or more from your vendor.

Having the expectation of 100 percent availability is a common mistake businesses make when considering a move to the cloud. Such a guarantee would require heavy investment from both the customer and service provider and would be cost prohibitive regardless of where software is provisioned. Even if a company has a solution installed in their own data center, achieving 100 percent availability would involve huge expense.

Questions for your vendor

Question	What you're looking for
Can you describe how your operational-level agreement (OLA) supports your cloud uptime and availability SLA?	It's best to think of uptime and availability SLAs as complementary layer on top of the company's OLA, which is essentially a framework of internal SLAs. For example, if there isn't always staff on hand when incidents arise, a 99.99% SLA would be difficult to meet.
What compensation would you offer if you didn't meet the agreed SLA?	Most vendors provide service credits in the event of unplanned downtime. Find out what these would be and what proportion of the overall service costs they would comprise.
What's covered in the exclusion clause of your SLA?	Determine exactly what isn't covered. Typical examples include acts of disruption caused by the customer, software maintenance and natural disasters.
In addition to a cloud service, what other supplementary services do you offer?	Many vendors typically offer a tiered service set with a hosting/infrastructure option which can then be supplemented with services such as application management. It is important to verify with each vendor exactly what their cloud does/doesn't include and what they provide as standard, both directly and through their service partners to outsource the different activities required as part of an applications operations model.

Final thoughts

The SaaS model has by now become pervasive and its business benefits widely recognized. At the same time, there is a sub-set of businesses for which SaaS may not be the best fit. One characteristic these businesses often share is that specific legislative restrictions, for example around the movement of data, prevent them from using cloud services.

We don't try to push a certain way of doings things on any customer. Instead, we take your unique set of requirements before guiding you through our options for ERP software.

About Enterprise Consulting

Enterprise Consulting is passionately committed to helping companies achieve business results with IFS. We offer services to support companies throughout their lifecycle including implementations, upgrades and optimizations. Enterprise Consulting can also manage a customer's IFS deployment in their Enterprise Managed Cloud hosting solution. Want to learn more about how we can help you? Request a free consultation at https://www.enterpriseconsulting.net/contact.

About IFS

IFS develops and delivers enterprise software for companies around the world who manufacture and distribute goods, build and maintain assets, and manage service-focused operations. Within our single platform, our industry specific products are innately connected to a single data model and use embedded digital innovation so that our customers can be their best when it really matters to their customers–at the Moment of Service.

The industry expertise of our people and of our growing ecosystem, together with a commitment to deliver value at every single step, has made IFS a recognized leader and the most recommended supplier in our sector. Our team of 4,000 employees every day live our values of agility, trustworthiness and collaboration in how we support our 10,000+ customers. Learn more about how our enterprise software solutions can help your business today at ifs.com.