10 Curveball Questions on Safety in the Cloud

What Every Business Should Be Asking Their ERP Provider Today

By Phil Wainewright

Commissioned by Acumatica

© Procullux Limited, 2014
Technology questions are important, but business outcomes are what really counts. These ten curveball questions will help you cut to the chase when assessing whether your ERP system will keep your business safe in the cloud. To keep the IT folks happy, we also included a more detailed checklist at the end of this document specially designed for IT decision makers.

1. Which century again?
If an ERP system wasn’t built for the cloud, then it’s unlikely to be safe for the cloud.

Unfortunately, many ERP systems in the market today were first designed in the twentieth century, long before the Internet became a pervasive feature of business life. They date from a time when commerce was confined to working hours, workloads were planned weeks or months in advance, and people had to be physically at their desk to access the system.

Modern enterprise demands business systems that can thrive in today’s fast-moving world of 24/7 operation, that can cope with unpredictable bursts of activity, and which are tuned for instant access from anywhere.

2. Is your ERP part-time?
Unlike people, computers don’t need to take breaks, sick days or vacations. So how come they seem to go offline so often?

NERVOUS about putting your company data in the cloud? Maybe you’re looking at this the wrong way around.

Many everyday business activities are already plugged into the cloud in some way. It is how people do business in today’s connected world.

But have you really thought through how to stay safe in the cloud? How do you know you haven’t already fallen prey to cyber intruders, data theft or online fraud?

In today’s always-on business environment, you don’t want a part-time ERP system. It must be there when you need it.

Ignore the service level promises and technical specifications. Ask what your proposed ERP system has actually achieved in live operation over the past one to two years. Expect 99.95 percent availability or better – that’s less than four hours unplanned downtime per year.

DON’T let your IT specialists bog you down in arcane debates about security technologies. Business people rightly take a broader perspective. Staying safe in the cloud has five dimensions:

- **Security** – protecting against network attacks and other vulnerabilities
- **Reliability** – ensuring systems are always available when needed
- **Compliance** – staying compliant with rules and regulations
- **Future-proofing** – preparing for the unexpected
- **Autonomy** – not getting locked in to a relationship that’s no longer working

Asking the right questions means covering all of these dimensions, not just one or two. It also means scrutinizing your in-house infrastructure just as rigorously as any cloud-based alternative.
EVERY business connects to the cloud. It’s just that some are more connected than others. The best connected businesses make sure their ERP systems are plugged into the cloud. There are three ways to do this, each with their own advantages and drawbacks when it comes to safety:

**On-premise:** The software runs on your own in-house servers, using your own connection infrastructure. This do-it-yourself approach puts you fully in control of your own safety, but puts a big burden on your in-house IT resources and skills.

**Hosted:** The software runs on servers at a third-party datacenter, either as managed hosting or Infrastructure as a Service (IaaS). Connections run over the provider’s infrastructure but the enterprise is responsible for managing them. This halfway house brings the benefit of a cloud-ready, shared infrastructure – but the buck still stops with you for ensuring safety.

**SaaS:** The ERP software is provided as a service, and the provider takes care of all the infrastructure and connections on behalf of the enterprise. This full-service arrangement lets you offload the burden of keeping everything safe, so long as the provider remains trustworthy.

Your choice of ERP vendor will often limit the options available. Many SaaS vendors offer no other option. Some on-premise vendors don’t offer SaaS – and their hosted versions may be poorly adapted for running in the cloud.

Only a few vendors allow you to choose between all three, making it easier to switch between models as your circumstances or requirements change.

Remember to check how much planned downtime there is and make sure it happens at times that won’t impact busy periods for your business.

**3. Who’s snooping my data?**

One of the biggest threats in the cloud is that confidential data will be exposed to prying eyes. You don’t want your organization in the headlines for a data breach. Demand encryption that lets you hold the keys that keep it safe.

You should also be alert to the risks of legally approved snooping by governments or litigants in possession of a court order. Make sure your data isn’t going to get into jurisdictions where the legal framework won’t meet your needs.

**4. Who gets the door keys?**

Many people obsess about datacenter security, forgetting that the most common access point for data theft today is by taking over a user’s client device or login credentials.

Make sure you retain control over user logins and access rights. Have systems in place that keep watch for signs of unusual or nefarious activity.

**5. Is it anywhere, anytime access for hackers?**

Mobile access is a prerequisite for any modern business system – but there are specific risks to be aware of. Make sure your content and apps are protected. You need to be confident mobile access doesn’t mean easy pickings for hackers.

**6. What’s the weakest link?**

Another common security vulnerability comes when data thieves piggyback onto automated
BEING in the cloud is far more than a technology choice: it’s how business gets done today. If your operations aren’t online for employees, customers and partners, then your business will lose out to more digitally savvy competitors.

Even when enterprises run everything on their own in-house IT systems, they still need safe connection to the outside world of the cloud:

- Customers and partners want to place orders online, check delivery status or send invoices electronically.
- Online Internet services provide many third-party resources that a business relies on to enhance its information and operations – from payroll and credit referencing to recruitment and marketing.
- When sales teams are out with customers, or managers are traveling or working from home, they want to use enterprise data and applications on their smartphones and laptops.

These outward-facing connection points and applications – called ‘systems of engagement’ by business author Geoffrey Moore – have to link up with the core ‘systems of record’ at the heart of enterprise operations.

Connecting core ERP systems to the cloud ensures everyone can work with up-to-date information and deliver results on demand.

external connections from third-party services – such as payment processors or social media sites.

All such connections should pass through security protection that’s at least as stringent as any other access.

The ERP vendor should also be able to vouch for the integrity of its ecosystem partners.

7. Will it keep me out of jail?

You can hand over responsibility for day-to-day operations but the buck still stops with you if things go awry.

Make sure that documented compliance processes are in place that protect your reporting and regulatory obligations.

8. How soon will it get stale?

One of the most challenging aspects of bringing ERP into the cloud is ensuring that the system stays up-to-date with the constant evolution both of new capabilities and of new threats.

Ask how often updates arrive with new features and security patches, and how quickly they can be implemented.

Many mid-sized organizations in particular find it is a constant struggle for their IT staff to keep pace with the rapid pace of technology change. They battle to stay ahead of newly emerging security vulnerabilities – all while trying to satisfy the often conflicting demands from business users to deliver the latest new features as rapidly as possible.
Many enterprises evaluate cloud ERP when they need to upgrade or replace an existing installed system. It’s attractive for organizations going through rapid technology or business change, or launching a new venture or subsidiary.

But cloud safety isn’t a topic to postpone to some future date. Today’s ERP platforms must offer the smarts to operate safely in the cloud while enabling businesses to take advantage of all the potential of today’s connected commerce environment.

That means supporting 24/7 operation at variable loads and with anytime, anywhere access from a wide range of different clients.

Getting the right core systems to take your business forward may mean lobbing a few curveball questions at your ERP provider.

But you’ll be glad you asked.

9. What’re the licensing gotchas?

The pay-as-you-go, as-a-service relationship gives vendors new scope to lock their customers into ever-rising financial commitments. Cloud makes it easier to extend access to new users, but many vendors charge exactly the same for light or inactive usage as they do for intensive power users. Make sure you understand what you’ll pay for and when.

10. How do I get out?

Cloud providers not only lock their customers into a software platform, they often control the operational infrastructure as well. This makes it exceptionally difficult for customers to move away if they become dissatisfied.

Being able to retrieve your data is small consolation if you first have to bring in a completely new system to run it. If a direct relationship doesn’t work out, hosting the application elsewhere is a more viable fallback.

About the author

Phil Wainewright is a trusted thought leader in enterprise computing, best known for his long-running Software as Services blog on ZDNet. He is a co-founder of diginomica, the tech media site launched in May 2013 to inform business decision makers about the transformation of 21st century enterprises by digital technology. He is also an advocate for cloud computing, both as a volunteer vice-president of EuroCloud and as CEO of strategic consulting group Procullux Ventures.

About Acumatica

Founded in 2007, Acumatica is the fastest-growing provider of customizable, Cloud-based ERP applications for small and midsized businesses; offering financial management, distribution, CRM, and project accounting suites. Acumatica Studio, the company’s technology development platform, gives ISVs and OEMs a rapid, cost-effective means of developing and integrating Cloud-based apps using industry-standard tools. The company’s products are delivered through a global channel partner network of resellers, ISVs, and OEMs. Headquartered in Kirkland, WA, Acumatica maintains offices in Washington DC, Moscow, and Singapore. In the Nordic countries and the Netherlands, Acumatica is sold as part of Visma.net; and in Australia and New Zealand, Acumatica is sold under MYOB’s brand name.
# The IT guys’ checklist for safety in the cloud

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
□ High performance at elastic levels of activity.  
□ Continuous protection of anytime, anywhere access by authorized users. |
| **2. Reliability** | □ Achieved uptime in the range of 99.93 to 99.97 percent or better over past 18 months.  
□ Reasonable provision for scheduled downtime at off-peak times to perform upgrades and system maintenance.  
□ Real-time monitoring and reporting of system health and performance. |
| **3. Data protection** | □ Data encryption both in storage and during transmission.  
□ Data stored and processed in specified legal jurisdictions – this includes backup, failover and disaster recovery (DR) as well as working copies.  
□ Data stored and processed in specified locations if required for regulatory reasons. |
| **4. User access** | □ Optional IP address restriction and/or two-factor verification of user logins.  
□ Ability to set inactivity time-out period.  
□ Access governed by policies based on user profiles that can be set by roles or groups as well as individually.  
□ Activity logs provide an audit trail of who has done what.  
□ Data and business logic remains on the server rather than being stored and processed on the client device. |
| **5. Mobile** | □ No data downloaded to local device storage.  
□ Two-factor user verification.  
□ Incoming data verified before writing to database.  
□ Compatible with third-party mobile device management systems. |
| **6. Add-ons** | □ Programmatic access to application data goes through the same policy-based security framework as authorized users.  
□ Proactive monitoring of programmatic access in case of third-party security breaches.  
□ Accreditation and certification of the vendor’s partner ecosystem. |
| **7. Compliance** | □ ISO27001 certified infrastructure.  
□ PCI DSS compliant e-commerce.  
□ Industry-specific requirements such as HIPAA.  
□ Audit tracking and reporting of all system changes. |
| **8. Updates** | □ Functional releases at least two to three times a year.  
□ Frequent program of security patches as required.  
□ Upgrades and patches implemented easily with minimal disruption. |
| **9. Licensing** | □ Ease and cost of adding or removing new users.  
□ Ease and cost of enabling external users at partners and customers. |
| **10. Exit** | □ Ability to export data for external storage and/or use.  
□ Ability to export application metadata.  
□ Scope of third-party and self-hosting options. |