MARKET SIGNALS™

WHITE PAPER

How Hybrid Should You Go? 3 Key Factors that Determine Your Hybrid IT Model

Rimini Street®

Summary

As the hybrid IT model becomes the new norm, an enterprise's version of hybrid IT will be shaped by how its suppliers, customers, and partners are using the cloud, plus how the enterprise approaches integration and security. Assess these three factors when determining what parts of IT to move to the cloud.

Analysis

A hybrid IT environment results from a strategy companies are using to selectively move some information technology to the cloud while retaining other technology in a noncloud environment (see "Leveraging Hybrid IT Now to Power Digital Transformation"). Most companies moving technology to the cloud must do so according to a paced, business-driven timeline.

For many companies, it may not be the best business move to shift all applications to the cloud. For example, moving core, tightly integrated systems such as ERP to the cloud as an SaaS suite usually does little to improve the business. At the same time, customer-facing systems and other systems of engagement can create competitive advantage by being deployed as SaaS. The resulting cloud/noncloud applications mix creates a hybrid IT environment. In another scenario, the timeline required to execute a cloud strategy can be long, resulting in a mixed hybrid IT portfolio for years.

From an IT perspective, moving an application and its supporting infrastructure to the cloud may be a suboptimal choice, particularly when there is more value to be gleaned from existing software licenses. Instead, many CIOs are choosing to move just the infrastructure to the cloud and then operate their licensed applications on the IaaS. This is another hybrid IT example.

FACTOR	How the Factor Shapes the Hybrid IT Model
1 Collaboration with other IT ecosystems	The composition of the hybrid IT model must accommodate the ecosystems with which a company interacts.
2 Integration risk tolerance	The integration risk that an enterprise is willing to tolerate affects how much data and process can be delivered via the cloud and how many cloud vendors can be absorbed into the hybrid IT portfolio.
3 Hybrid IT environment security	The level of trust that the hybrid IT environment is safe and secure will influence what can be deployed in the cloud, especially when visibility into the cloud vendor's security is opaque.

Factor 1: Collaboration with Other IT Ecosystems

The external systems that an enterprise interacts with are deployed across a variety of models (cloud and noncloud). Choosing deployment options that are similar to the enterprise's vendors, partners, and customers can increase business value through simplification.

From an external perspective, the location (cloud or noncloud) of supplier/partner/customer systems interacting with a company's technology ecosystem affects what business value may be derived when either moving applications to the cloud as SaaS or keeping them noncloud. An example of this can be seen in the healthcare industry where privacy regulations make it unlikely that cloud-based systems will be shared across the community, making a key business driver for moving to the cloud irrelevant for those systems.

Choosing options that are difficult to integrate or that make cross-supply chain processes more complex can potentially disrupt or degrade business outcomes. For example, if everyone else is moving a system to the cloud, consider moving your own. If no one else is doing it, now is probably not the right time to make a cloud move for that system.

Internally, the extent to which the IT organization develops custom systems and/or purchases packaged solutions influences the percentage of SaaS and custom solutions that comprise the hybrid model. The hybrid IT model is also shaped by those cloud development tools, platforms, and products used. Contrasting two examples:

> Enterprise A dabbles in system development but is set on a specific product path (such as Microsoft) for its SaaS components. It will likely use that vendor's cloud platform for system development (MS Azure in this example). Doing so will likely reduce compatibility issues and reap more value from commonality across its product line.
>
> Enterprise B employs a business model where application development is key (such as unique customer-facing banking solutions). Its hybrid IT model will be shaped around a cloud provider (AWS, for instance) that can support its development strategy and tool set.

Cloud complexity can increase quickly and make support and portfolio evolution difficult; poor cloud decisions may damage a business's ability to innovate and grow. Enterprises require rigorous, repeatable, consistent strategies for making decisions about what is/isn't moved to the cloud in order to ensure a compatible, supportable technology portfolio. Having a clear strategy that covers not only SaaS, but platforms and tools as well, will likely result in an application portfolio that supports the business and is easier to maintain and evolve.

Recommendations:

- **Establish a framework or application decision tree** to score cloud readiness and help articulate cloud direction. The goal is to let the business and IT clearly see the paths, options, and impacts of platform choices, cloud scope, and tools used. See Figure 1 for a sample framework.
- **Assess strategic areas** such as criticality to business; difficulty in performing actions such as a lift-shift; time and cost of the next onsite hardware upgrade and/or the next onsite OS upgrade; stability of application; ability to find IT staff; and longevity plans for the system (keep or replace in a specific time frame).
- **Create a scoring algorithm** and use the results to make a prioritized investment/project list.
- **Establish a migration strategy** and corresponding time horizon suitable to your industry that corresponds with your application development plans; publish the timeline to the business.

Sample Framework for Assessing Cloud Readiness and Direction

Business	**Business Rationale** **Business Case**	Company ABC has tangible and visible leadership/sponsorship for a migration to a cloud collaboration platform. Business and IT leaders are preparing to start the transition. The TCO estimate will help complete this area and finalize the rationale.
People	**Executive Sponsorship** **Collaboration** **Change Management**	Company ABC has identified critical executive leadership. Need to create a formal Cloud Center of Excellence (Cloud COE) to manage the program. IT has a good relationship with the business and conducts regular business reviews. IT leads formal change management internally and with the business. Suggest executive leadership begin periodic discussions/ presentations on cloud to encourage more adoption.
Governance	**Measuring Outcomes**	Company ABC uses formal business cases and will be able to use the cloud assessment to guide development of its Cloud COE and resolve any governance or compliance concerns.
Platform	**Cloud Provider**	Company ABC does not have an existing subscription to a cloud platform. Company ABC needs to decide on its application cloud partner.
Operations	**Infrastructure** **Agile Frameworks** **Operations and Responsibilities Alignment** **Collaboration**	Company ABC needs to build out network connectivity to the cloud. ERP application is ready to move to the cloud. Team understands agile development, which is important for driving the most value from cloud delivery. IT team needs to leverage training from the chosen cloud provider. Can be worked into the subscription contract. Company ABC should consider using a partner to support the initial cloud implementation post-g-live and then assess the TCO for external versus internal support. By using a partner, Company ABC can develop cloud change management best practices and make sure that the true value of business continuity planning in the cloud is fully realized.
Security	**Operational Cloud Security** **Documented Security Policies**	Company ABC has solid security policies for all its environments. This is a real strength of the organization. Need to translate those policies to the cloud. Additional security training is available from the chosen cloud provider.
Integration	**Integration Competence** **Integration Risk Tolerance**	Company ABC has no enterprise-level integration team. Need an integration competence center and cloud integration processes, policies, responsibilities. Company ABC has a data management team in place and has identified sensitive data and processes not suitable for cloud deployment.
Internal andExternal IT Ecosystems	**Partner Cloud Strategies** **Internal Cloud Development**	Company ABC has identified what its suppliers/partners/customers are moving to the cloud and has prioritized cloud projects to align with them. IT has not settled on which cloud development tools, platforms, and products will be used. Need to assess current cloud tool/platform/product use and determine whether to extend existing usage into company standards or establish new approaches for broad usage.

Good **Caution** **Don't Start**

Green text contains remediation tasks

Source: Rimini Street

Figure 1

Factor 2: Integration Risk Tolerance

Integration is a requirement for hybrid IT environments, but risk is introduced each time data or processes cross systems, products, or services. A hybrid IT portfolio may contain numerous cloud vendors, depending on the enterprise's tolerance for integration risk. Those with less appetite for varying levels of potential error in data synchronization, data integrity, etc. should consider maintaining fewer vendors in the hybrid IT portfolio and may choose to keep critical data and processes in house rather than with a cloud vendor.

From an external perspective, the more partners in the mix, the more integration risk exists. Some risks are common with those found in noncloud portfolios — for example, mismatched data creates data synchronization errors. Others are particular to the services nature of the cloud — mismatched SLAs make integration timing a risk for business disruption. Some integration risks are less obvious but just as disruptive to business operations; for example, mismatched change windows create a data synchronization risk during change events.

Internally, enterprises need to agree on what is an acceptable level of integration risk when making decisions about placing data and processes in the cloud, as well as when spreading them across multiple cloud services. Thoughtful, consistent principles applied across the hybrid IT portfolio will help provide seamless integration that enables timely, secure data flow where it benefits the business and ensures that process integrity is maintained at all levels of risk the company can tolerate.

Recommendations:

- **Establish a set of guiding principles** for determining acceptable integration risks.
- **Use an integration checklist** during solution selection and as a part of data management, based on those guiding principles, to identify potential issues that could arise with data residing in multiple places and the associated level of risk if that happens. See Figure 2 for a sample integration checklist.
- **Determine whether existing process integrity controls** will be lost or if new controls will be needed when a process crosses solutions.
- **Weigh different levels of risk** as they are applied to different types of data and processes based on criteria such as being business critical, time dependent, highly sensitive, or compliance constrained. Make sure the integration checklist includes factors for timing and security in order to determine the level of risk created by operating across systems. Risk factors should include product- and vendor-level risks as well as technical, data, and business-process risks.

Starter Checklist of Hybrid IT Integration Risk Factors

Integration Risk Category	Risk Factor
Data	■ Data duplication across the hybrid environment is identified and can be managed ■ Data definitions are consistent across the hybrid environment and definitional mismatches can be accommodated ■ Data disconnects are known and mitigation plans are in place (e.g., needed in a receiving solution but not available in the sending solution) ■ A data management team is in place and has identified sensitive data and processes suitable for cloud deployment
Process	■ Hybrid integration processes (that cross internally deployed and cloud environments) have no gaps or overlapping steps; inconsistencies are identified and can be accommodated
Application	■ Application architectures are compatible (e.g., master file configurations are consistent across solutions)
Security	■ Enterprise security policies can be applied to cloud-based data and processes
Integration Competence	■ Company ABC has an enterprise-level integration team ■ An integration competence center is in place ■ Cloud integration processes and responsibilities are defined ■ Cloud integration policies are in place

Source: Rimini Street

Figure 2

Factor 3: Hybrid IT Environment Security

From an external perspective, cloud security processes, controls, and governance are still evolving. The same applies to those for a hybrid IT environment, and in some cases, what has been established puts customers at a disadvantage. For example, in SaaS environments, because the software vendor is delivering a complete service, the customer doesn't have visibility into how cloud security works. Visibility is often needed to guide the decision-making process around the types of data the enterprise is willing to put into the hands of its cloud provider. Without that visibility, it is difficult to determine whether an enterprise's data will be secure enough.

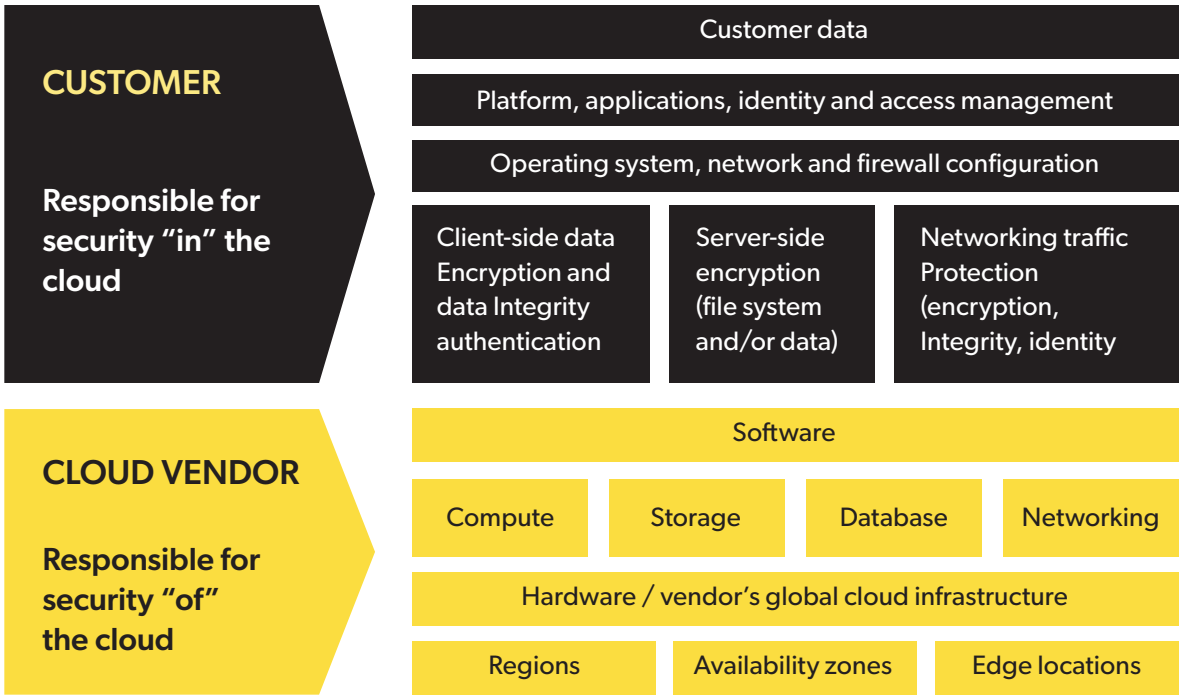
A policy of not disclosing security controls is standard operating procedure for most SaaS vendors. Most cloud vendors will certify that they are compliant and adhering to regulations and guidelines (for example, vendors provide attestations that they are payment card industry [PCI]-compliant in lieu of providing visibility into their controls). The level of trust that an enterprise has in its vendors' environments being safe and secure will influence what can be entrusted to the cloud and will ultimately shape its hybrid IT environment.

Internally, the enterprise must be willing and able to take extra security steps to secure a hybrid IT environment. Using data as an example, permission management in the cloud may not align with how the enterprise needs to use or secure its data. Clear and concise controls are needed at data choke points to ensure that data is secured properly, particularly when security varies across vendors. A strong internal security team that understands the cloud and noncloud environments is paramount in delivering hybrid IT security services and in ensuring solid security across the hybrid environment. The strength of the enterprise's security team will shape the hybrid IT portfolio by influencing the technology that can safely reside in the cloud.

Recommendations:

- **Nurture an element of trust** and good relationships with cloud partners. Understand (to the extent possible) what is going on inside the cloud services in order to create internal checks and balances where the vendor seems weak. If the level of trust is low, don't store the enterprise's "secret sauce" or critical data in the cloud.
- **Modify security policies** to ensure consistency across internal and cloud platforms, as the enterprise is still responsible for much of security in hybrid IT. For example, security needs to be consistent for each place where data resides or is transmitted.
- **Create a matrix for cloud and noncloud systems** to clarify for which systems' security the company is accountable. See Figure 3 for sample hybrid IT security responsibilities.
- **Define measures of control** over the cloud portions of the hybrid IT environment and staff appropriate to manage them. In the prior data example, data loss prevention (DLP) solutions can ensure that sensitive data doesn't accidentally leak into the cloud. However, if sufficient control can't be guaranteed, don't move the technology to the cloud.
- **Identify security roles and responsibilities** as a part of onboarding each cloud vendor.

Sample Hybrid IT Security Responsibilities



Source: Rimini Street

Figure 3

The Shape of Your Hybrid IT Environment Should Not Be an Accident

Address these three key factors and build your hybrid IT model strategically. Let the cloud portion of the hybrid IT portfolio be shaped by whether "as-a-service" truly adds any business value. Balance this with keeping integration risk low and ensuring the environment is secure. Create agility and flexibility by coordinating choices of SaaS, platforms, and tools. Finally, develop a comprehensive plan for managing the possibility of vendors failing, particularly when the elements of trust, transparency, and control are considered.

Learn more about developing a hybrid approach in this companion piece: "Leveraging Hybrid IT Now to Power Digital Transformation."

Rimini Street®

riministreet.com
info@riministreet.com
twitter.com/riministreet
linkedin.com/company/rimini-street

Rimini Street, Inc. (Nasdaq: RMNI) is a global provider of enterprise software products and services, the leading third-party support provider for Oracle and SAP software products, and a Salesforce® partner. The company offers premium, ultra-responsive, and integrated application management and support services that enable enterprise software licensees to save significant costs, free up resources for innovation, and achieve better business outcomes. Global Fortune 500, midmarket, public sector, and other organizations from a broad range of industries rely on Rimini Street as their trusted enterprise software products and services provider.