

PwC and Guidewire

Hello, tomorrow.
Cloud-forward is
future certain.



Preparing & mobilizing for the Cloud: Is your organization ready for a Cloud migration?

Migrating to the Cloud can seem like an uphill climb. The Cloud offers great possibilities - reducing total cost of ownership, new capabilities, greater speed to market - but deciding just when and how to migrate isn't easy. Furthermore, the task can seem especially daunting when you think beyond core systems and consider implications to your broader enterprise architecture, your workforce, and the impact Cloud could have on data security and privacy.

PwC's Cloud Fitness Framework

To assess migration effort, PwC uses a Cloud Fitness Framework that's based on our extensive experience with Cloud implementations and upgrades. The framework demystifies the Cloud journey by examining your enterprise, unveiling potential blind spots, and helping prepare you for future eventualities. Our clients have found the framework makes migration planning and execution a lot less intimidating than it would be otherwise.

Before embarking on a migration, we'll work with you to assess what it will require of your organization and exactly where you'll need to focus your efforts both from the outset and as the journey continues. Here are some key success factors to keep in mind both before you start and while you're engaged on the project:

Fitness Framework Highlights



Time boxed

Plan a short assessment to get the effort started.



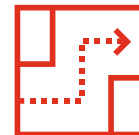
Modular

Understand where your capabilities are mature and where to target improvement.



Focused

Understand the key decisions and items to plan for early in the process.






Insightful

Don't try to answer every question too early. Create a path to build momentum for the transition.

To help prepare for Guidewire Cloud, carriers should take certain steps to better understand how to start their journey. Of note, it's important to go beyond Guidewire, because a migration will affect many parts of the organization.

Cloud fitness

As you plan core Guidewire systems transition, you'll need to evaluate three primary areas in order to better understand your Cloud fitness prior to starting your journey: 1) technical architecture, 2) human capital and 3) cyber security. Your current maturity levels will help you know what you'll need to prioritize. Wherever you land is likely to necessitate big changes for your organization, so let's take a look at all three areas to identify where you'll most likely need to start.

Guidewire Cloud & Beyond: Fitness Framework Components	Fitness Framework Details				
<p>1  Technical Architecture Evaluation</p> <table border="1"> <tr> <td data-bbox="164 953 370 1115">Application</td> <td data-bbox="375 953 581 1115">Integration</td> <td data-bbox="586 953 792 1115">Data</td> <td data-bbox="797 953 1019 1115">Infrastructure</td> </tr> </table>	Application	Integration	Data	Infrastructure	<p>Begin to understand the impact to your core Insurance and peripheral ecosystem across applications, integrations, data and infrastructure services.</p>
Application	Integration	Data	Infrastructure		
<p>2  Human Capital Readiness</p> <table border="1"> <tr> <td data-bbox="164 1346 370 1507">Comms Strategy</td> <td data-bbox="375 1346 581 1507">Workforce Planning</td> <td data-bbox="586 1346 792 1507">Org. Design Implications</td> <td data-bbox="797 1346 1019 1507">Training & Readiness</td> </tr> </table>	Comms Strategy	Workforce Planning	Org. Design Implications	Training & Readiness	<p>Assess the readiness of your people and organization to determine 1) communications strategy, 2) workforce planning, 3) potential organizational design implications and 3) internal/external training & readiness.</p>
Comms Strategy	Workforce Planning	Org. Design Implications	Training & Readiness		
<p>3  Cyber Security Assessment</p> <table border="1"> <tr> <td data-bbox="164 1738 370 1900">Application & Integration Security</td> <td data-bbox="375 1738 581 1900">Data Security & Privacy</td> <td data-bbox="586 1738 792 1900">Identify & Access Mgmt.</td> <td data-bbox="797 1738 1019 1900">Monitoring & Incident Response</td> </tr> </table>	Application & Integration Security	Data Security & Privacy	Identify & Access Mgmt.	Monitoring & Incident Response	<p>Assess how your agents, policyholders and employees will be protected on the Cloud through 1) application & integration security, 2) data security & privacy, 3) identity & access management and 4) monitoring & incident response protocols.</p>
Application & Integration Security	Data Security & Privacy	Identify & Access Mgmt.	Monitoring & Incident Response		



Experience-based insights: Technical/Architecture

Recognize the importance of compiling application architecture and high-level designs for integrations early in the program. A sound foundational plan will help you account for key aspects of internal and external integrations are accounted before implementation.

Technical architecture evaluation

We understand that shifting to Guidewire Cloud will have implications for your broader enterprise architecture. Today's technology leaders are always on the lookout for faster and simpler ways of integrating applications and often work with a hybrid portfolio of applications, with some on the Cloud and others on-premise.

Start with key architectural considerations for the planned upgrade/migration to the cloud, including applications, data, integrations and infrastructure. A technical architecture evaluation needs to:



Application

- Evaluate your current policy administration architecture both for core Guidewire and the broader application ecosystem.
- Evaluate existing DevOps practices (CI/CD, Monitoring, notification, environments, etc.).
- Assess the applications intended for migration to Guidewire Cloud.



Data

- Evaluate current enterprise data architecture.
- Assess regulatory/compliance requirements for data that must remain on-premise.
- Understand the data stores in scope, encryption strategy, tools and frameworks in use.
- Evaluate upstream, downstream, and external data needs (e.g. actuarial, 1099, stats, etc.).



Integrations

- Examine internal and external integrations.
- Assess integration strategy/platform used for Guidewire Applications integration.
- Examine in place controls from a system/process standpoint for each integration pattern.



Infrastructure

- Assess the current Infrastructure topology that revolves around the Guidewire ecosystem.
- Evaluate high-level technical specs/SLAs for each infrastructure component.
- Review existing business continuity, disaster recovery and capacity management plans.



Experience-based insights: Human capital

Develop an early understanding of the roles and training your organization will need to efficiently operate in a Cloud environment. You may need to establish new roles, such as a Cloud release manager. Training and certification requirements may take time to acquire. Having a plan in place in advance to prepare your employees will reduce the likelihood of unnecessary execution delays.

Preparing your people

Preparing your people for the Cloud will be critical to your success. While an upgrade to Guidewire Cloud will ultimately benefit your agents, policyholders and organization, your employees will be who most strongly feel the change. IT employees in particular will deal with more disruption than any other business unit, and you'll likely need to overcome at least some resistance to change.

You'll need to focus on four key areas to have your team members ready for the upgrade:



Communications Strategy

- Clearly communicating why have we decided to move in this direction.
- Being able to explain the “what’s in it for me?” (i.e. what’s the impact to me, my job/role/function?).
- Describe how we’re going to ensure success and the support people will receive.



Workforce Planning

- Define job descriptions, roles & responsibilities, and expectations for working in a Cloud environment.
- Identify new skill sets.
- Identify potential gaps and the need to hire new staff.



Organizational Design

- Assess how the current organizational structure may change, including any management or reporting structures.
- Determine if staffing changes need to occur.



Training & Readiness

- Assess how associates, agents and/or insureds may be affected by the changes.
- Identify and plan any required training.
- Conduct an assessment to gauge the organization's readiness from a sponsorship, culture, skills and structure perspective.

Change management, learning & development, and business unit leadership will need to be part of this assessment and planning exercise.

You'll need to need to communicate openly with staff. If they understand how migration will affect them, they're likely to take more personal ownership of the journey and therefore increase the organization's odds of success. Failure to properly support and encourage employees is likely to result in resistance, underskilled and unwilling staff, and cost overruns and delays.

As execution progresses, we recommend you communicate the benefits of migration to your agents and policyholders.



Experience-based insights: Cyber Security

Provide a holistic understanding of how cyber security capabilities play an important part in driving business enablement, maintaining technical and operational resiliency, and fostering digital trust in the cloud

Driving Business Enablement, Operational Resilience, and Digital Trust

Any conversation about the Cloud inevitably includes cyber security and how the organization can better protect applications, data, and the broader ecosystem. While appetite to move to and investments in the Cloud have increased, we understand that it can be difficult to comprehend the scope of security capabilities required to protect the business in the cloud.

To know where you stand and accordingly make a convincing case, you should assess your cloud security architecture from the perspectives of application & integration, data & privacy, identity & access management, and architecture engineering & hardening. Key areas to focus on early in the process include



Application & Integration Security

- Evaluate in-place capabilities for perimeter protection of cloud applications and infrastructure.
- Determine if defined architectural patterns - like secure API standards - are enforced and monitored..



Data Security & Privacy

- Enable encryption and data management capabilities that support cloud applications
- Evaluate how data is classified, tracked, and protected based on organizational, legal and regulatory requirements.



Identity & Access Management

- Integration with a centralized IAM governance and lifecycle management solution to support Cloud services.
- Assess how well you support customer identity and access needs.
- Use of adaptive authentication to protect cloud applications



Architecture Engineering & Hardening

- Validate that cloud infrastructure and services architected for security
- Determine if you've securely hardened your applications and cloud services to meet risk and customer needs.

Starting your Cloud journey the right way

After your organization has adequately assessed its readiness for a Cloud transformation, you'll be ready to mobilize your business and IT departments. This may seem familiar to you given that they'll mobilize in similar ways as on traditional transformations, but there are unique considerations for Cloud programs.

PwC's Fitness Framework helps your business and IT teams determine key objectives and will prepare your organization for the Cloud implementation journey.

Unique areas to consider when mobilizing a Cloud program

While Cloud-centric environment logistics may be simplified in some areas (e.g., flexibility in allowing team members to work remotely; streamlining of infrastructure and DevOps processes), there are areas where Cloud migration will be complicated.

For starters, the technical architecture assessment will identify areas where new solutioning and design may take place. To transform future state architectural diagrams into reality, your teams will need to create a Cloud-specific delivery model and governance structure. Notably, there may be enterprise groups, such as security, infrastructure, and release management, that need to be more heavily involved from the start. However, establishing the proper interaction model and delivery agreements at the start of the journey will reduce program risk later on.

Resources will require a set of Cloud skills and training prior to the start of the implementation phase. As part of the human capital analysis, you should identify how many additional certified Cloud experts you'll need to deliver the program. Guidewire training usually adds one to two additional weeks - and sometimes more - for Cloud-specific courses.

Lastly, your program management team will need to be able to respond to risks and challenges of Cloud implementations down the road. A variety of potential delivery risks, budget concerns unique to Cloud, and Sprint planning intricacies means your program management team will need processes and frameworks that can flexibly account for these potential issues. For example: How do we handle security challenges? What happens if Cloud servers are down during implementation?

Lessons that we have learned along the way

PwC's experience in leading cloud implementations have had their own fair share of learnings along the way, and many of those challenges are best resolved during the mobilization phase.

With new requirements around human capital being an area with notable change from traditional core transformation programs compared to Cloud transformation programs, it is especially important to set the expectations early with your integration partners on the number of certified resources they will bring. In addition, dedicate time to clearly communicate roles and responsibilities to all parties to avoid misalignment when it comes to execute.



In summary: How to start the journey on the right foot

Remember: migrating to the Cloud is a step, not a leap. You'll likely need to spend significant time migrating or going straight to Cloud. Beyond core systems, there are other key areas to target in order to increase confidence in the transition and build on early momentum. In particular, you should focus on your architecture, people and cybersecurity. Through early planning and by preparing your employees for the transition, you can make good progress.



Contact

Imran Ilyas | Partner

+1 (630) 699-0657

irman.imran.ilyas@pwc.com

Tirath Desai | Director

+1 (972) 904-1947

tirath.desai@pwc.com

Samit Bhandari | Director

+1 (312) 608-6996

samit.bhandari@pwc.com