Migrating Applications To The Cloud

Risk Management and Compliance Considerations

January 2015
Executive Summary and Key Takeaway

Moving Line of Business applications (LOB apps) to a Platform as a Service (PaaS) Cloud environment is often a slow and complex process, particularly around the re-factoring and re-building needed to take advantage of new Cloud service capabilities. Nowhere is this more true than related to the application level S/IAM* controls needed for PaaS and to mitigating risks associated with the deployment, configuration and monitoring of PaaS-based apps.

For a large Enterprise, there can be hundreds, if not thousands, of LOB apps that need to be assessed for Cloud readiness in on-premises environments, remediated against PaaS standards, migrated and tested, and be monitored once moved to PaaS. There are three key questions IT Executives are asking related to the adoption of PaaS:

1. What are the Enterprise standards for PaaS and app-level settings based on Cloud S/IAM policies and best practices?
2. How do we know if LOB apps, once re-factored, or built from the ground up, will be in compliance once deployed?
3. As Cloud environments are evolved by CSVs, apps are enhanced by developers, and/or controls are updated due to emerging threats, how will compliance “drift” be monitored, reported and remediated quickly?

Key Takeaway: The magnitude of the migration effort, complexity of both LOB apps and PaaS environments, and the requirement for ongoing app-level monitoring suggests the need for what Gartner calls a “programmable security infrastructure capable of supporting security policy ‘toolchains’. “ This paper details this need along with the UnifyCloud LLC approach and solutions to address key migration and IT Risk Management questions around PaaS.

* Security and Identity & Access Management (S/IAM)
The movement to the Cloud is accelerating and evolving...

The adoption of 3rd party applications delivered through the Cloud as Software as a Service (SaaS) solutions, often by Enterprise business groups other than central IT, and through the use of primarily outsourced, yet scalable, VM-centric Infrastructure as a Service (IaaS) environments were the first waves. These waves were about utilizing “born in the Cloud” services and/or “lifting and shifting” low criticality applications. What is next?

The next wave will bring us to the tipping point in Cloud utilization through the re-architecture and re-building of more critical LOB apps to take advantage of the real power of the Cloud...Platform as a Service (PaaS). Once potential candidate applications for PaaS have been discovered and assessed, the task of migration begins. It can be a slow, tedious and complex process, particularly related to IT Risk Management and Compliance. How soon will this next wave hit? Some suggest a lot sooner than many IT Executives expect.

The next wave of utilizing PaaS has clearly arrived and it brings with it both unique opportunities and challenges.

Public Cloud services will grow at over 7X the rest of the comparable market and that Public Cloud services will account for 17% of IT product spend by 2016 up from 7% in 2011.

Source: Accenture

The worldwide enterprise market for PaaS platforms will grow from $900M in 2011 to $2.9B in 2016, a 26.6% rise each year.

Source: Gartner

PaaS adoption went from 7% of respondents in 2011, to 41% currently (2013), and will rise to 62% by 2016.

Source: GigaOm Research
Gartner considers PaaS as “Transformational” over the next 2 to 5 years (as of July 2014). PaaS is more than a collection of outsourced infrastructure services that can support legacy apps tweaked for the Cloud. PaaS can provide the building blocks for innovative, new scenarios.

New PaaS services, such as Azure Data Factory, will provide on-demand, highly scalable capabilities that developers can utilize in ways they had, heretofore, been unable to imagine or that require a set of capabilities unavailable in traditional on-premises computing services or infrastructure.

PaaS allows developers to add S/IAM controls through services such as multi-factor authentication, data protection, and security capabilities (e.g., Web Application Firewalls).
From an IT Risk perspective, PaaS is not just fewer things to be managed...

One way to look at PaaS is in comparison to Infrastructure as a Service (IaaS) in terms of who (customer/client vs. Cloud Service Vendor) manages what. This perspective suggests that the customer/client only has to be concerned about managing their own applications, data and user access, leveraging the services available on the platform. This typical view masks reality.

The PaaS subscription administrator, often a developer who owns the LOB app, must determine which PaaS services need to be provisioned, configured and monitored. Yes, the PaaS CSV will manage those services in terms of availability, basic infrastructure security and scalability, but the app owner now has certain operational responsibilities that are new. That can be a lot.

As an example, Microsoft’s Windows Azure portal lists some 30 Cloud Service offerings in four major areas: Compute, Storage, Network and Application Services. Once sub-Services are considered (e.g., Storage: Blob, Storage: Table, Storage: Queue) the number is closer to 60...each with many configuration settings and sub-settings the developer now owns as well. For PaaS, this can be well over 300 settings. Not an issue, just a lot.

Source: DevOps.com
Moving to PaaS as an operating environment does change IT processes...

There is a point of view that suggests that the emerging practice of DevOps is enabled by the nature of deploying, configuring and monitoring PaaS components. As DevOps.com notes, “for core components that make up a delivery pipeline, each of the components need to be available as a service, in order to provide a complete ‘DevOps on PaaS’ solution,” as depicted to the right.

Whether planned for organizational adoption or not, elements of the DevOps philosophy become realities in a PaaS environment where a developer makes more Infrastructure decisions and has more IT Risk Management responsibilities than previously. Many developers are not Infrastructure, Security or Compliance SMEs in the first place.

Recent Gartner research, “DevOpsSec: Creating the Agile Triangle”, points to this issue, “Cloud operating models embrace the notion of DevOps, which, among many things, means the tearing down of silos between development and operations. However, DevOps cannot be successful if security is not an integral part of the vision.”

Source: DevOps.com
Whether DevOps-driven or not, Security and Compliance are critical to PaaS...

While the leading PaaS vendors report on the controls guiding their services as attested to by their auditors (e.g., SOC Reports), PaaS users are still responsible, all-up, for managing the risks associated with PaaS as well as managing the apps that run on it. PaaS users typically must manage:

- Compliance with applicable laws/regulations.
- Determining and implementing encryption for data.
- Determining the services configurations.
- Backup of data to local / Cloud storage.
- Security Development Lifecycle for applications.
- Application QA prior to moving to Cloud production.
- Monitoring the security of applications.

As Gartner notes in “Hype Cycle for Cloud Security, 2014”:

“The potential benefits of cloud services can be enticing, but with reward comes risk. The enterprise must decide whether the potential risk is within acceptable limits.

“The trick here is to develop a system that can make the cloud compliant and that can prove the compliance of individual customers during an inevitable compliance audit.”

“Current and potential cloud customers must avoid the trap of ‘cloud complacency’: assuming that anything that's as easy to use as a cloud-based service must automatically be secure and reliable.”
“Determining the Services configurations” is a new area for most Dev’s...

As LOB app owners / developers start to define, deploy and configure PaaS component Services, they need to think about... Which settings are most appropriate? What additional Cloud control services are needed (e.g., encryption, firewalls, backup)?

IT Executives will also have questions about the risk of the entire “system” including that part managed by a CSV but configured by a developer, and that part that sits on top of PaaS. These questions can include:

1. What are the Enterprise standards for PaaS and app-level settings based on Cloud S/IAM policies and best practices?
2. How do we know if LOB apps, once re-factored, or built from the ground up, will be in compliance once deployed?
3. As Cloud environments are evolved by CSVs, apps are enhanced by developers, and/or controls are updated due to emerging threats, how will compliance “drift” be monitored, reported and remediated quickly?

Source: Microsoft
The process to target, remediate, migrate and monitor PaaS apps is complex...

Not every LOB app can, or should, move to a PaaS environment. Some factors include:

- Retirement date
- Application type
- Control and ownership
- 3rd Party SaaS alternatives
- Dealing with MBI and HBI data
- Mission criticality requiring BCDR
- Hardware dependency (e.g., POC systems)
- Software dependency

For those selected LOB apps once moved to PaaS, there can be “drift” regarding compliance against a baseline of controls that have been established. This is particularly true regarding a baseline of S/IAM controls established by a CISO’s organization. As noted by NIST, “Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing... A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.”
Given this complexity, UnifyCloud has developed tools to support migration...

**Controls & Settings Knowledgebase / Repository - “Navigator”**
A Cloud database of information for developers related to moving applications to a PaaS environment. Key functionality: Contains cloud-based application development best practices; recommended PaaS settings for individual services based on Enterprise policies; and suggested remediation (scripts, sample code) to efficiently re-factor applications to run effectively in a PaaS environment.

**App Readiness Assessment and Remediation - “Validator”**
A tool to validate the On-Premises application before migration to a PaaS environment. Key functionality: Detecting app issues that could be remediated before moving to PaaS; reading database scripts to provide details (e.g., is a database eligible for moving to PaaS); identifying network related settings to validate recommended PaaS settings; and checking all Security compliance requirements.

**Final Cloud Compliance Verification - “Test”**
A highly automated testing tool for apps being moved to Azure. Key functionality: Tests the application after it is remediated and before it is moved to a PaaS staging environment. Similar to Validator, but more focused on Pass / Fail than remediation.

**Compliance Monitoring and Reporting - “Cop”**
A Cloud-based service to monitor compliance within a Cloud Subscription. Key functionality: Current configuration settings drift analysis against original settings and Enterprise IT recommended settings; ability to fix configuration settings to realign to IT recommended settings; PaaS Service and Security settings drift report; and monitoring data sharing across multiple PaaS subscriptions.
Enterprise standards: Navigator guides app remediation and migration...

Establishing the S/IAM controls and preferred service settings for PaaS is a critical first step in adopting a Cloud environment for LOB apps that are important to the business. These need to be consistent with the Enterprise IT Risk Management goals and objectives.

Once established, these controls and preferences are meant to help developers assess both app readiness and the viability of re-factoring apps to run on a PaaS environment. They will serve as a foundation for the remediation and migration processes. Navigator serves as both a data base for scanning candidate apps before and after migration as well as a knowledgebase for developers to search for PaaS best practices.

Navigator will be the authoritative repository of these Cloud controls and settings that are maintained, over time, by the Enterprise as PaaS environments are enhanced, apps change and the threat environment evolves.

Key Features:
- Best-practice guidance for PaaS settings in general and specific to configuration settings impacting security.
- Enabler to ensure the same setting in PaaS test and production environments, resulting in faster and easier security compliance, security configuration, and migration.
- Centralized, automated configuration settings and security baseline management.
- Effortlessly stay up-to-date with configuration settings and security configuration recommendations from SMEs.
- Configuration setting search.
- Export and import settings in development, test, and production environments.
- Role based access controls.
- Historical data for changes to configuration settings.
For certain app patterns moving to PaaS, a cookbook approach is of value...

In addition to serving as the database for Enterprise recommended PaaS settings and S/IAM controls, Navigator serves as a searchable knowledgebase and the foundation for developer-focused “cookbooks” that contain:

- Applicable Scenarios
- Configuration Settings
- Security Settings
- Tools and Scripts
- Performance and Scaling
- Business continuity
- Management and monitoring
- Troubleshooting the issues
- Things to consider / Checklists
- References and Resources
Beyond a change checklist, Validator can make PaaS migration easier...

To take advantage of PaaS, apps need to re-factored and moved. First to a PaaS staging environment where the configuration and app remediation can be tested.

The database of PaaS controls and settings used during discovery, assessment, and remediation should be the same as those used in the final test.

This architecture addresses one of the drivers of DevOps, ensuring consistency across Dev, Test and Prod environments.
Validator is helpful in determining the PaaS services for an app...

Certain apps follow basic patterns (e.g., Web, Mobile) that define and consume network, compute, storage and other app services. By understanding these patterns through scanning technology, the UnifyCloud validation tool can create a Cloud Map for a set of PaaS services.

Through the use of the Navigator repository database, Validator can both recommend the appropriate settings as defined by a central, Enterprise IT group, as well as guide the provisioning of PaaS services, appropriately configured, as well.

The value of this validation tool includes:

- Automating remediation, to the extent possible, through a combination of scanning, best practices, and custom questions;
- Requiring only light participation with app owner / developer resources; and
- Bringing together assessment, discovery, and target Cloud architecture.
Validator is needed to efficiently and rapidly remediate apps for PaaS...

With 1000’s of LOB apps in today’s modern Enterprise, the effort to discover and assess apps for possible re-deployment in a PaaS environment can be daunting for developers who already have more than enough to do.

Yet, data is available about the apps that can be interrogated and evaluated against PaaS capabilities based on a set of baseline app patterns. From this analysis, app owners can quickly determine the level and nature of the remediation required. And, IT management can see the effort and cost of this remediation.

Validator can be used by a centralized Program Management team, working with app owners/developers to only require scarce development resources when certain elements of the app need to be rebuilt. Further, the Navigator database can provide a baseline of scripts and sample code to increase the automation.
Understanding the “As Is” app architecture vis-à-vis PaaS is a critical step...

To start the Validator process, PaaS candidate apps need to go through an analytic step where the architecture and functionality is exposed in order to determine what PaaS services need to be provisioned.

In addition, any specific changes that need to be made to the app to run efficiently in a PaaS environment, or, in some situations, to run in PaaS at all need to be discovered.

Using code scanning, operational data from a CMDB, and/or information gathered from the app owner Validator will provide a clear “As-Is” picture from which to remediate.
The architectural needs of the app can be translated into PaaS services...

Once the As-Is architecture and functional aspects of the candidate PaaS app is determined by Validator, then using Best Practices for Cloud app architecture, Cloud coding practices, and PaaS service definitions...the To-Be architecture can be determined.

This architecture and PaaS service requirements will provide the app owner a high level view of the provisioning requirements that need to be ordered through the PaaS Management Portal.
Beyond architecture, a granular roadmap for PaaS provisioning is needed...

Once the Cloud architecture is understood and PaaS services are identified, then developers need to:

- a) configure their PaaS services to meet the app requirements and meet Enterprise Cloud Configuration Standards; and

- b) determine the specific changes they need to make to the app before moving it to a PaaS environment.

Validator provides the technical roadmap through the use of graphical outputs along with detailed technical specifications.
...along with a detailed application re-factoring blueprint...

Developers need to know, in a detailed way, what specific changes the app requires. A simple Go / No Go diagnostic is of little value.

Developers want to know where to make changes and why, be provided detailed recommendations (e.g., sample code), and what the level of effort likely will be to re-factor an app to run in a PaaS environment.

For the Enterprise, having a consistent set of Best Practices regarding Cloud-hosted apps will further drive standardization.
Assurance of compliance is needed before a final move to PaaS...

Whether Validator is used to remediate an app or it is a result of a non-automated effort by a developer, the LOB app needs to be tested against the Enterprise baseline service settings and S/IAM controls before deployment. The key is to use the same underlying PaaS knowledgebase in Navigator as a foundation for a basic Go / No-Go decision to move forward with the final move to PaaS. The Test tool provides this final review before PaaS deployment.
Once deployed, compliance must also be assured through a dashboard...

The PaaS environment, given its competitive nature with many CSVs vying for business, will continue to evolve as CSVs aggressively enhance their platforms with new capabilities.

While these new capabilities will add value to the business and enhance the apps that run on these environments, these new capabilities can come with risks that need to be assessed.

Cloud risk assessments can, over time, require changes to the original app-level PaaS settings and how S/IAM controls are enabled. This can create compliance “drift” in PaaS-based apps that must be discovered. Discovered first and then remediated back into compliance.
App owners need to manage compliance quickly and efficiently...

While a CSV’s standard management console can provide a basic overview of PaaS services and whether they are running or not, the key is being able to drill down to the setting and control level quickly, determine where the “drift has occurred, and fix the problem efficiently to assure compliance.
UnifyCloud’s tool architecture is Cloud-based at an Enterprise or BU level...

- **Controls & Settings Knowledgebase / Repository**
  - CMS
  - Enterprise Service
  - Business Unit Service with recommendation refinement ability.

- **Subscription Service**
  - Tools / scripts
  - Cookbooks
  - DB of Settings
  - Subscription agnostic
  - Knowledgebase update when tools are run in app(s) subscription

- **Enterprise Dashboard**
  - Optional reporting to central dashboard set by App Owner

- **Cloud App in Test / Prod**
  - Tool and thin DB downloaded to validate code
  - Tool and DB run as a Service to monitor settings and code within Test or Prod subscriptions
  - Tool and DB run as a plug-in to Visual Studio against PaaS Config File

- **Final Cloud Test**
  - On-Prem App
  - On-Prem App

- **Readiness Validation**
  - If present, update will occur with subscription-based tools associated with business units

- **Monitor Compliance**
  - App Owner UX

UnifyCloud’s tool architecture is Cloud-based at an Enterprise or BU level…
UnifyCloud has developed an app migration solution for use in PaaS...

UnifyCloud’s Mission is to drive the adoption of cloud-based services through the implementation of effective Enterprise-grade S/IAM controls and Cloud app development Best Practices. These controls are to be realized as:

- Native in a CSV’s IaaS / PaaS platforms (e.g., AWS, Azure)
- Configurable by the subscriber (i.e., customer IT)
- Provided by a 3rd party Cloud service (e.g., Barracuda)
- Delivered by a custom application/service (e.g., UnifyCloud)

The solution described in this document is currently being developed for a major technology company’s central IT group as an Alpha solution. The module names “Navigator”, “Validator”, “Test” and “Cop” are working names to convey the general functionality of the tools within the suite.

For more information on UnifyCloud LLC, our Cloud-focused consulting services, or the tools described in this document please contact:

Norm Barber, Managing Director; UnifyCloud LLC
normb@unifycloud.com