ABOVE PROPERTY SYSTEMS CHECKLIST

Version 1.0

Publication Date: 1 June 2017

About HTNG

Hotel Technology Next Generation (HTNG) is a non-profit association with a mission to foster, through collaboration and partnership, the development of next-generation systems and solutions that will enable hoteliers and their technology vendors to do business globally in the 21st century. HTNG is recognized as the leading voice of the global hotel community, articulating the technology requirements of hotel companies of all sizes to the vendor community. HTNG facilitates the development of technology models for hospitality that will foster innovation, improve the guest experience, increase the effectiveness and efficiency of hotels, and create a healthy ecosystem of technology suppliers.

Table of contents

1 Overview

For the purposes of this document, "Above Property" is defined as any system that is deployed outside of an individual hotel data center (this includes systems that only govern one hotel, all the way up to a system that governs an entire chain); this includes all typical X-as-a-service offerings (software, infrastructure, platform, etc). This may also include systems that have both "on premise" equipment (such as POS terminals), and a centralized processing service (housed in vendor data center, or Azure, or AWS, etc). Further, this document will include guidance or questions related to on-premises infrastructure required to support these applications.

This documentation is meant to help hoteliers and vendors resolve questions related to the deployment and selection of above property systems. Additionally, hoteliers need guidance on the appropriate questions to ask if "above property" systems providers, as selection criteria for above property systems, are different from on-premises solutions.

The following checklist depends on the hotels having existing policies, including:

- Data retention

- Data security

- BYOD policies

- Network security

Hoteliers without adequate IT knowledge should note the complexity and many details involved with moving to the cloud. If you do not have significant understanding of the details in this document, you should engage a consultant to understand the implications of the following guidance or answers to questions.

2 Document Information

2.1 Document History

Version	Date	Author	Comments
0.10	15 October 2017	Patrick Dunphy, Matthew FitzGerald, Nicole Wlasichuk	Outline Created Based on Workgroup Discussions
0.15	1 November 2016	Eric Sullender	API Updates
0.25	14 November 2016	Jai Govindani	Hosting Updates
0.40	20 December 2016	Thomas Nievergelt	Training, Identity Management Updates
0.50	10 January 2017	Jai Govindani	Business Considerations, Scalability, Scope, Continuity Updates
0.60	23 January 2017	Nicole Wlasichuk	Business Considerations Updates
0.70	17 February 2017	Jeffrey Parker	Financial Considerations Updates
0.75	25 February 2017	Brian Alessi	Security, Monitoring, Testing Updates
0.85	21 March 2017	Jeffrey Parker	Reporting Updates
0.90	7 April 2017	Jeffrey Parker, Jay Swearingin, Patrick Dunphy	Security Updates
0.95	13 April 2017	Jeffrey Parker	Introduction Updates
0.98	1 May 2017	Emily Wilson	Copy Edit
0.99	3 May 2017	Patrick Dunphy	Final Cleanup in Preparation for Vote
1.0	1 June 2017	Workgroup	Approved and Published to HTNG Members

3   Business Considerations

3.1 General Considerations

Hosted or true cloud environments typically have a much quicker restore option. In cases such as revenue management issues, which require a restore is feasible where on-premises issue may take so long to restore that it is infeasible.

- **Connectivity / Stability of Connection:** Since cloud systems rely on internet access, hoteliers need to evaluate back up plans, offline capabilities and have a very strong set of standard operating procedures during any offline instances. Consider the cost and lost revenue if service goes down and the data becomes inaccessible or standard procedures cannot happen (reservation, POS, etc). Ask about offline services that can allow staff to continue to work and get the data synced once back online.

- **Bandwidth/speed:** Ability for multiple users to connect at the same time without sacrificing speed.

- **Mobility:** On-premises systems generally provide access onsite and from a static location. Cloud offerings generally provide access from anywhere at any time. Consider both the benefits of mobility (check-in, housekeeping, reporting) and the potential risks (accessing data for illegal/criminal use).

- **Control and ownership of data:** Moving to the cloud requires different agreements around the ownership and control of data. A hotelier, franchisor or brand must always be the owner of the data, be in control of the data format (so it can be accessed/consumed by other proprietary systems), have 24/7 data access and be able to easily remove the data in an acceptable format for specified reasons (i.e. contract ends).

- **Data transfer:** Determine what is required to transfer your data into the cloud. Consider what needs to move, what preparation needs to be done (do you have the resources to scrub/prep data), who will move it, what are the risks, what (if any) costs are involved?

- **Transition period:** During the transition to the cloud, what (if anything) will be inaccessible and for how long? Consider guest/reservation data, external connections/channels (i.e. OTAs) and internal connections/channels.

- **Data privacy and protection:** Is your hotel in a region that has specific regulations around what data can reside where? Make sure your cloud provider is aware of these and can demonstrate they follow any legal requirements for both your locale and any customers who are protected by regulations of other locales. Ensure all channels that transmit data are highly secured (i.e. tokenize data prior to transmission).

- **Staffing:** What happens to any current IT staff? Do you need different skillsets?

- **Device policies:** Do you have a mobile device policy (i.e. BYOD, hotel provided kept onsite)? To enable mobile access to the above property system, staff will need mobile devices and policies must be in place.

- **Upgrades:** As the product is upgraded, updated, and/or receives new features, how and when do you become aware of them? What is your training plan?

- **Training**: Operational changes should occur at the hotel for staff to take advantage of mobile access in order to better assist guests and become more efficient. At the same time, staff must be better trained on the care and caution of how that access must be treated (i.e. data security/privacy).

- **Mobile Guest Access:** Does a move to a cloud-based technology allow you to openly access tools directly to guests (i.e. book spa or restaurant appointments on their own)? How this would be managed? Who would support it?

- **Data sharing:** A hotelier with more than one property may now be able to share data across properties more easily. Consider how this might be done – what can be shared, what should not be shared and procedures around 'ownership' of a guest.

3.2 Financial Considerations

Cloud Systems are typically paid as a service versus a software asset, this can dramatically change budgeting and tax implications for the hotels.

Traditional 'On-Premises' systems are paid upfront and typically capital dollars are used for this purchase. Capital Expenses (CapEx) can be considered assets, and can fall under certain recording and taxing guidelines. These guidelines allow the costs to be differed or 'written-off' in a manner that can be beneficial to the operation. Additionally, these CapEx can often be leveraged as a part of a loan or another financial vehicle that is not available to services.

Cloud or Hosted solutions are subscription-based, meaning a bill is paid at some interim agreed to in the contract. These Operational Expenses (OpEx) are due as long as the subscription is in contract and the software is being used. Unlike CapEx, there is no period where the operation uses the program and does not continue to make payments, so the service cannot be treated as an asset. In short, payments cease and access to the software is discontinued.

- These differences have dramatic financial impact because they cannot be differed in an economic downturn that CapEx/Asset purchase often can be.

- Hardware, if needed, can typically still be treated as an asset.

- Understand how updates work when you are in a cloud environment. While most solutions include patches and upgrades as part of the subscription, not all do. Also, if there are 'major' updates, a professional service fee to migrate to the newer software could be charged.

- If you are auto-scaling, refer to the scalability section. It is important to know how this can impact your monthly or annual costs.

3.3　Continuity

Continuity considerations affect how your hotel will continue operations in the event of a system, connection, or cloud-related outage. The questions below will help you understand how the service provider handles outages.

Consideration(s)	Response from Provider
Have you considered what your acceptable downtime is? If no downtime is acceptable, then you need redundant ISP connectivity, power back up, etc.	
Is the service or application available in an offline or degraded functionality in case of an outage?	
Have you considered acceptable service interruption levels, including duration, functionality, degradation vs. actual downtime?	
Is it clear to you and the provider regarding what constitutes downtime?	
Is it clear to you and the provider regarding what constitutes partial downtime? For example, is downtime considered partial if you are unable to process credit card transactions, but still check guests into the hotel?	
How is downtime measured, and what time frame is it measured across?	
Have you considered redundancy designs for your internal network to ensure application access?	
Does your provider have a plan for a regional-level disaster scenario?	
How does the provider communicate an outage? Is this communication part of an SLA?	
How does the provider handle communications at different severity issues?	

3.4 Vendor Management

Moving to an above property system places greater emphasis on vendor management. Hotels need to ensure that service providers are trusted partners.

Consideration(s)	Response from Provider
Have you and the provider agreed on which groups of staff and support meet under certain circumstances? For example, there should be an established point of contact for high severity issues.	
Have you established a point of contact on your staff across various knowledge domains including: security, development, implementation, general account management and help desk?	
How are contract changes made?	
How are multi-vendor issues coordinated? Does the provider have demonstrated experience with root-cause analysis?	
What other vendors does the provider partner with to deliver ancillary services?	
Does the provider produce adequate documentation regarding their services, process, and architecture?	

3.5 Testing

As with any software or hardware acquisition, thorough testing will ensure a smooth transition. The following considerations will help identify key areas to test.

Consideration(s)	Response from Provider
Have you established your testing requirements prior to moving the system into production?	
Is the provider willing to provide a proof of concept deployment?	
What are any limitations to a guest or test environment in comparison to a live or production environment?	

Are updates available to customers in a limited fashion prior to being rolled out across a large installation?	

3.6 Data Ownership

Data ownership is an important consideration in the franchise environment. Hoteliers need to clearly understand data ownership in the cloud.

Consideration(s)	Response from Provider
How does the vendor structure data so that information is compartmentalized and separate from other customer's (customer of the vendor) data?	
What compliance issues are at stake that require data segregation?	
How does the vendor handle roll–up reporting across multiple properties?	
Does the vendor have open and easily accessible data structures for extraction?	
Does the vendor have a defined process for pulling data out of their product?	
Does the hotel (customer) know and understand what data is important to be extracted?	
Does the hotel have a data retention policy that affects extraction or moving to another provider?	
Does the vendor use the data for aggregation purposes? What does the vendor do with your data, outside of provide access to the customer/hotel?	

3.7 Regulatory Issues

Moving to an above property system may transfer some responsibility for regulatory compliance to the service provider, but hoteliers still need to ensure that their systems meet requirements. The following considerations should be thoroughly reviewed to ensure compliance in a complex regulatory environment.

Consideration(s)	Response from Provider
Is the provider within PCI DSS scope? If so, has the provider attested to compliance?	
Has the provider accounted for individual regulatory regimes across municipalities, regions and/or countries?	
Are you, the customer, aware of the same regulatory issues? Have you communicated these requirements to the provider?	

3.8 Training

Training will ensure a smooth transition to a new service. Often, training is overlooked and neglected in a technology deployment.

Consideration(s)	Response from Provider
Is a dedicated training environment available?	
What types of users have training available to them?	
How is training documentation and support provided?	
Can you track which users have taken training, through a learning management system?	
What online support is available to the end user?	
Is training included in the service contract?	
Is in-person training provided?	

4 Technical Considerations

4.1 Hosting Considerations

Above property or cloud systems transfer some technical burden to the service provider. However, due diligence is required to ensure the service provider has adequate hosting facilities.

Consideration(s)	Response from Provider
Where is the data hosted? Is it in a single facility accessed from around the globe or are there multiple active data centers?	
If a single data center is used, how does the vendor handle jurisdictional restrictions on data movement?	
How is system failover handled?	
Does each data center have its own disaster recovery facility?	
What tier is the data center class?	
How are hardware replacements and refreshes handled? Is there an obvious end-of-life schedule for data center components?	
How is licensing handled for system components? This could include OS, utilities, or other application software.	
How is load balancing and distribution handled?	
How is patch management handled?	
How are security updates handled? How are unscheduled, or critical security updates handled?	
Are vulnerability scans regularly completed and remediated?	
Are penetration tests regularly completed and remediated?	
How is data segregated across tenants and customers?	
How is physical security handled in the data center?	
How does the system scale for additional users, customers, or guests?	
How does the system handle unbalanced loads across tenants? Will another customer's usage cause a bottleneck for my hotel?	

Is the system virtualized, containerized or made of physical servers?	
Are there any options for dedicated bandwidth for my needs?	

4.2 Scalability

Hotels should appropriately plan for capacity to ensure that costs do not inappropriately increase due to predictable circumstances. For example, night audits may increase PMS usage, but this should be accounted for during capacity planning stages. Other semi-regular or planned usage may include:

- Reporting (revenue management) also may increase system load
- Data pulls, batch files, import/export functionality may also increase system load
- Large group check-in
- Large batch operations/interfaces such as night audit, revenue management or major inventory loads
- Note worldwide scheduling: Different hotels operate night audits at different times during the 24-hour worldwide clock, so scaling may be cyclical and occur at many different times relevant to the application time

Advanced features and planning may include major operations (such as batch operations) would be best in a parallel environment to reduce load on the production system, and then synchronize to production when complete.

Applications should preferably scale in the region where demand increases to reduce latency.

Content Distribution Networks (CDN) may be appropriate in high-load situations where static content is in high demand, or where guest-facing components (i.e. TVs, signage, guest portals, etc.) need to be highly available.

Careful consideration is due for regional issues with CDNs (hoteliers should know their options). Hotels (or groups of hotels) in different regions are particularly susceptible, but individual hotels may have no need for a CDN.

Consideration(s)	Response from Provider
Does the application have a proven scalability track record in the market that matches your business growth trajectory?	
Based on the business' current size, would you be a low/medium/top tier user?	

Has proper sizing of requirements/resources been done to ensure that disruptive scaling (that would involve downtime or additional cost) will happen predictably and at intervals not disruptive to the business?	
What is the downtime associated with scaling capacity, and has this downtime been deemed acceptable?	
Will there be an additional cost for increased server capacity or additional software licenses?	
Optional: Does the application semi-autonomously add capacity (CPU, memory, bandwidth, VMs etc) as needed? If the application doesn't inherently support it, what is the company's plan to add capacity?	
Can the provider support your business time thresholds?	
Can the provider support your SLAs for normal operations?	
Can the provider support your SLAs for disaster recovery scenarios?	
Where does the provider's responsibility end and the customer's begin?	
How is latency measured?	
How is latency and performance monitored and reported?	
What penalties exist if an SLA is not met?	
What caching strategies are in place? If any, what data and how much of it is cached?	
To what extent can the system environment scale? Is there a limit to the number of users, amount of data, bandwidth?	

4.3 Identity Management

Identity management is important in any technology deployment. The proliferation of cloud services places additional emphasis on a centralized identity management strategy, and Single Sign On (SSO).

Consideration(s)	Response from Provider
What type of identity management solution is provided?	
Is Single Sign-On (SSO) provided/supported? What types of SSO options are available? SAML, HTTP-Fed, OAuth etc?	
Can the SaaS app be integrated with an existing Identity Management system?	
What type of user store is available? Can this user store be integrated with Active Directory or any other user store database?	
What type of user security, authentication and authorization options are available?	
How is primary authentication and application specific user role managed?	

4.4 Security

Hoteliers should thoroughly evaluate the physical and cyber-security capabilities of any service provider. The following questions should be carefully reviewed and verified with any potential partner.

Consideration(s)	Response from Provider
Does the facility and solution conform to all applicable PCI DSS standards? This may include security patching, vulnerability testing, penetration testing, remote access/password policies, access to protected data, encryption, storage & logging standards.	
Is the environment dedicated or shared/multi-tenant?	
If it is a shared environment, how is the data segregated from other customer data? What other security controls are in place to prevent unauthorized access?	
How is data structured and architected to prevent unauthorized access?	

Who has access to the infrastructure, hardware, software, data? Get specific information on the roles & responsibilities of administrators, profiles, hiring practices, etc.	
What application & data access audit logs are available? How often can you get this?	
How is the primary data encrypted? What encryption schemes are used? Who has access to the decryption keys? How often is this tested?	
Can the vendor provide a SOC II type 2 and or a SSA 16 or 18?	
How is the backup data stored? Is the data in raw files or encrypted format? What locations are the backup data stored in? Who has access to this backup data?	
What type of investigative support is provided in cases of breach?	
If the vendor is acquired, sold or dissolved, what options are available to get the data? Are there costs associated with it? How is the data wiped out of the environment?	

4.5 Change Management

A successful change management regime will ensure the success of an above property migration. Further, cloud partners should have a well-documented change management communication plan.

Consideration(s)	Response from Provider
How are software updates tested and deployed?	
What measures are taken to ensure backward compatibility with existing functionality and integrations?	
How are notices given and the options available for previewing/testing changes?	
Where (and what) are the past 12 months of product release notes for your product?	
What are your feature request and bug tracking methodologies, and what feedback will customers see on their raised issues?	

4.6 Monitoring

Proactive monitoring, by the hotel & the service provider, will ensure the above property system meets contracted expectations. Hoteliers should have a thorough understanding of the service provider's monitoring capabilities.

Consideration(s)	Response from Provider
What does the service provider monitor? How is it monitored?	
Can monitor thresholds be adjusted according to customer needs?	
Can third party monitoring systems integrate with the service provider system?	
Can the customer help desk team integrate with vendor provided monitoring tools?	
Is monitoring covered in any SLAs for the product?	

4.7 Reporting

Service provider reporting is an important consideration for hoteliers, and will help ensure that any contracted SLAs are met.

Consideration(s)	Response from Provider
What are the reports available in your application?	
Is the data in the reports real time or a summarization?	
Can the reports be retrieved on demand, via scheduled delivery and/or accessible via an API?	
What data formats are available?	
What are the minimum and maximum retention periods for reporting data?	

4.8 On-Premises Infrastructure & Devices

On-premise equipment may still be a requirement for certain types of cloud based applications. The following considerations will help hotels adequately plan for these devices.

Consideration(s)	Response from Provider
Are work stations needed on-site? What applications need to be installed for the solution to work?	
Are any workstation peripherals needed, such as a printer, scanner, or other input/output device? How are these devices connected (USB, networked, etc.)?	
Do workstations need to connect to a centralized command and control server before accessing the application?	
What network connectivity needs to exist between workstations, the application or backup systems?	
What impact will application usage have on my bandwidth through my ISP?	
Will the application require additional Wi-Fi or network coverage to ensure availability of the solution?	
Does the solution require any on-site equipment for offline access?	
What recommendations and best practices are available to secure the on-site equipment required for the solution?	
If applicable, does the application require administrative access to the local machine?	
Can access to physical ports be restricted to prevent data loss or unauthorized access on any required on-site equipment?	
Do I need redundant internet connections if no failover or offline capabilities exist?	

4.9 Application Programming Interfaces (APIs)

APIs are an important consideration in any software acquisition. Hotels have dozens of systems that need to communicate with one another.

Consideration(s)	Response from Provider
What are the service provider's available APIs? Where are they located? How are they documented?	
What connection methods, data formats, and retention mechanisms are used?	
What other systems do you have a demonstrable integration with?	
Can your service integrate with my existing PMS, CRM, POS or other strategic system?	
Does your system support or implement an enterprise service bus?	