Deciphering Total Cost of Ownership

Total Cost of Ownership, or TCO, is commonly defined as the estimate of all direct and indirect costs associated with an asset or acquisition over its entire life cycle. In the context of IT investments, TCO is traditionally broken down into three categories:

1. Direct costs of purchasing software and hardware.
2. Indirect costs of installing, operating and supporting the IT investment.
3. Direct costs of purchasing upgrades for new versions (average life cycle of three years).

Introduction

Increasingly, Human Resource Management Systems are considering Cloud-based as an alternative to traditional on-premise software. In comparing the two alternatives, they must analyze two different cost models: the monthly subscription-based of cloud computing offerings versus the up-front purchase and ongoing operating costs of on-premise software.

Consequently, the cost comparison between a desktop-based solution and a cloud-based or SaaS solution like HITS HRMS is not "apples-to-apples." Traditionally, people purchased a desktop-based software program faced a familiar acquisition model: an up-front purchase that varied based on the number of users, set-up and installation, and ongoing support and maintenance contracts for their particular version of the software package.

At first glance, decision makers assume that the ongoing feed associated with cloud-based software will surpass those of an on-premise solution over time. When examining all of the direct and indirect costs involved in an on-premise solution, however, it becomes clear that cloud-based HR management software offers a compelling, long-term cost saving over traditional desktop-based software.

Often, decision makers focus on the acquisition costs involved in making their purchase decision; in reality, each of the programs they buy require significant investments in terms of time and money for customization, installation, and ongoing operation, and these costs are just as much a part of the total cost of ownership for a new software product as the up-front purchase price.

Our goal in this whitepaper is to provide additional insight into the total cost of ownership of using HITS HRMS versus many of the existing HR management systems in the market.

HITS HRMS Cloud Model is not a desktop-based software program that requires installation, maintenance, and upgrades. It’s 100% web-based and runs on Microsoft Cloud. This means that both its software model and subscription pricing are paradigmatically different from traditional software norms.
Acquisition Costs

Acquisition costs for traditional technology investments can be divided into two categories: hardware purchases, such as servers and individual computer terminals, and software purchases, such as the CDs and license IDs for each user.

Each time a user upgrades their software version (approximately every one to three years) they essentially re-purchase the product and are subject to a new round of acquisition costs.

With HITS HRMS Cloud Model there’s absolutely no acquisition cost for the software, you only pay a monthly operating cost. Also, updates in HITS are implemented continually meaning no time-consuming upgrades for end-users.

Initialization Costs

In most cases desktop HR software are not immediately usable out of the box. They need to be installed, customized, and configured, thus requiring significant input from a consultant or as a part of the initialization process.

Once setup and installation are complete, users must then arrange to have their data migrated from their existing system to their new software program. This process is often charged in most cases.

With HITS CLOUD HRMS, installation and setup are as easy as creating an account and logging in. Data migrations are free. In conjunction, these factors make switching to HITS a “turn-key” operation – users sign up, we take care of the data migration, and users can focus on quickly learning and using HITS without delay.

Operating Costs

While acquisition and initialization costs are largely fixed expenses that require a one-time capital outlay for each new product purchase or upgrade, operating expenses are recurring fees that users must pay in order to run their HR management software. These can include fees such as support and maintenance contracts, required interim software upgrades, the operation of a data backup, regular outsourced IT support, and the energy bill for running the assortment of hardware their system requires.

These expenses are often overlooked when comparing the TCO of desktop software to SaaS alternative like HITS, but they are very much a part of the TCO equation and account for a significant portion of the expenses entailed in buying and running a desktop-based HR management system.

By using a SaaS model, HITS can offer an all-inclusive monthly subscription that is much more cost-effective than the operating cost associated with desktop-based alternatives. Users have unlimited access to HITS Support for support and maintenance questions. While HITS cloud-based storage system is a perfect geo-redundant data backup that lets users free themselves

Advantages of HITS Cloud - SAAS Model

- No Hardware... No Software Using Latest Microsoft Technology.
- “Pay-As-You-Go” Minimize Your CAPEX, Maximize Your ROI with HITS Cloud Methodology.
- Get Upgrade Is Periodically and Seamless.
- Adding Modules & Add-ons in Minutes.
- Get Support up to 24/7 From A Professional Consortium And Minimize the Headache of IT Administration.
- Eliminate Cost of On-Site Support.
- Enjoy Unlimited Bandwidth.
- Enjoy Rapid Deployment And Minimize The Headache of IT Administration.
- Implementation Including Corporate Standard and Best Practices as Per Market Industry.
- Keep Your Data Secured And Have Access To Your System Anywhere In The World.
- Starting By Monthly Subscription, Reduce The Budget Approval Cycle.
- THere's no initialization required – training, support, and data migrations are all included as part of the base subscription.
- No time-consuming in customizations and focusing instead on projects and improvements that provide a positive ROI for their clients.

The Cloud Provide Saving Up-Front Costs

By choosing HITS, new users are avoiding an array of up-front costs, including a variety of required hardware and software purchases, consulting, and IT support fees for initialization and training, as well as the costs associated with data migrations, which HITS provides free-of-charge.

Predictably, the total cost goes up with each year as there are ongoing and operational costs associated with each of the products. HITS low start-up cost, coupled with its low ongoing costs, tip the TCO comparison decisively in HITS favour.

Also predictably, the desktop software products are most expensive in the first year and trend downward over time. In contrast, the user fees for HITS stay constant year-over-year as the subscription price is fixed. Even after a three-year amortization period, the average cost per year for each of the desktop-based products remains notably higher than the SaaS like HITS cloud model.

The Cloud Provide Saving Up-Front Costs

By choosing HITS, new users are avoiding an array of up-front costs, including a variety of required hardware and software purchases, consulting, and IT support fees for initialization and training, as well as the costs associated with data migrations, which HITS provides free-of-charge.

Predictably, the total cost goes up with each year as there are ongoing and operational costs associated with each of the products. HITS low start-up cost, coupled with its low ongoing costs, tip the TCO comparison decisively in HITS favour.

Also predictably, the desktop software products are most expensive in the first year and trend downward over time. In contrast, the user fees for HITS stay constant year-over-year as the subscription price is fixed. Even after a three-year amortization period, the average cost per year for each of the desktop-based products remains notably higher than the SaaS like HITS cloud model.
Cloud Security Design

Windows Azure runs in data centers managed and operated by Microsoft Global Foundation Services (GFS). These geographically dispersed data centers comply with key industry standards, such as ISO/IEC 27001:2005, for security and reliability. They are managed, monitored, and administered by Microsoft operations staff that have years of experience in delivering the world’s largest online services with 24 x 7 continuity. In addition to data center, network, and personnel security practices, Windows Azure incorporates security practices at the application and platform layers to enhance security for application developers and service administrators.

Fundamentally, Windows Azure provides confidentiality, integrity, and availability of customer data, just like any other application hosting platform. It also provides transparent accountability to allow customers and their agents to track administration of applications and infrastructure, by themselves and by Microsoft.

3- Hardware Device Credentials Used by the FC

In addition to application keys, the FC must maintain a set of credentials (keys and/or passwords) used to authenticate itself to various hardware devices under its control. The system used for transporting, persisting, and using these credentials is designed to make it unnecessary for Windows Azure developers, administrators, and backup services/personnel to be exposed to secret information. Encryption based on the FC’s master identity public key is used at FC setup and FC reconfiguration time to transfer the credentials used to access networking hardware devices, remote power switches on the racks that are used to power cycle individual nodes, and other systems. The FC maintains these secrets in its internal replicated datastore (still encrypted with its master identity public key). Credentials are retrieved and decrypted by the FC when it needs them.

4- Availability

One of the main advantages provided by cloud platforms is robust availability based on extensive redundancy achieved with virtualization technology. Windows Azure provides numerous levels of redundancy to provide maximum availability of customers’ data. Data is replicated within Windows Azure to three separate nodes within the Fabric to minimize the impact of hardware failures.

Penetration Testing

Microsoft conducts regular penetration testing to improve Windows Azure security controls and processes. They understand that security assessment is also an important part of our customers’ application development and deployment. Therefore, they have established a policy for customers to carry out authorized penetration testing on their applications hosted in Windows Azure. Because such testing can be indistinguishable from a real attack, it is critical that customers conduct penetration testing only after obtaining approval in advance from Windows Azure Customer Support. Penetration testing must be conducted in accordance with Microsoft terms and conditions. Requests for penetration testing should be submitted with a minimum of 7-day advanced notice.

HITS Application SAAS

- HITS Cloud Version provides very strong password in terms of length, complexity, and unpredictability. System can store all the passwords encrypted by database highest security standards that cannot be decrypted.
- Password must be at least 8 characters, must include at least one upper case letter, one lower case letter, and one numeric digit.
- HITS Cloud Version has the capability to schedule password expiration date, account disabling, and account auditing. In addition to this it can restrict accessibility to the cloud services only from defined IP ranges.

Cloud Security Design

Windows Azure runs in data centers managed and operated by Microsoft Global Foundation Services (GFS). These geographically dispersed data centers comply with key industry standards, such as ISO/IEC 27001:2005, for security and reliability. They are managed, monitored, and administered by Microsoft operations staff that have years of experience in delivering the world's largest online services with 24 x 7 continuity. In addition to data center, network, and personnel security practices, Windows Azure incorporates security practices at the application and platform layers to enhance security for application developers and service administrators.

Fundamentally, Windows Azure provides confidentiality, integrity, and availability of customer data, just like any other application hosting platform. It also provides transparent accountability to allow customers and their agents to track administration of applications and infrastructure, by themselves and by Microsoft.

1- Confidentiality

Confidentiality ensures that a customer’s data is only accessible by authorized entities...

Windows Azure provides confidentiality via the following mechanisms:
- Identity and Access Management - Ensures that only properly authenticated entities are allowed access.
- Isolation - Minimizes interaction with data by keeping appropriate containers logically or physically separate.
- Encryption - Used internally within Windows Azure for protecting control channels and is provided optionally for customers who need rigorous data protection capabilities.

2- Identity and Access Management

The strongest security controls available are no protection against an attacker who gains unauthorized access to credentials or keys. Thus, credential and key management are critical components of the security design and implementation of Windows Azure.

1- Confidentiality

Confidentiality ensures that a customer’s data is only accessible by authorized entities...

Windows Azure provides confidentiality via the following mechanisms:
- Identity and Access Management - Ensures that only properly authenticated entities are allowed access.
- Isolation - Minimizes interaction with data by keeping appropriate containers logically or physically separate.
- Encryption - Used internally within Windows Azure for protecting control channels and is provided optionally for customers who need rigorous data protection capabilities.

2- Identity and Access Management

The strongest security controls available are no protection against an attacker who gains unauthorized access to credentials or keys. Thus, credential and key management are critical components of the security design and implementation of Windows Azure.

HITS Application SAAS

- HITS Cloud Version provides very strong password in terms of length, complexity, and unpredictability. System can store all the passwords encrypted by database highest security standards that cannot be decrypted.
- Password must be at least 8 characters, must include at least one upper case letter, one lower case letter, and one numeric digit.
- HITS Cloud Version has the capability to schedule password expiration date, account disabling, and account auditing. In addition to this it can restrict accessibility to the cloud services only from defined IP ranges.

Cloud Security Design

Windows Azure runs in data centers managed and operated by Microsoft Global Foundation Services (GFS). These geographically dispersed data centers comply with key industry standards, such as ISO/IEC 27001:2005, for security and reliability. They are managed, monitored, and administered by Microsoft operations staff that have years of experience in delivering the world's largest online services with 24 x 7 continuity. In addition to data center, network, and personnel security practices, Windows Azure incorporates security practices at the application and platform layers to enhance security for application developers and service administrators.

Fundamentally, Windows Azure provides confidentiality, integrity, and availability of customer data, just like any other application hosting platform. It also provides transparent accountability to allow customers and their agents to track administration of applications and infrastructure, by themselves and by Microsoft.

1- Confidentiality

Confidentiality ensures that a customer’s data is only accessible by authorized entities...

Windows Azure provides confidentiality via the following mechanisms:
- Identity and Access Management - Ensures that only properly authenticated entities are allowed access.
- Isolation - Minimizes interaction with data by keeping appropriate containers logically or physically separate.
- Encryption - Used internally within Windows Azure for protecting control channels and is provided optionally for customers who need rigorous data protection capabilities.

2- Identity and Access Management

The strongest security controls available are no protection against an attacker who gains unauthorized access to credentials or keys. Thus, credential and key management are critical components of the security design and implementation of Windows Azure.

HITS Application SAAS

- HITS Cloud Version provides very strong password in terms of length, complexity, and unpredictability. System can store all the passwords encrypted by database highest security standards that cannot be decrypted.
- Password must be at least 8 characters, must include at least one upper case letter, one lower case letter, and one numeric digit.
- HITS Cloud Version has the capability to schedule password expiration date, account disabling, and account auditing. In addition to this it can restrict accessibility to the cloud services only from defined IP ranges.

Cloud Security Design

Windows Azure runs in data centers managed and operated by Microsoft Global Foundation Services (GFS). These geographically dispersed data centers comply with key industry standards, such as ISO/IEC 27001:2005, for security and reliability. They are managed, monitored, and administered by Microsoft operations staff that have years of experience in delivering the world's largest online services with 24 x 7 continuity. In addition to data center, network, and personnel security practices, Windows Azure incorporates security practices at the application and platform layers to enhance security for application developers and service administrators.

Fundamentally, Windows Azure provides confidentiality, integrity, and availability of customer data, just like any other application hosting platform. It also provides transparent accountability to allow customers and their agents to track administration of applications and infrastructure, by themselves and by Microsoft.

1- Confidentiality

Confidentiality ensures that a customer’s data is only accessible by authorized entities...

Windows Azure provides confidentiality via the following mechanisms:
- Identity and Access Management - Ensures that only properly authenticated entities are allowed access.
- Isolation - Minimizes interaction with data by keeping appropriate containers logically or physically separate.
- Encryption - Used internally within Windows Azure for protecting control channels and is provided optionally for customers who need rigorous data protection capabilities.

2- Identity and Access Management

The strongest security controls available are no protection against an attacker who gains unauthorized access to credentials or keys. Thus, credential and key management are critical components of the security design and implementation of Windows Azure.

HITS Application SAAS

- HITS Cloud Version provides very strong password in terms of length, complexity, and unpredictability. System can store all the passwords encrypted by database highest security standards that cannot be decrypted.
- Password must be at least 8 characters, must include at least one upper case letter, one lower case letter, and one numeric digit.
- HITS Cloud Version has the capability to schedule password expiration date, account disabling, and account auditing. In addition to this it can restrict accessibility to the cloud services only from defined IP ranges.

Cloud Security Design

Windows Azure runs in data centers managed and operated by Microsoft Global Foundation Services (GFS). These geographically dispersed data centers comply with key industry standards, such as ISO/IEC 27001:2005, for security and reliability. They are managed, monitored, and administered by Microsoft operations staff that have years of experience in delivering the world's largest online services with 24 x 7 continuity. In addition to data center, network, and personnel security practices, Windows Azure incorporates security practices at the application and platform layers to enhance security for application developers and service administrators.

Fundamentally, Windows Azure provides confidentiality, integrity, and availability of customer data, just like any other application hosting platform. It also provides transparent accountability to allow customers and their agents to track administration of applications and infrastructure, by themselves and by Microsoft.

1- Confidentiality

Confidentiality ensures that a customer’s data is only accessible by authorized entities...

Windows Azure provides confidentiality via the following mechanisms:
- Identity and Access Management - Ensures that only properly authenticated entities are allowed access.
- Isolation - Minimizes interaction with data by keeping appropriate containers logically or physically separate.
- Encryption - Used internally within Windows Azure for protecting control channels and is provided optionally for customers who need rigorous data protection capabilities.

2- Identity and Access Management

The strongest security controls available are no protection against an attacker who gains unauthorized access to credentials or keys. Thus, credential and key management are critical components of the security design and implementation of Windows Azure.

HITS Application SAAS

- HITS Cloud Version provides very strong password in terms of length, complexity, and unpredictability. System can store all the passwords encrypted by database highest security standards that cannot be decrypted.
- Password must be at least 8 characters, must include at least one upper case letter, one lower case letter, and one numeric digit.
- HITS Cloud Version has the capability to schedule password expiration date, account disabling, and account auditing. In addition to this it can restrict accessibility to the cloud services only from defined IP ranges.
Thinking of SaaS Differently

The most significant takeaway of a TCO comparison between HITS SaaS model and existing HR Management systems is simple: HITS provides a cloud model of HR management system that is more affordable and more convenient for all the companies’ sizes irrespective to the market industry of each organization.

By capitalizing on the cloud-computing model, HITS offers a service that is both affordable and part of a paradigm shift in the Human Resource Management field. In addition to the cost saving users of HITS enjoy a system that is intuitive, comprehensive, and easy to use.