

Security and Cloud Services

Securing a business advantage



Viewpoint Paper

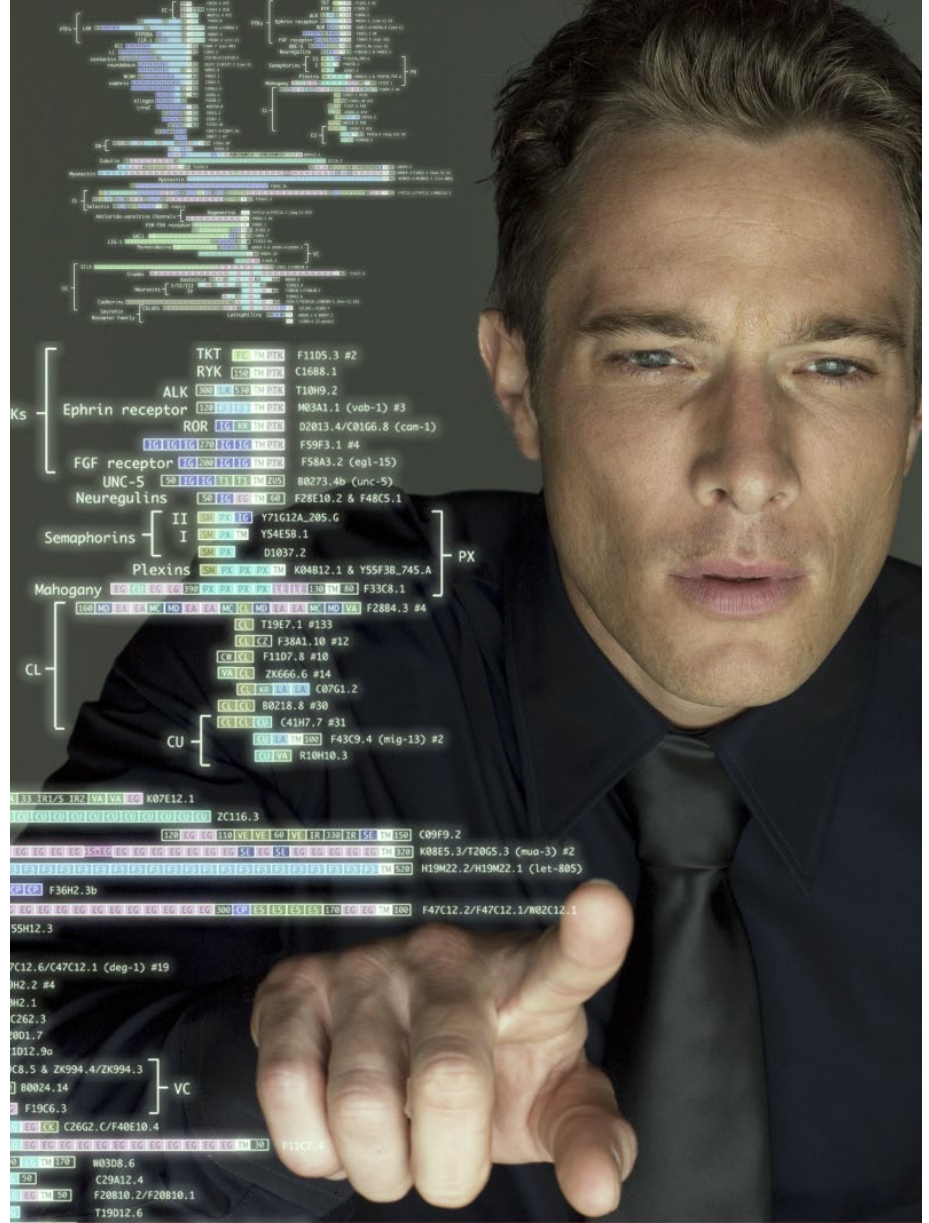


Table of contents

Cloud services: securing a business advantage for your enterprise	1
Introduction	2
The cloud ecosystem	5
Cloud delivery models	6
Hybrid cloud for optimal business outcomes	8
Cloud security concerns	9
Security and compliance framework	9
Cloud security strategy	10
Data protection and privacy management	10
Governance, risk, and compliance	11
Identity and access management (IAM)	12
Infrastructure security	12
Readiness	13
The enterprise organization	14
Cloud services standards	14
Cloud services standards—where are they?	14
HP Secure Advantage	15
Conclusion	16

Cloud computing as a concept is having a huge impact on business and IT strategy. Gartner identifies cloud computing as the #1 strategic technology that organizations need to plan for in 2010, up from #3 in 2009.¹ The appeal, of course, is expected cost savings; increased speed to market; and massive elasticity, scalability, and flexibility. Cloud computing, nevertheless, has many challenges ... beginning with finding an agreement on what defines cloud computing and how we talk about cloud services, the architecture, and delivery of cloud offerings. One point on which there is agreement, however, is that the top concern about cloud within enterprises is security, according to a recent survey by IDC.² This paper offers a point of view on cloud services, its definition, and an outline of the opportunities cloud services bring to the enterprise, while clearly detailing how to best manage the related technical and business security risks.

Cloud services: securing a business advantage for your enterprise

The usage of cloud services is seeing explosive growth, offering compelling, scalable, and elastic solutions in addition to benefits such as on demand, pay-per-use, and even resilience over existing Internet protocols. Because of this, vendors of all types are marketing a broad spectrum of products and solutions as “cloud services,” even relabeling their existing products with cloud terms. As a result, many organizations, and often individual business units, are jumping headlong into cloud computing, or—at the other extreme—trying to avoid it however possible. Because there is so much hype and confusion around the word and the concept, HP approaches cloud services as an opportunity to re-examine both business and IT strategies, with a focus more on desired outcomes and specific deliverables—for example, new compute capacities that adjust with business needs and offer countless ways to deliver.

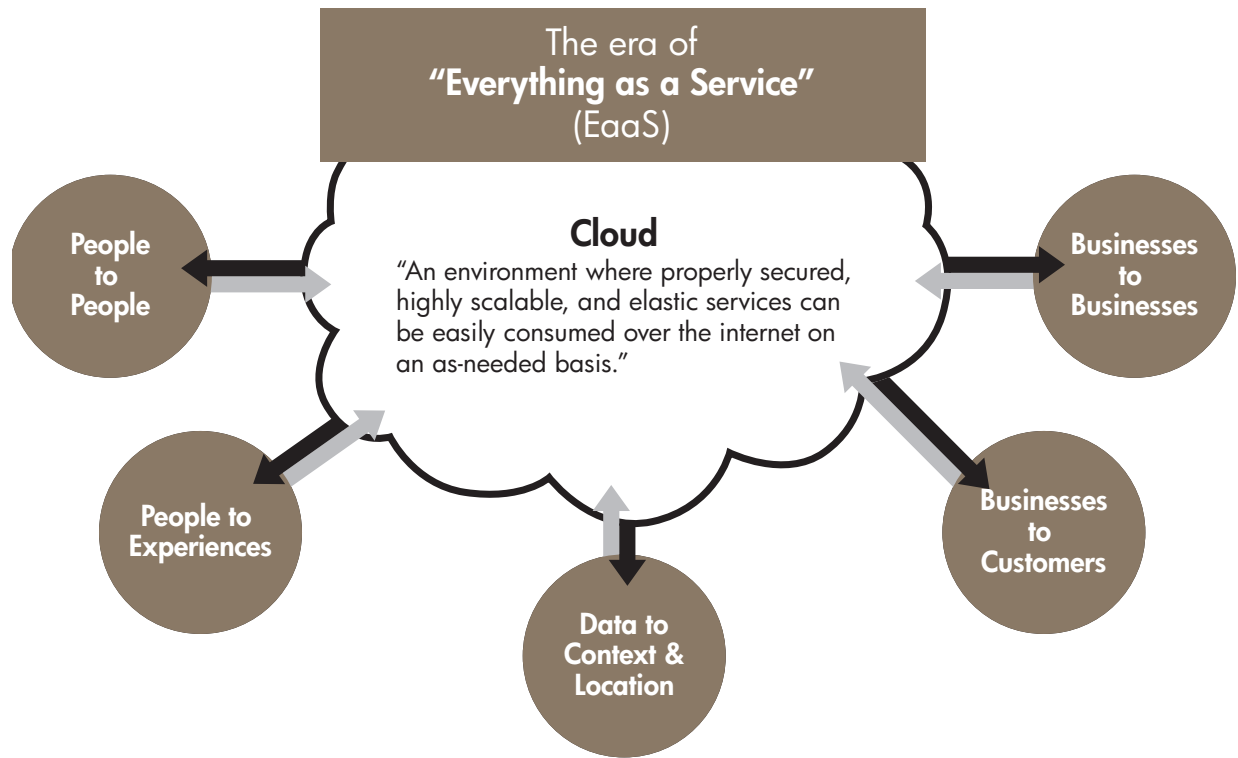
This new model for delivering solutions has many positive aspects, but it may not be suitable for many scenarios, especially as they relate to large enterprises and public service organizations. There are inherent issues of data integrity, compliance, service levels, architecture, and—most significantly—security. However, the blanket term “security,” like cloud computing itself, in many respects, is too broad. The requirement then is to clearly identify the specific components of an organization’s security posture, using an agreed-upon taxonomy. There are industry efforts under way, with key groups strongly supported by HP: The Cloud Security Alliance (CSA) published a set of guidelines for cloud security and created a set of use cases to help refine an understanding of the requirements; and The Jericho Group, part of the Open Group, offered a model for secure cloud collaboration before joining forces with the CSA to advance the effort. Using standards and industry approaches is a good baseline but requires a level of mapping to and from specific enterprises’ taxonomies and business requirements.

To secure the most benefit, HP recommends a classic risk management strategy alongside the integration of an evolved distributed computing and service oriented approach to enterprise architecture. It is not always wise, or possible, to utilize current cloud

¹ <http://www.gartner.com/it/page.jsp?id=1210613>

² IDC, Cloud Computing 2010, An IDC Update, #TB20090929, September 2009.

Figure 1: Cloud—Everything as a Service



computing models for critical enterprise applications or anything that incorporates critical business data. HP offers a comprehensive portfolio of products, services, and partners, along with 30-plus years in distributed systems security, to help clients defend, protect, and validate their long-term IT strategies for cloud computing. HP has defined a taxonomy that incorporates focus areas of: **Data Privacy and Protection; Identity Management; Governance, Risk and Compliance;** and **Infrastructure Security and Readiness** to collaborate with clients and identify their critical concerns and responses, and secure their business processes and IT.

This viewpoint paper details the above approach and discusses key examples of how to employ best practices and tools to gain critical business advantages and outcomes from cloud services.

Introduction

The cloud offers a vast selection of services that yield new kinds of business value for any organization wishing to take advantage of Internet technologies. HP sees cloud computing as a logical evolution of IT strategies including grid, utility, on-demand, and distributed computing.

Cloud services aligns closely with the HP strategy and vision for our partners and clients of "Everything as a Service" (EaaS). Many definitions exist for cloud, and most align with HP's and extend the previous memes of Web 2.0 and distributed computing. In a nutshell, it is a means by which highly scalable, technology-enabled services can be easily consumed over the Internet on an as-needed basis. This definition, like most others, doesn't accommodate any requirement for proper or even minimal security, assuming perhaps that security is inherent. This is far from the reality. Although many cloud service providers incorporate

Figure 2. Commonly cited benefits of cloud services

	Commonly cited benefits	Rationale
1	Simplify and optimize the IT environment	Less to own and operate
2	Avoid capital expenses	Consumption-based pricing
3	Faster ROI—less to build	No building assumes faster delivery & ROI
4	Better agility to meet business needs	Composing external services allows for quicker reaction to business needs
5	Low-cost disaster recovery	Assumed cloud services already have some level of disaster recovery

Figure 3: Commonly cited concerns of cloud services

	Commonly cited concerns	Rationale
1	Service level agreements	Poor or nonexistent service level agreements on performance, availability, and support
2	Data security, legal, and regulatory controls	Immature controls, processes, and certifications in place to manage risk
3	Vendor lock in	Lack of interoperability between cloud services (Platform as a Service [PaaS], Infrastructure as a Service [IaaS])
4	IT management issues	Services, data, and vendors still need to be managed; lack of adequate tools to manage and extract data
5	Market flux/immaturity	Concerns around vendor viability, service quality, and support

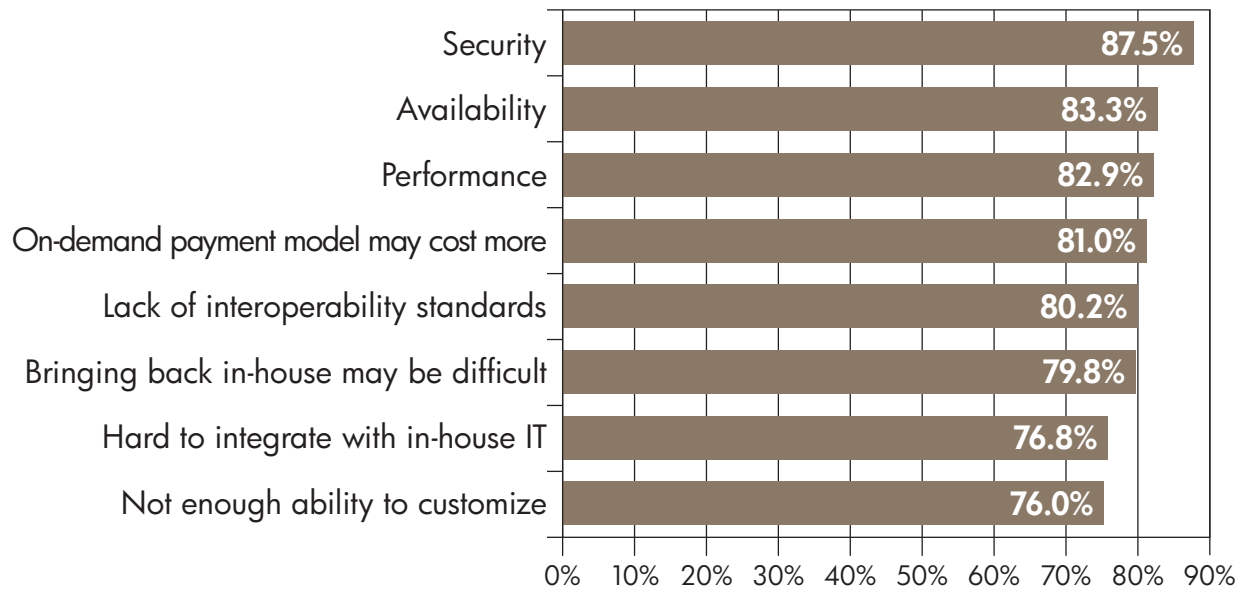
security into their approaches, they rarely align their security solutions with traditional enterprise client security approaches for reasons of scale, flexibility, and cost. Fundamentally, many clients and providers of cloud services achieve these obvious benefits at the expense of security. HP believes that secure cloud computing will allow you to more rapidly evolve business strategy. By refining your security requirements, there is the opportunity to identify cloud services to enable business outcomes while maintaining your security posture.

Regardless of the ultimate definition or terms used to describe this extended approach to business, it is more important to focus on your organizational needs in relation to the potential benefits, weighed against potential risks, in a classic approach to business risk management.

Figure 2 shows the commonly cited benefits of cloud services. The real business opportunity, as a result of such flexibility, is allowing organizations to rapidly adopt technology choices through an optimal method to mix-and-match cost structures for minimizing capital expenditure (CapEx) and funding new projects through operational expenditure (OpEx).

As a result, many are approaching cloud computing solutions with board or executive support and a resultant nonchalance, intentional or not. Business units and end users are buying IT services without understanding the fundamentals of maintaining enterprise functions. The most common cited concerns to HP around cloud computing are described in Figure 3.

Figure 4: IDC 2009 Enterprise Panel Survey—Rate the challenges/issues of the 'cloud'/on-demand model



(Scale: 1 = Not at all concerned; 5 = Very concerned)

Source: IDC, Cloud Computing 2010, An IDC Update, #TB20090929, September 2009.

Security is high on the list. This aligns closely with multiple analyst reports, including IDC's 2009 survey of 263 respondents to their IDC 2009 Enterprise Panel shown in Figure 4.

Assuming that cloud solutions are less secure than those housed in large IT data centers is a common reaction. While sometimes true, it is certainly not always so. By preparing to use cloud services with a risk-based approach in mind, concerns can be addressed through process, planning, risk analysis, and governance. Cloud solutions increase requirements associated with policy enforcement, while at the same time offering opportunities to decrease requirements around managing physical infrastructure. Considering that many especially smaller enterprises cannot staff a full-time security team, cloud or outsourced solutions provide compelling options in terms of cost and capability.

Understanding the risk-based requirements will position enterprises for business enablement with the appropriate level of security. IT departments have a critical role to play in this by advocating a measured approach, as well as offering an expedient framework for the business to securely use cloud computing solutions.

To succeed, however, requires a much better understanding of what the market means when it talks about cloud services. The amorphous properties that are used to describe cloud computing do not include security, or truly break cloud down into something that is manageable.

Figure 5: Cloud services and industry examples

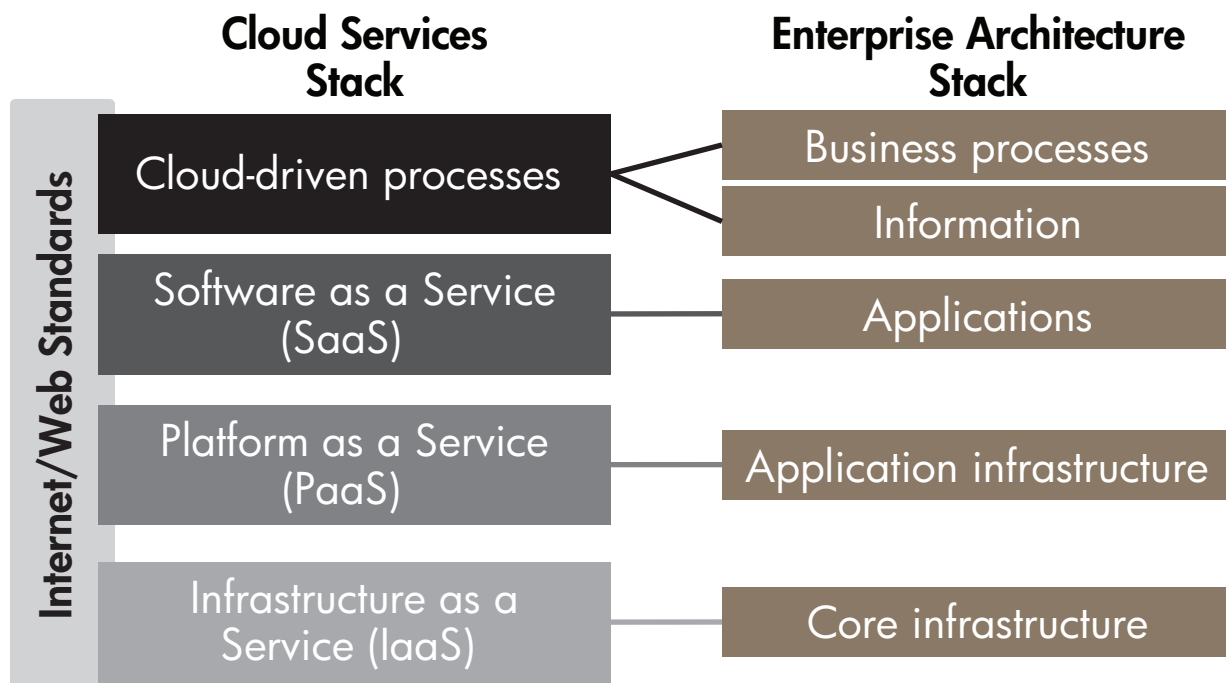
Types of Cloud Services	Description	Industry examples
Cloud-driven processes	<ul style="list-style-type: none"> Architecture of participation, crowd sourcing, perpetual beta, network effects 	<ul style="list-style-type: none"> Ratings, Review, Comments Open Source Software, Mark
Software as a Service (SaaS)	<ul style="list-style-type: none"> Consumer-focused web sites—rich Internet applications Multi-tenant business-focused web applications Collaboration, email, office productivity, CRM 	<ul style="list-style-type: none"> Flickr.com, Snapfish.com Myspace.com, Zillow.com Google Apps Right Now SalesForce Cisco WebEx
Platform as a Service (PaaS)	<ul style="list-style-type: none"> APIs for specific service or capability access or integration Data or capability web services Application composed (mash-up) via UI-centric configuration and scripting Configuration and scripting platform 	<ul style="list-style-type: none"> PayPal, Amazon FPS, DevPay Yahoo APIs (Search, Flickr) Google APIs (Payment, AdSense) JackBe BEA Aqualogic Rollbase Zoho App Creator Caspio SharePoint
Infrastructure as a Service (IaaS)	<ul style="list-style-type: none"> Hosted application development environment Application infrastructure capabilities Database, data stores Message queues Virtual servers, logical disks, compute capacity enabled by API-based provisioning 	<ul style="list-style-type: none"> Google App Engine, BigTable Microsoft Azure—SQL DS Amazon Simple DB, S3, SQS Force.com Amazon EC2 FlexiScale Elastra RightScale Mosso GoGrid

The cloud ecosystem

Most industry experts tend to consider cloud computing as a set of layered service-based solutions. The most common approach to defining cloud computing is a

three layer model of services—Infrastructure, Platform, and Software, each riding atop the lower layer. The cloud-driven processes connect business process workflow across enterprise processes and information. Figure 5 presents examples of each of these layers.

Figure 6: Cloud Services Mapped to Enterprise Architecture



One concern is that many go well beyond the three categories. Do not get caught up in cloud descriptor for a product or service; just consider how the common cloud services stack relates to a common enterprise architecture stack as highlighted in Figure 6.

off-premises options where third-party service providers exploit the ability to optimize the delivery in a dedicated environment. This can be delivered in a range of models, from simple co-location to a complete managed service.

Cloud delivery models

There is a logical evolution from traditional data center type solutions up from dedicated to shared services, as well as out from on-premises and across to off-premises options. Let's consider these before diving into the cloud approach.

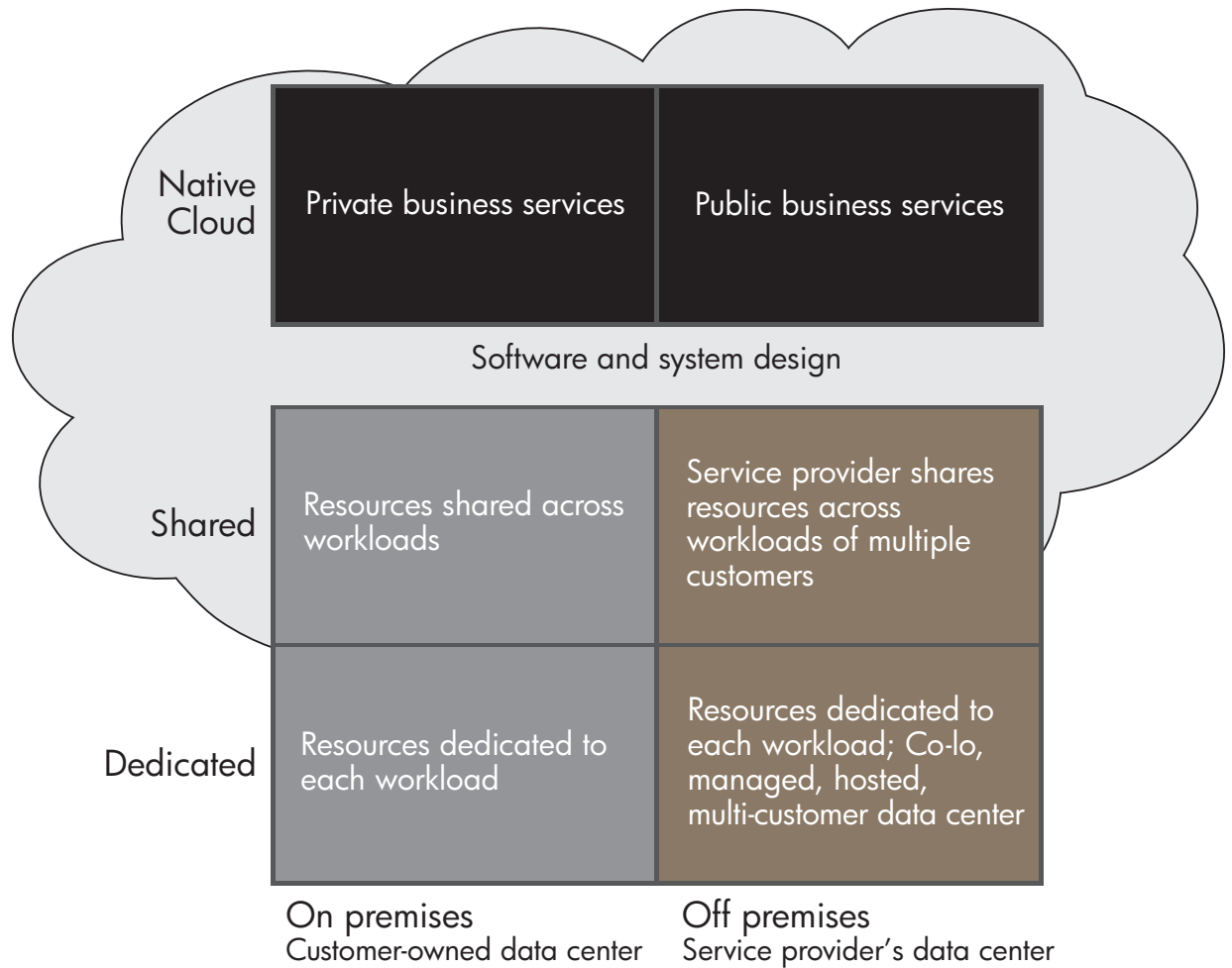
Most of workloads that run in a typical IT environment are not mission-critical and can be delivered in a form that balances sufficient level of services with business criticality. A majority of workloads aren't that critical, and therefore are good candidates to be placed in one of the shared delivery models.

The dominant delivery model of dedicated/on-premises involves generally large and often complex systems dedicated to specific workloads running in an organization's own data center. It works well when organizations are operating mission-critical workloads, and where the ability to serve clients is interrupted if the workload is unavailable or performs inadequately. This model gives an enterprise the most control—to tune and optimize that workload to whatever degree necessary.

The "Shared/On-Premises" model is that of newer data center approaches that use automation virtualization technologies to pull together required more than compute ... also storage, network capacity. In this model, you can dynamically bind workloads to a pool of infrastructure resources, but only if you first 1) consolidate 2) standardize 3) virtualize, then 4) automate. HP talks about this in part as "converged infrastructure" or "next-generation data center." This supports a model wherein most of the workloads aren't mission-critical, so a delivery model that meets business requirements at the lowest cost is attractive. Moving these workloads into an internal infrastructure utility can help lower costs.

Where an organization doesn't have the internal competencies, but does have the need for control, it might source those capabilities through dedicated/

Figure 7: Cloud delivery models



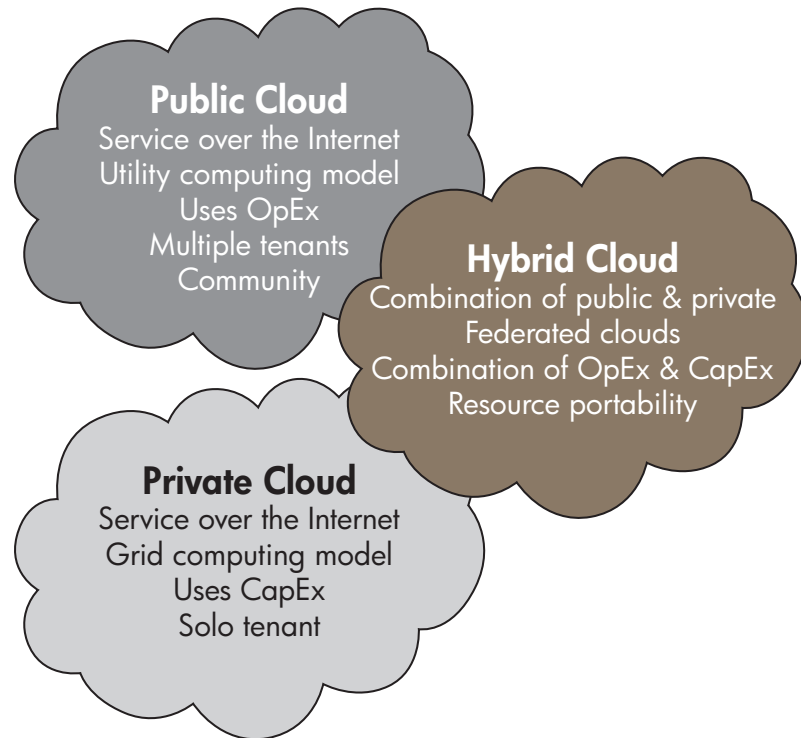
For most customers, the big value of shared/on-premises is less about cost and more about agility: the ability to put new workloads into production more quickly, and so improving IT's ability to respond to changing business needs. This agility can pay huge dividends in terms of business outcomes and in the business's satisfaction with the IT function.

The middle-right quadrant of "Shared/Off-Premises" provides a new alternative to sourcing infrastructure. In this model, a third-party service provider uses automation and virtualization technologies to pool computing capacity and to leverage it over multiple customers. This allows providers to balance demand across a

number of customers, which can allow them to operate at a higher level of utilization. It also moves the enterprise closer to the future state (top row) of a fully cloud-based environment. However, it's important to dig into the details a bit to understand the complete economic implications. It's that economic lever around irregular requirements for the capacity that makes the off-premise shared virtualized automated environments attractive.

These alternatives vary in more than just cost and agility. Security, performance, availability, ability to integrate, and other functional and nonfunctional considerations can influence which delivery model is right for a given workload.

Figure 8. Hybrid cloud for optimal business outcomes



Hybrid cloud for optimal business outcomes

Cloud services are the evolution of these approaches as shown atop the IT sourcing options. Bottom line, there are three logical approaches to cloud computing architectures: public, private, and a hybrid of the two.

Our view is that most enterprises will operate in a hybrid sourcing model for the long term—that the tradeoffs between these models result in a mixed solution being optimal. This IT environment—a mixture of in-house, shared, outsourced, and cloud services, each with different economics—is a more strategic and targeted way to invest IT dollars. Further, the fresh combination of bricks and mortar, web-based, mobile, and outside sourcing helps enterprises reach customers in new ways and explore new business models that were previously cost prohibitive. But this also means that every IT organization must excel at making the appropriate sourcing choices, and assure that the resulting services are delivered in a way that satisfies the business’s needs.

Because many CIOs and other IT decision-makers are not confident of the security levels of cloud computing, they plan to achieve the same capabilities within their own environments using private cloud as a model. Private clouds may not have the same scale-out capabilities as public clouds, but could achieve many of the benefits, at a potential fraction of the price of traditional IT data center approaches. Purists say this is nothing more than data center virtualization, utility computing, flexible computing, or any other buzzwords that have appeared and disappeared over the years. It is true that the guiding principles of cloud computing—“as-needed” rapid provisioning, low-cost implementation, and easily consumed services—are not part of traditional data center architecture, but they can be. So, what is the best way to optimally employ these options?

The ultimate objective is for IT to provide the required services allowing the business people to achieve their business outcomes at the lowest possible cost by sourcing from the most appropriate provider. As the public cloud may not be suited to run all functionalities required by the business, it fits in a larger environment that integrates the best of multiple worlds and IT can spill out into the public cloud when needed for the appropriate data types.

Figure 9: HP Security and Compliance Framework

Data Classification	Policy Alignment	Integration Strategies	Business Continuity
Data Protection and Privacy Management	Governance, Risk & Compliance	Identity & Access Management	Infrastructure Security
<ul style="list-style-type: none"> Secure application code testing Application penetration testing SOA security Web application firewall Web content filtering Email security Data loss prevention Database security Encryption/Key mgmt. Storage service Application integration Business continuity mgmt. Business service mgmt. High availability/backup/recovery 	<ul style="list-style-type: none"> Governance & compliance mgmt. Logging, auditing, & reporting eDiscovery & archiving Security training & awareness Compliance assessment Security event & incident mgmt. Security event response Vulnerability scanning Security operations ctr. Host OS security (hardening, config. mgmt.) Security dashboard 	<ul style="list-style-type: none"> Roles & entitlements Directory services Provisioning User administration Self-service Multi-factor authentication Risk-based authentication Privileged access mgmt. Federation Encryption models Token mgmt. Key mgmt. Remote access Web access mgmt. Single sign-on Application access mgmt. 	<ul style="list-style-type: none"> Physical & data center Virtualization Host threat mgmt. Host intrusion detection Endpoint protection Mobile device security Virtual networking Firewall Network intrusion detection Network access control Wireless security Host proxy — outbound Network integration
Provider Viability	Legal Obligations	Roles & Responsibilities	Contract, SLAs
READY?			

With respect to cloud security, HP offers two perspectives to consider, and they are far from mutually exclusive:

- How can we ensure that any cloud solutions we choose are secure?
- Can we use cloud services to increase our security and compliance posture?

Cloud security concerns

Large enterprises are often the target of cybercrime (deliberate attacks) and also afford many opportunities for internal fraud, making IT security a priority. Small and medium-sized enterprises tend to be rather different, however. Here the focus is to avoid any form of capital expenditure and relate the cost of IT directly to the growth of the company, often skimping on security precautions as a result. Since small enterprises typically have few requirements for specialized applications and tend to de-emphasize security and privacy, this is the sector that is most likely to adopt commodity cloud service provision in a significant way. An enterprise may freely choose to outsource, off-shore, or otherwise provision IT requirements, so long as it adheres to the regulatory environment of the countries within which it does business.

To assess the best approach, a business of any size must first understand what it wishes to gain from using cloud computing and then consider the risk model to determine if security concerns are a major issue in planning. An approach that simply bars use of cloud computing may cause an organization to miss out on significant gains. Consider this step to be yet another new cycle, similar to the infiltration of solutions ranging from personal computers, word processing software, database systems, wireless access points, and social media. Business units have often embraced these solutions ahead of IT support or sanctions, and it is always IT that is left to clean up any mess. This is true for business continuity issues, but especially for security issues. This is why the first step to properly managing cloud security concerns is to have a plan, not a response after the fact. Quite simply, don't be afraid of cloud computing; be prepared.

Security and compliance framework

To clearly address the critical security concerns that relate to an individual organization requires a common approach to understanding the security, governance, risk, and compliance pressures alongside a clear set

of focus areas relevant to each situation. HP takes a holistic view of security with respect to the cloud that parallels its overall view of security, which incorporates:

- **Governance, Risk, and Compliance:** Support geographic and industry-specific policy and regulations, enabling clients to get the most value from business information, while keeping it secure. Monitor and manage risks.
- **Data Protection and Privacy Management:** Maintain the availability, integrity, and privacy of data and information at rest or during use.
- **Identity and Access Management:** Provide identity assurance by establishing trust between individuals, systems, services, and partners while securing access.
- **Infrastructure Security:** Identify threats and points of vulnerability, deploy countermeasures to mitigate risk, and respond to incidents.

Furthermore, there is the supporting requirement of business readiness. Is the organization ready not only for cloud, but to deal with the reality of the risk management required by cloud computing?

Basically, to determine appropriate levels of requirement and risk acceptance to define security response—the equation remains the same, but the parameters change based on each organization’s unique circumstances.

Cloud security strategy

To implement a cloud services approach, HP recommends framing the overall cloud service strategy: implementing the components of a converged infrastructure; then securing, sourcing, and governing the solution. To secure and govern the solution, first plan how to ensure the security and performance of the services with a risk-based approach. HP suggests establishing a governance model, understanding the classification of data, ensuring policy alignment across the providers and buyers, defining an integration strategy, and ensuring business continuity plans are assured and tested. Organizations also need to assess the viability of providers across the whole ecosystem, including the division of responsibility between the provider and buyer and the related legal obligations. Lastly, monitor and validate appropriate contract terms or service level agreements.

Enterprises should also recognize that, by utilizing third-party services, they give up a level of control, and that, in turn, requires effort to manage the gap in a different way. In essence, to achieve some level

of governance around the usage of cloud computing, some of the savings achieved must be reinvested into increasing operational awareness and monitoring of the actual service provided.

So, the question then becomes whether an IT services provider can be trusted and provides appropriate levels of services. The question is actually a little more complex than that, as, when using web services, one may be dependent on more than one company. Indeed, a service provider may use another provider’s platform to deliver its services. Fundamentally, while the customer depends on consistent delivery chain, it may not know all the players in that chain. So it is important to keep that in mind when choosing a service. Outages happen regularly in the cloud, and some are highly publicized; also, many cloud services are still labeled “beta,” limiting the responsibility of the provider.

Using public cloud services creates an immediate dependency on a service provider. This dependency is measured in terms of trust and managed through—and measured against—common methods and tools such as contracts, agreements, terms of service, and acceptable use policies. These are usually standardized so that providers can maximize their costs at scale and minimize the amount of customization. In other words, there’s little or no customization to fit an enterprise’s requirements, unless one moves to a more outsourced approach where there is a little wiggle room for negotiation, and where additional service and contract options are more available ... at a cost.

Each of HP’s areas of security discipline will help identify the critical concerns for unique organizational needs, so that a plan can be created to manage and mitigate the associated risks.

Data protection and privacy management

An enterprise should assess whether its current data classification model matches its current and future needs. Consider how important each set of data is to the business and to its own client. Also consider the regional restrictions and industry obligations for specific data like personally identifiable information (PII) and credit card information (PCI). In setting this strategy, also remember that the overall risk management strategy is defined within the governance, risk, and compliance area; however, the execution of the controls reside within the domains, like data protection and privacy management.

Most providers of cloud services do not have a strong position in either data protection or privacy management. Yet data protection and privacy management are core to most enterprises in deciding how to use the cloud. As the network perimeters have dissolved with the sourcing of services across the Internet, protecting the data and the applications also needs to evolve. Some critical items in this domain are understanding data classification, protecting web applications, preventing loss of data, and ensuring appropriate backup/recovery of data and applications.

Attacks against Internet-facing web applications continue to be the most common cyber security threats. Companies considering cloud need to protect against the application vulnerabilities, as well as attacks against availability of services. Stealing data is the end goal of most web application attacks, so an organization needs to protect its web-based applications as well as its own customer-side software. This protection may run the gambit of secure applications development life cycle, static application code testing, active application penetration scanning, and web application firewalls.

As organizations work to decide the value and location of the data, content filtering or data loss prevention technologies are typically used to protect the business-critical data. Focused on the most valuable data, the enterprise monitors to prevent the unauthorized use or distribution of data. This type of technology should be deployed in multiple places, based on where the data is stored, transmitted, or used (ensuring data is not copied to other systems). If this capability is not offered by the provider, the business must determine whether to accept the risk, choose a different sourcing option, or deploy the filtering capability separately.

Another important aspect is the backup and recovery options. Existing business continuity plans help determine the appropriate solution, based on business requirements considering both workload and data availability. If data is lost due to a provider outage or data needs to be retrieved at the end of a contract, how will an enterprise get the data back? It is important to ensure that a good copy is available, but also consider the effort and activities needed to transfer the data from the provider back to enterprise control.

Some organizations may use data encryption to prevent unauthorized access to their data in the cloud. The impact of a performance hit against cost of ownership must be weighed appropriately. Also, consider that the private key infrastructure design and implementation needs to be reviewed. Is there one key for all clients? How is it shared?

Again, cloud providers vary greatly in the options available in protecting this domain. Make sure there is a common framework to understand how and what will be protected.

Governance, risk, and compliance

The importance of IT Governance, Risk, and Compliance (GRC) is based on the integration point between IT and the enterprise's overall risk management process. Arguably, the most important aspect is improving management insight and demonstrating added value to the business. When operating in a cloud model, some key areas of this domain are mapping to enterprise requirements; understanding litigation support and forensics; defining data location and accessibility of data by government subpoena; and controlling software license costs and complexity.

As discussed before, there is usually little room for customization of a public cloud services' terms. That means there needs to be a mapping of the organization's requirements to the services and controls of the provider. There also needs to be a governance framework put in place to track, monitor, measure, and audit the controls.

The business owners and the IT organization should ensure a common understanding with the enterprise legal team on the needs for data archiving and data retention for litigation support (electronic discovery) and forensics. Consider understanding and mapping the interfaces to internal security operations and incident response processes. Be sure the solutions cover all media or locations, the ability to preserve in the native format, and to be quickly assessable (preserving the meta-data). Procedures should also cover proper retention and management of the data as classified by company policy. It becomes more complex as services may be contracted by business users without due consideration of the impact.

Another concern by some organizations may be the silent subpoena. This allows the government agencies in the United States to get access to information stored in a third-party's environment without notification of the data owner. Some global corporations do not want their data to be subject to the US Patriot Act, so they don't want their information stored in the United States. Some cloud providers randomize the data location (no control by the enterprise on location), while others allow more regional control to alleviate these types of issues (at an additional cost).

Another issue to be addressed is software licensing. Most providers of large enterprise software have not developed their licensing schemes with the cloud in mind. If the enterprise owns a CPU, enterprise, site or seat licenses, how does the enterprise apply in a cloud environment? If the minimal license timeframe is 45 days, for example, how does that work with pay-per-use in the cloud? Software licensing in the cloud requires a completely different approach, so most SaaS providers have implemented the pay-per-use model. More visibility is the key, because it is important to understand so as to control cost and reduce complexity.

Identity and access management (IAM)

IAM supports the need to control who has access to what, when, and how. The concept in cloud computing of easy access creates the illusion that provisioning cloud services is also easy and quick. However, if internal process or controls around identity and access for employees and clients is poor, there is greater risk of security breach and business failure—and the cloud will likely not mitigate the situation. In addition, the potential for data breaches at cloud providers requires that a consumer of a provider's services be fully aware of the provider's security provisions around data access, such that providers do not expose client data as a result of internal security breaches, poor implementations, or even social engineering attacks.

For example, how can an organization protect data from administrators at the cloud provider? This can be done by adequately implementing and automating the identity and access management processes.

Provisioning should be automated with standard templates, and exceptions should be processed through workflow tools to both expedite access to services when needed and avoid mechanical failures. The de-provisioning process should make certain that dormant, inactive, unsecured, or inaccurate accounts are identified and disabled or removed expediently.

Another aspect is to minimize access. There should be mitigating process controls for privileged access users; only those with a business need have access. Access permissions must be certified on a continuous basis against the organization's and the cloud application's access control policies. Separation of duties must

be implemented for administration, audit, and role-based use, which must include appropriate controls for the cloud service provider. Strong authentication is required, and two-factor authentication should be used where possible (cost-effective) or required with a physical token, which is not easily shared with others.

The access management should also be supported with appropriate logging, reporting, and audit workflows that track access with appropriate granularity and supports nonrepudiation.

Federation and Single Sign On (SSO) should be used to minimize the proliferation and optimize the flow of identity-related data of users, clients, and their access requirements. Review and approval of integration can also be a point of control to existing systems and identities.

To automate these processes requires a comprehensive identity management solution, one which minimizes efforts to get access to required resources, but adequately protects the organizations against attack, inappropriate access being gained or maintained, and critically, one that supports the other security requirements for GRC. This is ultimately a question of appropriately managing policies.

Infrastructure security

Whether using mobile phones, laptops, desktops, or server to server, these endpoint devices represent the beginning of the chain that must be secured. There is limited value in having access to cloud computing or enterprise resources if the device or communication channel itself is insecure, and that ultimately fails to protect the private information stored in it. Many cloud providers require some level of security posture in the client endpoint as part of their terms of service. Thus, endpoint security is a critical aspect that must be managed by the client, including what is required of the enterprise, and what the provider offers.

Second, be aware of security issues along the communication chain. The Internet was designed with resilience against failure or attack as a primary design goal. That does not mean that today's Internet is 100% reliable in terms of performance or reliability—just that it is resistant to those effects. Without dedicated connectivity, traffic from one location to another may follow complex and, more critically, unsecured routes to its destination. So, organizations

need to ensure network security with appropriate technologies such as virtual private networks or secure sockets layer (SSL) transport.

Organizations also need to understand the data center and virtualization security as a foundation to ensure operational security and separation of workload and traffic within the provider's environment. Virtualization presents new technologies that need different, additional protection models and control points. The provider needs to provide transparency to its overall architecture including servers, networking, and storage systems. This also includes change management and patch management processes.

Readiness

HP proposes a four-step approach to developing a flexible environment, maximizing the utilization of the IT infrastructure while taking full advantage of the cloud where it makes sense. The four steps are as follows:

1. Develop a Service-Oriented Architecture and implement an integrated approach to governance, with an objective to manage the full life cycle of the enterprise and (later) cloud services used to address the business needs of the company. This will also facilitate virtualization.
2. Modernize the existing applications, exposing their functionality as services that can be called upon by others in an agile way.

3. Virtualize the IT landscape to optimize the use of the available capacity and as such develop a "cloud" class infrastructure on which other services can run.
4. Integrate this virtual environment with the cloud to ensure excess peak demand and specific services can be provisioned in the cloud in a transparent manner.

Step 2 and 3 can happen in parallel or in reverse order. The objective, however, is to drastically increase the utilization of the owned/hosted infrastructure, reducing its price point, while taking full advantage of the cloud where it makes sense. This ensures the required service levels, security levels, and other aspects discussed above can be addressed.

It also establishes an infrastructure that combines an enterprise class (dedicated and shared) environment with a global-class one, ensuring existing software investment is not lost in the process. An integrated service catalog ensures the applications can call upon each other's services to address the enterprise business requirements.

Until an enterprise has the right processes streamlined for its organization, cloud computing requires a broader set of skills than a traditional IT or Enterprise Architecture initiative. This includes legal, contracts, human resources, and more.

The enterprise organization

Cloud services requires a new view on how and what needs to be managed and secured. This has a direct impact on the team required to set and implement your strategy. The question is will the team be gatekeepers to cloud services, directly or indirectly? Do they set up agreements and simple processes that allow the organization to utilize these services directly, or do they manage the entire process for each new use? Certainly there are many parallels with outsourced services here, and utilizing both staff and partners with such experience will help improve an organization's experience with cloud computing.

Cloud services standards

Managing risk in cloud computing is complicated by the lack of common approaches, standards, and tools available, as vendors and clients rush to take advantage of the benefits available. Beyond the discussion so far, there are a few additional areas that are evolving and require the support of all constituents of the cloud computing community, including standards.

Cloud services standards—where are they?

Companies developing cloud services have to realize there is little standardization in the cloud space today, but a huge number of organizations pushing to fill the gap. This means, very practically, that an application developed in one cloud environment will not operate in another one.

When talking about future standards in relation to cloud services, there are few new ideas in the space. Cloud services is evolving, and in many ways, the area of standards support that categorization, as cloud computing rides atop most of the Internet, Web 2.0, and related standards already in play. This includes simple protocols such as HTTP and SSL through to more recent efforts such as XACML, SAML, WS-Federation, and further with virtualization standards.

The Cloud Security Alliance (CSA), “a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing,” is another source of fledgling standards. CSA details 15 domains to focus on with respect to cloud security.

The first version of the CSA guidelines was released early 2009, with an update released Q4 2009. These guidelines are an excellent starting point to review cloud security issues. The problem is that currently the CSA does not offer a framework for truly base-lining the potential metrics it defines as required elements. HP and the CSA jointly released research into the “Top Threats to Cloud Computing” www.hp.com/go/cloudsecurity in March 2010 to assist in best analyzing a secure approach to using cloud services.

Other standards offered in the market include:

- The National Institute of Standards and Technology (NIST)—a U.S. federal agency directed under the Obama administration to help define and evaluate cloud options and cloud security, in particular for the public sector. It has published its initial review, which provides some valuable data to consider.
- The Distributed Management Task Forum (DMTF)—announced in 2009 the initiation of a Cloud Lab alongside a submission by VMware of its API standards effort: vCloud. The intent is to enable consistent mobility, provisioning, management, and service assurance of applications running in internal and external clouds through a standard RESTful API, essentially an alternate to Amazon's proprietary EC2 API.

Beyond these we have a host of other organizations including the International Organization for Standards (ISO), the European Network and Information Security Agency (ENISA), TM Forum, The Open Group, the Institute of Electrical and Electronics Engineers (IEEE), the Open Cloud Consortium, and more.

So fundamentally, as it stands today, there are multiple standards efforts under way related to cloud services, as well as a few that incorporate approaches to securing them. To mitigate the business risks associated with these many approaches, most security-conscious clients and vendors are adopting the use of SAS 70 audits and utilizing ISO 27001 or NIST-related security standards to help evaluate and audit their solutions. Be aware—while SAS 70 audits show adherence to internal controls and ISO 27001 show evidence of information security management processes, neither guarantees overall security.

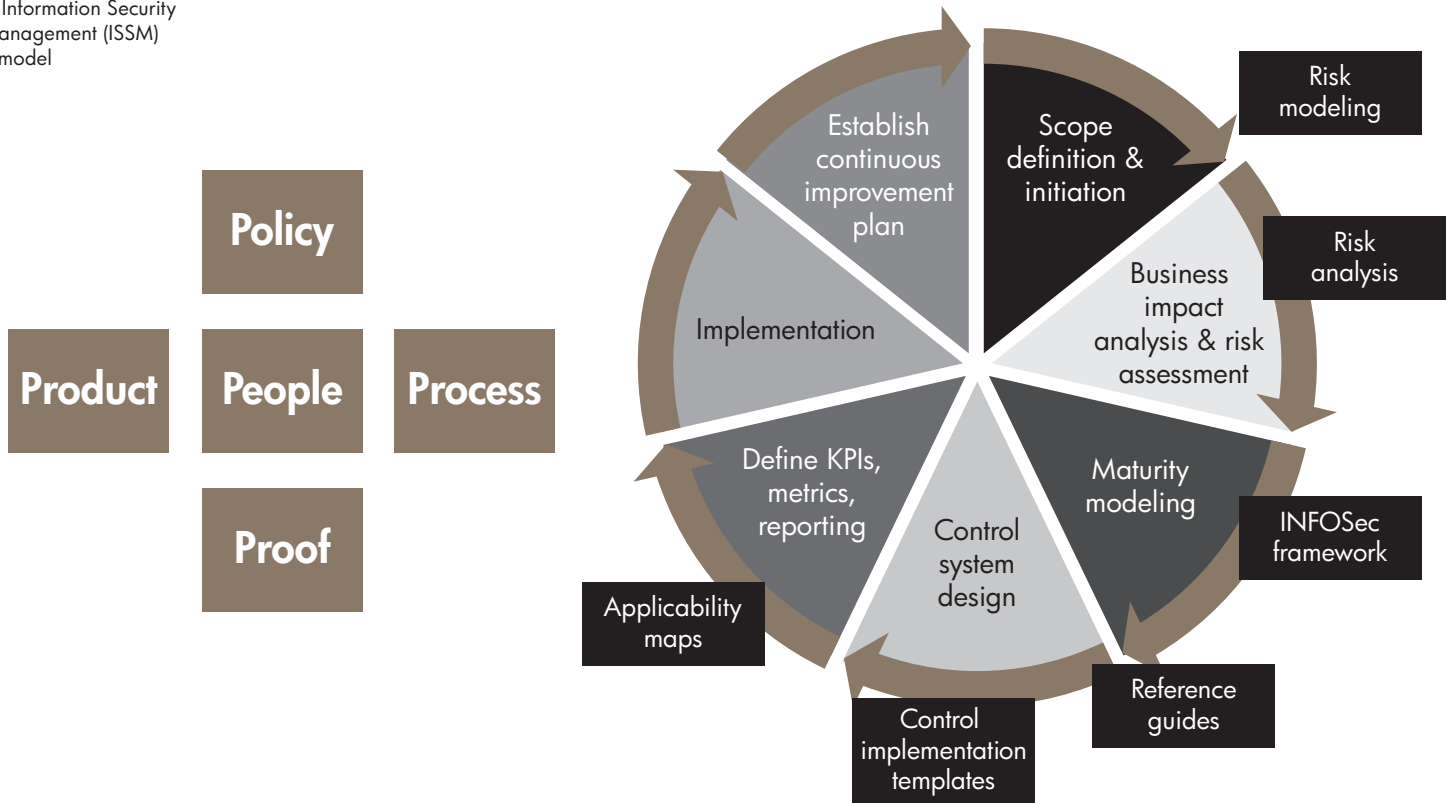
HP Secure Advantage

In a world where “everything is a service” and every technology-enabled service must directly impact the business outcome, HP puts a strong focus on service management, security, and governance. Through its services and software offerings, HP helps clients’ right-source their infrastructure services, application services, cloud services, and business processes services. This will be a tremendous advantage to our clients as they make the transition toward more cloud-based services.

HP has the comprehensive Secure Advantage portfolio, which protects data, resources, and validates regulatory compliance across the entire IT infrastructure—from the desktop, through the network, to the data center. This is a portfolio of servers, storage, software, and services that help clients securely share information, improve identity management and compliance controls, ensure business continuity, and defend against network attacks.

The HP Integrated Security Service Management (ISSM) Framework is a comprehensive approach to designing and deploying an enterprise information security program. ISSM is a scalable architecture of industry and open security standards and best practices that promote the confidentiality, integrity, and availability of IT assets and information.

Figure 11. Information Security Service Management (ISSM) reference model



Conclusion

Regardless of the overall market concerns around cloud services, it is clear that the adoption rate and expectations are accelerating. HP recommends that a clear risk management strategy guides enterprise security concerns and helps define the steps to take and the key areas that will impact an organization's adoption of cloud computing solutions. HP clients expect their data to be protected, communications to be secure, and their applications to be free of crippling vulnerabilities introduced by software flaws or the acts of individuals. All of HP's businesses sell products, services, or solutions that require varying levels of security, both to be acceptable to clients and to be competitive in the market. This expertise is leveraged as HP helps clients determine how to best take advantage of integrated solutions now that the cloud computing approach is evolving.

HP Enterprise Services offers a set of clear deliverables for preparation, planning, and secure delivery of cloud computing usage. HP's management solutions for cloud computing focus on intelligent, policy-driven control of computing devices and networks. Today's computer infrastructures and cloud architectures are becoming increasingly difficult to manage in a secure way simply because of the number of components, the complexity in the way these components function and interoperate, and the amount of data generated in daily use. Intelligent adaptive security built into our manageability solutions helps to ensure that the network, computers, and applications that use these resources remain secure and protected against unauthorized access.

About the authors

Archie Reed

Archie Reed is HP chief technologist for Cloud Security in the HP Security Office. He is a 20-year experienced manager and technologist, offering a wide range of leadership, architecture, product, R&D, and implementation experience gained in high profile environments. Reed has worked to deliver both commercial and internal business solutions, as well as managed both engineering and corporate development for hosted (150M+ user) multi-tenant (10K+) service providers. Reed has been an Industry advisor for multiple organizations, including Digital ID World (2003-8), Identity Engines (2005-8), and OASIS (DSML, XACML).

Reed is a regular speaker at executive events, conferences, and analyst meetings on topics from Security, Privacy, Cloud Computing, Identity Management, and Business Technology Optimization. He is a published author including "The Definitive Guide to Identity Management" (Realtime Publishers, 2003), "Migrating to Windows 2000 and Exchange 2000" (Realtime Publishers, 2001), and "Implementing Directory Services" (McGraw Hill, 2000), alongside many white papers and magazine articles. He is currently working on a new 2010 book "The Concise Guide to Cloud Computing."

Mary Ann Mezzapelle

Mary Ann Mezzapelle is the chief technologist for Security Services for HP in the Office of the CTO. In that role, she is responsible for technology strategy and planning for HP Enterprise Services.

Mezzapelle has 27 years' business experience applying advanced information technology capabilities for high business impact, serving clients in industries such as financial, insurance, travel, energy, transportation, and manufacturing. She joined EDS in 1988 and HP in 2008. She has been a programmer, applications manager, and infrastructure and systems consultant.

Mezzapelle earned her CISSP credentials in 2001 and CSSLP in 2009. She is an active member of the San Francisco chapters of InfraGard and the Information Systems Security Association (ISSA), including being a past president. She contributes to the security community as conference speaker, security conference planner, and CISSP domain coach. She also serves on the local planning committee for the Juvenile Diabetes Research Foundation (JDRF).



Technology for better business outcomes

To learn more, visit www.hp.com

© Copyright 2010 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA0-7102ENW, March 2010

