VIDERITY

STRATEGIC, CREATIVE, TECHNICAL

Information Security Management in a Government Cloud Environment

Viderity Inc

Table of Contents

Introduction

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." 1

Moving information assets to a cloud computing environment (CCE) offers an agency the potential for reduced costs, on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity, and measured service. CCEs are offered in a variety of deployment and service models, each with its own characteristics with regard to cost/benefit, efficiency, flexibility, risk, and consumer control. Although the advantages of operating in the cloud are compelling, cloud consumers need to carefully consider the security risks, compliance complications, and potential legal issues inherent in CCE use. Federal agencies seeking to reap the benefits of cloud computing must sow the seeds of success by investing in proactive and strategic management of the new environment. Doing so will require implementation and modification of information security management systems and governance programs to mitigate risks and ensure compliance with legal, regulatory, and contractual security requirements.

As with the adoption of other new technologies and service offerings, transition to the CCE will likely be evolutionary, not revolutionary. Many organizations, particularly federal agencies, will migrate some capabilities to the cloud while maintaining existing computing environments for others, thus operating in a hybrid mode for the foreseeable future. By presenting an information security governance framework and key considerations related to that framework, this paper aims to help inform agency leaders, information security professionals, and information security governance participants on how to best garner the benefits of a CCE without exposing their mission to excessive information security risk or the potential of legal and regulatory compliance failures.

Outcomes of Effective Information Security Governance in a CCE

- **Strategic Alignment** - Information security practices aligned with the agency's enterprise strategy and agreed-upon risk profile
- **Value Delivery** - A clear set of standards to effectively manage and monitor cloud provider security controls
- **Risk Management** - An understanding of acceptable risk exposure
- **Performance Metrics** - A measurement process with feedback provided on vulnerabilities and progress made

Information security governance is the mechanism through which organizations can ensure effective management of information security. Viderity developed the information security management and governance framework presented in this paper. We have customized the framework for, and implemented it in, several government and commercial client environments. The focus of this paper is the adaptation of our information security governance model for federal government entities planning to employ cloud computing services. Potential cloud service providers to the government will require a somewhat different approach to adapting the information security management and governance framework; their needs will be addressed in a separate white paper.

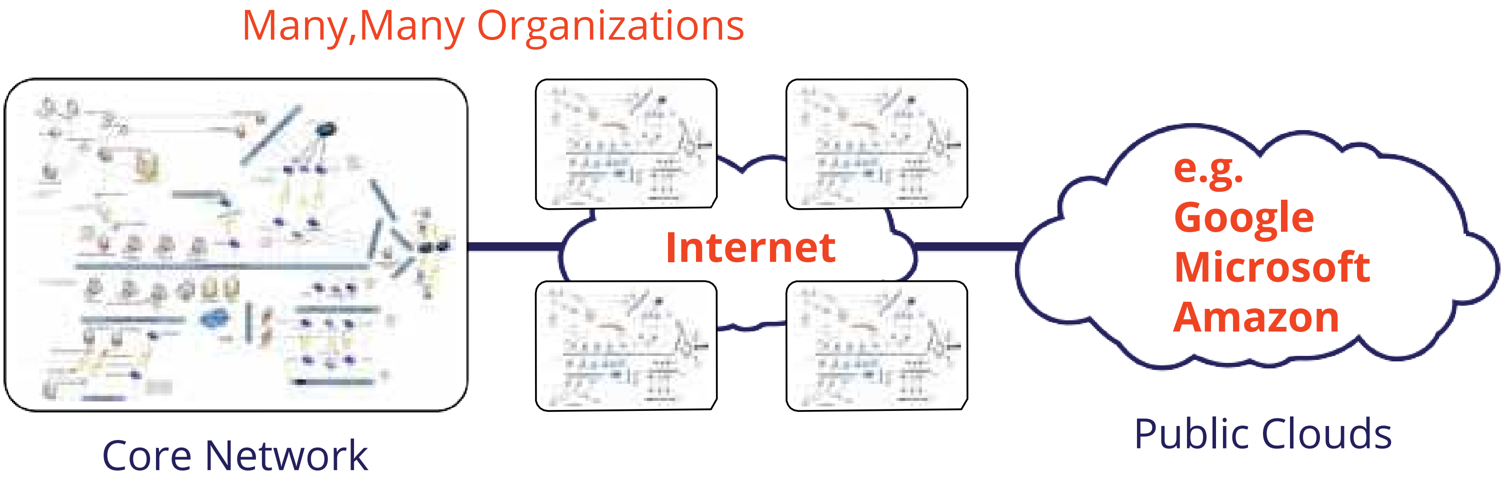
To provide the proper context for our presentation of the information security governance framework, we begin by reviewing the risks and compliance challenges associated with each of the four existing cloud computing deployment models. We offer a high-level description of each model, including a schematic depiction of its structure.

1. Please see http://csrc.nist.gov/groups/SNS/cloud-computing/index.html.

Public Clouds

The most common type of CCE is the public cloud. In this construct, the cloud infrastructure is owned and operated by an organization that provides services to multiple enterprises and individuals on a utility basis. Cloud consumers are often referred to as "tenants" (see Exhibit 1). Public clouds present the greatest security risk for federal agency cloud consumers. Risk factors include: global multi-tenancy with other users; lack of direct control over information security framework implementation and monitoring; limited service-level agreement (SLA) flexibility; contractual liability limitations; data location management uncertainties; and the lack of common legal and regulatory obligations between cloud providers and cloud consumers. Lack of structural visibility compounds these issues and prevents cloud consumers from effectively measuring or demonstrating compliance with security requirements. We expect that in the future, providers of public services will adapt their offerings and increase the flexibility of SLAs and contracts to better accommodate the unique legal, regulatory, and contractual information security compliance requirements of the federal government environment. Signs of movement in this direction are beginning to appear in the market, as evidenced by Amazon's recent introduction of optional "virtual private cloud" services that combine the outsourcing advantages of public clouds with increased visibility, customer control, and service tailoring. For the present, however, organizations should limit public cloud deployment to public information and systems with acceptable risk profiles and no legal or regulatory security requirements.

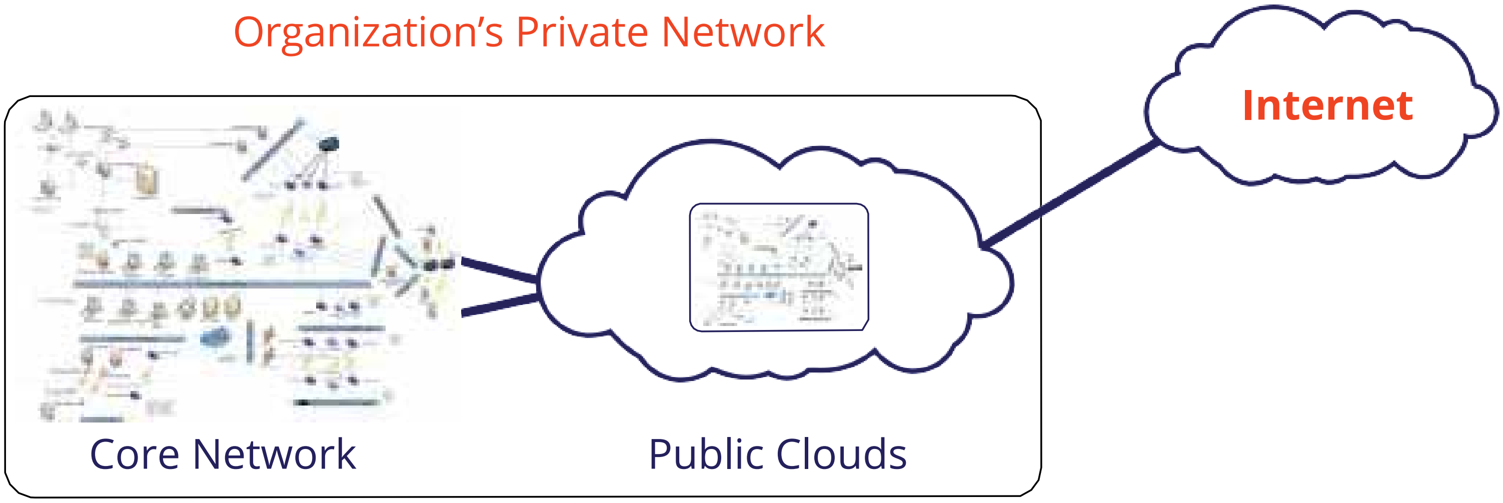
Exhibit 1 | Public Cloud Illustration



Private Clouds

In sharp contrast to the public cloud is the private CCE. In the private cloud, the cloud infrastructure is owned/leased and operated by a single organization solely for the user community of that organization (see Exhibit 2). For example, a federal government agency might deploy a cloud accessible only to entities within that agency. Cost efficiencies and economies of scale are likely to be more limited with private clouds than with public clouds, but information security risk and governance issues are minimized because of the shared mission goals and legal/regulatory security requirements of the cloud service provider and the cloud consumers.

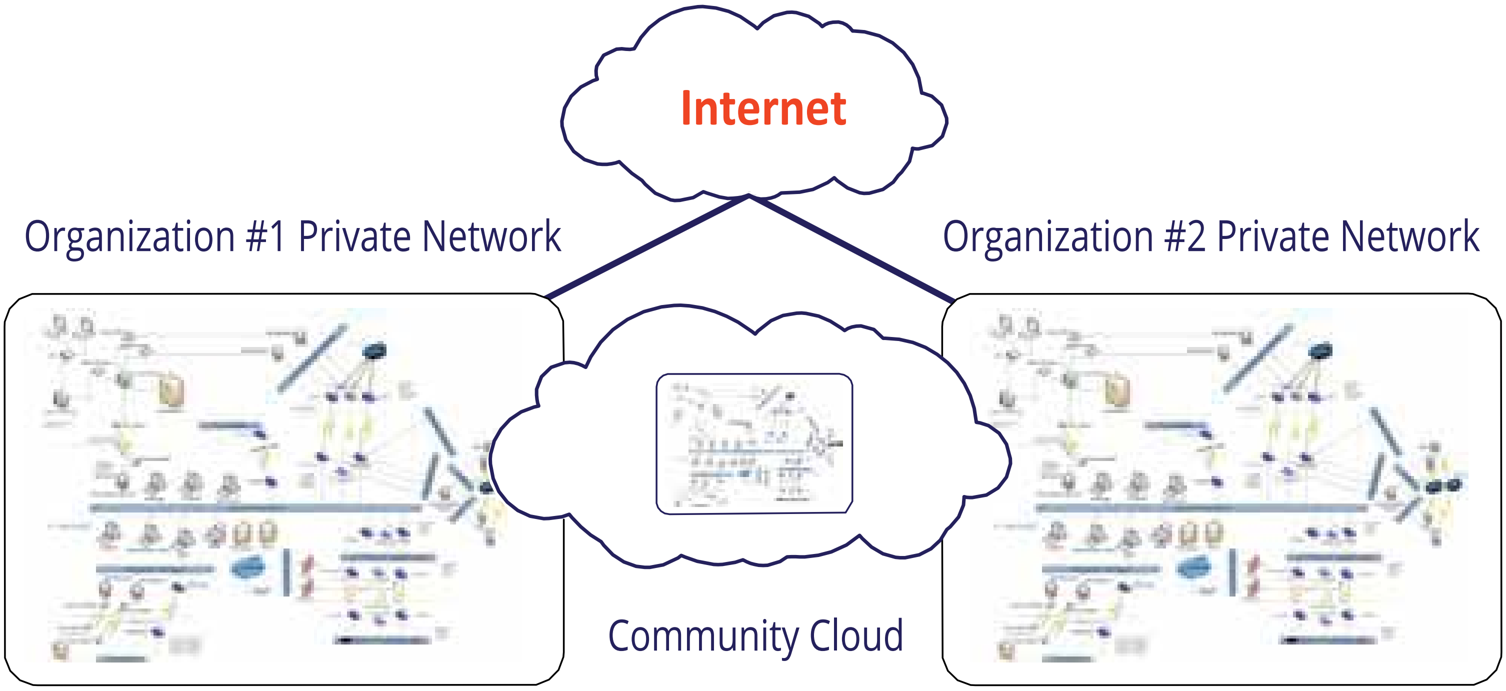
Exhibit 2 | Private Cloud Illustration



Community Clouds

In a community CCE, multiple tenant organizations with common characteristics (e.g., mission goals, legal and regulatory security requirements, compliance considerations) share the cloud infrastructure, thus forming a user "community" (see Exhibit 3). The cloud owner may be a community tenant or an independent service provider with an understanding of member organizations' specific needs and goals. Within the federal government, the Defense Information Systems Agency (DISA) Rapid Access Computing Environment (RACE) and the National Aeronautics and Space Administration's (NASA) Nebula, both still in the early stages of development, follow the community CCE model. A community cloud represents a lower information security risk profile than a public cloud and, due to the customization potential, poses fewer legal and regulatory compliance issues. A certain degree of risk associated with multi-tenancy is unavoidable, however.

Exhibit 3 | Community Cloud Illustration


Internet
Organization #1 Private Network
Organization #2 Private Network
Community Cloud

Hybrid Clouds

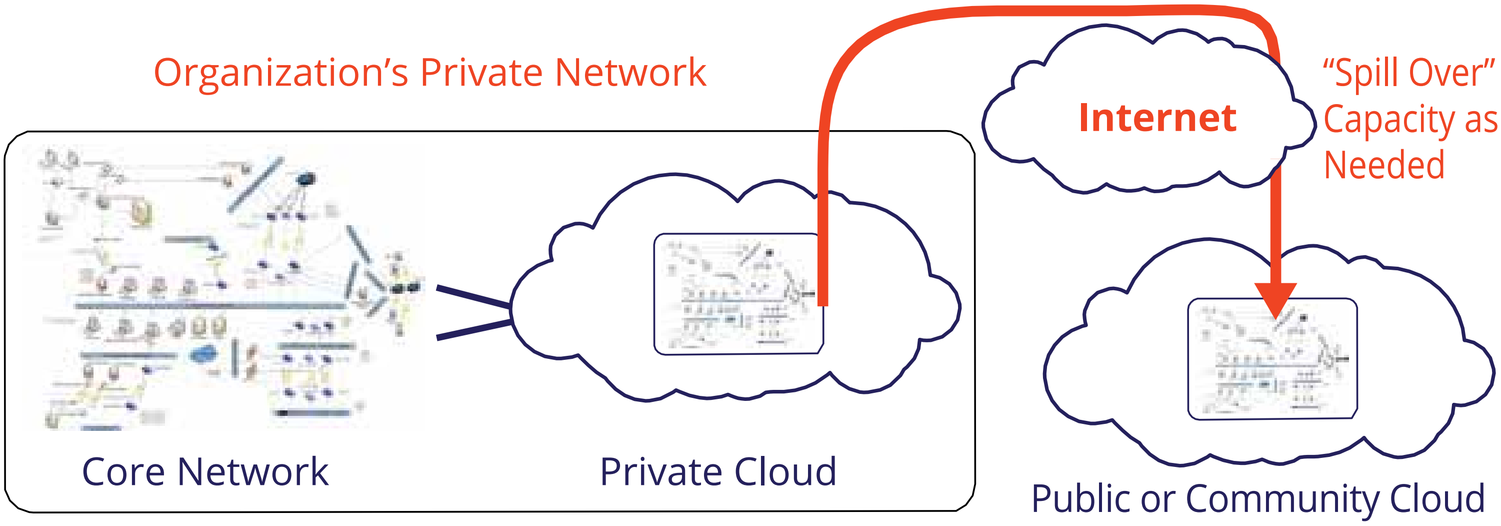
Hybrid CCEs consists of a combination of two or more cloud deployment models (e.g., two public clouds or one public and one community cloud). The component clouds remain distinct entities but are bound together by standardized or proprietary technology that enables data and

application portability throughout the environment (see Exhibit 4). A hybrid cloud thus presents a combination of the information security risks and governance challenges inherent in the deployment models it comprises. A combination of private and community clouds represents the lowest risk; a combination of multiple public clouds poses the greatest information security risks and regulatory compliance challenges.

Each CCE model presents a different profile of benefits and risks that must be carefully considered before adoption. Organizations should choose a framework that meets their requirements while helping them address risks. Although the information security management and governance framework

we present in the next section can be adapted to any CCE deployment model, we focus our discussion primarily on community cloud environments, which represent the most likely near-term adoption and migration strategy for federal government agencies.

Exhibit 4 | Hybrid Cloud Illustration


Organization's Private Network
Internet
"Spill Over" Capacity as Needed
Core Network
Private Cloud
Public or Community Cloud

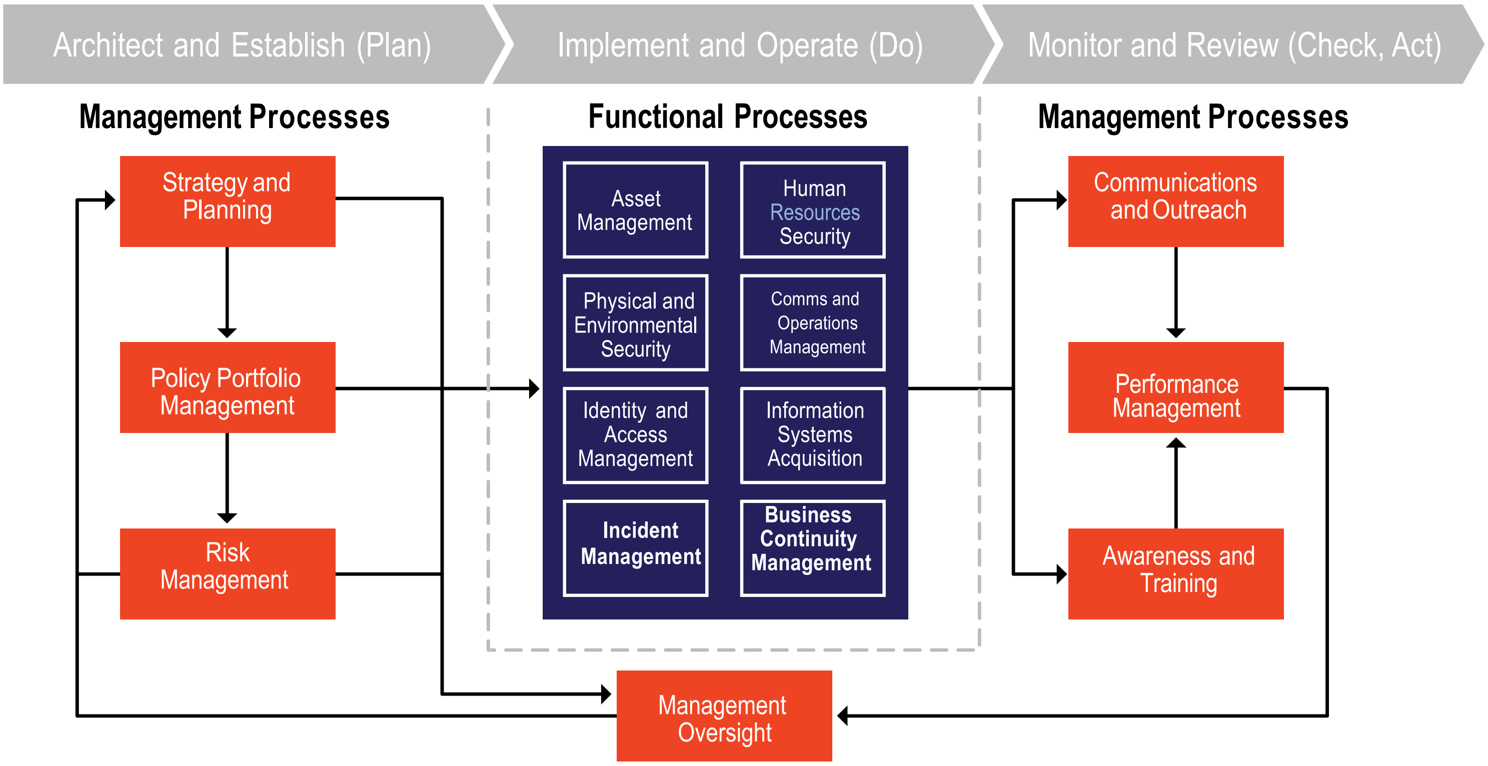
The Information Security Management and Governance Framework

Viderity developed the information security management and governance framework and has customized and deployed it within a variety of client environments. This framework is a system of management and functional processes implemented in a standard quality management cycle of continuous improvement (PLAN, DO, CHECK, ACT). The framework is based on evolving international standards[2], including the planned evolution of the National Institute of Standards and Technology (NIST) Risk Management Framework.[3] Seven management processes -strategy and planning, policy portfolio management, risk management, awareness and training, communication and outreach, compliance and performance management, and management oversight - comprise this framework and support the functional processes of the DO phase (see Exhibit 5).

Although the purpose of each of the seven framework processes will not change when applied to a CCE, many of the process considerations and required actions will need to be modified to effectively plan, manage, and govern information security in the cloud environment . In all cases, it will be necessary to clarify specific roles, responsibilities, and accountability for each major process step. Some steps may be points for negotiation with prospective cloud service providers during the drafting of SLAs and contracts.

Our assumption in the following discussion is that the primary responsibility for information management and governance processes within a federal government agency rests with a centralized security function such as the office of the Chief Information Security Officer (CISO), with considerable participation by information technology management, including the office of the Chief Information Officer (CIO). This centralized security and technology group would perform the cloud provider acquisition function and manage the service provider relationship over the duration of the agreement. This group would also provide all needed policy guidelines to be followed when implementing cloud computing-based services.

Exhibit 5 | Information Security Governance Framework


Architect and Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check, Act)
Management Processes
Strategy and Planning
Policy Portfolio Management
Risk Management
Functional Processes
Asset Management
Human Resources Security
Physical and Environmental Security
Comms and Operations Management
Identity and Access Management
Information Systems Acquisition
Incident Management
Business Continuity Management
Management Processes
Communications and Outreach
Performance Management
Awareness and Training
Management Oversight

[2] ISO/IEC 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements.

[3] NIST SP 800-39 Managing Risk from Information Systems.

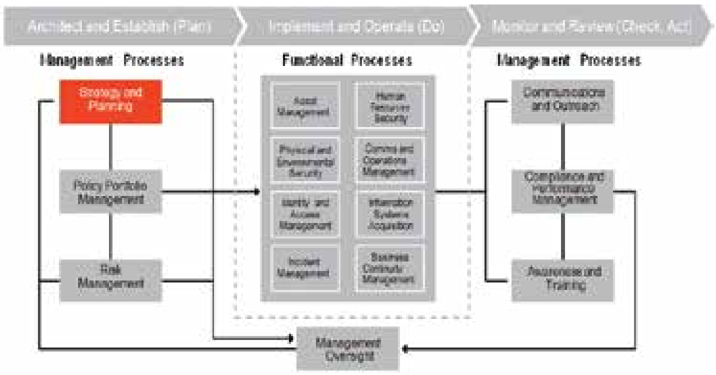
Architecting and Establishing the Information Security Program (PLAN)

Designing an effective information security governance structure hinges on the constructive interaction of three major management processes: strategy and planning, policy portfolio management, and risk management. Together, then, these processes comprise the PLAN phase of the continual improvement process.

Strategy and Planning Process

Strategy and planning are essential to an effective information security management and governance program. The primary aims of the strategy and planning process are:

- To establish information security program direction and guide activities
- To ensure alignment of the information security program with mission goals and objectives
- To define the information security program vision, goals, requirements, and scope

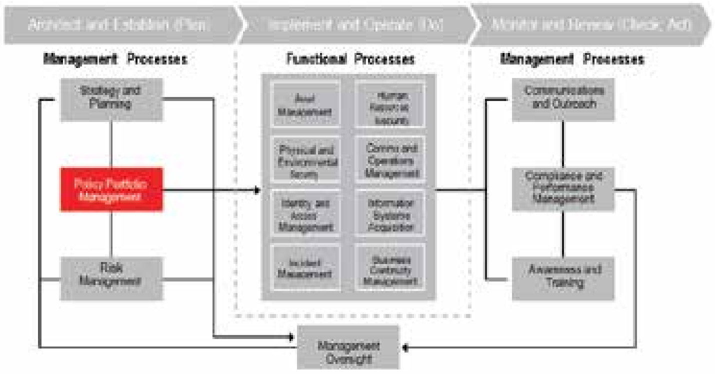

Architect and Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check, Act)
Management Processes
Strategy and Planning
Policy Portfolio Management
Risk Management
Functional Processes
Asset Management
Human Resources Security
Physical and Environmental Security
Comms and Operations Management
Identity and Access Management
Information Systems Acquisition
Incident Management
Business Continuity Management
Management Processes
Communications and Outreach
Compliance and Performance Management
Awareness and Training
Management Oversight

- To ensure consistency with the enterprise information security architecture
- To proactively plan activities to achieve goals and meet requirements
- To determine the best operating model to enable enterprise program efficiency.

The process is performed in collaboration with the risk management and policy portfolio management processes to ensure that program specifications effectively communicate management intent, clearly define roles and responsibilities, sufficiently identify and address information security risks, and provide management with clear choices for resource allocation and optimization.

The activities of the strategy and planning process need not change significantly to accommodate the use of cloud computing services. However, additional knowledge and understanding of the information security risks and compliance and performance management issues that arise in varying cloud computing deployment models will be required. The major impact of the CCE on the strategy and planning process will be the development of CCE-based cost/benefit analyses that include the cost of effective governance to manage risk and ensure legal, regulatory, and contractual compliance. In conjunction with the risk management process, the strategy and planning process will define information security implementations that are allowable for each cloud computing service model based on the relative risk rating of the information and systems migrating to the cloud (e.g., cloud services allowed by system categorization—see Risk Management Process below for further information). In addition, the process will clarify roles, responsibilities, and accountability for baseline information security capabilities within each environment allowed. The planning process will also establish the contractual requirements that will serve as the basis for negotiations with cloud service providers, and will include provisions for the long-term management of the provider relationship.

Policy Portfolio Management Process


Architect and Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check, Act)
Management Processes
Strategy and Planning
Policy Portfolio Management
Risk Management
Functional Processes
Asset Management
Human Resources Security
Physical and Environmental Security
Comms and Operations Management
Identity and Access Management
Information Systems Acquisition
Incident Management
Business Continuity Management
Management Processes
Communications and Outreach
Compliance and Performance Management
Awareness and Training
Management Oversight

The major purposes of the security policy portfolio management process are:

- To define and communicate management expectations for information security
- To translate goals and requirements into actionable mandates

- To establish clearly defined roles and responsibilities for information security
- To inform compliance measurement
- To facilitate efficient and consistent implementations with supporting standards, guidelines, and procedures.

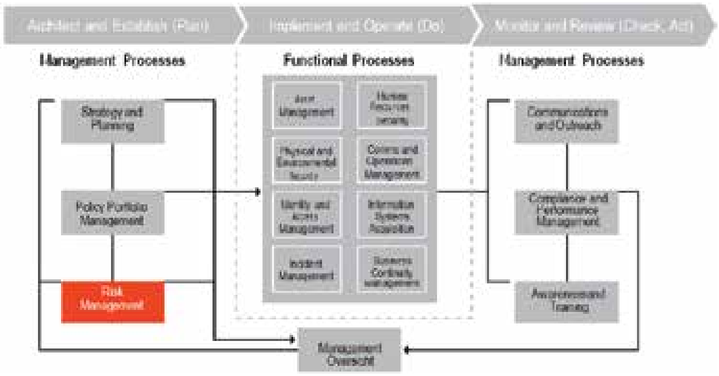
These purposes will not materially change when applied to a CCE. However, the policy portfolio will require additional policies, guidelines, standards, and procedures to effectively direct and govern information security in a CCE. Overarching policies governing agency acquisition and deployment of cloud services will be needed in order to communicate leadership intentions for the safe use of cloud computing, as well as to delineate the authorization process required to initiate such use. Agencies will also need to document guidelines for the appropriate evaluation and contracting of cloud service providers and the selection of environments that meet their information, system risk, and compliance requirements. In coordination with the other two processes making up the PLAN phase, and with the approval and authority of management oversight (ACT phase), the policy portfolio management process will also need to identify the minimum information security and compliance management requirements to be included in SLAs and contracts with cloud service providers.

A thorough audit of all agency security policies must be conducted to ascertain the nature and extent of changes needed to ensure effective governance in a cloud environment. Each policy should be tailored to the chosen cloud deployment model and the specific information and systems authorized for cloud migration. New policies and supporting guidance, standards, and procedures will be necessary in order to effectively manage functional control processes when operating in a CCE. (Such processes include configuration and incident management, chain of evidence and e-discovery procedures, mission continuity management, monitoring and reporting of cloud-based service compliance, and system and data lifecycle assurance.) Guidelines may also be developed to specify mandatory and recommended tools for the monitoring and evaluation of compliance and performance, such as certification and accreditation (C&A) tools, or technical compliance tools such as Layer7. Policy decisions regarding each of the functional control processes must account for the level of control each organization is willing to transfer to the cloud provider while ensuring that the goals and requirements of the information security program are met.

Risk Management Process

An agency's risk management process must be modified in light of the additional variables that arise when migrating agency services to a CCE. The aims of the risk management process include:

- To enable information asset-based protection and mitigation planning
- To enhance the organization's ability to select and apply protection based on the specific risks and threats affecting an asset
- To ensure consistent information security risk assessment methodologies are used throughout the organization
- To facilitate optimization of security expenditures, resources, and activities


Architect and Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check, Act)
Management Processes
Functional Processes
Management Processes
Strategy and Planning
Policy Portfolio Management
Risk Management
Asset Management
Human Resources Security
Physical and Environmental Security
Comms and Operations Management
Identity and Access Management
Information Systems Acquisition
Incident Management
Business Continuity Management
Communications and Outreach
Compliance and Performance Management
Awareness and Training
Management Oversight

- To inform security priorities and planning
- To provide the basis for measuring information security program efficiency and effectiveness.

Risk management methodologies must be revised and updated to effectively consider, treat, or accept the risks inherent in migrating agency information and systems to a cloud environment. For practical reasons, we limit our discussion here to the use of private, community, or private-community hybrid CCE models as the most likely environments for federal agency CCE transition. As noted earlier, until the providers of public cloud services make significant changes to their current offerings and SLAs, the use of those services by the federal government will necessarily be limited to public information and systems with minimal risk and no legal or regulatory security requirements.

Even with our discussion limited to the use of private, community, or associated hybrid cloud services, it is still necessary to consider and include additional risk factors related to the relative degrees of agency control over the service models adopted. The methodology will also need to identify risk mitigations and any residual risks present in each service model for all levels of the agency's risk profile hierarchy for information and systems. For example, agencies will need to modify their current risk calculations focusing on system categorization, privacy, and regulation to appropriately assess risk elevations that will occur when migrating to a CCE utilizing one or more of the three cloud service models under consideration here.

Exhibit 6 summarizes the three models and their relative risk. These suggested risk ratings may be modified to fit with agency-specific risk assessment methodologies, but are in general consistent with the degree of direct agency control associated with each service model. Each cloud service model can be assessed as an information service asset with unique risk ratings and resultant control selection for risk mitigation (e.g., contract terms, SLA content, compliance, monitoring tools).

The relative risk ratings increase as the cloud consumer moves from IaaS to PaaS and finally to SaaS. The service models build on one another, resulting in accumulating risk as the cloud provider assumes more direct control. (PaaS builds on IaaS, and SaaS builds on both IaaS and PaaS, resulting in an increasing assumption of control by the cloud

provider, and corresponding increasing security risks to the cloud consumer.)

New risk analysis methodologies should be closely monitored during the compliance and performance management process (CHECK phase) and modified as necessary to reduce overall information security risk over time. In all cases, the modified risk analysis methodologies and resulting risk rankings must be reviewed during the management oversight process (ACT phase) to ensure management participation, agency-wide risk awareness, and ongoing review and acceptance of both risk treatment options and resultant residual risks.

Exhibit 6 | Service Model Risk Characteristics

Service Model	Risk Characteristics	Relative Additional Risk
Infrastructure as a service (IaaS)	The capability provided to the cloud consumer is to rent processing, storage, networks, and other fundamental computing resources and to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers).	Medium
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy consumer-created applications onto the cloud infrastructure using programming languages and tools supported by the provider (e.g., Java, Python, Net). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.	High
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin client interface, such as a web browser (e.g., web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or individual application capabilities, with the possible exception of limited user-specific application configuration settings.	Very High

Representative CCE-Related Artifacts of the PLAN Phase

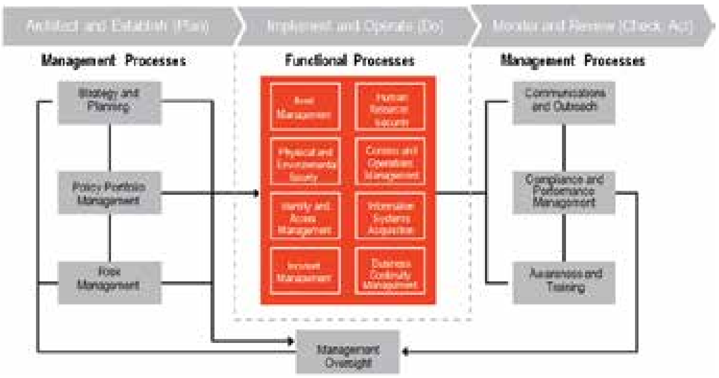
The three management processes of the information security governance framework's PLAN phase will produce several documents to inform and guide users in the effective and appropriate use of cloud computing services. Some specific examples have been included in each process description, but Exhibit 7 summarizes artifacts that are typical outputs of the governance model and will likely have specific references to operating in a CCE. In some cases, the cloud provider may be partially or completely responsible for these artifacts, depending on the nature of agreements between the cloud consumer and the provider.

Exhibit 7 | Plan Phase Artifacts

Management Process	Example Artifact	Contract/SLA Implications
Strategy & Planning	• Security Strategic Plan • Consolidated Security Requirements • Organization Model Modifications • Roles & Responsibilities Charts • CCE Implementation Plans • Budget & Resource Requirements • CCE Contract & SLA	• Goal Performance • Requirements Compliance • Relationship Management • Consumer/Provider • None • None • Terms & Conditions
Policy Portfolio Management	• CCE Security Policy • CCE Acquisition Policy • CCE Authorization Procedure • CCE Standards/Guidelines • CCE Monitoring/Compliance Tools • CCE Configuration Guidelines • CCE-Specific Processes • Risk Management Procedure	• Terms & Conditions • Terms & Conditions • None • None • Terms & Conditions • Technical Compliance • Terms & Conditions • None
Risk Management	• Risk Methodology Modifications • Service Model Risks • Risk Assessment Reports • CCE Controls & Risk Treatments • Systems/Assets Allowed in CCE	• None • None • None • Terms/Responsibilities • None

Implementing and Operating the Information Security Program (DO)

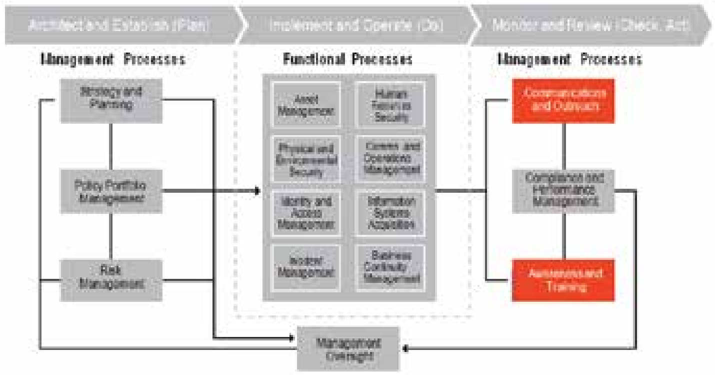
Because this paper focuses on information security governance, we will not discuss in detail the functional processes that constitute the DO phase of the PLAN, DO, CHECK, ACT cycle. The implementation and operation of information security controls contained in each of the functional process areas will vary significantly depending on CCE deployment strategy and the service models used. Other papers address the implementation and operation of information security functional processes and controls, but this topic is not essential to discussions related to the effective management and governance of information security in a cloud environment.


Architect and Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check, Act)
Management Processes
Strategy and Planning
Policy Portfolio Management
Risk Management
Functional Processes
Asset Management
Human Resource Security
Physical and Environmental Security
Control and Operations Management
Identity and Access Management
Information Systems Acquisition
Incident Management
Business Continuity Management
Management Processes
Communications and Outreach
Compliance and Performance Management
Awareness and Training
Management Oversight

Monitoring and Measuring the Information Security Program (CHECK)

Three management processes are included in the CHECK phase of the information security management and governance framework: awareness and training, communication and outreach, and compliance and performance management. Of these three, the compliance and performance management process raises the most significant issues for consideration when migrating services to a CCE.

Awareness and Training and Communication and Outreach Processes

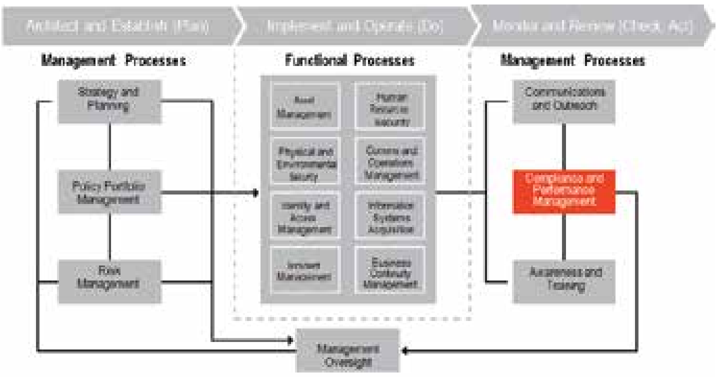

Architect and Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check, Act)
Management Processes
Strategy and Planning
Policy Portfolio Management
Risk Management
Functional Processes
Asset Management
Human Resources Security
Physical and Environmental Security
Comms and Operations Management
Identity and Access Management
Information Systems Acquisition
Incident Management
Business Continuity Management
Management Processes
Communications and Outreach
Compliance and Performance Management
Awareness and Training
Management Oversight

These management processes serve complementary and similar purposes. Those purposes include:

- To consistently communicate the importance of information security throughout the organization
- To educate staff on required actions related to changes in regulatory, legislative, and other mandates
- To broaden and deepen the security awareness of the organization
- To enhance compliance through better understanding and knowledge agency-wide
- To clarify roles and responsibilities
- To drive the ongoing competency of information security staff.

Execution of these management processes will not change as a result of the introduction of a CCE. However, the processes will need to include formal awareness training, outreach efforts, and communication to inform all agency cloud users of the new policies, guidelines, standards, procedures, risks, and compliance issues related to the migration of information services to a CCE.

Compliance and Performance Management Process


Architect and Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check, Act)
Management Processes
Strategy and Planning
Policy Portfolio Management
Risk Management
Functional Processes
Asset Management
Human Resources Security
Physical and Environmental Security
Comms and Operations Management
Identity and Access Management
Information Systems Acquisition
Incident Management
Business Continuity Management
Management Processes
Communications and Outreach
Compliance and Performance Management
Awareness and Training
Management Oversight

Compliance and performance management is the key process in the CHECK phase of the framework. Its principle purposes are:

- To create regular measurement and reporting of progress and issues
- To inform and prioritize program improvements
- To record progress toward achieving strategic goals and compliance with requirements
- To drive continuous improvement of the information security program
- To minimize potential for recurrence of systemic issues
- To optimize consistency and efficiency of security implementations
- To inform modifications to risk analyses and risk mitigations
- To measure and report on compliance with legal, regulatory, and contractual requirements; internal policies; and technical guidelines and standards.

The purposes of the compliance and performance management process remain unchanged in a CCE, but the execution of the process will require significant modification to effectively monitor and measure compliance and performance in the cloud. Focusing again on agency use of private clouds, community clouds, or combinations of the two will lead to enhanced information security compliance and performance in a public cloud environment.

Compliance includes legal, regulatory, and contractual security compliance; compliance with internal policies, guidelines, standards, and procedures; and technical compliance verification. All compliance and performance checking is dependent on a comprehensive measurement and management reporting system. This system must examine every area of compliance, as well as the information security program's effectiveness in meeting goals and objectives. Successful compliance and performance measurement depend on detailed specifications in all SLAs and contracts with the cloud service provider, covering each service model utilized.

In the case of private or community cloud service providers, there will be a greater level of trust, understanding, and flexibility in the agreement negotiations because the provider and the consumer share mission goals as well as legal and regulatory compliance requirements. Federal agency cloud consumers can determine their minimum information security requirements and needed controls for each level of cloud service, based on the cloud service risk profiles; strategic planning of the cloud service; and CCE-specific policies, guidelines, standards, and procedures defined in the PLAN phase. Such knowledge will enable them to drive the SLA and contract negotiations to a satisfactory agreement. SLAs and contracts must minimize security risks; enable effective monitoring and measuring of all legal, regulatory, and contractual

security requirements (by either the service provider or the cloud consumer); and clearly define accountability and legal liability related to any information security breach in the cloud.

Management should present measurement and monitoring reports within periodic reviews of the entire information security program to the information security governance body, along with recommendations for corrective and preventive actions.

Managing and Improving the Information Security Program (ACT)

Participation by management representing all agency stakeholder organizations is essential to the effective oversight of any information security management system. The oversight process and the managerial bodies that execute it form the governance program and represent the ACT phase of the continuous improvement model.

Management Oversight Process

An information security governance body performs the functions of the management oversight process. This body, consisting of senior leadership and representatives from each functional area of the organization, has as its primary purposes:

- To ensure ongoing management involvement in program direction and priorities
- To establish enterprise information security governance
- To ensure the information security program supports mission goals and objectives
- To reinforce the importance of information security throughout the organization
- To oversee risk management, balancing mission goals and information security costs
- To track and optimize information security resource allocation
- To authorize improvements to the information security program on a continuing basis.

These management oversight objectives are valid regardless of the information security operating environments deployed. However, the governance body will need to actively participate in the review, authorization, and communication of all information security plans, policies, and supporting documentation, as well as regularly assess risks and compliance issues related to the use of cloud-based services. Therefore, the governance body will need to include or consult with cloud computing technology and information security experts. The group should also include or consult with agency counsel to ensure a complete understanding and inclusion of legal and liability issues specific to a CCE and to verify sufficient coverage of all issues in negotiated SLAs and contracts for cloud-based services. It is imperative that management sponsors and monitors the effectiveness of cloud- specific awareness training and communication, along with outreach programs to ensure broad knowledge of agency policy and guidelines among all users. Finally, management must be vigilant in its review of compliance and monitoring of cloud services and must drive continuous improvement in the overall information security program.

Representative CCE-Related Artifacts of the CHECK and ACT Phases

The four management processes of the CHECK and ACT phases of the information security management and governance framework will result in several documents and reports to inform and guide users in the effective and appropriate use of cloud computing services, and to report on the compliance and performance of cloud-based systems. Some specific examples have been included in each process description, but Exhibit 8 summarizes artifacts that are typical outputs of the governance model and are likely to have specific references to operating in a CCE. In some cases, the cloud provider may be partially or completely responsible for these artifacts, depending on the agreements between the consumer and the provider.

Exhibit 8 | Act Phase Artifacts

Management Process	Example Artifact	Contract/SLA Implications
Awareness & Training; Communication & Outreach	• User Security Awareness – CCE Policy – CCE Authorization – CCE Guidelines/Standards – CCE Procedures • CCE Security Technical Training • Awareness Tests & Records	• Provider Participation? – Yes – No – Sometimes – Sometimes – No – No
Compliance & Performance Management	• Compliance/Performance Measures • Legal, Regulatory Compliance • Policy Portfolio Compliance • Privacy Compliance • Technical Compliance • Log Monitoring Reports • Incident Management Reporting • Internal Compliance Audits • Performance Measurement Reports • Technical Controls Testing • SLA Reporting • Recommended Improvement Plans	• Terms & Conditions • Roles, Responsibilities • Roles, Responsibilities • Roles, Responsibilities • Roles, Responsibilities • Roles, Responsibilities • Roles, Responsibilities • Terms, Responsibilities • Terms, Responsibilities • Terms, Responsibilities • Terms & Conditions • Negotiation
Risk Management	• CCE Management Review Reports • Authorized Improvement Plans	• None • Negotiation

Summary and Conclusions

Cloud computing takes advantage of economies of scale to offer compelling cost benefits to federal agencies for information services performed in support of their mission. Migration of agency information assets and systems to a CCE can also provide impressive benefits related to deployment flexibility and service on demand, and can enable capabilities not feasible in many enterprise computing environments, such as massive data and intelligence analysis.[4] However, the nature of cloud deployment and service models presents new information security risks and introduces compliance complications for cloud consumers with respect to legal, regulatory, and contractual security requirements. Some of these complications have serious legal liability implications.

Key to the successful adoption of a CCE and subsequent migration of information systems to the cloud is the implementation/modification of a strategic, proactive information security management and governance framework. Viderity has developed a framework that we have successfully implemented in several commercial and federal government client environments. Our model consists of a set of management processes that interact in a PLAN, DO, CHECK, ACT cycle of continuous improvement to effectively manage and govern enterprise information security. The major steps in the execution of the management processes of the governance model require some modifications to effectively manage the risk and compliance issues inherent in a CCE. Information security governance is a critical component of a successful transition to the cloud.

An organization's mission and risk profile must drive the implementation of the management processes described in this paper, as well as the artifacts those processes produce. It is also vital to treat the management processes as integrated components of a larger information security governance framework, rather than as individual silos. Using this framework to guide the transition to and ongoing use of the CCE will ultimately enable an organization to maximize the benefits derived from cloud computing while sensibly and cost-effectively addressing the inherent risks.

Glossary of Acronyms

C&A	Certification and Accreditation
C3F	Viderity's Cloud Computing User Transition Framework
CCE	Cloud Computing Environment
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DISA	Defense Information Systems Agency, part of the Department of Defense
IaaS	Infrastructure as a Service
NIST	National Institute of Standards and Technology.
NIST	guidelines on information security are officially standard practice for federal information technology and are codified in information security regulations
PaaS	Platform as a Service
RACE	Rapid Access Computing Environment. This refers to a working prototype cloud developed by DISA. As of this writing, it is being used for open-source software development, and many additional functions are in the works
SaaS	Software as a Service
SLA	Service-Level Agreement. In this case, this refers to a contract between the cloud computing provider and client(s)
SP	Special Publication

Glossary of Terms

Cloud

The "cloud" consists of computing resources (software, operating platform, memory, and processors) that are abstracted from the user by some form of virtualization and (often) physical separation between the user and the infrastructure on which the services are supported. "Cloud computing" refers to the use of a cloud for IT functions.

Cloud Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Cloud Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer- created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Community Cloud

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premises or off premises.

Hybrid Cloud

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain distinct entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Multi-tenancy

Property of a cloud environment used by multiple customers ("tenants"). Contrast with the "single-tenancy" private cloud, which is used by only one customer.

Private Cloud

The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premises or off premises.

Public Cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Service Model

Refers to the ownership of the cloud infrastructure. See the Introduction for descriptions of different service models.

VIDERITY

STRATEGIC, CREATIVE, TECHNICAL

www.viderity.com