

Security Authorization

An Approach for Community Cloud Computing Environments



by

Perry Bryden

bryden_perry@bah.com

Daniel C. Kirkpatrick

kirkpatrick_daniel@bah.com

Farideh Moghadami

moghadami_farideh@bah.com

Booz | Allen | Hamilton

delivering results that endure

Security Authorization

An Approach for Community Cloud Computing Environments

The objective of this paper is to provide an approach to performing assessment and authorization of cloud computing environments (CCE) in accordance with existing National Institute of Standards and Technology (NIST) guidance. Although the assessment and authorization approach described in this paper can be adapted to all of the private, public, hybrid, and community cloud deployment models, the primary focus of this paper is providers and consumers of CCE services for civil agencies utilizing the community cloud deployment model. Consistent with the full transformation of the certification and accreditation (C&A) process into the six-step Risk Management Framework (RMF) described in NIST Special Publication (SP) 800-37 Revision 1, Guide for Security Authorization of Federal Information Systems: A Security Life Cycle Approach,¹ throughout this paper we use the term “security authorization” when referring to the assess and authorize steps of the RMF. In addition, we use the term “provider” to refer to the organization providing CCE services to other organizations and “consumer” to identify an organization acquiring and utilizing the CCE services of a provider.

The following sections provide a brief introduction to cloud computing services and security authorization processes and the significant issues encountered when attempting to perform traditional security authorization for CCE services. The introduction is followed by “A New Approach to Cloud Computing Security Authorization,” which provides guidance for performing security authorization of CCE services. This approach differs from the traditional approach and is tailored specifically to the cloud environment. The final section summarizes the proposed approach.

Cloud Computing

According to NIST—

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. This cloud model promotes availability and is composed of five essential **characteristics**, three **service models**, and four **deployment models**.²*

In some ways, cloud computing is an expansion of server hosting, outsourcing, web-based computing, managed security services, and other past and present service offerings. New and different in cloud computing are the five essential characteristics of—

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service.

The community CCE deployment model, or community CCE, discussed in this paper will also provide one of three service models:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS).

NIST defines the community cloud deployment model as “the cloud infrastructure shared by several organizations in support of 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 premise or off premise.”³

Appendix B includes the full NIST definition of the five essential characteristics, three service models, and four deployment models.

¹ <http://csrc.nist.gov/publications/drafts/800-37-Rev1/SP800-37-rev1-IPD.pdf>.

² <http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>.

³ *Ibid.*

Security Authorization

Security authorization is the successful application of the RMF process described in NIST SP 800-37, illustrated in Exhibit 1. NIST developed the RMF to provide organizations with a structured yet flexible process for managing risk related to the operation and use of information systems. Organizations use the RMF to determine the appropriate risk mitigation needed to protect the information systems and infrastructure that support organizational mission and business processes. The RMF incorporates a well-defined set of information security standards and guidelines for

federal agencies and support contractors to facilitate and demonstrate compliance with the Federal Information Security Management Act of 2002 (FISMA).

Information Security

Security is a property of a well-designed system. As defined by FISMA, “The term ‘information security’ means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction”⁴ to provide—

- **Confidentiality.** Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information
- **Integrity.** Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity
- **Availability.** Ensuring timely and reliable access to and use of information.⁵

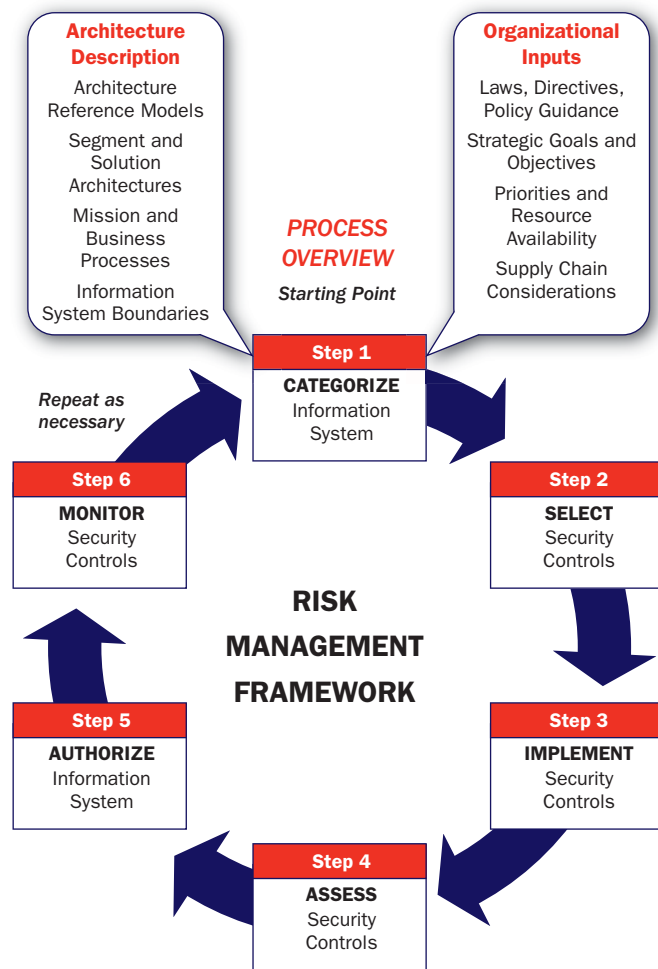
Security is not a feature; it is a property of a system. It results from thorough analysis of security requirements, sound architecture and design, and secure coding practices.

Purpose of Security Authorization

NIST SP 800-37 Revision 1 defines security authorization as the means to—

- Ensure that managing risk from the operation and use of federal information systems is consistent with the organization’s mission/business objectives and overall risk strategy established by senior leadership through the risk executive function
- Ensure that information security requirements, including necessary security controls, are integrated into the organization’s enterprise architecture and system development lifecycle (SDLC) processes
- Support consistent, well-informed, and ongoing security authorization decisions (through continuous monitoring), security transparency, and risk-related information

Exhibit 1 | Risk Management Framework



Source: NIST SP 800-37 Revision 1

⁴ <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>.

⁵ Ibid.

- Achieve more secure information and information systems within the Federal Government through the implementation of appropriate risk mitigation strategies.⁶

Security authorization is a process for assessing the security of a system or application by identifying risks and determining which identified risks have been mitigated to the extent that the cost (time, difficulty, etc.) to exploit them is greater than the expected gain from exploiting them. Where risks cannot be sufficiently mitigated, security authorization provides a process for documenting these residual risks. This documentation provides information for an authorizing official or designated representative to use in determining whether or not to allow the system to operate within the enterprise. A new or updated security authorization is required when the system is initially deployed, periodically in accordance with federal or agency policy, and whenever a significant change to the system or the operational environment occurs.

Practice of Security Authorization

In traditional (non-cloud computing) environments, information resources are allocated to an information system to define the boundary for that system. Performing security authorization on these traditional systems requires defining the boundary; selecting, implementing, and assessing the security controls; and making an authorization decision. Section 2.3 of NIST SP 800-37 Revision 1 states that—

One of the most challenging problems for information system owners, authorizing officials, chief information officers, senior information security officers, and enterprise information security architects is identifying establishing appropriate boundaries for information systems. Well defined boundaries establish the scope of protection for organizational information systems (i.e., what the organization agrees to protect under its direct management control or within the scope of its responsibilities) and include the people, processes, and information technologies that are part of the systems supporting the organization's missions and business processes.

⁶ Ibid.

*The application of security controls within a complex information system or a system of systems, can present significant challenges to an organization. To make this problem more manageable, the information system owner, in collaboration with the authorizing official, senior information security officer, enterprise information security architect, and information system security engineer, examines the purpose of the information system and considers the feasibility of decomposing the system into more manageable components. The decomposition of an information system into multiple components, or subsystems each with its own subsystem boundary, facilitates a more targeted application of security controls to achieve adequate security and a more cost-effective risk management process. The system decomposition into subsystem components is reflected in the security plan for that system.*⁷

Even though the complex information system (system of systems) is decomposed into subsystem components that can be assessed independently, the components of the system are defined up front and the authorization is applied to the entire information system.

Each subsystem component of a traditional information system includes hardware, an operating system, network components, the data store, and the application with its user interface. Security controls, as defined in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, address all of these layers for each system. The selection, implementation, and assessment of these security controls, which are the criteria for security authorization testing, are based on a view of systems as pre-defined collections of platforms, data sources, applications, and user interfaces that are owned and operated by a single organization for a known set of users.

Cloud Computing Security Authorization Challenges

The traditional approach to security authorization lacks the flexibility to address CCE services. Exhibit 2 shows a notional architecture for an IaaS CCE with multiple

⁷ Ibid.

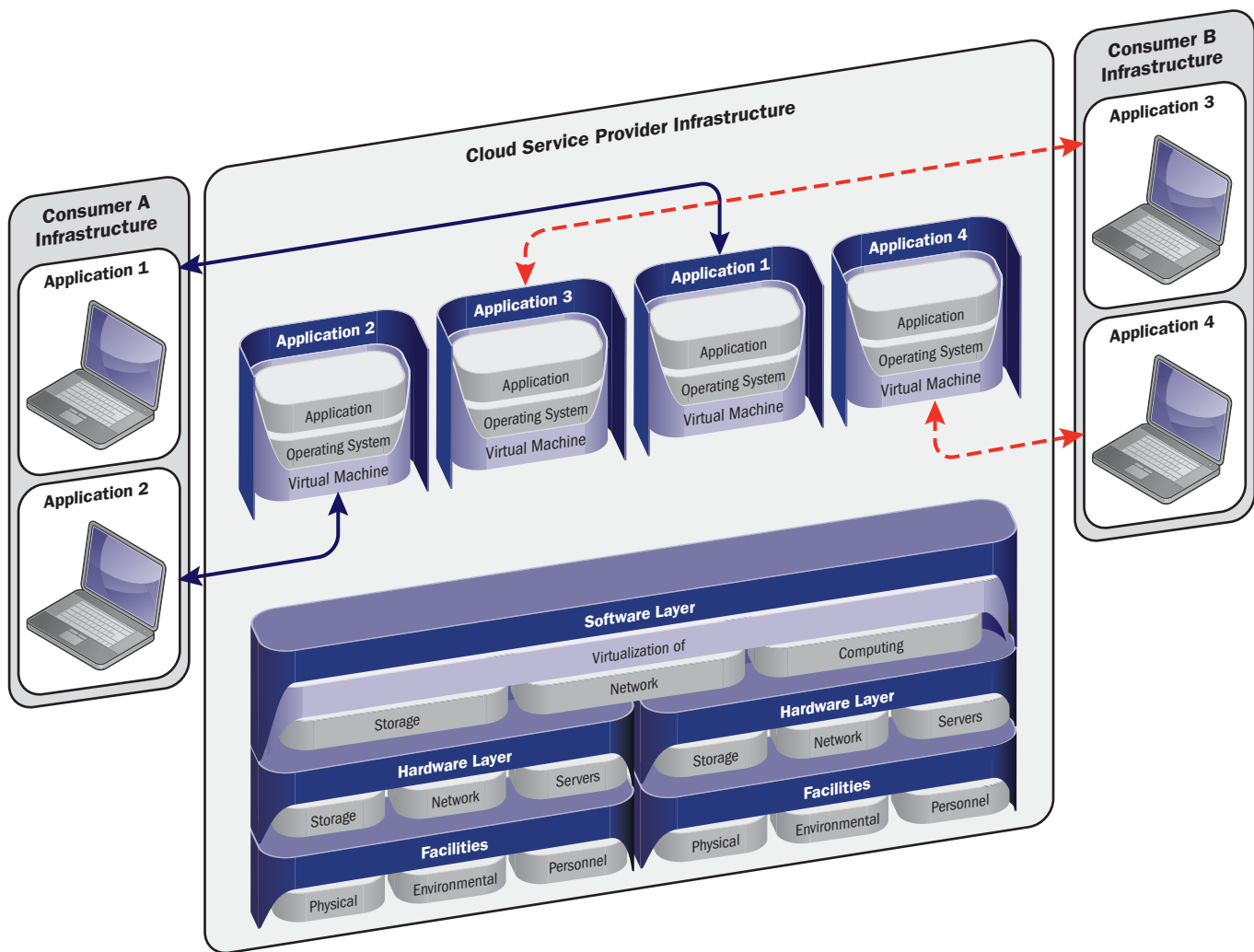
consumers—also known as tenants—each operating unique applications.

The CCE depicted in Exhibit 2 shows that the physical, environmental, personnel, computing, storage, and network security controls are under the direct management control of the CCE provider. The “software layer” forms the foundation on which the CCE consumer’s information systems and applications depend. In the community CCE, the provider has potentially hundreds of consumers or tenants, each of

which is required to perform a security authorization of their information system. Specific challenges to the traditional security authorization approach encountered in community CCEs include the following:

- Traditional security authorization approaches require a separate security authorization of the CCE provider for each of the potentially hundreds of consumers (tenants).
- The capability for near real-time expansion and contraction (or elasticity) of CCEs is a challenge

Exhibit 2 | Notional IaaS CCE With Traditional Security Authorization Boundary



Source: Booz Allen Hamilton

in the traditional security authorization approach, in which systems and components are statically defined.

- The varying degree of direct management control by the CCE consumer in the IaaS, PaaS, and SaaS service models and the directly associated degree of risk for the corresponding service model must be addressed.

A security authorization approach is needed that addresses these new security authorization challenges within the community CCE.

A New Approach To Cloud Computing Security Authorization

Ideally, security authorization for CCE services will complement the flexible design and rapid deployment features of the services. Booz Allen Hamilton's recommended approach for achieving this goal is to define each CCE provider service as an independent information system with its own security authorization boundary, as shown in the red box in Exhibit 3 (page 6). As a result, the line of demarcation between security controls under the direct management control of consumer and provider organizations is more easily and consistently determined.

In Booz Allen's recommended approach, each community CCE provider service is independently authorized, so each CCE consumer must authorize only the portion of the CCE services under its direct management control. The CCE provider now performs one authorization per service offering, and each CCE consumer is accountable for authorizing the instantiation of its information system, thus inheriting the provider's authorization of the underlying layers. Instead of relying on static information system boundaries, in Booz Allen's approach the authorization is centered on a given service offering, with specific requirements for any hardware, software, networks, storage, and facilities used in support of the service.

This shift in approach addresses the challenges outlined in the previous section. Redefining the

security authorization boundary in this fashion requires addressing four different considerations:

- Establishing standardized system configurations that can be authorized by "type"
- Managing the potentially large and rapidly changing number of subsystems within a CCE
- Appropriately measuring the risk of the CCE provider and consumer configurations
- Carefully analyzing the level of service the CCE provider is able to provide.

Service-level agreements (SLA) must be in place between provider and consumer to ensure all parties understand and agree on the services being provided.

The independent authorization of the CCE provider can allow the CCE consumer to inherit operational security protections, just as traditional information systems inherit operational security protections from their operational environment. This inheritance model of security authorization can be applied within the provider CCE as well. For example, a separate assessment of each facility could be performed, and the storage environment could be assessed separately. The individual assessments would be combined to create an entity called the provider CCE security authorization.

CCE Provider Security Authorization

CCE provider services comprise a collection of networks, servers, storage, and applications. These hardware platforms exist in one or more physical sites, as shown in the "facilities" and "hardware layer" of Exhibit 2. This CCE provider environment can be authorized following the existing approach for independently authorizing information systems.

NIST SP 800-37 Revision 1 defines three types of security controls that must be allocated:

- **System-Specific Controls.** Controls implemented within an information system

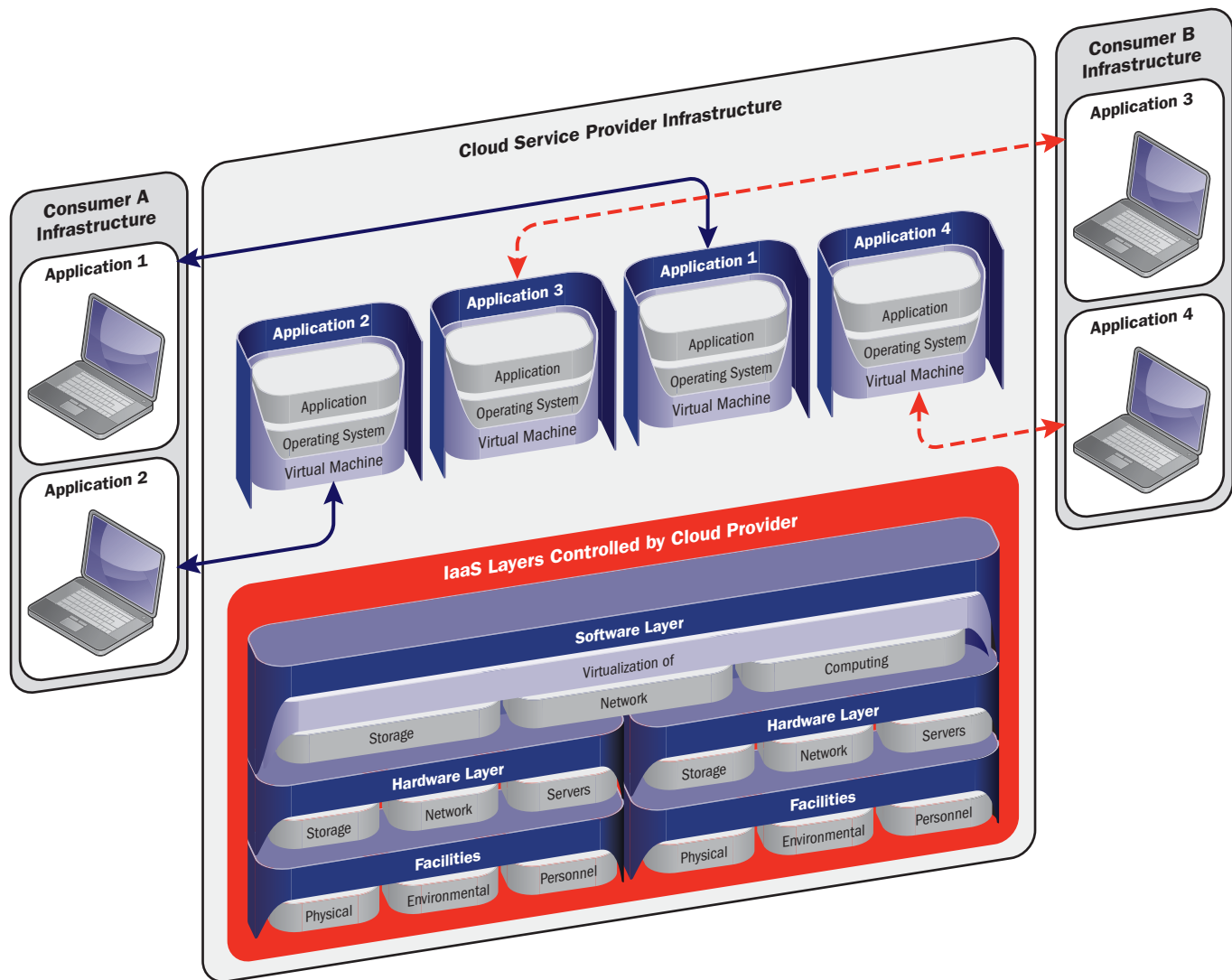
- **Common Controls.** Controls inherited by an information system
- **Hybrid Controls.** Controls that have both system-specific and common characteristics.⁸

NIST SP 800-37 Revision 1 also explains the following:

Security controls are allocated either to an information system or its environment of operation. The allocation of security controls is consistent

with the organization's enterprise architecture and information security architecture. By allocating security controls to an information system (e.g., access controls, identification and authentication controls, audit controls) or the system's environment of operation (e.g., physical and environmental protection controls, personnel security controls), the organization assigns responsibility to specific organizational entities for the development,

Exhibit 3 | Notional IaaS CCE With Redefined Security Authorization Boundary



Source: Booz Allen Hamilton

⁸ Ibid.

implementation, assessment, authorization, and monitoring of those controls.⁹

Using this model, the CCE provider and consumer establish a collaborative workgroup involving the chief information officer, senior agency information security officers, authorizing officials, information system owners, and information system security officers from each organization. The purpose of this workgroup is to establish an agreement allocating security controls to the CCE provider or the CCE consumer. The CCE consumer then inherits the CCE provider security controls as “common security controls” for the purposes of the CCE consumer security authorization. Exhibit 4 shows the shift in levels of inherited security controls by CCE service model. This variation of inherited security controls does not affect the security authorization approach.

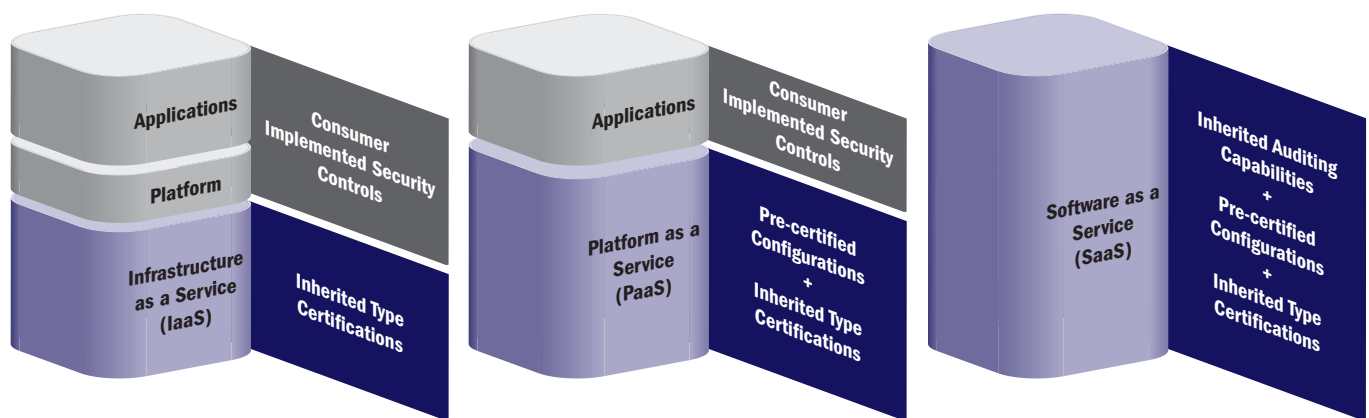
Evaluating the risks associated with deploying an information system for which components outside the information system’s own authorization boundary provide the majority of its security control enforcement is a challenge. The following strategies help address this challenge:

- Establish and follow a governance framework that considers the unique challenges of the CCE. Our

recommended information security governance framework comprises seven management processes: strategy and planning, policy portfolio management, risk management, awareness and training, communication and outreach, compliance and performance management, and management oversight.¹⁰

- Establish terms and conditions for the provider and consumer CCE through SLAs, including the following:
 - **Information Ownership.** The organization documents the ownership of information and asserts ownership [Assignment: organization-defined ownership type] of information stored on information systems provided by the cloud services provider through an SLA with that provider.
 - **Right to Audit.** The organization asserts the right to audit the cloud services provider’s assurance documentation and to review [Assignment: organization-defined frequency] third-party assessment reports of the cloud services provider through an SLA with the cloud services provider.
 - **Unauthorized Disclosure.** The organization asserts through an SLA with the cloud services provider that the provider may not disclose

Exhibit 4 | Shift of Controls by Service Model



Source: Booz Allen Hamilton

⁹ Ibid.

¹⁰ This topic is addressed in depth by Booz Allen’s *Information Security Governance: Implications for the Cloud Computing Environment*; available at www.boozallen.com.

organization-owned information without prior written approval of the organization's authorizing official.

- **Investigations.** The organization asserts through an SLA with the cloud services provider the right to obtain results of security incident investigations at the cloud services provider's facilities and conduct follow-up investigations.
- **Information Dispersal.** The organization documents information dispersal restrictions [Assignment: organization-defined restrictions] and enforces these restrictions through an SLA with the cloud services provider.
- **Cloud Services Availability.** The organization defines acceptable levels of availability [Assignment: organization-defined system uptime, throughput and response time] through an SLA with the cloud services provider.
- Establish formal communication procedures between CCE provider and consumer regarding upgrades and maintenance, computing resource allocation, and incident and emergency response.
- Conduct an independent risk assessment of the CCE.
- Allocate security control enforcement responsibilities to the CCE provider and consumer and identify dependencies.
- Establish standardized system, subsystem, and application configurations that can be authorized by type and then create hardened images implementing applicable security controls to simplify the deployment of each subsystem type.
- Employ (for information system components under the CCE's control) automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory for use in monitoring and management to address the dynamic nature of CCEs (done by the CCE provider and consumer).
- Establish effective security change management processes, including security impact analyses on

actual or proposed changes to the information system and its environment of operation.¹¹

- Test the system in a representative CCE environment.
- Authorize the provider CCE independently.
- Authorize the consumer CCE system for deployment on provider CCE.

CCE providers and CCE consumers can apply this same approach, resulting in a set of security controls and identified vulnerabilities associated with the service delivered by the CCE provider to each CCE consumer. The set of security controls and identified vulnerabilities for each CCE provider may be different. Therefore, the residual risk associated with each service offering may be different for each consumer CCE. It is important to take this into consideration when designing and deploying each consumer CCE.

A recommended list of security controls from NIST SP 800-53 Revision 3 that are applicable to CCEs is available separately from this white paper.¹² These controls should be considered a supplement to the control baseline for a given system.

CCE Consumer Security Authorization

Using the CCE provider security authorization approach described above, individual CCE consumers still require a new or updated security authorization package under some circumstances, including—

- When the system is initially deployed
- Periodically in accordance with federal or agency policy
- Whenever a significant change to the system or the operational environment of the consumer CCE occurs.

To demonstrate compliance with the assigned security control baseline, it is necessary to first determine which organization (provider or consumer) is responsible for enforcing each security control and then to identify dependencies between the consumer

¹¹ This topic is addressed in depth by Booz Allen's *Security Change Management: The Answer to Evolving Security Requirements*; available at www.boozallen.com.

¹² Booz Allen-recommended security controls for CCEs; available at www.boozallen.com.

CCE and the provider CCE. The System Security Plan, as defined by NIST SP 800-37, provides the means to document the security controls designated as system-specific controls, common security controls, and hybrid security controls. It is also important to identify operational conditions for the consumer CCE relevant to the specific provider CCE where the system will be deployed. The conditions associated with that environment will generally provide significant indicators of the risk associated with the system environment.

Because the provider CCE security authorization addresses many of the security controls for a consumer CCE, the process of performing security authorization for a consumer CCE can be streamlined. Consumer CCEs require continuous monitoring that provides visibility into the provider CCE, combined with effective security change management processes. Changes to the provider CCE necessitate an update of the security authorization for individual CCE consumers.

Subsystem “Type” Authorization

Subsystems are approved for operation based on the level of risk they introduce to the organization, which depends on several factors. Two risk factors are (1) the degree of compliance with the assigned set of security controls from NIST SP 800-53 and (2) the number and severity of the vulnerabilities identified in the subsystem design. Booz Allen recommends the use of hardened images with all of the applicable security controls applied wherever possible. All subsystems exist within network boundaries and rely on the boundary protection devices of the network to provide security. Subsystems that exist within a common set of boundary protection devices are authorized separately. NIST SP 800-37 Revision 1 allows for a subsystem (with its own subsystem boundary) to be authorized by type to facilitate a more targeted application of security controls to achieve adequate security and a more cost-effective risk management process. This type authorization of standardized subsystems or applications, within the provider or consumer boundaries, allows the inheritance of

security controls from the CCE where they reside. This inheritance simplifies the requirements for security authorization of the type of system. Each unique subsystem configuration and set of system-specific controls is implemented using hardened images and, in turn, authorized without affecting the authorization status of the provider or consumer CCE. This approach supports the dynamic nature of a CCE, in which a number of authorized subsystems can rapidly increase or decrease to support demand. The use of hardened and authorized subsystem images further streamlines the deployment of each system type.

Automated Security Authorization Tool

NIST SP 800-37 Revision 1 guidance encourages the use of automation and automated support tools to provide senior leaders the necessary information to make credible, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions. In harmony with this guidance, we strongly recommend that the CCE provider and consumer implement an automated security authorization process/compliance tool and create “parent-child” relationships between the environments. This tool would automate and streamline the security authorization process and generate all required NIST security authorization package deliverables, while helping information assurance (IA) managers and senior decision makers comprehend the scope and state of IA activities across their enterprise. Specifically, this tool would track security control allocations, dependencies, and inheritance; simplify the generation of security authorization evidence required by CCE consumers; and simplify the maintenance of CCE provider security control implementations.

Conclusion

Security authorization can be accomplished in a community CCE—while maintaining the rapid elasticity and other characteristics of CCEs—by implementing the following six actions:

- **Redefine the Concept of Information System Boundaries.** CCEs comprise resource pools of networks, servers, storage, applications, and services that expand and contract to support demand. As a result, each CCE is considered a system for the purposes of security authorization.
- **Authorize Provider CCE, Consumer CCE, and Subsystems.** Subsystems are dependent on the environment in which they operate, which includes the provider CCE and consumer CCE. Subsystem type authorization is performed today, enabling streamlined security authorization for provider and consumer CCEs as independent systems.
- **Identify an Appropriate Inheritance Mechanism for CCEs.** Authorization of individual CCEs requires identifying which security controls each consumer CCE inherits from its provider CCE so that the security authorization of the consumer CCE can focus on only the controls the service does not inherit.
- **Identify an Appropriate Mechanism for Monitoring and Management of CCE.** CCEs comprise resource pools of networks, servers, storage, applications, and services that expand and contract to support demand. As a result, each CCE must leverage automated tools to maintain an up-to-date, complete, accurate, and readily available inventory of information system components for use in monitoring and management.
- **Measure the Risk of the CCE Provider and Consumer Configurations Appropriately.** Risk assessment of the CCE must address the unique analysis, mitigation, and continuous management and identification of risks within CCEs. The output of the risk assessment should be strategies for sustained compliance with the guidelines of NIST SP 800-53 during the SDLC.

- **Establish SLAs Between CCE Provider and Consumer.** SLAs must be in place between the provider and consumer to ensure all parties understand and agree on the services provided. Six key areas for SLAs are described in the CCE Provider Security Authorization section.

Booz Allen understands the unique security authorization challenges our federal government clients face when deploying CCEs. Our approach to security authorization for civil community CCEs provides a framework to help organizations successfully address the challenges of these environments. We have the experience to identify and solve today's problems, and we can tailor our approaches to any organization's specific needs. Booz Allen offers a full spectrum of security services for program assessment, risk management, security architecture, design and system implementation, security monitoring, solution integration and testing, security authorization, operations security assessment, and compliance determination.

Appendix A Acronyms

C&A	Certification and Accreditation
CCE	Cloud Computing Environment
CIO	Chief Information Officer
FISMA	Federal Information Security Management Act
IaaS	Infrastructure as a Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PaaS	Platform as a Service
RMF	Risk Management Framework
SaaS	Software as a Service
SDLC	System Development Lifecycle
SLA	Service-Level Agreement
SP	Special Publication

Appendix B Cloud Computing Definitions¹³

Essential Characteristics

On-Demand Self-Service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad Network Access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, PDAs).

Resource Pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid Elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models

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 e-mail). 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.

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 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, and deployed applications and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models

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 premise or off premise.

Community Cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns

¹³ Draft NIST working definition of cloud computing v15; <http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>.

(e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organization or a third party and may exist on premise or off premise.

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.

Hybrid Cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique 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).

About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for 95 years. Every day, government agencies, institutions, corporations, and not-for-profit organizations rely on the firm's expertise and objectivity, and on the combined capabilities and dedication of our exceptional people to find solutions and seize opportunities. We combine a consultant's unique problem-solving orientation with deep technical knowledge and strong execution to help clients achieve success in their most critical missions. Providing a broad range of services in strategy, operations, organization and change,

information technology, systems engineering, and program management, Booz Allen is committed to delivering results that endure.

With more than 22,000 people and \$4.5 billion in annual revenue, Booz Allen is continually recognized for its quality work and corporate culture. In 2009, for the fifth consecutive year, *Fortune* magazine named Booz Allen one of "The 100 Best Companies to Work For," and *Working Mother* magazine has ranked the firm among its "100 Best Companies for Working Mothers" annually since 1999.

Contact Information:

Perry Bryden

Associate

bryden_perry@bah.com

703/984-1105

Daniel C. Kirkpatrick

Associate

kirkpatrick_daniel@bah.com

703/377-4165

Farideh Moghadami

Associate

moghadami_farideh@bah.com

703/377-7979

To learn more about the firm and to download digital versions of this article and other Booz Allen Hamilton publications, visit www.boozallen.com.

Principal Offices

ALABAMA

Huntsville

CALIFORNIA

Los Angeles

San Diego

San Francisco

COLORADO

Colorado Springs

Denver

FLORIDA

Pensacola

Sarasota

Tampa

GEORGIA

Atlanta

HAWAII

Honolulu

ILLINOIS

O'Fallon

KANSAS

Leavenworth

MARYLAND

Aberdeen

Annapolis Junction

Lexington Park

Linthicum

Rockville

MICHIGAN

Troy

NEBRASKA

Omaha

NEW JERSEY

Eatontown

NEW YORK

Rome

OHIO

Dayton

PENNSYLVANIA

Philadelphia

SOUTH CAROLINA

Charleston

TEXAS

Houston

San Antonio

VIRGINIA

Arlington

Chantilly

Falls Church

Herndon

McLean

Norfolk

Stafford

WASHINGTON, DC

The most complete, recent list of office and addresses and telephone numbers can be found on www.boozallen.com by clicking the "Offices" link under "About Booz Allen."