Creating Business Value with Effective, Pervasive Cloud Security and Cloud Enablement Services

Managing Governance, Risk, and Compliance for Cloud Information Security

Introduction

Businesses today are facing and responding to increasing economic and market pressures to adopt new IT models like cloud computing. As a result, cloud computing adoption rates are increasing, and some analysts predict that 30 to 50 percent of IT services could move to the cloud in the coming decade. Sometimes called Internet- or web-based computing, cloud computing abstracts IT resources and services from the underlying It infrastructure, cost-effectively pools the infrastructure resources, and provides them on demand and at scale in a shared, multitenant, and elastic cloud environment.

Cloud computing can help enterprises to lower infrastructure costs, including security infrastructures, and maximize limited capital and operational spending. It also facilitates the management of a multitenant infrastructure while aligning and optimizing internal processes. In addition to securing the user experience, cloud computing can enable the rapid delivery of service-level agreements (SLAs) for applications, as well as help meet the demand for rapid service provisioning and services coupled with chargeback processes.

Yet, according to a 2010 ISACA Survey on the security implications of cloud computing, only 17 percent of respondents believed that the benefits of cloud computing outweighed the risks.

One source of worry for IT is the very thing that makes cloud computing so cost-effective: other tenants who are sharing the multitenant cloud. Many business leaders and service providers see multitenant clouds and their tenants as potential entry points for viruses and malware or points where users are exposed to account/service and traffic hijacking. When combining lines of business as part of consolidation efforts or migrating businesses to a shared environment, failure to segregate and isolate users, data, policies, and procedures can put everyone at risk. Other cloud security concerns include: data loss and leakage; enabling business continuity and disaster recovery in the cloud; and managing service-level agreements (SLAs) and the security environment.

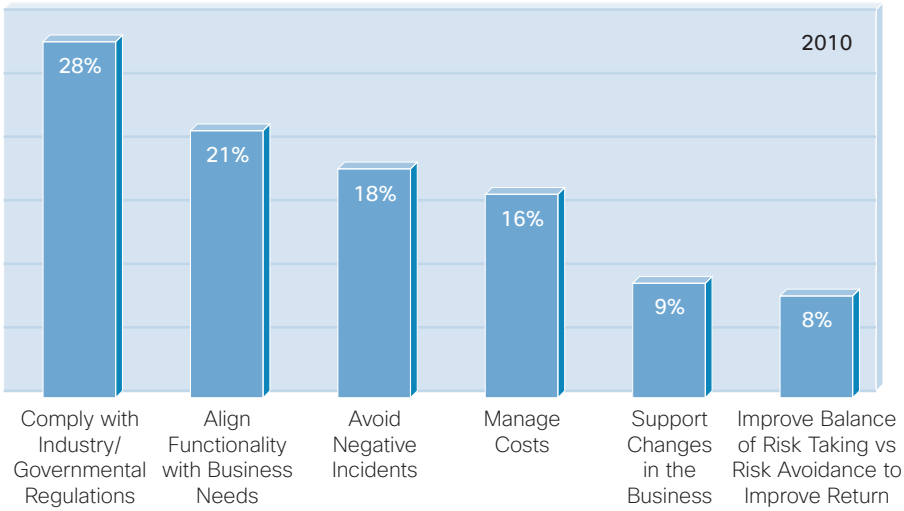
"Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions."

Security Guidance for Critical Areas of Focus in Cloud Computing V2.1
Cloud Security Alliance 2009

Enterprise risk managers, much like business stakeholders, have similar cloud concerns including demonstrating regulatory compliance, developing a strategy for aligning IT with business need, and avoiding security incidents during these shifts in IT. (See Figure 1).

While concerned about risk, enterprise and cloud stakeholders realize that, without taking and controlling business risk, there can be little business value.

Figure 1. IT Risk Management Priorities



Source: ISACA

Aligning Your Business and IT Needs

As evidenced by the ISACA survey, developing a strategy for aligning IT needs with business needs is a priority in managing cloud computing risks. As an organization considers adopting specific cloud infrastructures and deployment models to meet business needs, the importance of a security program that aligns with the cloud architecture becomes apparent. The security requirements involved include strategic and operational policies, risk assessments and risk management plans, organizational and technical controls, and metrics to assess the effectiveness of the entire security program. Whether you are utilizing a physical or virtualized cloud infrastructure, your ability to successfully manage cloud security is defined by an interdependent portfolio of security policies, investments, and controls, known as IT governance, risk, and compliance (IT GRC).

IT governance, risk, and compliance is an industry term that reflects the holistic management of information technology (and security) that enables an organization to successfully implement its business goals and objectives. When applied to cloud computing, IT GRC can be a very effective framework for building robust security architectures that protect and promote the business value of the cloud.

- Governance represents the management of IT security as a strategy, rather than a collection of disparate components and technologies. IT security governance treats security as a business process, aligning technology needs with business requirements and monitoring the effectiveness of the entire portfolio of security assets and investments.
- Risk management is about determining the probability and magnitude of uncertain, undesirable events and then using that data to make more informed decisions. For the cloud, the question is not whether adoption is risky (any technology adoption is risky), but where those risks exist, what they really are, and how to reduce losses and maximize gains from cloud deployments.

- Compliance addresses the need of organizations to meet their obligations, whether imposed by government, industry bodies, contractual arrangements, or their own policies. Today's IT environments are under increasing scrutiny and oversight, and the need to prove due diligence to auditors, partners, and customers is a major factor in driving enterprise IT security efforts.

Enterprises should begin evaluating their cloud security strategy by answering basic questions:

- What is our cloud strategy? Targeted cloud type/model? How does the cloud benefit our business?
- What new risks does our cloud strategy introduce? What are the business risks (including the risks of not adopting cloud computing)? What are the security risks?
- What assets and data will support or live on the cloud? Of these, which are protected under law, regulation, contract, or policy?
- How must we adapt our existing security and compliance programs to address cloud security risks? Which policies, architectures, controls, and technologies must we address, add, or change?

The answers to these and other security questions, as part of a formal strategy for cloud governance, risk management, and compliance, will help you to shape your development of an information security management system (ISMS) for your cloud architecture. The ISMS concept is drawn from ISO/IEC 27001, an international standard for information security, and represents a comprehensive process of security management and improvement. A cloud ISMS includes policies and processes, risk assessment and treatment, security controls, and metrics to evaluate and improve the effectiveness of the system. The ISMS can and should become a central business function in your overall cloud strategy and technology architecture blueprint.

Building an Information Security Management System for the Cloud

For many organizations, the cloud has brought information security management into renewed focus. But for organizations struggling to define and articulate their security strategies and value for traditional IT, securing new cloud-based architectures can seem nearly impossible. Many organizations lack a mature ISMS and struggle with the governance, risk, and compliance efforts necessary to help ensure the success of their IT security. Building an enterprise ISMS is no easy task. Security programs are large in scope, encompassing information security policy, the organization's security, asset classification and control, personnel security, physical and environment security, communications, operations, access control, system development/maintenance, and compliance. Organizations tend to have many information security management systems that have been built over time, with security controls often described as ad hoc. These systems sometimes suffer from a failure to include all assets, a lack of business continuity planning, little or no coverage for physical security, and inconsistent or even nonexistent human resource alignment with controls.

There are currently no cloud-specific security standards or compliance frameworks, although some organizations have begun to develop best practice frameworks around cloud security. Some organizations have instead applied existing information security standards to cloud adoptions as an extension of the existing IT environment. Internationally recognized as a standard for managing information security, ISO/IEC 27001 is also applicable to cloud security. Furthermore, organizations can certify against ISO/IEC 27001 as a way of objectively demonstrating the effectiveness of their ISMS. The standard thus provides objective verification for those seeking to demonstrate to their regulators, partners, and customers that they take security seriously.

While ISO/IEC 27001 is not the only security governance framework available to cloud adopters, certification and the international recognition of the standard provide the standard with additional credibility. ISO/IEC 27001 defines the operation of an ISMS that functions effectively at the planning, implementation, management, and continuous improvement of information security operations. Risk-based and metrics-driven, an ISO/IEC 27001-compliant ISMS represents a mature capability for protecting an organization's data, assets, and users. ISO/IEC 27001 uses both a process management system and a comprehensive body of IT security controls across several domains and objectives. Operational controls included in ISO/IEC 27001 are described in detail, with specific guidance for implementation, in a supporting standard, ISO/IEC 27002. Together, these standards are two components of the ISO/IEC 27000 family of standards supporting information security practices. The ISMS concept, structure, and supporting controls promulgated by ISO/IEC 27001 are readily applicable to cloud environments, enabling an organization to formulate strategic goals, assess risks, implement controls, and measure effectiveness in a systematic and often transformational way.

Achieving formal ISO/IEC 27001 certification is a long-term and resource-intensive effort, and many organizations choose to certify only those components that are mission-critical or require objective verification of security maturity. But these organizations often adopt the principles of the standard as a best practices framework in order to guide and direct security operations. In considering new cloud computing deployments, an enterprise can benefit significantly from considering the creation of an ISMS based upon ISO/IEC 27001 to manage security and risk for the enterprise. Some mission-critical cloud applications might be appropriate targets for formal audit and certification against the standard.

Enabling Your Governance, Risk, and Compliance Program for the Cloud

While ISO/IEC 27001 provides an excellent framework for managing information security, governance in the cloud must take more into account than security vulnerabilities and threats. Cloud governance must consider the business value that security brings to the environment, including how secure cloud operations directly support the profitability of service delivery, revenue generation, internal productivity, and reputation. These aspects of the cloud must be effectively measured and managed as part of a security portfolio that aligns closely with other business investments and objectives.

Assessing business and security risk in the cloud is challenging as well, both because the risks of new cloud technologies and deployments are just emerging, and because the risk assessment techniques of the IT security industry have not much improved or evolved in the past two decades from simplistic heat maps and basic loss expectancy formulas. Cloud computing, like more recent but still traditional IT infrastructures, requires much more sophisticated risk management processes than have been available to security managers.

In addition, multitenant cloud environments contain many users and information assets with potentially unique as well as overlapping regulatory, industry, and legal compliance requirements. The sheer number and complexity of these requirements make them difficult to implement in the data center and in the cloud. The cloud as a multitenant environment demands policies, processes, and controls for each tenant's governance and compliance needs. Cloud providers are faced with the daunting task of identifying and addressing a potentially enormous body of customized protection requirements, including (but not limited to):

- Federal Information Management Security Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA)
- State and local data breach notification laws

- Sarbanes-Oxley Act (SOX)
- European Union Data Privacy Directive
- Payment Card Industry Data Security Standard (PCI DSS)
- ISO/IEC 27000 standards
- CoBIT
- ITIL
- Statement on Auditing Standards (SAS) No. 70

It is currently unclear who has responsibility for protected information that traverses or lives within cloud environments, but organizations should be prepared to show due diligence in protecting such data if they want to avoid adverse litigation or undesirable public relations. Understanding what a compliance requirement allows or prohibits, as well as what controls and processes it mandates, will drive everything from service provider agreements to incident response and disaster recovery processes. As recent high-profile security incidents have also shown, compliance "on paper" as the result of an audit does not guarantee operational security. Organizations will find themselves under additional scrutiny if security problems occur in systems that are assumed to be well-managed and protected.

Yet IT GRC can deliver measureable benefits to the business. The IT Policy Compliance Group, in its annual report, found that effective IT GRC programs resulted in tangible business value, including:

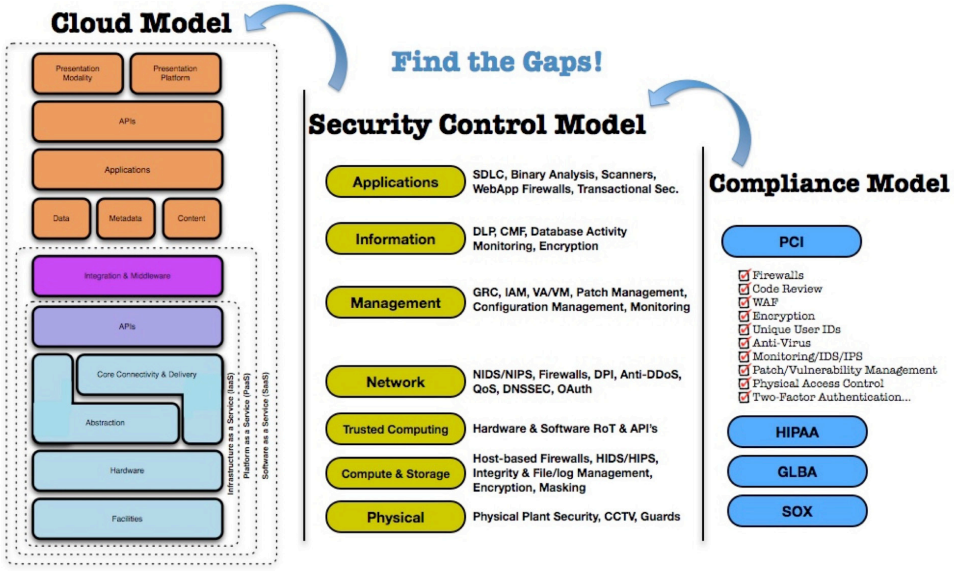
- 17 percent higher revenue
- 14 percent higher profits
- As much as 50 percent reduction in auditing costs
- 96 percent reduction in costs from the loss of customer data
- Significantly fewer business disruptions
- Increased customer retention: 18 percent higher

Cisco® Cloud Enablement Services help you approach security as a *business process* by developing governance and management strategies, assessing risks, achieving compliance at both audit and operational levels, and measuring security program effectiveness. These services help you address your unique cloud security challenges. From governance and compliance support, to risk and cost assessment, to technical testing of network security architectures, Cisco experts can help you:

- Define a robust cloud security strategy that aligns with business goals and objectives
- Build an effective ISMS for your cloud initiative that enables you to plan, implement, measure, and improve your cloud security
- Conduct sophisticated risk assessments, including scenario analysis and probabilistic risk modeling for cloud security and business risks
- Create a common control framework (CCF), including the Cisco Security Control Framework as a subset, that identifies required controls from multiple compliance sources and aggregates these controls into a single authoritative control framework

A similar approach has been recommended by the Cloud Security Alliance. (See Figure 2.)

Figure 2. Mapping the Cloud Model to the Security Control and Compliance Model, Cloud Security Alliance 2009



Source: Security Guidance for Critical Areas of Focus In Cloud Computing V2.1
Cloud Security Alliance 2009

Assessing Your Data Center and Cloud Security Requirements

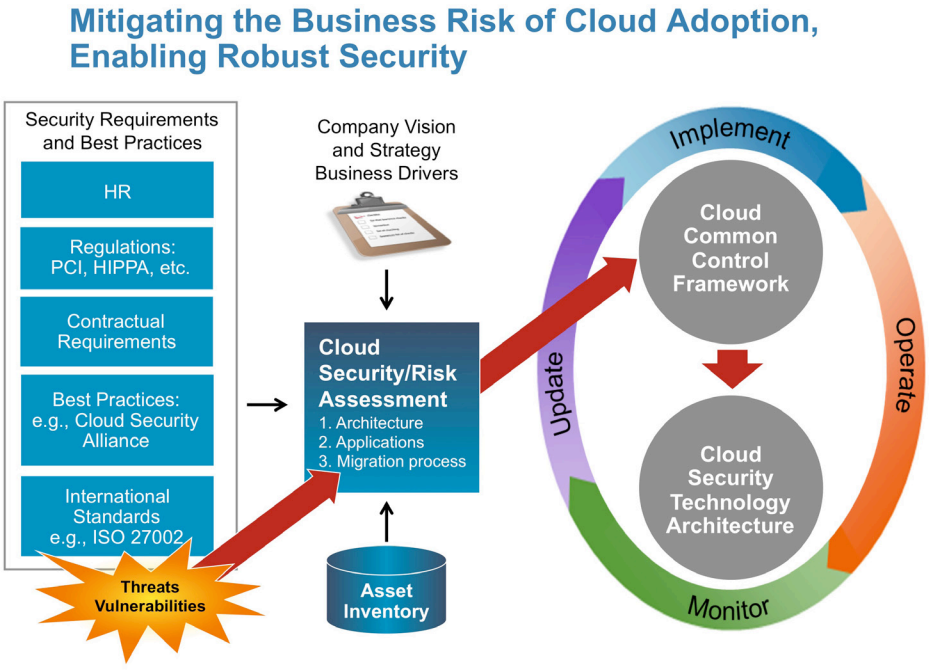
Since the challenges around security are different for every business, Cisco Cloud Enablement Services begin with strategic cloud security assessments. For enterprises, these assessments address how to:

- Solve cloud multitenant security challenges when consolidating previously isolated lines of business into the cloud
- Manage and control the security of data as it moves through the cloud across dispersed network, compute, and storage resources
- Assess whether an application, data, or service is suitable in terms of its security for the cloud and which providers have the security capabilities to meet enterprise security requirements

For the public sector, Cisco Services helps address security requirements around, how to control and protect data with role-based access and other controls; enable compliance with security auditing and testing; provide data isolation for data, service provisioning, and processes; and prevent infrastructure visibility loss due to abstraction in multitenant cloud environments.

Cisco Services enables service providers to deliver the same security controls in the cloud as in the enterprise, especially on-demand security controls for users. Cisco Services helps build-in data isolation, secure service provisioning and processes, and prevent infrastructure visibility loss due to abstraction in multitenant cloud environments. (See Figure 3.)

Figure 3. Cisco Cloud Security Approach



Beginning with a Technology Architecture and Security Assessment

The foundation to Cisco's Cloud Enablement Services is a cloud strategy/risk assessment of your existing architecture (network, storage, and compute), applications and services, and the migration process to the cloud. This top-down requirements gathering includes:

- Service offerings affecting technology and security architecture decisions
- End-to-end security
- Compute and server virtualization
- Storage
- Network (Layers 2–3)
- Network services (Layers 4–7)
- Data center interconnect
- Scalability modeling

Cisco provides several IT GRC service capabilities to help you create and deploy your cloud architecture at the levels of strategy, process, and policy. Cisco can help you create a security strategy for the cloud that directly aligns with your business needs or can develop specific security risk models and assess policies and controls that allow your cloud ISMS to contribute true business insight and value around your cloud deployment.

Developing A Pervasive Security Control Framework for the Cloud

Cisco also has developed a Security Control Framework (SCF) to aid in the architecture, design, and implementation of secure systems. The Cisco SCF offers two compelling benefits:

- Total visibility: In order to know what to control and how effective controls are, a business must have total visibility of users, devices, services, and resources deployed on a given network.
- Active control: A business must have the ability to completely control the communication, resource usage, and activity of users, devices, services, and resources deployed on a given network.

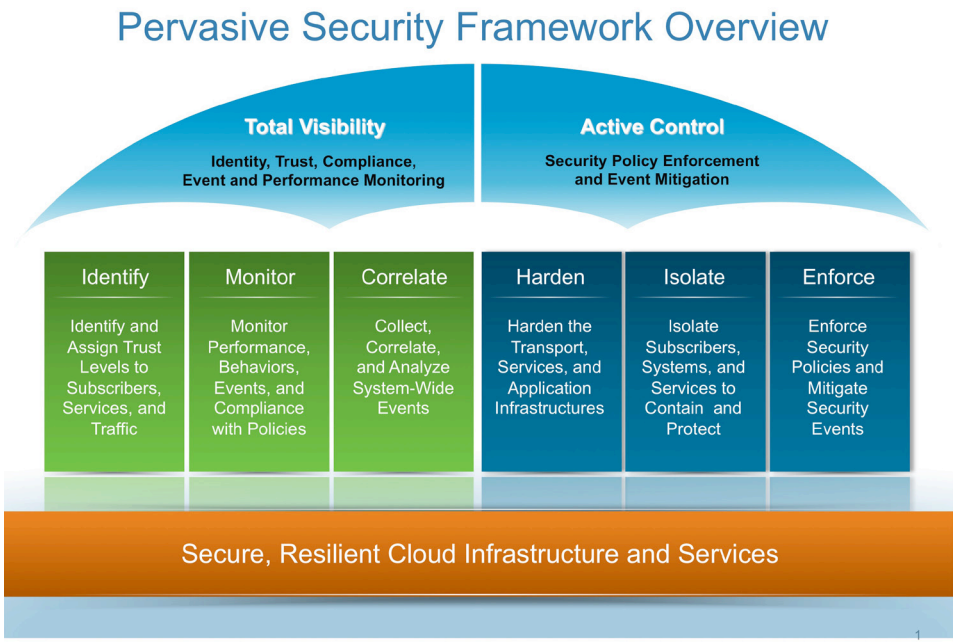
Your cloud security architecture should deliver **complete visibility and active control.**

Complete visibility includes assigning trust based on identity and authorization levels and continuous monitoring and correlation of events to look for bad behavior and malicious activities, since, in the cloud, you have less visibility because of abstraction and sharing.

Active control of the cloud includes high availability and resiliency for the infrastructure in the event of system failures. Active control of data isolation, data loss prevention, data retention policies, provisioning, and service delivery helps protect cloud users, as well as meet the SLAs of the cloud service.

Figure 4 visualizes these security steps that further define the Cisco security framework.

Figure 4. Cisco Pervasive Security Framework



Total visibility includes three elements.

- **Identity and trust** define the ability of a system to identify entities accessing a given resource and determine a trust level or state of trust: for example, traffic entering a network. The trust level might be established through the inspection of credentials or through other means. With identity-aware networking, single-access authentication provides security policy controls and monitors activity where users first connect—both inside and outside a corporate firewall—and throughout the entire network, including shared files, databases, and system applications. Trust is established through credentials in addition to inspecting IP addresses. Data is secured across the entire path it takes through the network.
- **Monitoring** provides monitoring of the behavior and usage of the network including its resources, connected systems, users, applications, and IP traffic. It provides the fundamental instrumentation to facilitate security visibility. Monitoring and management using a single, central security dashboard provide control over policy configuration, as well as real-time event and network visibility for resources, connected systems, users, applications, and IP traffic. Behavioral-based monitoring—anomaly detection—in addition to signature-based detection technologies is essential for detecting and preempting attacks.
- **Correlation** involves interpreting, disseminating, analyzing, and classifying visibility data into meaningful operational information through the process of examining the context of seemingly unrelated events or changes. From a security operations perspective, it provides the foundation to apply policy enforcement and isolation controls. Correlation turns activity data into insight by providing context for events and changes. Continuous analysis of events quickly identifies irregular activity and correlates the event to policy controls.

Control includes three elements:

- **Enforcement** provides the ability to enforce allowed behavior of connected systems, users, applications, and IP traffic. Policy enforcement might either be static, where a control is applied on a permanent basis, or dynamic where a control is applied to specifically mitigate some discrete event or security incident. Communication between systems should operate on the least privileged model (LPM), meaning systems should only be able to communicate to other systems as required to perform their job. Policy enforcement is implemented in infrastructure and enables unified application of best practices across the entire environment.
- **Isolation** provides the ability to isolate areas of a network (or system) into security zones so as to control (or prevent) access between network areas or parts of the system and limit the scope of exploits. As a result, the effects of disturbances to a system are limited in scope and minimally affect other users, services, or systems. It helps ensure that cloud tenants fairly share resources and that SLAs are met. It also makes it easier to enforce policy consistently for users, connected systems, applications, IP traffic, endpoint devices, and networking components.
- **Resiliency** enables the architecture to withstand, adjust to, and/or recover from adverse uncontrolled circumstances. Reducing points of vulnerability—or **hardening**—involves removing or deactivating nonessential features, services, and accounts systems and components.

Aligning the monitoring (visibility) and management (control) of the cloud security policies, especially those helping to ensure compliance and privacy, creates pervasive cloud security architectures.

Pervasive security operates consistently regardless of where network resources are located and wherever business takes place. Pervasive cloud security is architectural, which includes securing the technical, business, and process requirements within the architecture across network, network services, compute, storage, and management resources. Because the cloud is now another entry point into the business, the network infrastructure is the right place to deploy the security architecture for cloud.

Unlike a device- or application-level only approach to security, Cisco takes a comprehensive architectural approach. Security is integrated into every layer of the architecture, and all service delivery elements have security. This core capability is customized to your environment and business mandates.

Migrating Your Applications Securely to the Cloud

Security risks and issues can affect your transition from the current data center to a cloud-based solution. The goal for this stage is to minimize and eliminate these risks in a comprehensive manner. We identify the gaps in your current non-cloud data center security architecture required to cover cloud migration, assess the security architecture for an existing data center being upgraded to cloud (brownfield), and assess the security architecture for a new or proposed cloud deployment (greenfield).

We also identify business assets that might be affected by the planned cloud transition, for example, data, applications, business processes, data volumes, and transaction rates. Then we evaluate them for their security risk and threat analysis. We also provide mapping to potential cloud deployment models and provide a crucial evaluation of both cloud service models and service providers from a security perspective. We examine models and providers based on:

- Available security controls and risk mitigation techniques (ownership/classification/governance)
- Appropriateness of internal and external third-party discovery/subpoena
- Public and private encryption access control
- Derivation/aggregation/integrity
- Access controls
- Encryption
- Legal and compliance policies and controls
- Offsite, media, and information retention policies and procedures

For data flows to and from the cloud, we map and assess the security implications.

Technology Controls for Managing Your Cloud Security Architecture

Finally, managing the technology aspects of the cloud security architecture requires technology controls that help enable end-to-end security and protect against security breaches.

Reviewing your business goals, architectural growth requirements, and current security policies can help identify compliance issues, security concerns, and previous security incidents. We also review and document current security policies, procedures, architectures, and configurations, while also analyzing security controls on the existing data center architecture. The goals here are to refine security control objectives, identify missing controls, and evaluate the monitoring and reporting of controls. We identify security gaps in the current state architecture, as well as the planned cloud architecture and work to improve the overall security architecture with, for example, detailed device configuration recommendations.

Conclusion

Cloud computing offers both security advantages and security risks. Cloud homogeneity can make security auditing/testing simpler, which can help organizations demonstrate that legal and regulatory compliance has been met. Clouds enable automated security management, which help ensure consistent and auditable application of security policies and controls. Clouds also can provide cost-effective redundancy/disaster recovery services through virtualized cloud infrastructures.

Since most businesses designed their systems, computing, and storage resources before or as the Internet developed however, strategic security assessments of existing infrastructure, policies, controls, and governance are necessary to help ensure compliance with new legal and regulatory requirements and to meet the demands of doing business in the cloud.

With new cloud computing deployments, an enterprise should consider the creation of an ISMS based upon ISO/IEC 27001 to manage security and risk for the enterprise and the cloud. As a framework for building robust security architectures, Cisco's Cloud Enablement Services incorporating IT GRC help enable regulatory and legal compliance and protect and promote the business value of the cloud. This approach can result in tangible business benefits, such as fewer business disruptions and data privacy and protection.

After developing your strategy for aligning policy, controls, and governance with business goals, Cisco's Security Control Framework (SCF) now can facilitate the architecture, design, and implementation of secure systems. Cisco's SCF helps provide total visibility of users, devices, services, and resources, as well as active control of communication, resource usage, and the activity of users, devices, services, and resources, including those in the cloud. So whether the challenge is continuous monitoring and correlation of events to detect malicious activities or active control of data isolation and segregation of cloud users, Cisco's SCF creates the confidence you need to operate in the cloud securely.

In addition, given the scarcity of IT expertise around cloud security according to the 2010 State of Enterprise Security Survey – Global Data (Network World, February 2010), choose a partner who can help you implement a secure cloud infrastructure. Your partner should offer previous experience delivering other cloud security projects, access to underlying cloud technology, the ability to transfer best practices and unique insights to your organization, and validated delivery of the promised security.

Whether the cloud challenge is information security, bridging complex data center and cloud infrastructures, who can access what data, where data is located, or how to protect a tenant's privacy, your best cloud strategy is to enable policies, governance, and compliance and pervasive architectural security across network, computing, and storage to enhance business value with your cloud.

For more information about cloud enablement services, please visit www.cisco.com/go/cloudenablement, or contact your account manager.

For more information about ISMS and IT GRC for cloud, please visit www.cisco.com/en/US/products/ps10372/serv_home.html, or contact your account manager.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in the USA C11-649815-00 02/11