Today, you are expected to actively spur innovation in your business, stay aligned with evolving business objectives, and deliver new and unique experiences to your customers. The move to cloud has been steadily gaining acceptance because it promises to help you achieve these goals faster, more efficiently, and more cost effectively. And with the Internet of Everything (IoE) accelerating the pace of change, line-of-business (LoB) owners are increasingly turning to the cloud to capitalize on the new opportunities it enables as a powerful engine and innovation catalyst.

While cloud brings an array of opportunity, it can also include unforeseen risks and vulnerabilities that you must identify and effectively manage. The ability to provide complete end-to-end security solutions across cloud environments remains a critical success factor for the adoption of cloud services. Whether you want to formally define how you use cloud services as part of your IT strategy, deploy a new cloud service, evaluate a set of cloud providers, or assess the viability of your existing cloud strategy, Cisco Security Services can help you understand, prioritize, and mitigate risks to make the most of your cloud investments.

**Strategy Development**

Cisco Security Services helps you develop secure and effective cloud strategies. Our approach is based on an understanding of business benefits balanced with a firm perspective on the associated risks introduced by cloud providers. With these insights, we detail the types of services to be transitioned to a cloud provider; service-level expectations; security, privacy, and other compliance requirements; and ongoing monitoring approaches.
Security Services for Cloud

Analysis includes:

• **Strategy:** A customized, risk-adjusted cloud services strategy

• **Roadmap:** A roadmap outlining steps required to meet cloud services business objectives including identification of initial services appropriate to target for cloud deployments

• **Architecture:** Specification of the internal architecture, software, and processes needed to support security, monitoring, and performance requirements

• **Assessment:** Regular assessments of cloud providers in relation to service-level, security, and compliance expectations

**Risk Modeling and Impact Analysis**

Whether you are building your cloud strategy or have an existing program in place, you need to understand the risks to your organization. We will help you understand the risks associated with existing strategies and build a risk-adjusted program to protect your data, applications, and infrastructure.

We start by reviewing your organization’s business goals related to the cloud, as well as your risk tolerance and unique technology, compliance, and security requirements.

We then assess potential cloud risks across eight areas:

1. **Fitness:** Are the targeted business processes, applications, or infrastructure appropriate for the cloud?

2. **Integration:** What are the cloud integration requirements and are these included in your business case?

3. **Compliance:** How will a cloud provider affect your ability to comply with industry standards and regulations?

4. **Security:** How secure are your organization’s critical information assets?

5. **Demand and capacity management:** Do you have the right tools and processes in place to properly measure and manage demand and capacity requirements?

6. **Availability, resilience, and continuity:** Do your existing service level agreements (SLAs) address your availability needs? Do your cloud services meet your resilience and business continuity needs?

7. **Portability:** What are your portability risks? How do you ensure the right level of flexibility from your cloud architecture?

8. **Relationship management:** What are your unique support and communications needs related to the cloud?

After the cloud risk identification and assessment, risks are adjusted based on probability and impact. We map your risk tolerance to strategic and operational requirements to determine your cloud readiness and provide a strategy for ongoing risk mitigation through the following deliverables: cloud services readiness analysis, cloud services IT risk analysis, IT risk universe summary and heat map, and cloud services risk reduction and monitoring plan.

**Assessment**

Security assessments ensure that current and future cloud providers do not expose their customers’ organizations to unacceptable levels of risk. Critical areas of assessment include:

1. **Applications:** Analysis of key variables including transaction and data volume, network throughput, capability models, and security requirements

2. **Databases:** Assessment of data models, schema, transaction volume and history, stored procedures, and SLAs

3. **Network:** Analysis of variables such as topology, security infrastructure, server configuration, monitoring tools, and storage volume requirements

4. **IT processes:** Review of processes related to procurement, demand management, capacity management, contingency planning, incident management, and access management

After we have identified risks based on the readiness of your technology and processes, we conduct a risk assessment, examining SLAs and contractual obligations, technical architecture, security architecture, data management capabilities, archival and data retention mechanisms, monitoring tools, portability and flexibility, automation capabilities, and billing, usage tracking, and reporting.

In addition to a documentation-based risk analysis, Cisco conducts technical assessments, which can include:

• Blackbox security testing of provider’s application, external computing, or virtualization interfaces

• External network-based vulnerability assessment and/or penetration testing

• Internal penetration testing

• Logical and physical network and server environment review

• Application architecture review
Strengthening Cisco Security Solutions

The acquisition of Neohapsis allows Cisco to deliver even stronger security solutions to help customers address complex security challenges in the dynamic threat landscape.

Learn More

For more information visit www.cisco.com/go/securityservices.