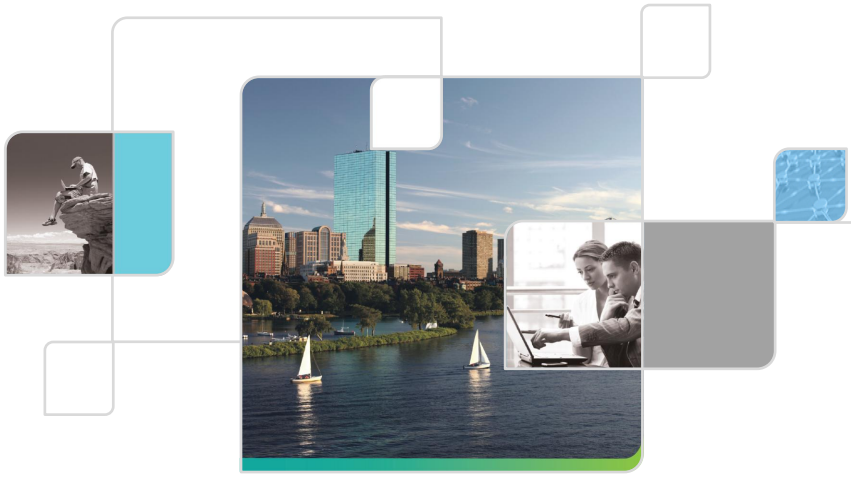
Whitepaper:

7 Steps to Developing a Cloud Security Plan

NaviSite



Executive Summary:
7 Steps to Developing a Cloud Security Plan

Designing and implementing an enterprise security plan can be a daunting task for any business. To help facilitate this endeavor NaviSite has developed a manageable process and checklist that can be used by enterprise security, compliance, and IT professionals as a framework for crafting a successful cloud computing security plan. It defines seven steps—sequentially—that have been tested and refined through NaviSite's experiences helping hundreds of companies secure enterprise resources according to best practices. This plan enables organizations to gain the economic advantages of secure and compliant managed cloud services.

NaviSite

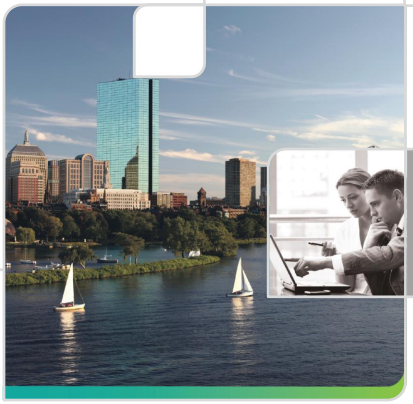


Table of Contents

Introduction

"…THERE ARE SEVEN TANGIBLE STEPS ENTERPRISES CAN TAKE TO GAIN THE COST AND BUSINESS ADVANTAGES OF CLOUD SERVICES WITHOUT COMPROMISING THE SECURITY OF ENTERPRISE APPLICATIONS."

Cloud computing provides compelling cost and strategic benefits, including: scalability with reduced capital expenditure; more efficient use of IT resources; and the ability for an organization to focus on their core competency. Many well established security technologies and procedures can be applied to cloud computing to provide enterprise-class security. In many cases the cloud provider can achieve better security in a virtualized environment than enterprises can achieve internally.

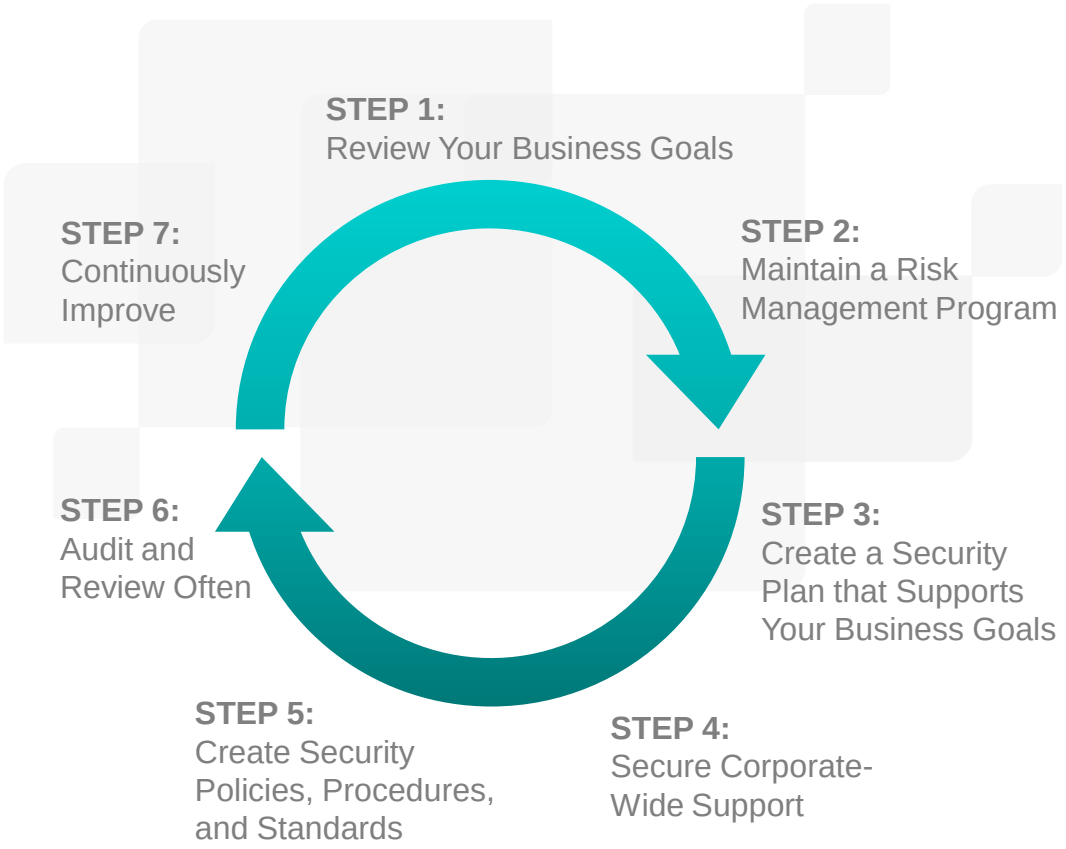
Selecting a service provider with strong security procedures and services in cloud computing can be a strategic move, but enterprise organizations need to continue to take an active role in security and risk management. Working together, the cloud provider and the enterprise can ensure that existing security practices are being complemented and that enterprise resources are protected according to industry best practices.

Cloud infrastructure services enable improved efficiencies for IT, allowing companies to reduce capital expenses even as resource demand increases. They also provide companies a competitive edge through greater scalability and flexibility to address business opportunities. Concerns around the security of cloud infrastructure have been viewed as a barrier to adoption, but there are seven tangible steps enterprises can take to gain the cost and business advantages of cloud services without compromising the security of enterprise applications.

By following these steps the enterprise can rely on a proven methodology for cost-effectively and securely leveraging cloud services. NaviSite takes pride in ensuring its enterprise customers services are secure and reliable but encourages all businesses—no matter what provider they are partnering with—to take an active role in being sure their specific security and compliance requirements are met.

Secure cloud services plan breaks down into the following seven steps:

FIGURE 1: 7 STEPS.



By following these steps organizations can structure security and compliance programs to take advantage of the economic advantages of managed cloud services while meeting organizational security and compliance objectives.

SECURITY IS NOT A ONE-SIZE-FITS-ALL SCENARIO

Step 1:

REVIEW YOUR BUSINESS GOALS

It is important that any cloud security plan begins with the basic understanding of your specific business goals. Security is not a one-size-fits-all scenario and should focus on enabling:

- TECHNOLOGIES: Authentication and authorization, managing and monitoring, and reporting and auditing technologies should be leveraged to protect, monitor, and report on access to information resources
- PROCESSES: Methodologies should be established that define clear processes for everything from provisioning and account establishment through incident management, problem management, change control, and acceptable use policies so that processes govern access to information
- PEOPLE: Organizations need access to the proper skill sets and expertise to develop security plans that align with business goals

Too often, organizations view internal security and compliance teams as inhibitors to advancing the goals of the business. Understanding the business objectives and providing long-term strategies to enable business growth, customer acquisition, and customer retention is essential to any successful security plan.

The best way to do this is to develop cloud security policies based on cross-departmental input. A successful security program includes contribution from all stakeholders to ensure that policies are aligned and procedures are practical and pragmatic.

The broader the input the more likely the final security plan will truly align with, and support corporate goals. Executive input is not only essential to ensure that assets are protected with the proper safeguards, but also to ensure that all parties understand the strategic goals. For example, if a company plans to double in size within a few years, security infrastructure needs to be designed to support scalability.

CASE IN POINT: At NaviSite, we often see customers faced with the challenge of making major security and technology changes to address evolving corporate goals. For example, a customer that hosts multiple merchant sites had a Payment Card Industry (PCI)-compliant application, but when it was acquired, its parent company required stricter controls that conformed to the enterprise-wide PCI program. The acquired company came to us with a small company perspective, while the new parent company wanted to enforce even tighter security across its divisions.

We worked with them to realign and bolster the goals of the acquired company's security and compliance programs with the corporate goals of the parent company. By reviewing the business goals with the stakeholders from the parent company, the newly acquired company, and our security team, we were able to identify and document the objectives for the new compliance program and ensure that they were aligned with the over-arching PCI program.

Step 2:

MAINTAIN A RISK MANAGEMENT PROGRAM

AN EFFECTIVE CLOUD COMPUTING RISK MANAGEMENT PROGRAM IS IMPORTANT FOR REDUCING THE OVERALL RISK TO THE ORGANIZATION.

It is naïve to think that your applications will never be breached, whether they are hosted in your data center or in a managed data center. Every organization needs to develop and maintain a risk management program, and it should be done centrally and viewed holistically.

An effective cloud computing risk management program is important for reducing the overall risk to the organization. It is also essential for prioritizing the utilization of resources and for providing the business with a long-term strategy. If a growing organization can identify and reduce the risk of new products, technologies, processes, people, and vendors, it can better focus on revenue growth and improved profitability.

It is only through a well-defined and carefully maintained risk management program that you can provide an aggregated view of the risk that a company is willing to accept. The generalized view is that you assess the value of the asset, assess the loss expectancy probability, and then quantify whether the organization is willing to accept the risk of loss or whether steps should be taken to mitigate the chances of that loss. Security professionals are encouraged to regularly conduct careful analysis to develop responsible programs and build in the necessary controls and auditing capabilities to mitigate threats and maintain a reasonable security program that protects organizational assets, given budgetary resources.

The cloud computing risk assessment policy requires buy-in from the very top. This program should be audited, and policies defined that explicitly state who can accept risk on behalf of the organization.

If you have a well-developed risk management program in place, then you have identified your critical assets and established appropriate levels of protection. By moving some or all of your business applications to the cloud, you gain the additional benefits of your providers business continuity planning and protection from unthinkable events, such as natural disasters. Seamless failover to a redundant data center thousands of miles away provides shareholders with increased comfort in knowing their business is protected and secure.

At NaviSite, we continue to see disaster recovery and business continuity initiatives gaining increased corporate focus as a direct result of the migration of ERP applications to the cloud. For example, a publicly traded company outsourced its financial applications to NaviSite. However they did not have a business continuity and disaster recovery (BCDR) plan.

As we worked with them on their risk management program - identifying risks, evaluating the value of the assets, and looking at annualized loss expectancies to build out the level of assurance they needed - they realized the economic argument and value for enabling seamless failover to a redundant site across the country.

Management went back to the Board of Directors and quickly received approval. The company now has a solid disaster recovery program in place with annual testing to ensure business continuity. They did not initially understand the risk its shareholders were incurring until it developed a formal risk management program, and by quantifying that risk the company was able to take appropriate steps to mitigate and protect itself adequately while ensuring business continuity.

Step 3:

CREATE A SECURITY PLAN THAT SUPPORTS YOUR BUSINESS GOALS

MANY OF THE NEEDS TO CHANGE SECURITY PLANS ARE NOT A RESULT OF CORPORATE STRATEGIES BUT EVOLUTIONS OF COMPLIANCE REQUIREMENTS.

Your cloud computing security plan should include goals with measurable results that are consistent with providing support for the growth and stability of the company. The plan should include compliance programs, technologies, and processes with very specific results. For example, a growing IT services company may pursue a data center compliance program, such as SSAE 16 (the successor to the SAS 70 standard) a service management framework which requires in-depth audits of control activities that include: security monitoring, change management, problem management, backup controls, physical and environmental safeguards, and logical access. Goals should include:

- Specific date for completion
- Verification of achievement, such as a Service Organization Controls (SOC) report
- Measurable expected result, such as a reduction in reported incidents by five percent, improvement of risk mitigation by reduction of Annualized Loss Expectancy (ALE) by ten percent, or successful passing of customer audits increasing by twenty percent

The security plan in many ways becomes a natural extension of the previous two steps. For example, if a U.S. company is planning for an IPO, becoming compliant with the Sarbanes-Oxley Act (SOX) requirement is essential. Section 404 of SOX explicitly requires management and the external auditor to report on the adequacy of the company's Internal Control on Financial Reporting (ICFR). Companies have to assure that the data is valid and has not been altered. It is primarily the responsibility of the IT group to ensure SOX compliance.

Many of the needs to change security plans are not a result of corporate strategies but evolutions of compliance requirements. For example, at NaviSite, we help clients maintain compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Health Information Technology for Economic and Clinical Health Act (HITECH) addresses the privacy and security concerns associated with the electronic transmission of health information and it extends the privacy and security provisions of HIPAA. By partnering with cloud providers, organizations are more nimble and can more easily modify their security plans to support evolving corporate strategies or regulatory requirements.

Step 4:

ESTABLISH CORPORATE-WIDE SUPPORT & ALIGNMENT

GAINING ACCEPTANCE ON SECURITY POLICY AND PROCEDURE AHEAD OF TIME STREAMLINES ADOPTION THROUGHOUT THE ORGANIZATION.

A key element of a successful cloud computing security plan is the involvement and support of the plan across the organization. Many security departments build out vast arrays of policies that are difficult to implement across the organization. Prioritizing these policies and ensuring that they are not in conflict with other policies from different departments is essential for establishing support and acceptance.

A given security policy may not rely on the latest technology or provide the most secure results, but balancing ease of deployment and organizational acceptance with security is a necessary tradeoff. Organizations need to establish levels of security that meet business goals and comply with regulatory requirements and risk management policies, but that can be centrally managed and conveniently implemented across the organization with minimal negative impact to productivity. Recognize that it is impossible to completely eliminate risk, but it is prudent to mitigate it in a reasonable manner.

At NaviSite, we have found that the key is to take time to gain a solid understanding of how a company develops its products and services and delivers them to its customers. The majority of your time spent building support for security policies should not be spent in writing those policies, but instead should be spent in learning how the business truly functions so that security can better contribute to its success, and not be viewed as a hindrance or a daily obstacle.

For example, we have worked with manufacturing companies that were building highly sensitive products. In one company, the security team designed a security plan that was so restrictive the plant had to ignore the mandated controls to function productively. This led to the failure of the third-party audit and ultimately a recall of the product manufactured with the circumvented controls. We also worked with an insurance company that developed an application for estimating the cost of insurance that secured the data sources used by the application; they wrote security policies such that they restricted internal departments from viewing critical data needed to perform their jobs.

Companies need to ensure that the security plan is not only aligned with the goals of the organization, but also with the goals of the major departments that will be implementing it. Gaining this acceptance streamlines adoption throughout the organization.

Step 5:

CREATE SECURITY POLICIES, PROCEDURES, AND STANDARDS

A set of guidelines is important to ensure that all compliance measures are identified and the entire organization is driving toward achievement of the same goals. For example, for a healthcare provider, it may be important to provide HIPAA- and HITECH-compliant health care services to new and existing patients. In order to do so, the organization must build security policies that define the constraints in the handling of Protected Health Information (PHI), procedures that define the process of acquiring PHI, and guidelines that encourage the general adoption of best practices.

When you are audited for SOX, PCI Data Security Standard (DSS), or any other relevant compliance standard that affects your business, the auditor will look at existing policies, how you have implemented them, and whether they are being followed throughout your organization. Every company audited wants to make sure it passes the audit, and if you have completed all the previous steps outlined in this process, it will make it easier for you to create security guidelines that can be consistently enforced.

New clients often ask, "What's the easiest way to create security policies, procedures, and standards," and the answer is simple—turn to best practices. When it comes to establishing security guidelines, it is much easier, more practical and productive to edit than it is to create. Assuming you have gone through the previous four steps, security and compliance teams have had to establish many of the policies necessary to address business requirements. Read everything you can and apply best practices to creating policies that align with business goals, develop procedures that are realistic and that will be acceptable to the organization, and wherever possible turn to industry standards to guide you.

Cloud services are a major advantage for growing organizations that have not yet embedded established policies and procedures into the company. The enterprise can rely on the best practices the service provider has developed over years of experience in similar environments.

As with many enterprise cloud service providers, including NaviSite, change management is a clearly defined process governed by well-established guidelines. Each change must be approved by the proper personnel, and then implemented in a quality assurance environment. Once it is tested and approved through a user acceptance procedure, it is introduced to the end-user community in the least intrusive manner possible with a clearly defined back-out procedure in place in case there are unforeseen problems or issues with user adoption.

By turning to high-performance cloud computing, the enterprise can dramatically reduce the learning curve for developing security policies, procedures, and standards. Organizations can accelerate the adoption of best practices for protecting enterprise resources by adopting proven security methodologies.

Step 6:

AUDIT AND REVIEW OFTEN

It is important to review the security plan on a regular basis, report on achievements of goals, and audit the compliance of the organization to the security policies and procedures. If it is part of your overall business plan, a third-party audit can provide an impartial review of the controls and report on compliance to established programs, such as SSAE 16, PCI DSS, or Safe Harbor. Some industries mandate audits, and U.S. publicly traded companies have to conduct internal audits every quarter when they release financial statements. Understanding the auditing requirements for your business and the frequency of your audits is essential not only for ensuring compliance with relevant requirements but also for maintaining best practices for securing enterprise resources.

For example, SSAE 16 Audits are conducted every six months but at NaviSite we conduct internal audits every three months to ensure ongoing compliance and provide assurance that our data centers and our support infrastructure remain current with SSAE 16 requirements. The SSAE 16 Audit is aligned with our security goals because it assures customers that our processes, procedures, and controls have been formally reviewed. It also demonstrates our compliances with Section 404 of the Sarbanes-Oxley Act. By auditing and reviewing the results regularly, companies can implement a constant audit cycle that ensures that the controls remain in place and that that they are being followed. If problems occur, they can be identified and remediated before the next audit cycle.

AUDIT AND REVIEW OFTEN CHECKLIST

Step 7:

CONTINUOUSLY IMPROVE

A well-developed security plan will allow for the continuous improvement of security and compliance. At a minimum, annually review your cloud computing security plan with senior executives and your cloud services provider, and revise goals and objectives as needed. Review and edit security policies and procedures, and actively report back to the organization the accomplishments of the security and compliance teams.

Many companies believe that once they have solid policies and procedures in place they do not need to revisit them—but your industry and your business will change over time, and the technology available to support your security plan will evolve. Just ten years ago remote workers had limited access to enterprise applications, but rapid advances in VPN technology and massive demand for secure remote access have driven most companies to develop policies and procedures to support a mobile workforce. And the technology to support these policies and procedures are enabling businesses to provide the flexibility for employees to work from virtually anywhere.

Review all of your generally accepted security policies at least annually. At NaviSite, we review our security policies on an even more frequent basis. An annual review is designed into some compliance policies; if that's the case for your business consider reviewing your security policies every six months so you have the time to evaluate your current policies, update them when needed and change procedures when necessary before your next audit. Continuous improvement is the key to your security plan. Understanding the dynamic nature of your business and constantly evaluating security requirements are the foundation for implementing a successful continuous improvement strategy.

CONTINUOUS IMPROVEMENT CHECKLIST

Conclusion

Properly managed cloud infrastructure provides better security than most enterprise data centers, applications, and IT infrastructure. It allows companies to more efficiently deploy scarce technical personnel. Use this proven process and the summary checklist provided in Appendix A as an easy guide to structuring your cloud computing security plan.

Selecting a stable cloud service provider with world-class data centers, enterprise cloud computing infrastructure, application expertise, and a proven security methodology will help the enterprise reap the financial rewards of cloud computing while implementing a security framework optimized for the requirements of cloud architectures.

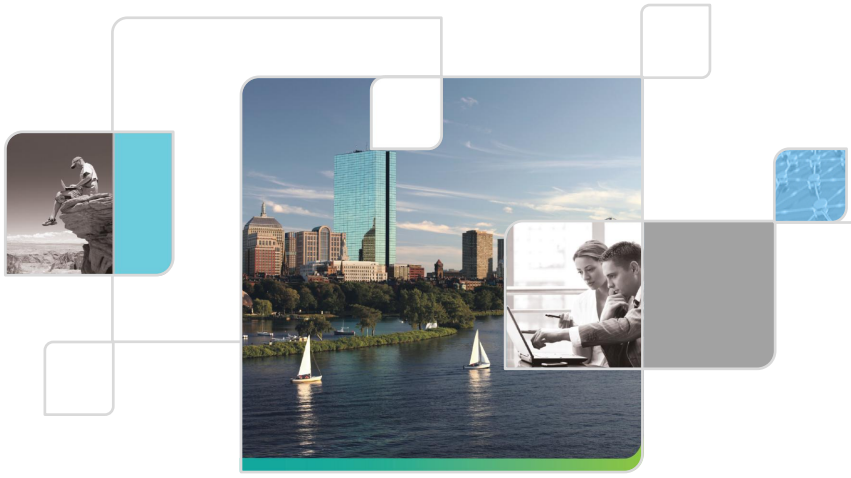
These seven steps are meant to serve as a framework to guide companies as they develop a secure cloud-computing plan. By following these guidelines, organizations can structure security and compliance programs to take advantage of the financial benefits of managed cloud applications and services while meeting organizational security and compliance objectives.

ABOUT NAVISITE

For more information about secure cloud computing services from NaviSite, please visit www.navisite.com or send an e-mail to us at webinfo@navisite.com or call us at 1.888.298.8222 to discuss your secure cloud computing requirements.

FOR MORE INFORMATION

TO LEARN ABOUT CLOUD SERVICES FROM NAVISITE, VISIT: www.navisite.com



Appendix A:

7 STEPS TO DEVELOPING A CLOUD SECURITY PLAN CHECKLIST

By following these seven steps to developing a secure outsourcing plan developed by NaviSite, the enterprise can rely on a proven methodology for cost-effectively and securely outsourcing IT services.

STEP 1: REVIEW YOUR BUSINESS GOALS

- Understand your business goals and direction
- Develop cloud security policies based on cross-departmental input that includes insights from senior management and all of the stakeholders
- Ensure that all security policies are aligned with strategic goals, and that the procedures are practical and pragmatic

STEP 2: MAINTAIN A RISK MANAGEMENT PROGRAM

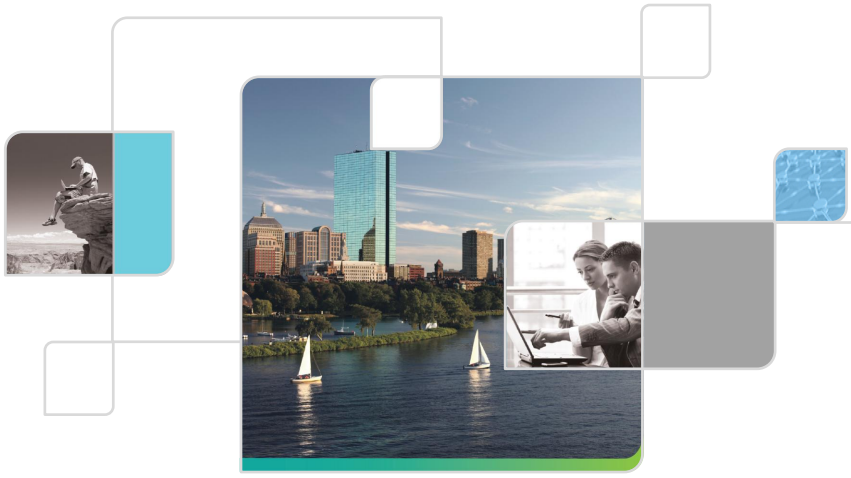
- Develop and maintain a risk management program centrally, and view it holistically
- Carefully define exactly who is authorized to accept risk on behalf of the enterprise
- Implement a well-defined and carefully maintained risk management program so you can provide an aggregated view of the risk that a company is willing to accept
- Ensure that security professionals regularly conduct careful analysis to develop responsible programs and build in the necessary controls and auditing capabilities to mitigate risks and protect organizational assets
- Gain executive-level buy-in to the cloud computing risk assessment policy, and for publicly traded companies, gain Board-level approval if necessary
- Consider seamless failover to a redundant data center and disaster recovery planning integral to risk management

STEP 3: CREATE A SECURITY PLAN THAT SUPPORTS YOUR BUSINESS GOALS

- Develop goals with measurable results that are consistent with providing support for the growth and stability of the company
- Include compliance programs, technologies, and processes with specific metrics
- Work with your cloud service provider to ensure that your security plan is nimble enough to support evolving corporate strategies or regulatory requirements

STEP 4: ESTABLISH CORPORATE-WIDE SUPPORT

- Gain the approval of your cloud computing security plan from not only executive management but also the general workforce
- Make sure security policies are not in conflict with other policies from different departments, and that they are not too time-consuming
- Establish levels of security that can be centrally managed and conveniently implemented across the organization



Appendix A:

7 STEPS, *CONTINUED*

STEP 5: CREATE SECURITY POLICIES, PROCEDURES, AND STANDARDS

- Establish a set of guidelines to ensure that all compliance measures are identified
- Make sure that compliance requirements are reflected in your policies and procedures
- Ensure that auditors can clearly review your policies and how you have implemented so they can that they are being followed.
- Design a comprehensive, layered approach based on a security framework to address common regulatory requirements. This will make it easier to adopt and maintain security procedures that can be audited so you can achieve your security and compliance goals.
- Turn to this 7-step plan as the foundation for your internal audits. If you don't have these steps in place, you won't have a structure that auditors can easily follow
- Read everything you can and apply best practices to creating policies that align with business goals.
- Develop procedures that are realistic and that will be acceptable to the organization

STEP 6: AUDIT AND REVIEW OFTEN

- Review the security plan on a regular basis, report on achievements of goals, and audit the compliance of the organization to the security policies and procedures
- If it is part of your overall business plan, turn to a third-party audit to provide an impartial review of the controls and report on compliance to established programs
- Understand the auditing requirements for your business and the frequency of your audits not only for ensuring compliance with relevant requirements but also so you can implement best practices for securing enterprise resources
- Audit and review the results regularly to ensure that the controls remain in place and that that they are being followed
- If an audit reveals any potential security or compliance problems, ensure they are remediated before the next audit cycle

STEP 7: CONTINUOUSLY IMPROVE

- Annually review your cloud computing security plan with senior management and your cloud services provider
- Re-establish goals
- Review and edit security policies and procedures
- Actively report back to the organization the accomplishments of the security and compliance teams

These steps should be implemented sequentially, and it is an iterative process based on best practices and focused on continuous improvement.

By following these guidelines, organizations can structure security and compliance programs to take advantage of the economic advantages of managed cloud applications and services while meeting organizational security and compliance objectives