Building a **Security and Compliance Strategy** for the Cloud

FIVE STEPS FOR MAINTAINING COMPLIANCE WHILE IMPROVING SECURITY PRACTICES

Accretive SOLUTIONS

ARMOR™

THE FIRST TOTALLY SECURE CLOUD COMPANY™

Facing your **cloud compliance fears**

Cloud compliance is a journey, not a destination. As such, organizations must develop strategies that ensure secure, compliant functioning controls even when they are not undergoing an audit or assessment.

Operating in this manner engenders a continual approach to refining and maintaining cloud security while also helping to ensure optimal security reporting and threat protection. As a result, compliance attestation is streamlined while the threat of a breach is significantly reduced.

Embrace the challenge

That's the "why" of operating in the cloud while the "how" is a different and often insurmountable challenge for many organizations. It is certainly understandable why this is an obstacle, especially when an organization's current resources and processes are stretched to cope with rapidly evolving expectations and threats. What you end up with is an ad-hoc strategy rife with vulnerabilities - the type that put compliance and, more importantly, customer data at risk.

It is the kind of scenario that could inspire trepidation for those considering cloud-based resources for their workloads and applications. It is also the exact obstacle this white paper was designed to solve.

And, it does this through five direct and actionable steps. >>

Five steps for maintaining compliance while improving security practices

The steps below outline an approachable framework for embracing the cloud through security-focused activities.

1. **Know what you are securing**
2. **Determine your internal capabilities**
3. **Choose your third-party service providers carefully**
4. **Monitor and maintain service providers and your internal team**
5. **Plan for WHEN not IF**

Of course, everyone's cloud journey is unique, so some recommendations made here may not directly correlate to the specifics of your organization in all instances. However, the insights and best practices included were selected for their ubiquitousness and approachability - making them relevant for most all cloud environments.

We hope they serve as the first of many steps on a successful, secure and compliant cloud road map.

Understanding the difference between compliance requirements and strong security practice

Before we dive into how to build an effective program that solves for both security and compliance in the cloud, it is essential that we resolve a few misconceptions - the most critical being that compliance and security are one in the same.

This mistaken parity is exceedingly common and the major point of contention for compliance professionals. It empowers organizations to focus solely on passing compliance audits and assessments instead of instituting reliable and maintainable security operations (fig. 1) - the type that we will advise you toward in the last portion of this paper.

Defining compliance

Compliance is determined by governmental, non-profit or industry groups and serves as a generic blueprint for the security of certain kinds of data. The regulatory organizations that govern compliance standards issue them as a minimum bar for security which is evaluated through audits or assessments that are either self-administered or coordinated by a third party. Audits act as a snapshot of how your organization fared at one moment in time. As is common with regulatory standards, cloud compliance is often responsive as opposed to proactive – creating a lag time between qualified detractors and their prescribed solutions.

In the realm of cyber security, advancements in threat actor tactics and their defensive counterparts develop at a rate that compliance standards cannot keep pace. This limits their effectiveness to mandate how cloud-ready companies establish a reliable level of coverage for cloud data. However, this is not meant to downplay the importance of compliance and passing all requisite audits. Instead, it is an important distinction to understand when developing a cloud security program.

Defining security

For the purposes of this white paper, we are defining security in broad terms – that it is a risk-driven approach to protecting IT enterprise systems and data from unauthorized access or manipulation.

The key difference between security and compliance, as you can see from the focused definition above, is that security is inherently risk-based. Instead of measuring effectiveness based on adherence – or lack thereof - to prescribed controls, its success is defined by the ability to protect against and respond in the event of a threat to enterprise resources or data.

According to the Center for Internet Security (CIS), this objective equates to 20 critical security controls that are prioritized to protect against persistent cyber threats.

In essence, these objectives are not dissimilar from that of most compliance standards. The government and industry groups that craft these mandates are ostensibly reacting to perceived risks and structuring remedies accordingly. The key distinction remains, though, with the affected parties that are responsible for adhering to these standards and how they go about succeeding in that regard.

CIS top 20 critical security controls

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Example of compliance-driven vs. risk-based security

Figure 1 - illustrates the comparison between companies who approach compliance and security differently.

	Company A	Company B
Goal	Bare minimum to meet compliance standard.	Strong security practices using compliance requirements as a foundation.
Objective	Maintain the bare minimum to pass compliance audits/ assessment.	Built into standard operating procedures. Compliance becomes a natural byproduct of strong security practices.
Culture	Viewed as additional work to prepare for an audit/ assessment. "Check the box" for compliance.	Built into standard operating procedures. Compliance becomes a natural byproduct of strong security practices.
Talent	High IT talent turnover, hard to attract and retain security experience.	Low turnover, easy to attract and retain security experience.
Assessment Cost and Time	Increases due to lack of compliance in routine areas can result in frequent extensions and extra reporting to key stakeholders (clients, banks, boards).	Typically decreases relative to other companies of equal size and industry, makes it easier to achieve multiple compliance standards and increase market reputation/confidence.
Risk	**HIGH RISK** More potential for incidents/breaches, fines, fraud, poor market reputation or loss of business.	**LOW RISK** Less potential for incidents/breaches, good market reputation or increased business opportunities.

Five steps for maintaining compliance while improving security practices

1 Know what you are securing:

First and foremost, complete an assessment of what you are securing. Data is everywhere and as a result, you will need to gather an inventory of cloud-hosted data and classify it into tiers. From there, determine what is considered restricted, private, and public information. Based on this data classification, allocate security controls accordingly.

After the data has been classified, spend some time cleaning it. Purge non-critical and time expired data based on your corporate records retention policy and records destruction process. If no policy is in place, follow the government guidelines and create a corporate records retention policy and destruction process.

Considerations

- What are you securing? (Classify, clean, purge, map)
- How do you purge data in a secure fashion?
- How much security do you need?
- Where to secure it? (On-Premises, cloud)
- How do you monitor security? (On-Premises, cloud)

2 Determine your internal capabilities:

Be realistic about your internal capabilities.

- Are you staffed today to do what is required for your business?
- Can you compete for talent in today's competitive market?
- Do you have the budget for the latest tools to secure your data?

Finding tools and talent may be possible in the short term, but you may not be able to maintain these resources long term.

A potential solution may be co-sourcing with qualified partners to minimize the burden of addressing ever-changing security requirements.

Considerations

- What is the budget capacity today and in the future?
- How do you attract and keep sought after talent?
- How do you train staff on the latest tools and techniques?

3 Choose your third-party service providers carefully:

If you have elected to outsource services to a third party, it is essential that you gather necessary requirements and complete due diligence for all potential providers. This will confirm they are able to deliver and meet your security requirements.

Ensuring the service providers adhere to your security and compliance requirements is your responsibility. So, how do you get comfort and clarity that the service providers meet your requirements? Begin by reviewing their industry standard compliance reports such as PCI, SOC 1 and SOC 2.

A provider being unable to provide these reports is a red flag and will require extended due diligence on your part. In this market, it is best to avoid service providers who do not have independent security assessments or are not planning to go through an independent assessment in the near term.

Also, be skeptical of service providers who grade their own papers. Those who fill out their own assessments may not be truthful about their own environments or be incorrect in how they interpret the standard requirements.

If you still want to work with a service provider who does not have an independent security assessment, then you or your auditors can do an onsite assessment of the service provider's environment against your security requirements. Make sure you factor in the cost of time and resources to do the assessment when negotiating your service agreement. If you choose to go this route, plan for periodic security checks, at least annually, to ensure continued compliance.

Considerations

- Review the shared responsibility matrix (fig. 2) to verify tasks covered by the service provider. The rest is up to you.
- Verify geographic data housing considerations. Where does the data reside (onshore or offshore)?
- How effective is their network operations center (NOC)?
- How good are they at supporting forensic needs (e.g. adequate log details, access to logs or law enforcement support)?

What about **shared responsibility**?

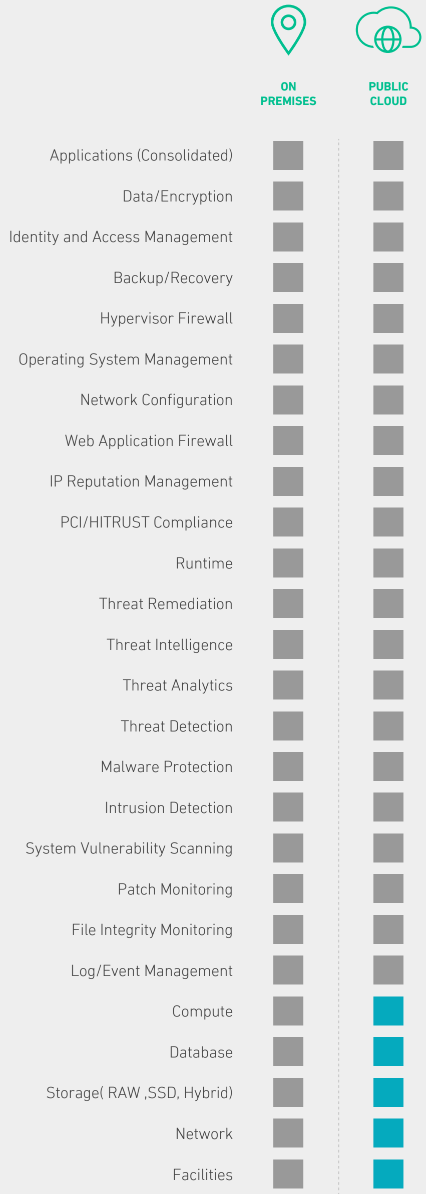
What is shared responsibility and how does it impact compliance in the cloud?

When discussing compliance in the cloud, it is critical that we explore the impact of shared responsibility between organizations and cloud service providers. This criticality is due to the significant role cloud services providers play in an organization's compliance either as a helper or a liability.

By understanding where this separation of responsibilities and identifying potential pit falls, organizations can more effectively maintain compliance and heighten data security.

What is shared responsibility?

Shared responsibility refers to a general framework (fig. 2) created by cloud service providers that outlines the agreed-upon separation of security and maintenance obligations between providers and their customers. Often presented as a model that varies between providers, this framework outlines responsibilities that are typically split so that service providers are only accountable for securing and maintaining cloud infrastructure while the organization manages their data and applications.



	ON PREMISES	PUBLIC CLOUD
Applications (Consolidated)	■	■
Data/Encryption	■	■
Identity and Access Management	■	■
Backup/Recovery	■	■
Hypervisor Firewall	■	■
Operating System Management	■	■
Network Configuration	■	■
Web Application Firewall	■	■
IP Reputation Management	■	■
PCI/HITRUST Compliance	■	■
Runtime	■	■
Threat Remediation	■	■
Threat Intelligence	■	■
Threat Analytics	■	■
Threat Detection	■	■
Malware Protection	■	■
Intrusion Detection	■	■
System Vulnerability Scanning	■	■
Patch Monitoring	■	■
File Integrity Monitoring	■	■
Log/Event Management	■	■
Compute	■	🟦
Database	■	🟦
Storage(RAW ,SSD, Hybrid)	■	🟦
Network	■	🟦
Facilities	■	🟦

Figure 2- Shared Responsibility Model that outlines the general separation of obligations between cloud customers and various cloud services providers.

🟦 Public Cloud Provider

■ Cloud Customer

4 Monitor and maintain service providers and your internal team:

Once you have your internal and third-party service provider's responsibilities in place, create a plan for monitoring controls. The plan should include periodic monitoring of the service provider's controls, including annual review of independent reports, onsite audits, and questionnaires. For your organization, make security part of your company's day-to-day operational controls through training, scorecard metrics, periodic security awareness campaigns, mock security incident exercises and educational emails.

Once you build security into your corporate DNA, your compliance requirements become a natural byproduct of your standard operating procedures and not a separate "project."

Considerations

- Review your responsibility matrix periodically
- Set a cadence for reviewing service providers
- Incorporate proper security controls into your corporate DNA
- Continuously test internal staff

5 Plan for WHEN not IF:

No matter how much you spend, educate, monitor and plan, you will never be 100% secure. There is always someone building a better mouse trap; threats become more sophisticated by the day. The best thing to do is measure your tolerance for security risk and build a foundation to mitigate the risks that pose the highest risk to operational integrity. Part of that effort is to plan for incidents that will occur. Well-thought-out incident handling processes save companies time, money and reputation.

Training is another critical aspect of the plan and process. People are your weakest control point. You can spend as much as you want on technology, but if you don't adequately train your people and if one occurs, even the most robust security tool won't be able to save you. Train everyone in your company on security best practices. Train those with more access, like your administrators and other IT support staff, on how to detect and prevent deeper security issues.

Considerations

- Identify your threat vectors
- Write, review and test your incident response/disaster recovery plans as well as business continuity planning
- Train your team on security best practices

Conclusion

If there's one thing you take away from this white paper, it should be that limiting your cloud security to compliance requirements is never a viable option. With the plethora of cyber threats, forgoing a risk-based security program in favor of a compliance-based strategy is a recipe for disaster – or, at the least, several sleepless nights for your IT organization.

So, what does this mean for organizations solely focused on maintaining compliance and surviving their next audit? Ostensibly that their focus is misplaced. This is an issue that is not going away any time soon. Gartner predicts that 95% of cloud failures through 2020 will be due to customers and their mismanagement of cloud resources. Do not become a statistic! We have established that limiting a cloud security strategy to compliance requirements fails to adhere to the true intention of the standards it's chasing.

Being compliant in the cloud requires organizations build on the framework established by compliance standards and truly codify and operationalize the requirements – instead of treating them like a checklist. This paradigm shift, combined with a firm understanding of any requisite shared responsibility models, is essential to maintaining compliance and – most importantly – effective threat protection in the cloud.

> “95% of cloud failures will be due to customer failures through 2020.”

Gartner Inc.,

Top Strategic Predictions for 2016 and Beyond: The Future Is a Digital Thing

Sajeev Prelis | Accretive Solutions

Sajeev Prelis is a National Director in the Risk Management and Security practice at Accretive Solutions. He is responsible for the firm's PCI practice nationally and the Risk management practice in the Texas region.

He has more than 20 years of information systems, security, and business experience in the following industries: telecom, banking, manufacturing, distribution, insurance, retail, entertainment, healthcare and energy.

He holds a BBA in Finance from Southern Methodist University, an MBA in Information Technology and an MS in Telecommunications from The University of Texas at Dallas, and the following certifications: QSA, PCIP, CCSFP, CISA, CGEIT, CRISC.

+1 214 739 1553
www.accretivesolutions.com

Jeff Schilling | Chief Security Officer, Armor

Jeff Schilling (Colonel, Retired) is Armor's Chief of Security and is responsible for the cyber and physical security programs for the corporate environment and customer hosted capabilities.

Before joining Armor, Jeff was the Director of the Global Incident Response practice for Dell SecureWorks where his team supported more than 300 customers with incident response planning, capabilities development, digital forensics investigations and active incident management.

Jeff retired from the US Army after 24 years of service in July of 2012. In his last assignment, Jeff was the Director of the Army's global Security Operations Center under US Army Cyber Command. In this position, Jeff was responsible for synchronizing the global security operations/monitoring and incident response for more than one million computer systems, on 350 wide area networks, supporting all Army organizations in more than 2500 locations.

+1 844 682 2858
www.armor.com