IN THE TRENCHES:

Building A Risk Management Program From the Ground Up

BARR ADVISORY

Table of Contents

Introduction

Security and compliance are two critical aspects of the modern cybersecurity landscape, often used interchangeably but with distinct nuances.

Security

Security goes beyond being safe from threats; it encompasses reliability and consistent performance. In the context of evolving threat models, security involves safeguarding the confidentiality, integrity, and availability of systems.

Compliance

Compliance, on the other hand, involves adhering to standards and regulations applicable to an organization. However, compliance also serves as a means of communicating an organization's security posture to internal and external stakeholders. It establishes a common language for discussing security measures and controls and allows organizations to build demonstrable cybersecurity programs to provide assurance to customers that their data is safe.

> **“Compliance should be seen as the common language of security.”**
>
> Larry Kinkaid, CISSP, CISA, CRISC

Both security and compliance are key components of building a risk management program from the ground up. In this whitepaper, we’ll explore the relationship between security and compliance, key risks in the cloud (particularly vendor risk management), how to use compliance frameworks to address those risks, and more.

Security vs. Compliance

While compliance ensures alignment with standards and helps avoid regulatory penalties, it does not guarantee comprehensive security. Regulations struggle to keep pace with rapidly evolving technologies and the growing spectrum of cyber threats. When compliance outweighs security, you end up with "check-the-box" security which detracts from the overall credence of a security program, especially as it relates to creating a culture of security.

The fear of noncompliance penalties has fueled a culture of hiding vulnerabilities to avoid reputational damage. A shift in focus from security to compliance hinders progress within the cybersecurity industry.

For some organizations, compliance can be an introduction to security. Security should be the ultimate goal, with compliance serving as a foundation. By prioritizing security, organizations can address evolving threats and protect data, which in turn simplifies compliance efforts. Striking a balance between security and compliance is crucial, fostering a culture of transparency and genuine risk management.

Key Risks in the Cloud

Governance, Risk Management, and Compliance (GRC)

In the cloud, GRC gains heightened importance due to the third-party/vendor relationships involved. Cloud environments necessitate robust identity and access management (IAM) to counter eavesdropping, data manipulation, and unauthorized activity.

Infrastructure Security

Effective vulnerability and patch management are vital due to the shared multi-tenant nature of cloud infrastructure. Advanced Persistent Threats (APTs) demand continuous monitoring to identify and counter stealthy data extraction. Furthermore, penetration testing summaries have become a foundational piece of evidence to demonstrate the technical security of an application from a third party.

System Security

Network security, encryption, cryptography, and cloud configuration are pivotal in securing cloud systems.

Application Security

Secure development practices, Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), code scanning, and open-source management (e.g., Dependabot) are essential for robust application security.

Business Resilience and Availability

Multi-region availability zones, Service Level Agreements (SLAs), logging, monitoring, and cyber liability insurance contribute to business continuity and disaster recovery planning.

Vendor Management

Effective vendor risk management is vital as organizations increasingly rely on external vendors. Business risk assessment, compliance evaluation, and clear contractual terms are key aspects of successful vendor partnerships.

Vendor Risk Management

Vendor risk management is one of the most critical and complex challenges faced by organizations when building their risk management programs. Modern businesses typically rely on external vendors for specialized services for a number of reasons, including expertise, cost, and convenience.

When establishing vendor risk management processes, it’s crucial to focus on business risk, compliance, and contractual obligations.

Business Risk

Collaboration between security, leadership, and finance is vital to understand specific risks associated with vendor relationships. Involving relevant stakeholders ensures alignment and buy-in for risk mitigation strategies.

Compliance

Balancing reliance on compliance standards like SOC 2 with contractual obligations is essential. Prioritizing breach response time and contractual language aids in reacting effectively to security incidents. In addition to understanding the cybersecurity functionality offered by the vendor, such as Single Sign-On (SSO), DLP (Data Loss Prevention), or increased availability (class of nines).

Contracts

Legal and security collaboration is necessary to establish contractual obligations, ensuring that security concerns are adequately addressed in vendor partnerships. Information security addendums give cybersecurity expectations structure when it comes to the rules of the relationship and establishing accountability.

Compliance Frameworks

When building a risk management program, it's important to take into account relevant frameworks for your organization. For organizations in the beginning stages of their security and compliance journey, it can be easy to become overwhelmed with the number of frameworks out there, which is why it's often best for organizations to choose one compliance framework to stick to.

There are several frameworks to choose from, each with their own benefits and complexities:

SOC 2 Type 2
Offers flexibility tailored to diverse business needs. Provides a self-defined approach to security compliance.

ISO 27001
Balances prescription and flexibility. International-friendly and aligns well with SOC 2 Type 2 requirements.

NIST 800-30
Guides comprehensive risk assessments. Regarded as a gold standard in many sectors, particularly for government-related projects.

FAIR Methodology
Translates risk statistics into business-understandable terms—i.e., capital. Cash is the common language of business and FAIR allows cybersecurity to have a seat at the table. Enables better communication between security professionals and business stakeholders.

Cybersecurity is a journey, not a destination. Balancing security and compliance is essential, as the two are complementary forces. By prioritizing security, organizations can maintain a proactive approach to risk management, enhance vendor partnerships, and choose the most suitable compliance framework to match their needs.

About BARR Advisory

BARR Advisory is a cloud-based security and compliance solutions provider specializing in cybersecurity and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud Platform. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements in highly regulated industries including technology, financial services, healthcare, and government.

Our Services

SOC Examinations
[SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]

Healthcare Services
[HIPAA/HITRUST]

ISO 27001 Assessments

FedRAMP Security Assessments

PCI DSS Assessment Services

Penetration Testing and Vulnerability Assessments

Cybersecurity Consulting and vCISO Services

Compliance Program Assistance

Connect with BARR

Want to learn more about building a risk management program for your organization? Contact us today.