Two Security Strategies That Help You Remain Agile in Today's Cloud Environment

You Don't Have to Own **IT** to Control **IT**SM

Introduction

The Information Age brings new efficiencies and with it, new challenges. Cloud computing and provisioning introduced tremendous opportunities to streamline Information Technology (IT) practices through leveraging. However, a perceived loss of control complicates an already difficult cybersecurity ecosystem.

Competitive forces have driven the adoption of cloud computing; however, that adoption brings a far more complicated view of cybersecurity risks.

> The organizations that effectively minimize the cost of managing cybersecurity risk, while reaping the efficiency rewards of integrated, interconnected and leveraged electronic systems that cloud provides, will thrive. Cybersecurity risk management is an existential question for organizations in this century. While it is no longer a competitive option to minimize the impact of these business decisions, it is not clear how to apply focused principles to this practice. This is even more relevant when considering cloud solutions. Remaining agile in determining the most efficient choices in applying approaches in choosing proven security principles and the application of these principles is an organization which will thrive in a cloud driven environment.

This paper introduces key strategic cybersecurity principles and concepts already in existence and widely adopted by both commercial and governmental agencies which can effectively be leveraged to help drive strategic decision making in choosing security technologies and processes for your cyber-security requirements while remaining effective, efficient and secure.

COMPANION DATA SERVICES®
A CELERIAN GROUP COMPANY

The Challenge

In today's complex world, public and private entities must perform activities that require the storage and transmittal of electronic information. This is unavoidable and happens at a corporate and individual level. Therefore, it only makes sense that these entities take cyber risk into consideration at a pragmatic level. The question is not that some level of risk management must be performed. The question is how much and of what variety is required to remain effective and efficient with your core service delivery.

Generally, there are two developing strategic approaches that continue to provide the right level of information assurance in a given business practice. Although a short definition for each is included below, the intent is to break out each area to reach strategic clarity of application.

- ### Certification and Accreditation (C&A) / Authorization Approach

  This approach uses a highly controlled and lengthy process to determine the risk posed by a given system and subsequently generate a list of security activities or controls to mitigate the risk. Controls are selected from one or more external risk frameworks. The sum of this activity is periodically validated and reviewed by a governance body. Extensive cybersecurity planning, auditing, documentation and residual risk assessment occurring over several years are hallmarks of this approach.

  The traditional challenge with this approach is related to the sheer number and complexity of potential risk frameworks available to select controls from. Risk frameworks have followed a traditional Gartner Hype Cycle in that many were introduced early in the development of the cyber risk practice; however, the risk framework space is rapidly coalescing into the plateau of productivity. Organizations that take advantage of this standardization can leverage hard efficiencies for their respective strategic cybersecurity practice.

- ### Continuous Monitoring Approach

  This option applies the principles of initial risk assessment and subsequent control implementation as noted; however, it differs in the timeliness and near real-time view of the risk. This approach is operational in nature and drives into governance only when predetermined criteria are met. This is a relatively new trend in the cybersecurity strategic space. Alerting, predetermined escalation, dash-boarding and continuous control validation are hallmarks of this approach.

The implementation of these practices can and should overlap. They are not mutually exclusive, as some would assume. Mature cybersecurity practices that appropriately blend these approaches tend to see mature cybersecurity business results.

COMPANION
DATA SERVICES®
A CELERIAN GROUP COMPANY

Trends in Security

Security Framework Convergence and Standardization of Cybersecurity Controls

One of the biggest challenges when strategically managing cyber security risk used to be the simple determination of which risk framework to choose from. Many different risk frameworks were developed across the space as organizations started to grapple with the strategic implementation of cybersecurity risk mitigation. In this early phase of framework development, numerous, complicated, specialized and contradictory controls were defined such as:

- International Organization for Standardization (ISO) 27001
- Information Technology Infrastructure Library (ITIL)
- Control Objectives for Information and Related Technology (COBIT)
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information System Controls Audit Manual (FISCAM)
- Unified Control Framework (UCF)
- Department of Defense (DoD) 8200

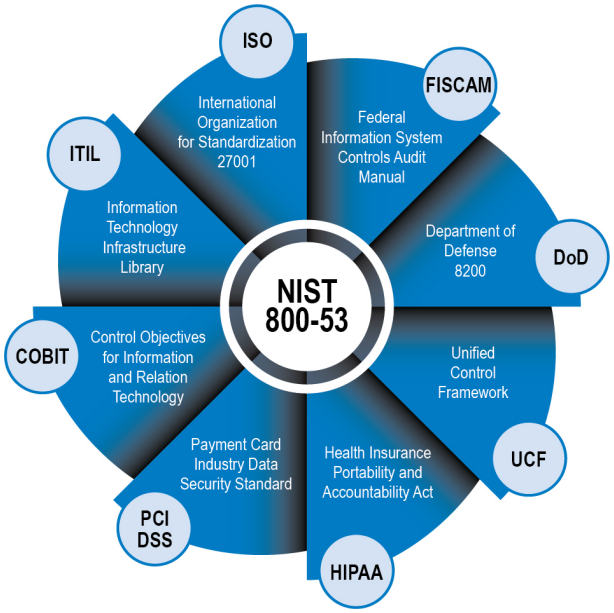
This problem was exacerbated when governance organizations determined that compliance was required from multiple control frameworks for the same systems to meet business needs.

This led to large scale operational inefficiencies. The implementation and practical execution of any given security control practice requires resource and operational focus. The key to operational efficiency is tied to the ability to streamline, standardize and leverage policies, processes and work activities in a repeatable and measurable way. The selection of conflicting and asymmetric controls, from various families, leads to duplicative and ineffective cybersecurity practices.

In the last several years, cybersecurity framework governance has undergone a subtle but powerful consolidation that continues to march toward a unifying practice. Powered by the National Institute of Standards and Technology (NIST), the various risk frameworks have increasingly begun to provide a direct mapping of their proprietary controls to those noted in NIST 800-53. The NIST 800-53 is a federal publication that recommends security controls for federal information systems and organizations.

The adoption of federal cybersecurity control standards across the risk framework space is a trend that will allow a unified and leveraged operational control execution to meet a multitude of governance obligations. This trend ensures that governance organizations that select and adapt cybersecurity controls from the NIST 800-53 publication to meet risk management obligations will see efficiencies to their bottom line while meeting a risk posture that fits their needs.

COMPANION
DATA SERVICES®
A CELERIAN GROUP COMPANY



NIST 800-53 unifies risk frameworks to meet governance obligations. Organizations that select cybersecurity controls from the NIST 800-53 publication tend to see efficiencies to their bottom line.

Evolution of Practical Continuous Controls Monitoring

As governance organizations drive toward control selection from a unified set of cybersecurity controls, the subsequent ability to implement continuous monitoring of individual control execution becomes possible. This trend of continuous controls monitoring is the operationalization of the control execution. This is a similar development to that of Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) evolutions previously matured in the business space.

Cybersecurity control execution is monitored, measured and managed in a near, real-time state using organizationally integrated Governance, Risk and Compliance (GRC) systems. Individuals responsible for the operational execution of standardized controls provide continuous evidence of completion through periodic automated or manual system submission through planned workflows.

COMPANION DATA SERVICES®
A CELERIAN GROUP COMPANY

This practice can only be effective within the context of standardized control execution that can be leveraged to meet multiple governance risk frameworks. Benefits include:

- Cybersecurity assurance can be provided on demand with the ability to show effective compliance to audit and governance bodies in a planned, controlled delivery.
- Operational prioritization and decision making are clarified through the delivery of metric based dashboards and reporting.
- Threat posture, control execution and operational cybersecurity readiness are available to governance bodies as needed. Triggering events can be modeled that allow automated governance escalation.

CDS Security Solves the Problem

To ensure the most efficient execution of cybersecurity controls, Companion Data Services, LLC (CDS) executes directly to NIST 800-53 controls while preserving the specific control reference to any other risk framework. CDS executes mature implementations of NIST family controls and leverages them to meet customer needs without the cost of extensive customization.

In the rare event that a given customer governance framework requirement does not already map back to standard NIST controls, CDS maintains the expertise to design an appropriate cross reference for the customer. Recent examples of customer specific compliance frameworks mapped back to our mature, NIST-based risk practice include:

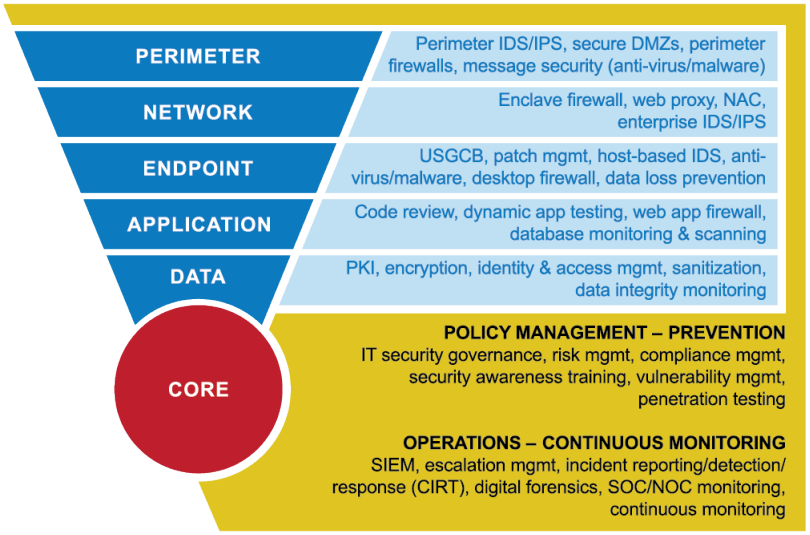
- Criminal Justice Information Services (CJIS)
- Medicare Acceptable Risk Safeguards for Exchanges (MARS-E)
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)

Through the use of this practice, CDS provides one way of meeting any given control requirement in a standard, cost-effective, repeatable way for our customers regardless of the compliance framework need by using this practice.

COMPANION DATA SERVICES®
A CELERIAN GROUP COMPANY

Although continuous controls monitoring is a new concept in the cybersecurity space, we are already performing this work and have integrated it into CDS' defense-in-depth access approach to:

- Monitor and execute continuous monitoring through the effective use of an extensive GRC implementation
- Deliver near, real-time control reporting and management information that provides our customers with near, real-time visibility of a hosted system risk posture
- Integrate into continuous control monitoring at an individual control owner level through developed work practices



CDS' defense-in-depth access approach

Secure data access and dissemination services are provided from the perimeter to the data core. Each layer is independently implemented and monitored to ensure services are protected across the environment.

Coupled with standardized NIST control implementation, CDS has built the mechanism to deliver out-of-the-box control monitoring for your GRC system or to provide you with visibility into ours. This approach allows for true transparency to your systems security posture without the need to own the IT asset.

Conclusion

By considering the principles and choices outlined in this paper, organizations can effectively minimize the cost of managing cyber security risk, while reaping the efficiency rewards of integrated, interconnected, leveraged electronic systems that cloud provides. Companies that survive and thrive do so in part by the efficiencies they can leverage as stated above by establishing and leveraging already proven and known concepts for a secure cloud computing environment.

COMPANION DATA SERVICES®
A CELERIAN GROUP COMPANY