Managing the Business of Cybersecurity Risk Management

A Proactive, Collaborative and Balanced Approach for Managing, Securing and Improving the Digital Services that Drive Today's Enterprise

By

Rick Lemieux & David Nichols

September 2020

Copyright and Trademark Notice

Notice of Rights / Restricted Rights Legend

itSM Solutions LLC
742 Mink Ave #135
Murrells Inlet
South Carolina, 29576
401-480-5872
Web http://www.itsmsolutions.com

Notice of Liability

Introduction

Three things are certain in today's business world: first, digital services are now at the center of all businesses; second, business value is a moving target and third businesses are under attack from those trying to steal or damage the digital assets companies rely on for the creation of business value.

The demand for a proactive and balanced approach for managing, securing, and improving digital services across stakeholders, supply chains, functions, markets, and geographies has never been greater.

Cybersecurity risk management is fundamental to the business and their successful digital business transformation initiatives. Cybersecurity risk management decisions, like all other business decisions, must consider both the value and risk the service will contribute to the customer experience. In-light of this, a solid, sound business case exits for organizations to make the investments necessary to make cybersecurity a core/mission critical organizational capability. There are no silver bullets, there are no shortcuts, there are no "cybersecurity-in-a-box," there is only the work it takes for the organizations to make cybersecurity a core/mission critical organizational capability. When an organization seeks the collective experience of all stakeholders in the pursuit and execution of a single customer experience strategy, the integrated whole is much greater than the sum of the individual parts.

To support a digital business model, enterprises must adopt and adapt a best practice approach to cybersecurity risk management**.** The cybersecurity risk management program must deliver a proactive, collaborative, and balanced approach for adopting and adapting the

incremental improvements necessary to manage and improve the cost, quality and security of an organization's digital services portfolio.

Today's Digital Enterprise

Before an enterprise can operate as a digital business, it must demonstrate three main characteristics; an unambiguous understanding of its customer's need, repeatable processes to ensure consistency of secure delivery, and the ability to innovate and secure its services in a structured manner.

To achieve an unambiguous understanding of the customer's needs, enterprises must, in a structured repeatable manner, define and categorize its processes, technology and cybersecurity risk management capability requirements. The next step is to compare these requirements to the existing environment to understand what it will take to achieve and manage the required capability. The adopting organization must do this in the context of governance based on strategic digital business and cybersecurity policies with achievement measured against expected outcomes.

Repeatable processes are required to ensure consistency of execution. This is critical because day-to-day business processes rely so much on embedded technology that failure to execute consistently directly impacts the enterprise's ability to deliver and protect its products or services.

The organization's business objectives must represent the integration of the business strategy with the digital transformation and cybersecurity strategies to ensure that cybersecurity becomes core/mission critical to the business. Such a strategy would include the adoption of the NIST

Cybersecurity Framework and the adaptation and integration of one or more of its informative references with the organization's Customer Value Management System (CVMS) capabilities. Such an approach would enable the organization to ensure the cybersecurity controls that are implemented are fit for use in achieving the organization's desired cybersecurity posture, and also enable the continual improvement of both the operational controls and the cybersecurity strategy.

Underpinning all of this is the need for a model that helps identify what services need to be sourced internally and what services can be sourced externally. This model will provide the guidance the enterprise needs to classify the services and processes that are critical to quality service delivery and differentiation in the marketplace (See Figure 1). The internally sourced services are prime candidates for investment, as they are critical to the success of the business. The business may source other activities according to the capability of the enterprise using established sourcing policies and guidelines such as Carnegie-Mellon's eSCM capability model.

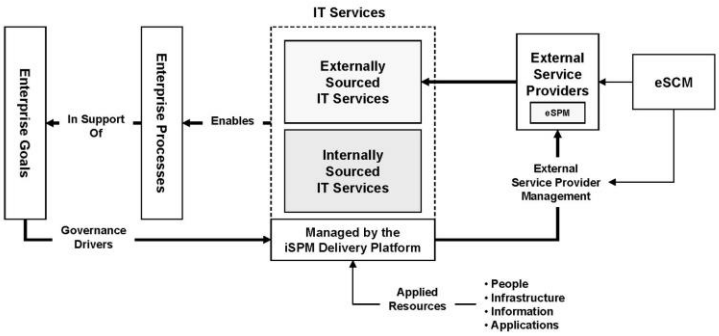


Figure 1

Delivering Customer Value Using Best Practice Frameworks

To support a digital business model, the enterprise needs to transform the traditional Business – **IT paradigm from one focused on technological value to one focused on customer value.** This service provider paradigm encompasses widely accepted best practice frameworks, methodologies and standards focused around managing the cost, quality, compliance, security, risk, and business continuity of an organization's digital services portfolio.

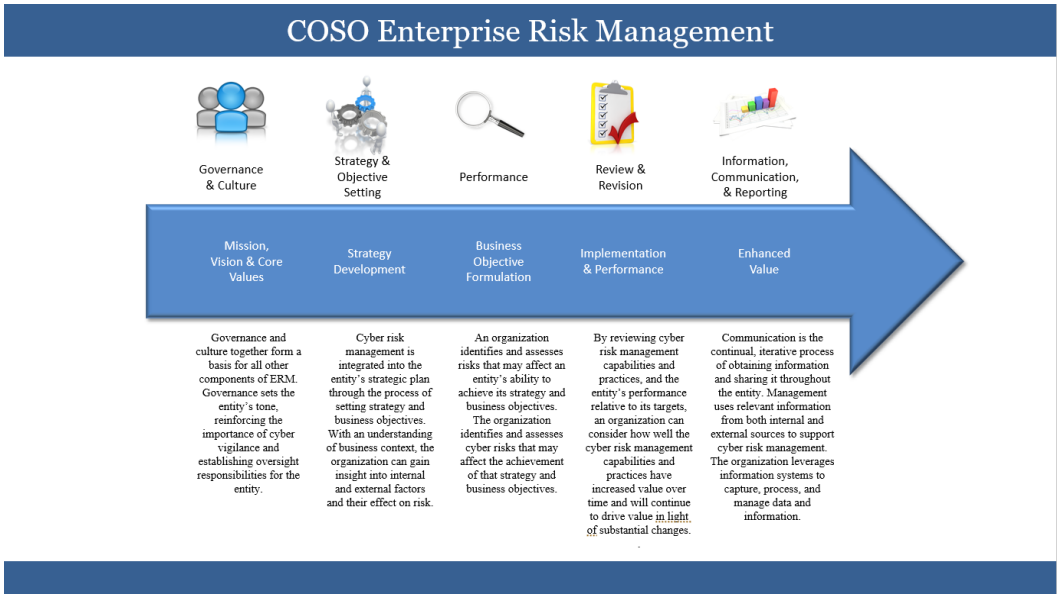
IT Service Management & Governance Best Practice Frameworks

Today, enterprises are presented with a wide variety of best practice options each being promoted as the "silver bullet" to enabling a secure agile enterprise. Over the years, framework's from ISACA and Axelos have led the way for organizations to operationalize the controls and management systems for effective and reliable digital service delivery and governance.

Enterprise Cybersecurity Risk Management Best Practice Frameworks

Most recently, the Committee of Sponsoring Organizations (COSO), the National Institute of Standards (NIST), and the Cloud Security Alliance have been added to the list of enterprise best practice frameworks for their work in the areas of enterprise and cybersecurity risk management.

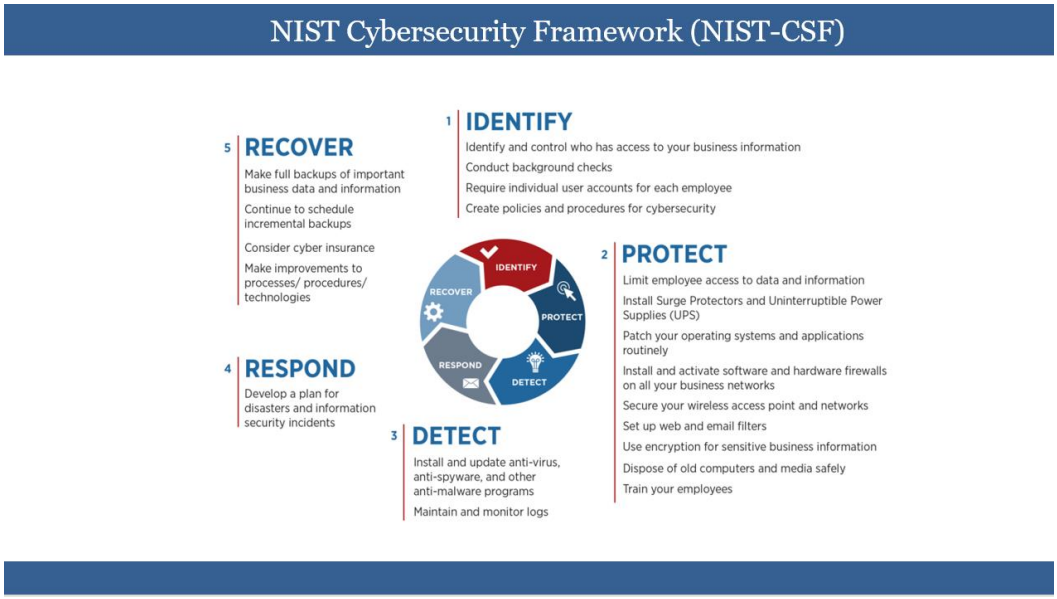
The COSO Enterprise Risk Management Framework was created to help executives prioritize cybersecurity investments by aligning those investments with its digital business and cybersecurity risk management policies.



The COSO Framework has now been approved as the governing framework for enterprise risk management by:

- **American Accounting Association (AAA)**
- **American Institute of CPAs (AICPA)**
- **Financial Executives International (FEI)**
- **The Institute of Management Accountants (IMA)**
- **The Institute of Internal Auditors (IIA)**

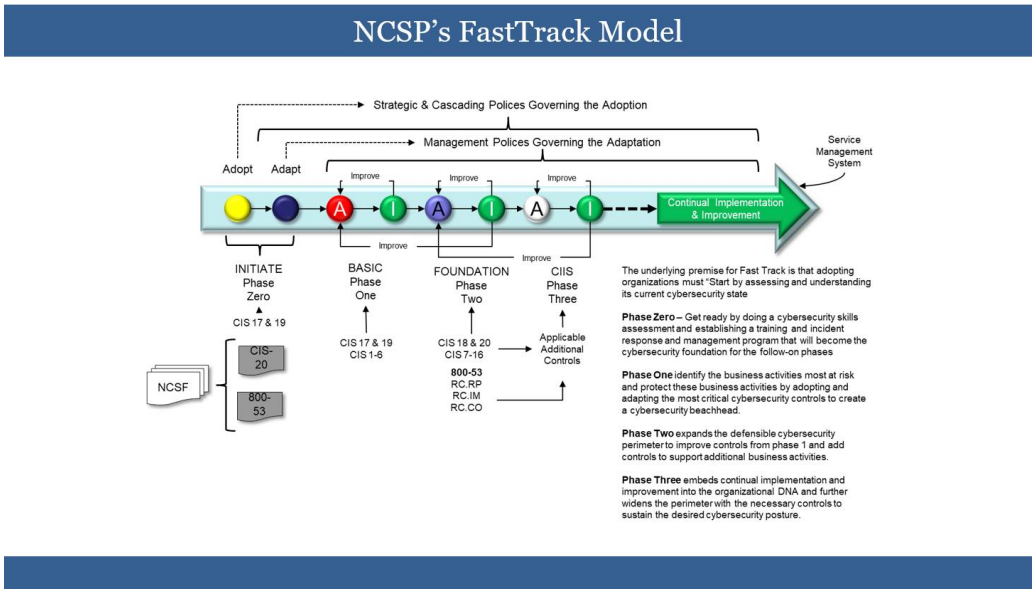
The NIST Cyber Security Framework was created under Executive Order to provide a uniform standard that government and businesses could adopt to guide their cybersecurity activities and risk management programs in terms of Identifying, Protecting, Detecting, Responding and Recovering from cyberattacks.



The NIST Framework has now been approved as the governing framework for the US government, a growing number of critical infrastructure sectors (financial services, healthcare, energy etc.) and a long list of international governments.

A Fast-Track Approach to Adopting and Adapting the NIST & COSO Frameworks

itSM's **NIST Cybersecurity Professional (NCSP) Practitioner** certification training programs teach organizations a **Fast-Track** approach on **how to** engineer, operationalize and continually improve a NIST/COSO cybersecurity risk management practice across an enterprise and its supply chain.



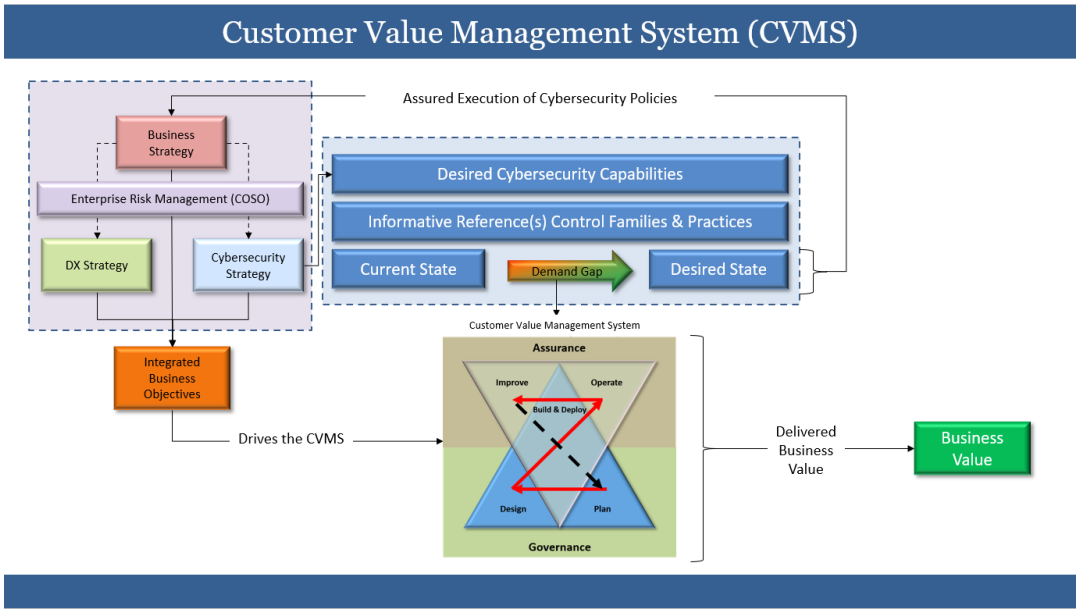
The Fast-Track model teaches organizations how to:

- **Assess** and understand its current cybersecurity state
- **Design** a cybersecurity program using COSO guidance and NIST-CSF informative reference controls to realize an its future cybersecurity state
- **Implement & Operationalize** a Continual Implementation & Improvement Management System (CIIS) to automate, sustain and continually improve its future cybersecurity state.

A Customer Value Management Approach to Adopting, Implementing & Operationalizing NIST-IR Controls & Management Systems

itSM's **NIST Cybersecurity Professional (NCSP) Specialist** certification training programs teach organizations how to **Adopt, Implement & Operationalize** the NIST informative reference controls

(NIST 800-53, 800-171, CIS-20) and management systems (ISO 27001) using a **Customer Value Management System** that will ensure the **Capability, Quality and Efficacy** of the enterprise cybersecurity risk management program.



The CVMS approach looks at the impact of adapting a principled approach to enterprise risk management framework to better support cybersecurity decisions within the context of the selected informative reference. It guides organizations on the best approach to adapt, implement, and operate (AIO) a comprehensive cybersecurity program capable of integrating into existing organizational capabilities.

NCSP Strategic Partnerships

The following companies have partnered with itSM Solutions to create and distribute its NCSP Practitioner and Specialist accredited certification courses across the globe.

- HPE Education Services
- Raytheon Professional Services
- Bryant University
- Cybersecurity Professionals
- Deep Creek Center
- QA Ltd.
- TaUB Solutions
- Creative Disruptions
- CyberTec Academy
- New Horizons Learning Centers
- Interprom
- Cybiant
- The ITSM Hub
- APMG International
- The Stationery Office Ltd (TSO) a William Lea Company
- Career Academy
- CyberSaint

About itSM Solutions LLC

Founded in 2002, itSM Solutions LLC is the creator of the NIST Cybersecurity Professional (NCSP) certification training program. NCSP teaches organization **how to** design and operationalize a NIST/COSO cybersecurity practice capable of Identifying, Protecting, Detecting, Responding and Recovering from cyberattacks.

About the Authors

David Nichols is the President and CEO of itSM Solutions LLC, an ITSM consulting and training company. He has over 35 years' experience in Information Technology. As an early adopter of the IT Service Management processes as described in the IT Infrastructure Library (ITIL), he has utilized his hardware and software engineering background as a foundation for implementing sweeping changes in how IT Services are delivered at several fortune 100 companies in the US. Working closely with the executive management teams, David has helped the strategic goals of the IT organization with those of the company and develop a more effective IT Strategy. Strategies that are customer focused, process-oriented and cost/performance optimized, and help business and IT organization establish the value of IT Services. David holds ITSM Expert certification.

Rick Lemieux is a managing partner and Chief Revenue Officer at itSM Solutions. Rick has been involved in selling IT solutions for the past 33 years. Prior to itSM, Rick led the Sales and Business Development teams at software companies focused on automating the best practices guidance outlined in ITIL and other frameworks. Rick holds a Foundation Certificate in IT Service Management and was recently identified as one of the top 5 IT Entrepreneurs in the State of Rhode Island by the TECH 10 awards.