



Cyber Service Management

**A Proactive, Collaborative and Balanced Approach for
Managing, Securing and Improving the Online Services
that Drive a Cyber Enterprise**

By

David Nichols & Rick Lemieux

December 2018

Cyber Service Management

Operationalizing Cyber Service Management Across an Enterprise and its Supply Chain

Copyright and Trademark Notice

Copyright © 2018 itSM Publishing. itSM Solutions® is a Registered Trademark of itSM Solutions LLC. ITIL® is a Registered Trademark, and a Registered Community Trademark of the Axelos, and is registered in the U.S. Patent and Trademark Office and is used here by itSM Solutions LLC under license from and with the permission of Axelos (Trademark License No. 0002). Other product names mentioned in this guide may be trademarks or registered trademarks of their respective companies.

Notice of Rights / Restricted Rights Legend

All rights reserved. No title or ownership of this document, any portion thereof, or its contents is transferred. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written permission of itSM Solutions LLC. Reproduction prohibitions do not apply to this document when reproduced for non-commercial use, or to excerpts or quotes for use in reviews or attributed quotes in other works of any type as allowed for in copyright law. For additional information, please contact:

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

Notice of Liability

This guide is distributed "As Is," without warranty of any kind, either express or implied, respecting the content of this guide, including but not limited to implied warranties for the guide's quality, performance, merchantability, or fitness for any particular purpose. Neither the authors, nor itSM Solutions LLC, its dealers or distributors shall be liable with respect to any liability, loss or damage caused or alleged to have been caused directly or indirectly by the contents of this whitepaper.

Cyber Service Management

Operationalizing Cyber Service Management Across an Enterprise and its Supply Chain

Three things are certain in today's business world: first, **cyber services** are now at the center of all businesses; second, business is a moving target and third businesses are under attack from those trying to steal the critical information companies rely on for daily business operations and revenue generation.

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

Cyber services are fundamental to corporate success, and cyber service 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 for cyber investments requires mature business, and risk judgment. Unfortunately, there are no shortcuts to developing maturity or to developing judgment – both take time and experience. There is only one way to gain traction in these circumstances and that is to apply the collective experience of all stakeholders in the pursuit and execution of a single customer experience strategy. In this case the integrated whole is much greater than the sum of the individual parts.

To support this new cyber service business model, enterprises must adopt and adapt a best practice approach to **Cyber Service Management (CSM)**. The CSM program must deliver a proactive, collaborative and balanced approach for adopting and adapting the incremental improvements necessary to manage & improve the cost, quality, compliance, security, risk and business continuity of a cyber service portfolio.

Cyber Service Management

Operationalizing Cyber Service Management Across an Enterprise and its Supply Chain

Shaping the Future – Cyber Service Management (CSM)

Before an enterprise can adopt and adapt a CSM program, it must demonstrate three main characteristics; an unambiguous understanding of their customer's need, repeatable processes to ensure consistency of execution, and the ability to innovate in a structured manner.

To achieve an unambiguous understanding of the customer's needs, enterprises must, in a structured repeatable manner, define and categorize the enterprise process, technology and 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 provider must do this in the context of governance based on enterprise goals and 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 its products or services.

Finally, the enterprise must develop a utility grade delivery platform and practice management model that is capable of supporting emerging utility-based architectures and applications such as Real Time Infrastructure (RTI), Service Oriented Architecture (SOA) and Software as a Service (SaaS). The delivery platform provides the portal through which the enterprise receives its business enabling technology. The enterprise brokers those services irrespective of their source, internal or external. Therefore, the enterprise can deliver utility grade, business-aligned services as needed, and manage technology investments and innovation in a structured manner.

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

Cyber Service Management

Operationalizing Cyber Service Management Across an Enterprise and its Supply Chain

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.

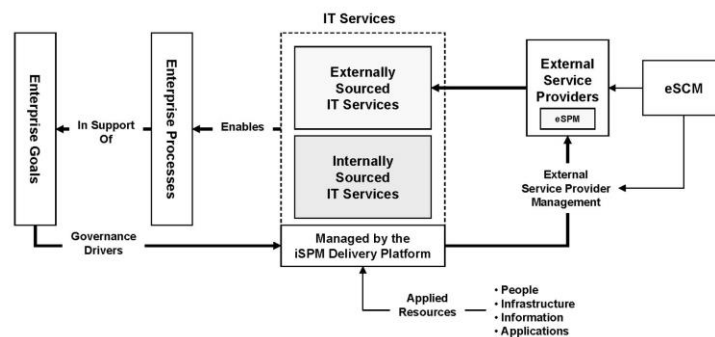


Figure 1

Frameworks, Methods & Standards

To support this new CSM model, enterprises need to transform the traditional Business – IT paradigm from one focused on technological value to one focused on service 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 the organization's cyber services portfolio.

Today, enterprises are presented with a wide variety of cyber service best practice options (See Figure 2) Over the years, enterprises were presented with a wide variety of management options to stabilize and

Cyber Service Management

Operationalizing Cyber Service Management Across an Enterprise and its Supply Chain

optimize IT services. Frameworks and standards from Axelos, ISACA and ISO have become the defacto standards for most organizations. Most recently, NIST, the Cloud Security Alliance and the Institute for Digital Transformation have been added to the list for their work in cybersecurity, cloud security and cyber organizational readiness.

When examined carefully, one discovers that there is some overlap between these frameworks, models and standards. So, while created from different viewpoints, they all address a similar set of enterprise business problems. The result is a mish-mash of framework's, methods and standards designed to support the end game of a delivering a proactive, collaborative and balanced approach for managing, improving and securing an enterprise cyber services portfolio.

itSM Solutions CSM Model

The itSM Solutions CSM model integrates eight best practice capabilities in support of operationalizing an enterprise CSM program.

CSM Capability	Framework, Standard or Methodology
Cybersecurity	NIST Cybersecurity Framework
Cyber Enterprise Readiness	Digital Enterprise Readiness Framework
Cloud Security	Cloud Security Alliance Framework
Cyber Resilience	RESILIA Cyber Resilience Framework
Cyber Service Management	ITIL Service Management Framework
Cyber Governance	COBIT 5 Governance Framework
Software & Application Security	Software & Application Testing Methodology
Cyber Project Management	PRINCE2 Project Management Methodology

NIST & NICE Cyber Security Frameworks provides guidance and training's on how to proactively manage and improve a cyber service portfolio in terms of cybersecurity risk and workforce development.

Cyber Service Management

Operationalizing Cyber Service Management Across an Enterprise and its Supply Chain

Digital Enterprise Readiness Framework provides guidance and training's on how to manage and improve a cyber business in terms of operational sustainability, organizational agility, strategic agility, and operating in a disruptive culture.

Cloud Security Alliance Framework provides guidance and trainings on a practical and actionable approach to adopt the cloud paradigm safely and securely

ITIL Service Management Framework provides guidance and training's on how to proactively manage and improve a cyber service portfolio in terms of agility, development, operations, cost, quality and compliance.

RESILIA™ Cyber Resilience Framework provides guidance and training's on how to proactively manage and improve a cyber service portfolio in terms of business resiliency and recovery.

COBIT Governance Framework provides guidance and training's on how to proactively manage and improve a cyber service portfolio in terms of risk policies and controls.

Software & Application Testing Methodology provides guidance and training's on how to make software systems and applications safer regardless of their operating environment (web, IoT, Cloud)

Cyber Service Management

Operationalizing Cyber Service Management Across an Enterprise and its Supply Chain

PRINCE 2 Project Management Methodology provide guidance and training's on how enterprises can improve the success of its cyber service projects by using knowledge and techniques that result in a desired business outcome.

itSM Solutions – CSM Training & Mentoring Program

Listed below is a five-phase approach to acquiring the best practice trainings and skills to operationalize an enterprise CSM program.

Phase 1 – Executive Team Training

Organization Role	Objective	Training Programs
CEO, CFO, CIO, CISO CRO, CCO, PMO Director, SMO Director, Governance Director	To help the executive team understand the benefits associated with operationalizing a CSM program	CSM Executive Overview CSM Executive Simulations Digital Readiness Training

itSM's CSM executive training and simulation services are designed to help the executive team to:

- **Understand** the benefits of adopting an CSM program
- **Understand** the value of Digital Readiness
- **Secure** funding for the CSM program
- **Select** a leadership team to drive the CSM program

Cyber Service Management

Operationalizing Cyber Service Management Across an Enterprise and its Supply Chain

Phase 2 – Program Leadership Team Training

Organization Role	Objective	Training Programs
Practice Owners, Service Owners, Change Mgrs. Operation Mgrs. CSI Mgrs. Business Analysts	To help the leadership team acquire the knowledge and skills to develop an actionable CSM plan	CSM Assessment Training NCSF Assessment Training Digital Readiness Training Planning to Change Workshop Internet of Things Training ITIL® Training RESILIA Training Prince 2 Training NIST Cybersecurity Training CSM Simulations

itSM's CSM leadership training and simulation services are designed to help the leadership team acquire a systemic structure for thinking and planning and the skills to:

- **Become** thought leaders for the CSM program
- **Understand** the value of Digital Readiness
- **Perform the Assessment** to identify and document CSM GAPS
- **Organize and Condition** the enterprise for CSM

Phase 3 – Enterprise Readiness Training

Organization Role	Objective	Training Program
All IT staff, senior leadership, stakeholders and supply chain partners	To help condition the enterprise for CSM change through a series of online awareness and simulation trainings	CSM Awareness CSM Simulations Digital Readiness Training

Cyber Service Management

Operationalizing Cyber Service Management Across an Enterprise and its Supply Chain

itSM's CSM enterprise training and simulation services enable the enterprise business stakeholders and supply chain partners to:

- **Understand** the CSM program and its value to the organization in terms of improving the quality, risk and security of an enterprise digital service portfolio
- **Understand** the value of Digital Readiness

Phase 4A – Practitioner Training

Organization Role	Objective	Training Programs
1st Line Mgrs. Practice & Service Owners Architects & Strategists Operation & System, Analysts Business & Quality Analysts Program & Project Managers Operation & Change Mgrs. Service Level & CSI Mgrs. Tool Administrators	To provide the CSM practitioners the knowledge and skills to plan, design, implement, operate and improve a CSM program.	CSM Training NIST Cybersecurity Framework Training NIST Cybersecurity Employee Training NICE Cybersecurity Workforce Trainings Internet of Things Training ITIL Trainings RESILIA Trainings Prince 2 Trainings ISO 27001 Training Cobit Training CSM Simulation Trainings

itSM's CSM information technology training and simulation services will enable the IT organization to acquire the knowledge and skills to:

- **Plan, Design, Implement, Operate and Improve** a CSM program

Phase 4B – Supply Chain Training

Organization Role	Objective	Training Programs
Business Stakeholders Supply Chain Partners	To provide basic cyber awareness training to all business stakeholders and supply chain partners	CSM Simulation Training NIST Cybersecurity Employee Training Digital Readiness Training

Cyber Service Management

Operationalizing Cyber Service Management Across an Enterprise and its Supply Chain

itSM's CSM enterprise training and simulation services enable the enterprise business stakeholders and supply chain partners to:

- **Learn** the techniques cyber criminals are using to break into networks
- **Understand** the results of poor cyber practices
- **Understand** the value of Digital Readiness

Phase 5 – Career Pathway Training

Organization Role	Objective	Activities
HR Manager	To establish HR policies and procedures for training new employees and a career pathway for existing employees practicing CSM	Setup both eLearning and role-based Blended Learning CSM best practice training solutions for new and existing employees

itSM's HR CSM trainings help HR departments to:

- **Establish** policies and procedures for training new employees
- **Identify** career pathways for existing CSM practitioners.

Summary

Three things are certain: first, cyber services are now at the center of most businesses; second, business is a moving target, third organizations are under attack from those trying to steal the information companies rely on for daily business operations.

The itSM Solutions **Cyber Service Management (CSM)** assessment, remediation, certification and skills training programs enable organizations to learn the knowledge, skills and capabilities to build a proactive, collaborative and balanced approach for managing and protecting its cyber services portfolio.

Cyber Service Management

Operationalizing Cyber Service Management Across an Enterprise and its Supply Chain

About itSM Solutions LLC

Founded in 2002, itSM Solutions LLC is the creator of the Digital Service & Security Management (DSSM) model. DSSM is a proactive, collaborative and balanced approach for adopting and adapting the best practices necessary to manage & improve the cost, quality, compliance, security, risk and business continuity of an enterprise digital service portfolio. DSSM suite of training, mentoring and certification solutions enables organizations to adopt and adapt a systemic structure for thinking when planning and designing digital services plus the skills to operate as a service provider integrated into the business value chain.

About the Authors

David Nichols is the President and CEO of itSM Solutions LLC, an ITSM consulting and training company. He has over 25 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 Service Manager certification.

Rick Lemieux is a managing partner and the Vice President of Business Development. He is responsible for overseeing the company's Sales, Marketing & Business Development programs. Rick has been involved in selling IT solutions for the past 33 years. Prior to itSM, Rick, an early proponent of ITSM and ITIL, led the Sales and Business Development teams at software companies focused on automating the best practices guidance outlined in ITIL. 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.