



# NISTCSF.COM

NIST Cybersecurity Framework Solutions

## **A Controls Factory Approach To Design, Build, Test and Manage a Cyber Security Program Based on the NIST Cybersecurity Framework (NCSF)**

### **Prepared by:**

Larry Wilson

[lwilson@umassp.edu](mailto:lwilson@umassp.edu)

Chief Information Security Officer

University of Massachusetts – President's Office

Rick Lemieux

[rick.lemieux@itsmsolutions.com](mailto:rick.lemieux@itsmsolutions.com)

Managing Partner

itSM Solutions LLC

## The Digital Innovation Economy

Three things are certain in today's business world: first, digital 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 and securing enterprise digital assets and services across stakeholders, supply chains, functions, markets, and geographies has never been greater.

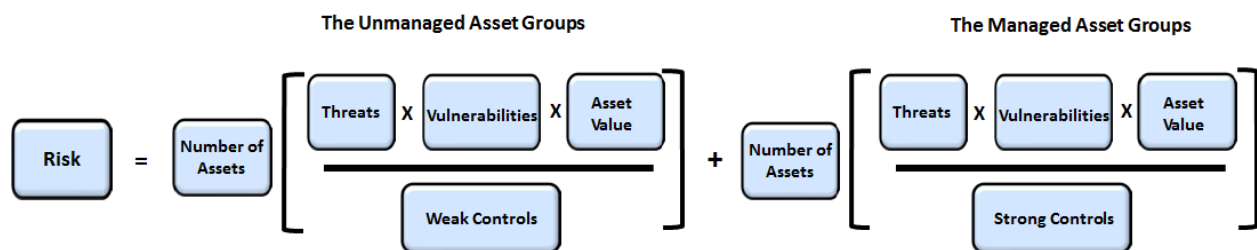
In order to achieve the potential benefits of the innovation economy, an enterprise must ensure that it can build and maintain a reliable, resilient, secure and trusted digital infrastructure.

In order to do this an organization must be able to identify its assets so it can understand its attack surface and the threats and vulnerabilities associated with that attack surface. With the growth of the Internet of Things (mobile devices, security cameras, video recorders, electrical boxes etc.) the attack surface along with its threats and vulnerabilities is constantly changing. To deal with this, organizations must build and maintain a continual service improvement program that delivers the right set of security controls to mitigate the latest cyber threats, remediate the critical vulnerabilities and protect the high value assets.

## The Cyber Security Problem

Cybersecurity is all about managing risk. But, before you can manage risk, you need to understand risk. The main idea is that if organizations have a solid understanding of the risk components, including the threats, the vulnerabilities, the assets (and their relative value), and the controls, they will be in a better position to safeguard their most valuable information resources. An effective cybersecurity program involves a thorough understanding, assessment, and handling of these key risk components. The equation for risk is shown below, which identifies the key components of risk.

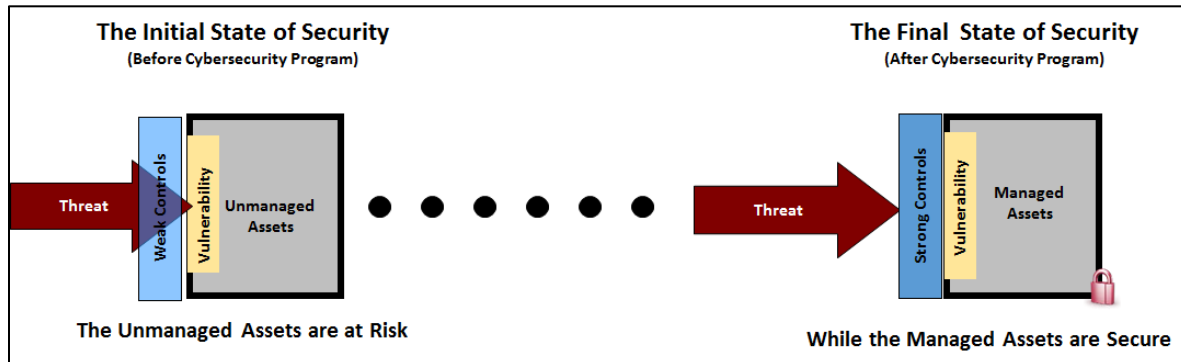
### The Risk Equation



So, how do we calculate risk?

1. Risk is based on the likelihood and impact of a cybersecurity incident or data breach ... which is based on the percentage of unmanaged assets v. managed assets
2. Threats involve the potential attack against IT resources and information assets
3. Vulnerabilities are weaknesses of IT resources and information that could be exploited by a threat
4. Asset Value is based on criticality of IT resources and information assets
5. Controls are safeguards that protect IT resources and information assets against threats and/or vulnerabilities (see note)

Managed assets are characterized by strong controls, while unmanaged assets have weak, missing or ineffective controls. All cybersecurity programs focus on protecting the organization’s high value assets. Early stage programs typically have a higher percentage of unmanaged assets, which are those with weak security controls. As programs mature, the percentage of managed assets increase and the percentage of unmanaged assets decrease. This means that the controls are stronger and the program is more effective.



### The Cyber Security Solution - The NIST Cybersecurity Framework

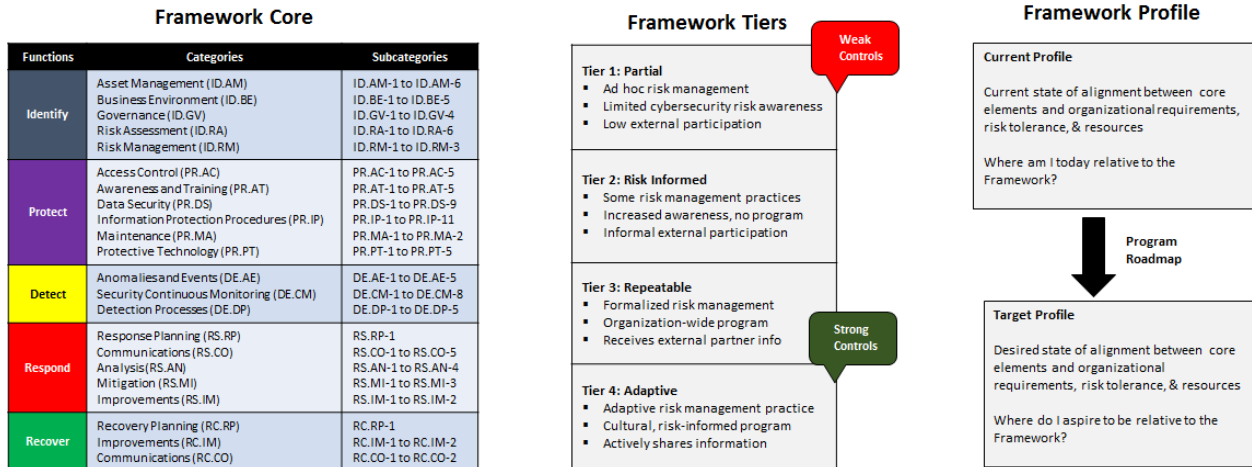
In February 2013, President Obama issued Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” which called on the Department of Commerce’s National Institute of Standards and Technology (NIST) to develop a voluntary risk-based Cybersecurity Framework for the nation’s critical infrastructure—that is, a set of industry standards and best practices to help organizations identify, assess, and manage cybersecurity risks. NIST issued the resulting Framework in February 2014.

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts; the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities:

The **Framework Core** is a set of cybersecurity activities, desired outcomes, and references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level.

The **Framework Implementation Tiers** provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive).

A **Framework Profile** represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile is characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile (the “as is” state) with a “Target” Profile (the “to be” state).



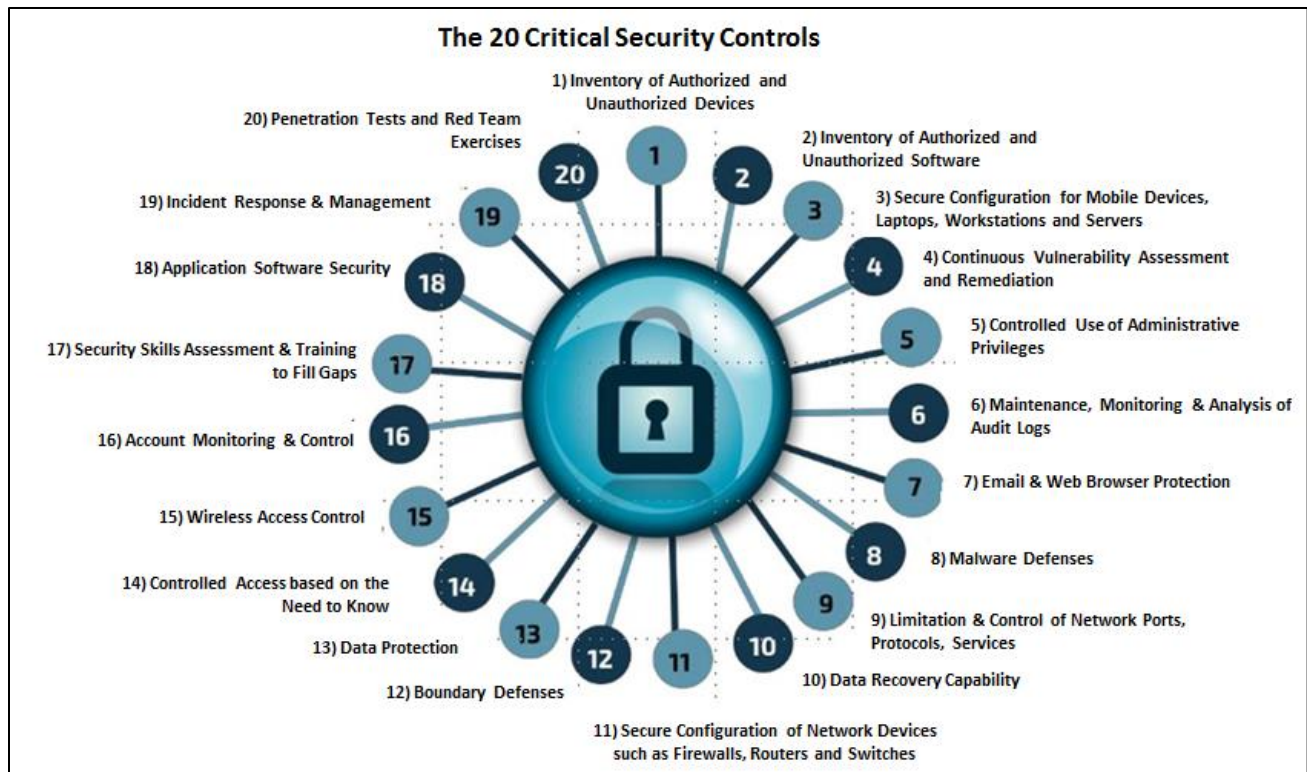
The Framework provides organizations with a **risk-based compilation of guidelines** that can help them identify, implement, and improve cybersecurity practices. The Framework does not introduce new standards or concepts; rather, it leverages and integrates cybersecurity practices that have been developed by organizations like NIST and the International Standardization Organization (ISO).

This means, that organizations must look to other security standards and best practices for the detailed controls. This program focuses on the 20 Critical Security Controls for the technical program and the ISO 27002 security controls for the business program.

**The Technical Controls: 20 Critical Security Controls:**

The CIS Critical Security Controls (CIS Controls) are a concise, prioritized set of cyber practices created to stop today’s most pervasive and dangerous cyber-attacks. The CIS Controls are developed, refined, and validated by a community of leading experts from around the world. **Organizations that apply just the first five CIS Controls can reduce their risk of cyberattack by around 85 percent. Implementing all 20 CIS Controls increases the risk reduction to around 94 percent.**

The CIS Critical Security Controls provide specific and actionable ways to stop today’s most pervasive and dangerous attacks. The Controls prioritize and focus a smaller number of actions with high pay-off results. The Controls are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners.



In addition to being grounded in current attack data, the Controls align with numerous other frameworks, such as PCI-DSS, ISO 27001, US CERT recommendations, NIST SP 800-53, and the NIST Framework. The Controls don't try to replace these other frameworks, but they are frequently used by enterprises to make sense of other frameworks. The Controls are a highly practical approach to prioritize the overarching security strategy for an enterprise. Once a program for cyber security is in place and operational, the Controls can also be used with the Critical Security Controls Measurement Companion to assess the effectiveness of the organization's security efforts.

## 20 Critical Controls Mapping to the NIST Cybersecurity Framework:

CIS Critical Security Controls (V 6.0)	Asset Family	Tier	NIST Cybersecurity Framework (CSF) Core Functions				
			IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
CSC-01: Inventory of Authorized and Unauthorized Devices	Systems		ID.AM	PR.DS			
CSC-02: Inventory of Authorized and Unauthorized Software	Systems		ID.AM	PR.DS			
CSC-03: Secure Configuration of Endpoints, Servers, etc.	Systems			PR.IP			
CSC-04: Continuous Vulnerability Assessment & Remediation	Systems		ID.RA	PR.IP	DE.CM	RS.MI	
CSC-05: Controlled Use of Administrative Privileges	Systems			PR.AC PR.AT PR.MA			
CSC-06: Maintenance, Monitoring and analysis of Audit Logs	Systems			PT.PT	DE.AE DE.DP	RS.AN	
CSC-07: Email and Web Browser Protections	Systems			PR.PT			
CSC-08: Malware Defenses	Systems			PR.PT	DE.CM		
CSC-09: Limitation and Control of Ports, Protocols, Services	Systems			PR.IP			
CSC-10: Data Recovery Capability	Systems						RC.RP
CSC-11: Secure Configuration of Network Devices	Networks			PR.IP PR.PT	DE.AE		
CSC-12: Boundary Defense	Networks			PR.AC PR.MA	DE.AE		
CSC-13: Data Protection	Applications			PR.AC PR.DS PR.PT			
CSC-14: Controlled Access Based on Need to Know	Networks			PR.AC PR.DS PR.PT			
CSC-15: Wireless Access Control	Networks			PR.AC			
CSC-16: Account Monitoring and Control	Applications			PR.AC	DE.CM		
CSC-17: Security Skills Assessment and Appropriate Training	Applications			PR.AT			
CSC-18: Application Software Security	Applications			PR.PT			
CSC-19: Incident Response and Management	Applications				DE.AE	RS.RP	RC.CO
CSC-20: Penetration Tests and Red Team Exercises	Applications		ID.RA			RS.IM	RC.IM

### The Business Controls: ISO 27002 Code of Practice

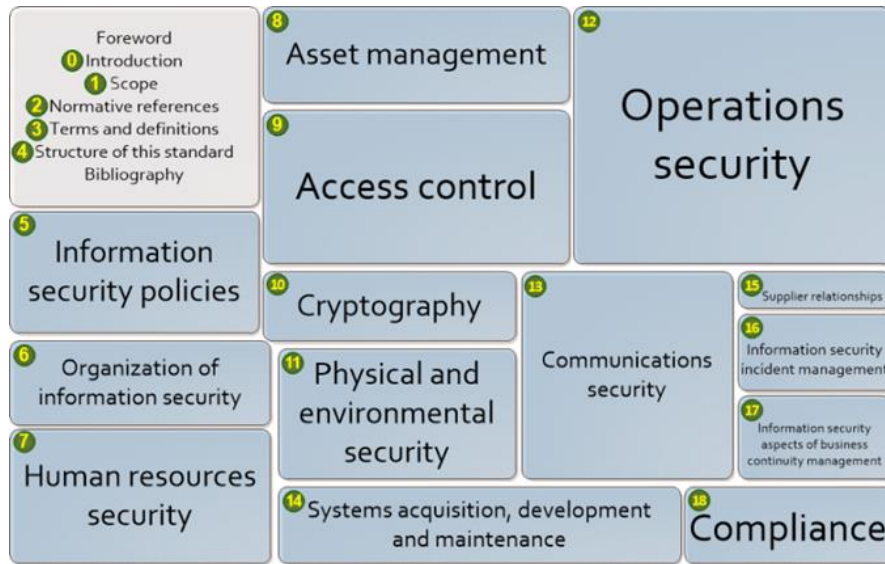
Organizational assets are subject to both deliberate and accidental threats while the related processes, systems, networks and people have inherent vulnerabilities. Changes to business processes and systems or other external changes (such as new laws and regulations) may create new information security risks. Therefore, given the multitude of ways in which threats could take advantage of vulnerabilities to harm the organization, information security risks are always present.

Effective information security reduces these risks by protecting the organization against threats and vulnerabilities, and then reduces impacts to its assets. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met.

ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). It is designed to be used by organizations that intend to select controls within the process of implementing an Information Security

Management System (ISMS); implement commonly accepted information security controls; develop their own information security management guidelines.

### ISO 27002: 2013 Code of Practice for Information Security Management



### ISO 27002 Controls Mapping to the NIST Cybersecurity Framework:

ISO 27002: Code of Practice for Information Security Controls	Tier	NIST Cybersecurity Framework (CSF) Core				
		IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
ISO-05: Information Security Policies		ID.GV				
ISO-06: Organization of Information Security		ID.AM ID.GV ID.RA	PR.AC PR.AT PR.DS	DE.DP	RS.CO	
ISO-07: Human Resource Security		ID.GV	PR.AT PR.DS PR.IP			
ISO-08: Asset Management		ID.AM	PR.DS PR.IP PR.PT			
ISO-09: Access Control			PR.AC PR.DS PR.PT			
ISO-10: Cryptography						
ISO-11: Physical and Environmental Security		ID.AM ID.BE	PR.AC PR.DS PR.IP			
ISO-12: Operations Security		ID.RA	PR.DS PR.IP PR.PT	DE.CM	RS.AN RS.MI	
ISO-13: Communications Security		ID.AM	PR.AC PR.DS PR.PT			
ISO-14: System Acquisition, Development and Maintenance			PR.DS PR.IP	DE.CM DE.DP		
ISO-15: Supplier Relationships		ID.BE	PR.MA	DE.CM		
ISO-16: Information Security Incident Management			PR.IP	DE.AE DE.DP	RS.RP RS.CO RS.AN	RC.RP
ISO-17: Information Security Aspects of Business Continuity Management		ID.BE	PR.IP			
ISO-18: Compliance		ID.GV ID.RA	PR.IP	DE.DP		



## The Risk Management Controls: The Baldrige Excellence Builder

The *Baldrige Cybersecurity Excellence Builder* is a voluntary self-assessment tool that enables organizations to better understand the effectiveness of their cybersecurity risk management efforts. It helps leaders of organizations identify opportunities for improvement based on their cybersecurity needs and objectives, as well as their larger organizational needs, objectives, and outcomes.

Using this self-assessment, organizations can

- determine cybersecurity-related activities important to your business strategy and critical service delivery;
- prioritize your investments in managing cybersecurity risk;
- determine how best to enable your workforce, customers, suppliers, partners, and collaborators to be risk conscious and security aware, and to fulfill their cybersecurity roles and responsibilities;
- assess the effectiveness and efficiency of your use of cybersecurity standards, guidelines, and practices;
- assess the cybersecurity results you achieve; and
- identify priorities for improvement.

Like the [Framework for Improving Critical Infrastructure Cybersecurity](#) (*Cybersecurity Framework*) and the [Baldrige Excellence Framework](#), the *Baldrige Cybersecurity Excellence Builder* is not a one-size-fits-all approach. It is adaptable and scalable to your organization's needs, goals, capabilities, and environment. It does not prescribe how you should structure your organization's cybersecurity policies and operations. Through interrelated sets of open-ended questions, it encourages you to use the approaches that best fit your organization.

The *Baldrige Cybersecurity Excellence Builder* is intended for use by the leaders and managers in your organization who are concerned with and responsible for mission-driven, cybersecurity-related policy and operations. These leaders and managers may include senior leaders, chief security officers, and chief information officers, among others.

Key areas of focus include:

1. Senior and Cybersecurity Leadership: How do your senior leaders lead cybersecurity policies and operations?
2. Governance and Societal Responsibilities: How do you govern cybersecurity policies and operations and fulfill your organization's societal responsibilities?
3. Strategy Development: How do you develop your cybersecurity strategy?
4. Strategy Implementation: How do you implement your cybersecurity strategy?
5. Voice of the Customer: How do you obtain information from your customers?
6. Customer Engagement: How do you engage customers by serving their needs and building relationships?
7. Measurement, Analysis, and Improvement of Performance: How do you measure, analyze, and then improve cybersecurity-related performance?
8. Knowledge Management: How do you manage your organization's cybersecurity related knowledge assets?
9. Workforce Environment: How do you build an effective and supportive workforce environment to achieve your cybersecurity goals?
10. Workforce Engagement: How do you engage your workforce to achieve a high performance work environment in support of cybersecurity policies and operations?
11. Work Processes: How do you design, manage, and improve your key cybersecurity work processes?
12. Operational Effectiveness: How do you ensure effective management of your cybersecurity operations?
13. Process Results: What are your cybersecurity performance and process effectiveness results?
14. Customer Results: What are your customer-focused cybersecurity performance results?
15. Workforce Results: What are your workforce-focused cybersecurity performance results?
16. Leadership and Governance Results: What are your cybersecurity leadership and governance results?
17. Financial Results: What are your financial performance results for your cybersecurity operations?



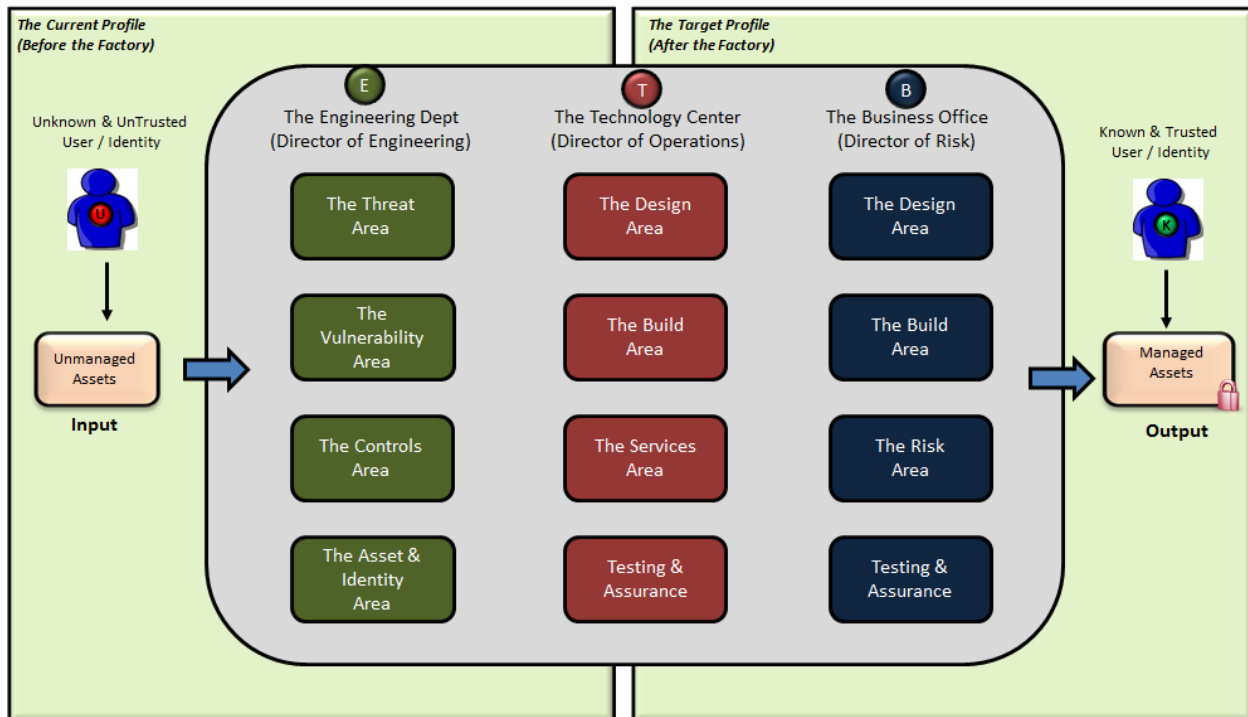
## The NIST Cybersecurity Controls Factory Model

### Operationalizing the NIST Cybersecurity Framework Across and Enterprise and its Supply Chain

The controls factory concept is used to help organize the engineering, technical and business functions of a NIST cyber security program. The program is completely adaptable which means that each of the modules can easily be updated, replaced or modified with minimal impact on the overall solution. Organizations are free to choose the minimum set of controls its need to improve its framework profile and then over time incrementally adopt other controls that will take it to its identified target state. The factory approach allows for changes in the cybersecurity threat landscape, new vulnerabilities and the addition of incremental improvements while still keeping a focus on the critical assets and identities.

The Engineering Department organizes all of the engineering functions / capabilities such as threats, vulnerabilities, assets and controls. The Technology Center organizes the key technical capabilities such as technology / solution design (design guides), technology build (build guides), managed security solutions (from MSSPs), and testing / assurance functions. The Business Office organizes business functions focused on people and policy including design (based on ISO 27002), build (sample policies, communications plan, and gap analysis templates), cybersecurity advisory services and employee roles, business testing and assurance based on ISO 27002. It includes a capability for executives to evaluate Risk Management practices based on the Baldrige Cybersecurity Executive Builder.

**The Controls Factory (Our Model)**



The NIST CSF controls factory approach is modular. This means if there are changes within a particular functional area, it can be updated without impacting other related functions. For example, if an organization wishes to implement NIST 800-171 controls as the foundation for business controls, the Business Office Design Area would replace ISO 27002 code of practice with NIST 800-171 security controls. All of the other business functions would be modified to align with NIST 800-171. The Engineering Department would adjust all capabilities that were based on ISO 27002 with similar capabilities based on NIST 800-171. The Technology Center capabilities would not

change, because they are based on the Critical Security Controls. This approach provides maximum flexibility for organizations who choose to build their programs based on the control factory model.

### **NIST/NICE Cybersecurity Workforce Framework (NCWF) Training Program**

The NCWF program is built around a three tier training model.

The first tier will be focused on teaching the knowledge and skills to build a NCSF program using Larry's control factory methodology. The program will consist of a Foundation training and certification program for cybersecurity and IT professionals who play a passive but need to know role in the program and a Practitioner training and certification program for those who are responsible for designing, building and managing the program. ITSM is planning to add four class lecture based & lab workshops that will provide practitioners with the hands-on skills they need to become productive cybersecurity employee's upon graduation.

Beyond NCSF certification, the program will also offer the trainings required to sit for the professional INFOSEC examinations associated with the Specialty Areas and Work Roles outlined in the NCWF. These training include CISSP, CISA, CISA Security+, Vulnerability Assessment Manager, Risk Manager, Certified Ethical Hacker and 20 more specialty cybersecurity certifications.

Finally, the program will offer employers an online solution to train its employees in good cyber behavior. The employee awareness program will include modules covering topics in phishing, social engineering, online safety, social media, BYOD (Bring Your Own Device), removable media, password safety, personal information, information handling and remote and mobile working. Student assessment testing and reporting tools are available with this program.

The program has already been implemented at college campuses across Massachusetts and has won the following industry awards:

- **SANS** Person who made a difference in Cybersecurity, 2013
- **ISE (Information Security Executives)** Finalist for Executive of the Year for North America, 2013
- **ISE** Information Security Program of the Year for Higher Education & Government Category, 2013
- **Security Magazine** most influential cyber security professionals in North America, 2016

#### **NCWF Training Programs**

Our phase 1 go to market programs will include the following NCWF programs:

##### **NCSF Foundation Certification Training**

The NIST CSF Foundations Course outlines current security challenges and explains how organizations who implement a NIST Cybersecurity Program can mitigate these risks

This program prepares students to function successfully in NICE workforce framework entry, level cybersecurity work role positions.

**Location of Training:** Onsite or Online

**Means of Instruction:** Instructor Led Classroom or Virtual Classroom, Self Paced Video

**Number of Hours: 8 (1 Day)**

**Credentials or Certificate Attained:** Certificate of Completion, PDU's, CEU's, College Credits

**Course Description & Outline:** Can be found [here](#)

##### **NCSF Practitioner Certification Training**

The NIST CSF Practitioners Course explains in detail current security challenges, and how organizations design, build, maintain and test a comprehensive Cybersecurity Program and Risk Management Program based on the NIST Cybersecurity Framework. The NIST CSF Practitioners Course includes detailed capabilities organizations can use to build a comprehensive program.

This program prepares students to function successfully in NICE workforce framework entry, mid and advanced level cybersecurity work role positions, but also prepares students with the knowledge and skills to move on to the specialty roles (ethical hacker, vulnerability assessment manager etc.) also outlined in the NCWF.

**Location of Training:** Onsite or Online

**Means of Instruction:** Instructor Led Classroom or Virtual Classroom, Self Paced Video

**Number of Hours:** 24 (3 days)

**Credentials or Certificate Attained:** Certificate of Completion, PDU's, CEU's, College Credits

**Course Description & Outline:** Can be found [here](#)

#### **NCWF Work Role or Specialty Certification Library**

itSM's careeracademy.com certification training portal enables students be trained to sit for up to 25 NCWF work and specialty area professional certifications in Cybersecurity from CompTIA, ISACA, ISC<sup>2</sup>, Mile2 and others.

**Location of Training:** Online

**Means of Instruction:** Self Paced Video

**Number of Hours:** Varies based on Program Selected

**Credentials or Certificate Attained:** Certificate of Completion, PDU's, CEU, College Credits

**Course Description & Outline:** Can be found [here](#)

#### **NCWF Employee Cybersecurity Awareness Training**

itSM's employee online cybersecurity awareness training program includes modules covering topics in phishing, social engineering, online safety, social media, BYOD (Bring Your Own Device), removable media, password safety, personal information, information handling and remote and mobile working. Student assessment testing and reporting tools are available with this program.

**Location of Training:** Online

**Means of Instruction:** Games, Animations and Simulations

**Number of Hours:** Varies based on Program Selected

**Credentials or Certificate Attained:** Certificate of Completion

**Course Description & Outline:** Can be found [here](#)

Phase 2 of the program will include deliver of the following workshop and lab programs:

#### **NCSF Engineering "Lecture-based" Cybersecurity Workshop and Lab**

This workshop will include the design requirements and build specifications based on the 22 Framework Categories and 5 Core Functions of the NIST Cybersecurity Framework. The "Lecture-based" Workshop will be supplemented with a "Hands-on" workshop in partnership with vendors providing solutions for the operationalizing of the NIST CSF across an enterprise and its supply chain.

**Location of Training:** Onsite or Online

**Means of Instruction:** Instructor Led Classroom or Virtual Classroom, Self Paced Video

**Number of Hours:** To Be Determined

**Credentials or Certificate Attained:** Certificate of Completion, PDU's CEU's, College Credits

**Course Description & Outline:** Coming Soon

#### **NCSF Technology "Lecture-based" Cybersecurity Workshop and Lab**

This workshop will include the design requirements and build specifications based on the 20 Critical Security Controls. The "Lecture-based" Workshop will be supplemented with a "Hands-on" lab in partnership with vendors providing solutions for the management and monitoring of the 20 critical controls.

**Location of Training:** Onsite or Online

**Means of Instruction:** Instructor Led Classroom or Virtual Classroom, Self Paced Video

**Number of Hours:** To Be Determined

**Credentials or Certificate Attained:** Certificate of Completion, PDU's CEU's, College Credits

**Course Description & Outline:** Coming Soon

### **NCSF Business “Lecture-based” Cybersecurity Workshop and Lab**

This workshop will be based on the ISO 27002 or NIST 800-171 standards. This workshop includes the design requirements and build specifications based on either ISO 27002 or NIST 800-171. The lecture based workshop will be supplemented by a hands on lab developed for this lecture – since this program is more about business controls and not technical controls the hands-on component is more or less practice exercises and case studies.

**Location of Training:** Onsite or Online

**Means of Instruction:** Instructor Led Classroom or Virtual Classroom, Self Paced Video

**Number of Hours:** To Be Determined

**Credentials or Certificate Attained:** Certificate of Completion, PDU’s CEU’s, College Credits

**Course Description & Outline:** Coming Soon

### **NCSF Risk “Lecture-based” Cyber Risk Workshop and Lab**

This workshop will be based on the Baldrige Excellence Framework and the FAIR Institute Cyber Risk methodology. This program will also include lab exercises.

**Location of Training:** Onsite or Online

**Means of Instruction:** Instructor Led Classroom or Virtual Classroom, Self Paced Video

**Number of Hours:** To Be Determined

**Credentials or Certificate Attained:** Certificate of Completion, PDU’s CEU’s, College Credits

**Course Description & Outline:** Coming Soon

## **NCSF Professional Service Programs**

### **NISTCSF.COM Testing & Monitoring Solutions**

This service provides enterprises with the option to perform its own assessment of its technology, business and risk controls or outsource that responsibility to a NISTCSF licensed partners.

The NISTCSF.COM assessment capabilities are modular. This means that clients can pick and choose the technology, business and risk controls that best meets the needs of the business. For example, if an organization wishes to implement NIST 800-171 controls as the foundation for business controls, the Business Office Design Area would replace ISO 27002 with NIST 800-171 security controls.

This approach provides maximum flexibility for organizations who choose to build their programs based on the NISTCSF.COM model.

### **NISTCSF.COM Testing & Monitoring Solutions**

This service provides enterprises with the option to learn the knowledge and skills to build their own testing and continuous monitoring program or outsource that responsibility to a NISTCSF.COM licensed partners.

The NISTCSF.COM program is managed 24/7 by industry experts working around the clock to monitor, report and resolve security incidents that offer a threat to an organizations operational viability.

## About the Authors



**Larry Wilson** is the Chief Information Security Officer (CISO) in the UMASS President's office and is responsible for developing, implementing and managing the University of Massachusetts Information Security Policy and Written Information Security Program (WISP). The University program is based on a "Controls Factory" approach Larry created to help organizations operationalize the NIST Cyber Security Framework and its industry best practices (ISO 27001, SANS 20 Critical Controls etc.) across an enterprise and its supply chain. Larry's approach has been implemented consistently across all five campuses plus six other universities in the Commonwealth of Massachusetts.

Prior to joining, Larry was the Vice President, Network Security Manager at State Street Bank. Larry's industry experience includes IT audit manager for Deloitte Enterprise Risk Services (ERS) consulting practice. In this role he managed a staff responsible for developing and completing a Sarbanes Oxley compliance audit for MasterCard International.

Larry holds a Master of Science degree in Civil / Structural Engineering from the University of New Hampshire. His industry certifications include CISSP, CISA and ISA (PCI Internal Security Assessor). He serves on the Advisory Board for Middlesex Community College and CISO Advisory Board for Oracle. He co-chairs the Massachusetts State University and Community College Information Security Council, and serves as Certification Director for ISACA New England. Larry has been teaching CISA certification training for ISACA for 5 years

His major accomplishments include Finalist for Information Security Executive® (ISE®) of the Year for both the Northeast Region and North America; the SANS People who made a difference in Cybersecurity award in 2013 and one of the top two most influential people in cyber security as selected by Security Magazine in 2016.



**Rick Lemieux** is a co-founder of NISTCSF.com and its Chief Revenue Officer. He is responsible for overseeing the company's Sales, Marketing & Business Development programs. Rick has been involved in developing and marketing IT and Cyber Security workforce development solutions for the past 15 years. Rick's has been a driving force behind many companies including itSM Solutions LLC, itSM Mentor, Careeracademy.com and Agile Sales & Marketing. Rick is certified IT professional and was recently identified as one of the top 5 IT Entrepreneurs in the State of Rhode Island by the TECH 10 awards for his work in developing innovative, online workforce development solutions for Information Technology, Cybersecurity and Business professionals.