Designing, Building and Managing a Cyber Security Program Based on the NIST Cybersecurity Framework (NIST CSF)

A Business Case

Prepared by:

Larry Wilson
lwilson@umassp.edu
Chief Information Security Officer
University of Massachusetts – President's Office

Rick Lemieux
rick.lemieux@itsmsolutions.com
Managing Partner
itSM Solutions LLC

Background and Introduction

The following business case outlines the cost to design, implement and manage a cyber security program based on the NIST Cyber Security Framework The business case is based on a program designed and implemented by the University of Massachusetts and six surrounding universities.

The first section introduces the digital innovation economy and why enterprises need to build and maintain a reliable, resilient, secure and trusted service delivery infrastructure in order to protect the information it relies on for daily business operations and revenue growth.

The second section introduces the cyber security problem in the context of risk management and the management of risk components which include assets (and their relative value) threats, vulnerabilities and the controls that need to be in place to safeguard an organizations most valuable information resources.

The third section introduces the cost associated with designing, building and maintaining a NIST cyber security program using the UMASS Controls Factory program. Areas covered include:

1. **The cost to educate** an enterprise on the UMASS approach to operationalizing the NIST CSF across an enterprise and its supply chain.
2. **The cost to assess the risks** so the enterprise can identify and prioritize the threats and vulnerabilities the organization needs to deal with.
3. **The cost to implement, test, manage and improve** the cyber security program. The costs will include the fees for enterprises to do it themselves and the cost to outsource the program to UMASS or one of its licensed partners.

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.

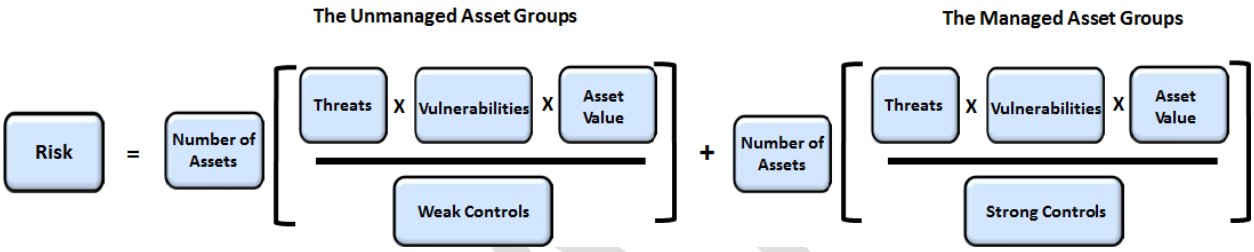
In order to achieve the potential benefits of the innovation economy, an enterprise must ensure that it can build and maintain a reliable, resilient, secure and trusted digital infrastructure.

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.

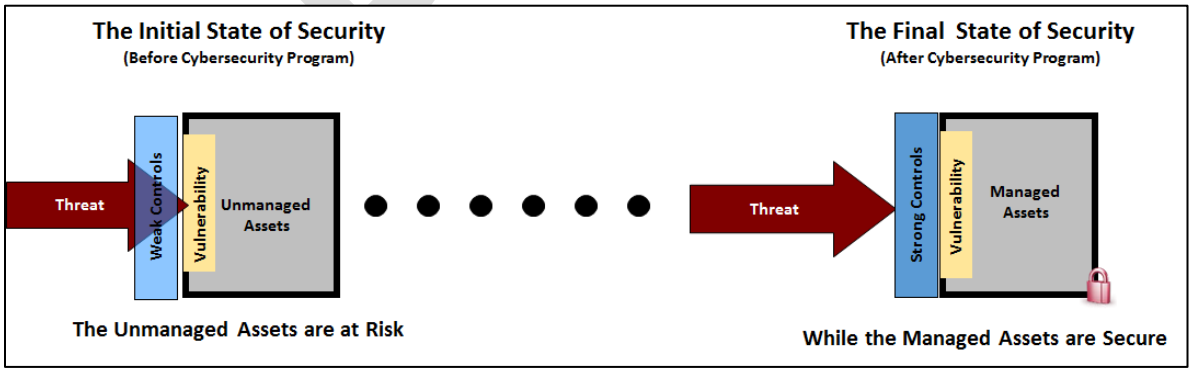
The Risk Equation



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.

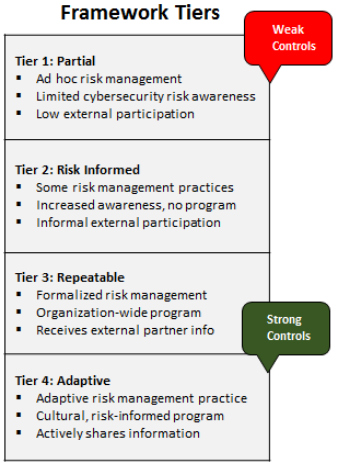
The **Framework Implementation Tiers** provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g.,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

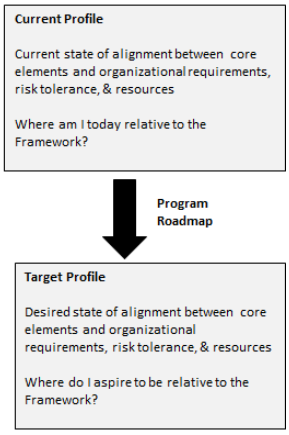
Framework Core

Functions	Categories	Subcategories
Identify	Asset Management (ID.AM) Business Environment (ID.BE) Governance (ID.GV) Risk Assessment (ID.RA) Risk Management (ID.RM)	ID.AM-1 to ID.AM-6 ID.BE-1 to ID.BE-5 ID.GV-1 to ID.GV-4 ID.RA-1 to ID.RA-6 ID.RM-1 to ID.RM-3
Protect	Access Control (PR.AC) Awareness and Training (PR.AT) Data Security (PR.DS) Information Protection Procedures (PR.IP) Maintenance (PR.MA) Protective Technology (PR.PT)	PR.AC-1 to PR.AC-5 PR.AT-1 to PR.AT-5 PR.DS-1 to PR.DS-9 PR.IP-1 to PR.IP-11 PR.MA-1 to PR.MA-2 PR.PT-1 to PR.PT-5
Detect	Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP)	DE.AE-1 to DE.AE-5 DE.CM-1 to DE.CM-8 DE.DP-1 to DE.DP-5
Respond	Response Planning (RS.RP) Communications (RS.CO) Analysis (RS.AN) Mitigation (RS.MI) Improvements (RS.IM)	RS.RP-1 RS.CO-1 to RS.CO-5 RS.AN-1 to RS.AN-4 RS.MI-1 to RS.MI-3 RS.IM-1 to RS.IM-2
Recover	Recovery Planning (RC.RP) Improvements (RC.IM) Communications (RC.CO)	RC.RP-1 RC.IM-1 to RC.IM-2 RC.CO-1 to RC.CO-2

Framework Tiers



Framework Profile

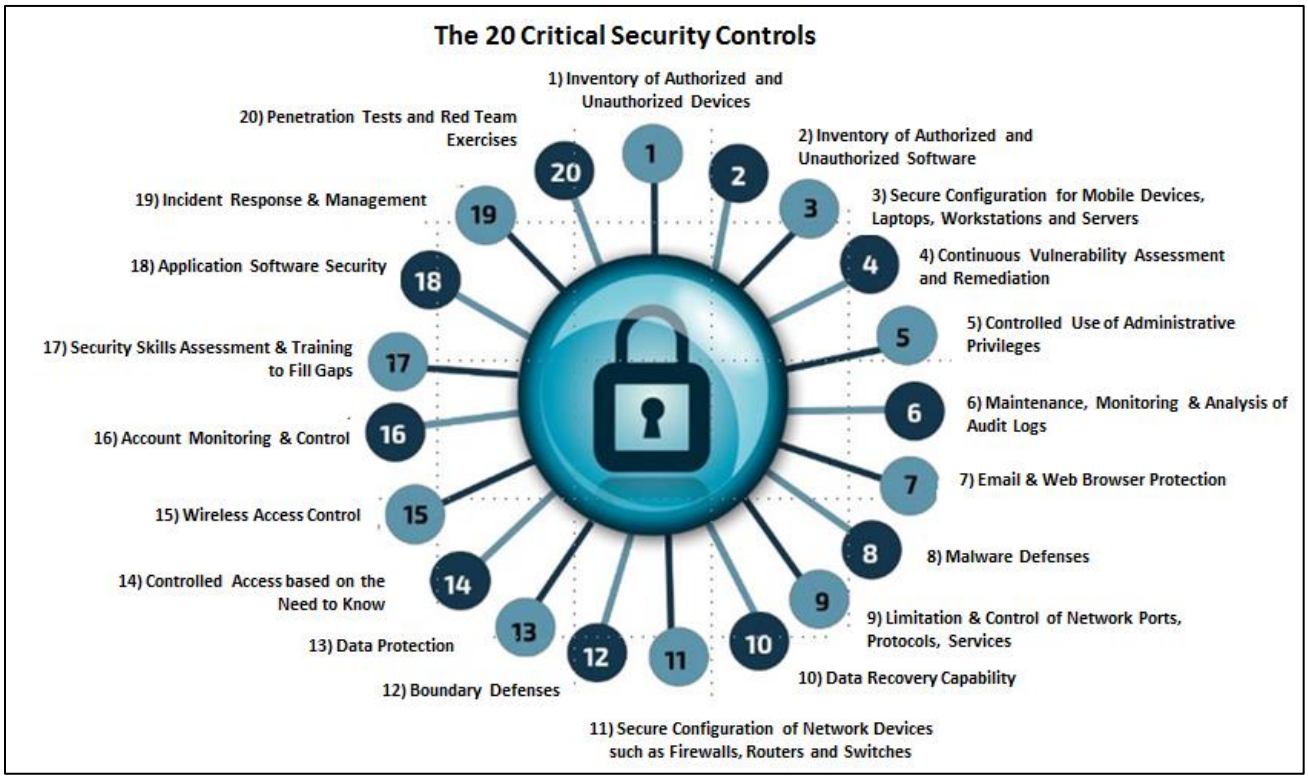


The Framework provides organizations with **a risk-based compilation of guidelines** that can help them identify, implement, and improve cybersecurity practices. The Framework does not introduce new standards or concepts; rather, it leverages and integrates cybersecurity practices that have been developed 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 course 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:

			NIST Cybersecurity Framework (CSF) Core Functions				
CIS Critical Security Controls (V 6.0)	Asset Family	Tier	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

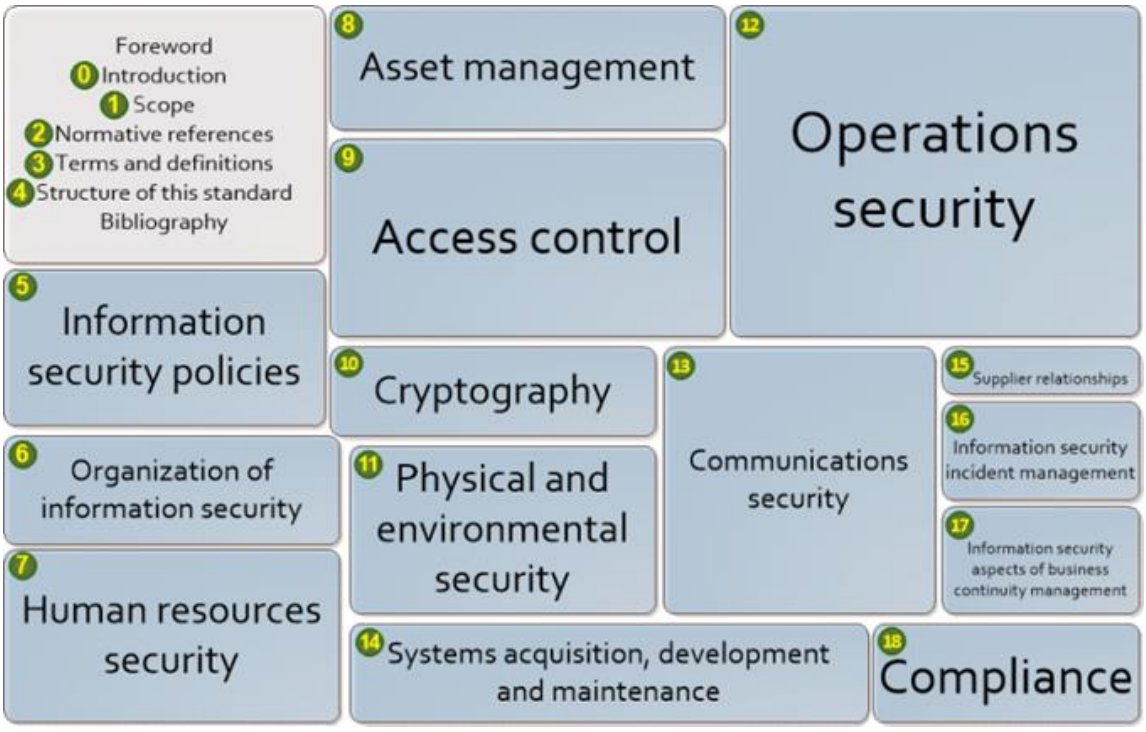
The Business Controls: ISO 27002 Code of Practice

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:

		NIST Cybersecurity Framework (CSF) Core				
ISO 27002: Code of Practice for Information Security Controls	**Tier**	**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:

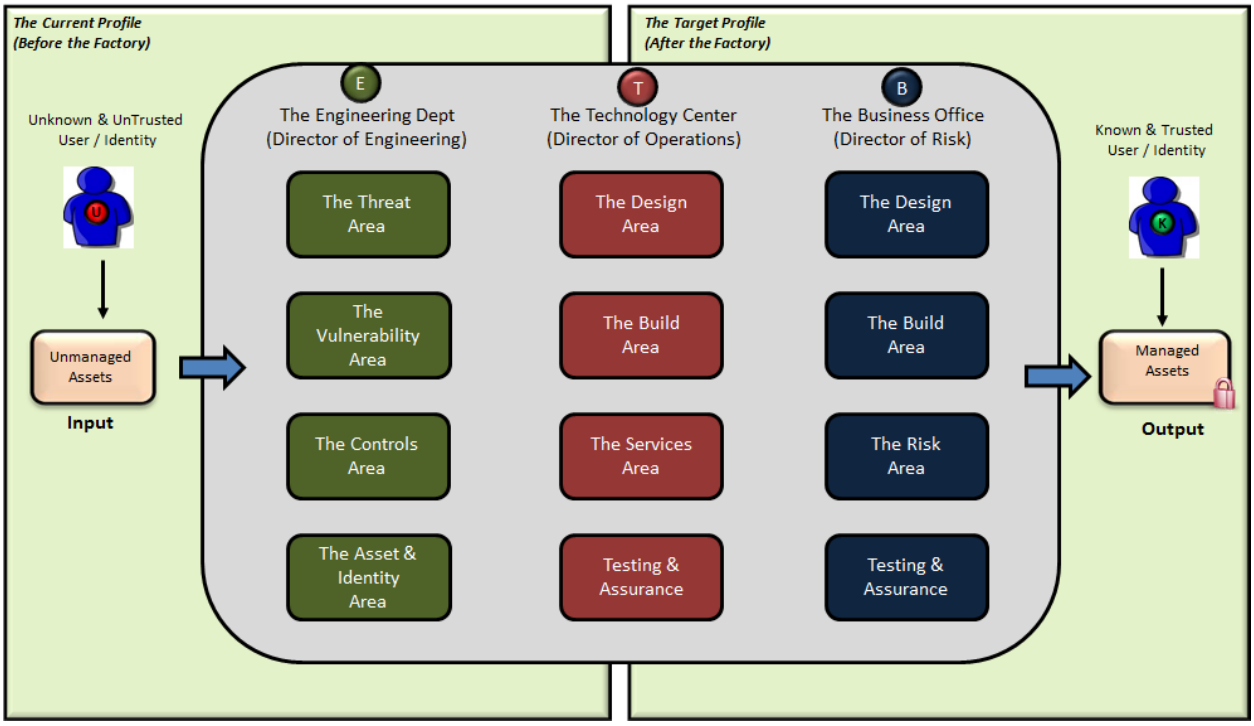
1. Senior and Cybersecurity Leadership: How do your senior leaders lead cybersecurity policies and operations?
2. Governance and Societal Responsibilities: How do you govern cybersecurity policies and operations and fulfill your organization's societal responsibilities?
3. Strategy Development: How do 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 UMASS NIST Cybersecurity Controls Factory Model
Operationalizing the NIST Cyber Security 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. It 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 Baldridge Cybersecurity Executive Builder.

The Controls Factory (Our Model)



Please note that the capabilities are 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.

The NIST Cyber Security Framework Business Case

This following outlines the cost associated with using the UMASS Controls Factory model to operationalize NIST CSF cyber security program across an enterprise and it supply chain.

Areas covered include:

1. **The cost to educate** an enterprise on the UMASS approach to operationalizing the NIST CSF across an enterprise and its supply chain.
2. **The cost to assess the risks** so the enterprise can identify and prioritize the threats and vulnerabilities the organization needs to deal with.
3. **The cost to implement, test, manage and improve** the cyber security program. The costs will include the fees for enterprises to do it themselves and the cost to outsource the program to UMASS or one of its licensed partners.

NIST CSF Cyber Security Training & Mentoring Services

NIST CSF & Cyber Security Video Training Library for Instructor Led Online, Onsite Blended Learning and Self-Paced Mentored Training Programs

- **NIST CSF Foundation Video Course with Digital Courseware** – 12 Month License
  $395 per student
- **NIST CSF Practitioner Video Course with Digital Courseware** – 12 Month License
  $895 per student
- **Cyber Security Certification Video Training Library (1400+ videos)** – 12 Month License
  $99 per student
- **Cyber Security Awareness Training Using Games, Animations & Simulations** – 12 Month License
  Call for Pricing - On Site or Cloud Hosted
- **Instructor Services** - Client has the option to supply its own instructor for Online, Onsite or Blended Learning instructor led programs or contract one from UMASS a licensed partner
  $1,500 per day plus Travel & Expense

NIST CSF Assessment Services

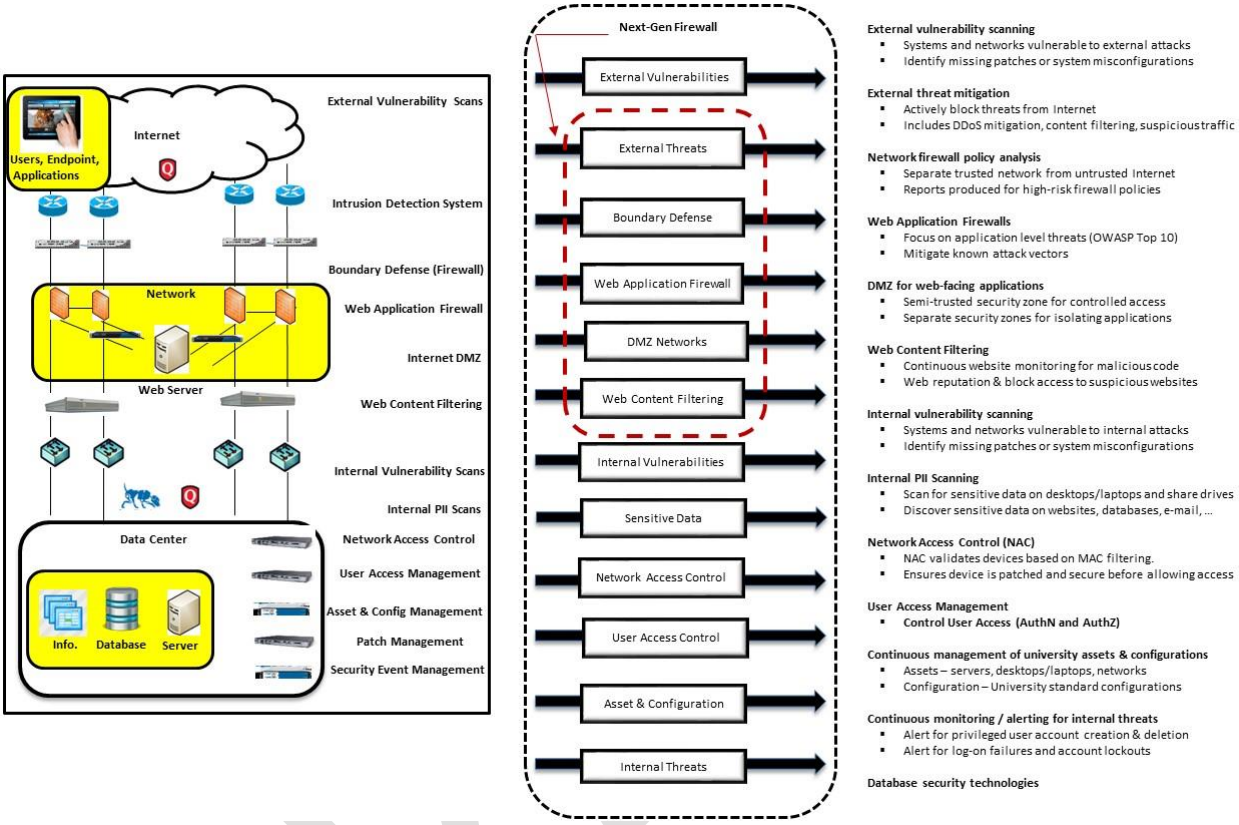
Once the education program has been completed, the enterprise staff has the option to perform the assessment itself or outsource that responsibility to UMASS

NIST CSF Assessment Services Cost - $

NIST CSF Managed Service

Once the education program has been completed, the enterprise staff has the option to implement and maintain the management program itself or outsource that responsibility to UMASS. For the Do It Yourself option, UMASS does offer CSC (Critical Security Controls) design guides and mentoring services for the Security Architecture Diagram listed below.

Security Architecture Diagram



The UMASS managed service program consists of both staffing and technology for your cyber security program.

Staff

- UMass Full Time Security Analyst supports 1st shift (Monday through Friday only)
- UMass Part Time Student Intern supports 1st shift (Saturday and Sunday only)
- UMass Part Time Student Intern supports 2nd shift (All seven days)
- UMass Part Time Student Intern supports 3rd shift (All seven days)

The following schedule will be maintained by UMass in support of managed services security monitoring:

Shift No.	Hours	Primary Contact(s)	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1st Shift	7 AM – 5 PM	Security Analyst	On-Call	Full Shift (8 Hours)	Full Shift (8 Hours)	Full Shift (8 Hours)	Full Shift (8 Hours)	Full Shift (8 Hours)	On-Call
1st Shift	7 AM – 5 PM	Student Intern	Full Shift (8 Hours)	N/A	N/A	N/A	N/A	N/A	Full Shift (8 Hours)
2nd Shift	4 PM - Midnight	Student Intern	Full Shift (8 Hours)	Full Shift (8 Hours)	Full Shift (8 Hours)	Full Shift (8 Hours)	Full Shift (8 Hours)	Full Shift (8 Hours)	Full Shift (8 Hours)
3rd Shift	Midnight – 8 AM	Student Intern	Full Shift (8 Hours)	Full Shift (8 Hours)	Full Shift (8 Hours)	Full Shift (8 Hours)	Full Shift (8 Hours)	Full Shift (8 Hours)	Full Shift (8 Hours)

Workload Assumptions:

- Number of customers supported by Analyst and Intern = 10 customers (10 % utilization)

- Total shifts worked per week: UMass Security Analyst = 5
- Total shifts worked per week: UMass Student Intern = 16
- Hourly Wage for UMass Analyst = $ 50 plus benefits = $ 400 per shift (8 hours)
- Hourly Wage for UMass Intern = $ 15 (no benefits) = $ 120 per shift (8 Hours)

Workload Breakdown:
- UMass Security Analyst: $ 400 [W] x 5 [S] x 1.30 [B] x 1.30 [M] x 0.10 [U] = $ 338 per week
- UMass Student Intern: $ 120 [W] x 16[S] x 1.00 [B] x 1.30 [M] x 0.10 [U] = $ 250 per week

Cost Assumptions:
- Wages [W] = Wages paid (per shift) to Security Analyst ($ 480) and Student Intern ($ 120)
- Shift [S] = Number of 8 hour shifts worked per week by Security Analyst (5) and Student Intern (16)
- Benefits [B] = Benefits paid to UMass Security Analyst (30% of Wages)
- Mark-up [M] = Mark-up / profit that UMass will realize for providing services (30%)
- Utilization [U] = Utilization per shift (10 %) for UMass Security Analyst and UMass Student Intern

Cost for Services (per customer):
- Weekly Cost = $ 338 + $ 250 = $ 588
- Monthly Cost = $ 588 x 52 / 12 = $ 2,548
- Annual Cost = $ 588 x 52 = $ 30,567

Technology

The following technologies / tools are included:
- Asset and Configuration Management Solution
- Patch Management Solution
- Endpoint Management Solution
- Anti-Virus Solution
- Next Generation Firewall Solution (IPS, URL Filtering, WAF, Policy Analysis, etc.)
- Vulnerability Management Solution
- Security Incident and Event Management (SIEM) Solution
- Data Loss Protection (DLP) Solution
- Network Access Control (NAC) Solution
- Identity and Access Management Solution
- Privileged Identity Management (PIM) Solution
- Database Security Solution

NIST CSF Managed Service Cost - $

About UMASS NIST CSF Cybersecurity Services

NIST CSF Cybersecurity Services is a new initiative for the University of Massachusetts (UMass). The initiative started in May 2015, when the UMass CISO was approached by The Boston Consortium with a request to provide Cybersecurity Services to under-resourced academic institutions in New England. Key representatives of the UMass President's Office met with the management team from The Boston Consortium to discuss how UMass could assist consortium members with the design, implementation and operations of their NIST cybersecurity programs. After a detailed discussion and review of the key UMass capabilities, a pilot program was initiated. The pilot program has since expanded to include the following:

- **NIST Cybersecurity Training & Mentoring Services** that teach enterprises how to design, implement and manage a cyber security program based on the NIST Cybersecurity Framework.
- **NIST Cybersecurity Assessment Services** so the enterprise can identify and prioritize the threats and vulnerabilities the organization needs to deal with.
- **NIST Cybersecurity Managed Services** where the university MAST team or one if its licensed partners designs, implements and manages for the client a cyber security program based on the NIST Cybersecurity Framework.

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 UMASS campuses plus six other universities in the Commonwealth of Massachusetts.

Prior to joining UMASS, 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 managing partner and the Vice President of Business Development at itSM Solutions LLC and the creator of the itSM Mentor IT and Cyber Security Workforce Development Training Portal. 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 best practice solutions for the past 15 years. Prior to itSM, Rick, led the Sales and Business Development teams at software companies focused on automating best practices across enterprises and its supply chain. Rick is certified professional 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 for his work in delivering innovative, online workforce development solutions.