A Controls Factory Approach To Designing, Building and Managing a Cyber Security Program Based on the NIST Cybersecurity Framework (NIST CSF)

Agenda and Objectives

- Introduction to NISTCSF.COM
- The Digital Innovation Economy
- The Cyber Security Problem
- The Cyber Security Solution
- The UMASS Controls Factory
- UMASS NIST CSF Services

NISTCSF.com

- NISTCSF.COM℠ is a new initiative from itSM Solutions LLC in partnership with the University of Massachusetts (UMASS). The program is designed to help organizations acquire the knowledge and skills to build a NIST CSF program itself, or outsource that responsibility to UMASS or one of its licensed affiliates.

- The program is built around a "controls factory" methodology (CFM)" created by Larry Wilson the CISO in the University Presidents Office. This easy to use approach to cybersecurity enables organizations of all sizes to quickly operationalize the NISTCSF across its enterprise and supply chain

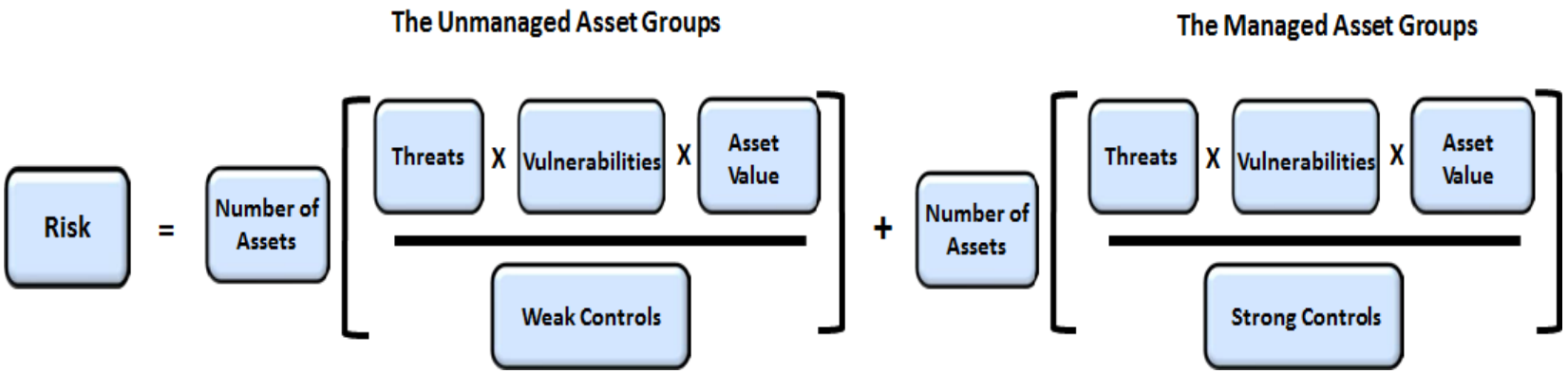
- The program and its author have won the following industry awards:
  - SANS Person who made a difference in Cybersecurity, 2013
  - ISE (Information Security Executives) Finalist for Executive of the Year for North America, 2013
  - ISE Information Security Program of the Year for Higher Education & Government Category, 2013
  - Security Magazine most influential cyber security professionals in North America, 2016

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 securing enterprise digital assets and services across stakeholders, supply chains, functions, markets, and geographies has never been greater.

The Cyber Security Problem

- Cybersecurity is all about managing risk. Before you can manage risk, you need to understand what the risk components are
- Risk components include the threats, vulnerabilities, assets (and their relative value), and the controls associated with an organizations information resources
- The equation for risk, which identifies the key components of risk is shown below



The Cyber Security Solution

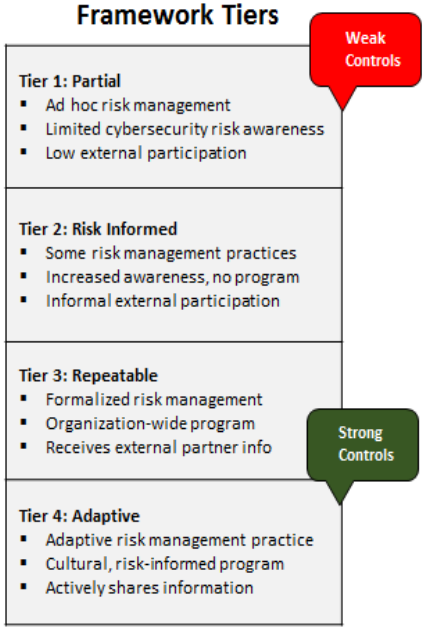
NIST Cybersecurity Framework

- The National Institute of Standards (NIST) under executive order was instructed to work with government and commercial stakeholders to develop a voluntary framework for reducing cyber risks to the nations critical infrastructure
- The Framework is composed of three parts; the Framework Core, the Framework Implementation Tiers, and the Framework Profiles and is based on existing standards, guidelines, and industry best practices

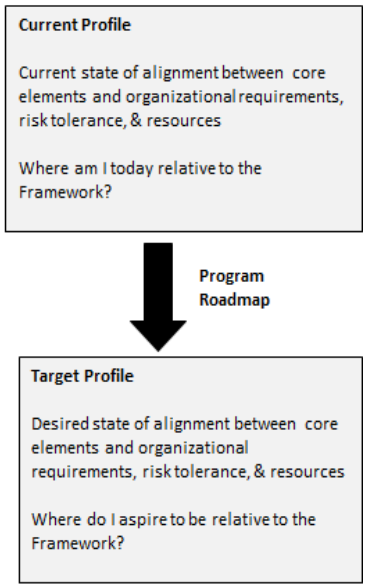
Framework Core

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 NIST CSF Controls

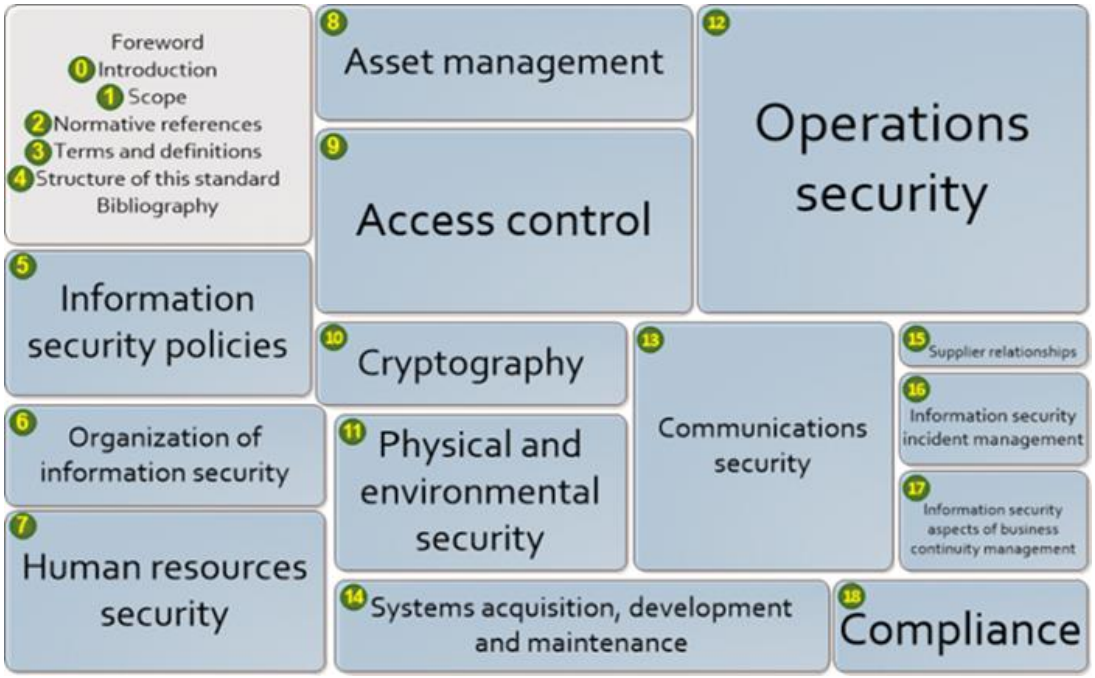
- The Technical Controls
  - The CIS Critical Security Controls (CIS Controls) are a concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyber-attacks
  - Organizations that apply just the first five CIS Controls can reduce their risk of cyberattack by 85 percent. Implementing all 20 CIS Controls increases the risk reduction to 94 percent

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 NIST CSF Controls (cont.)

- The Business Controls
  - ISO/IEC 27002:2013 provides guidelines for organizational information security management practices including taking into consideration the organization's people and process risk environment(s)
  - The ISO/IEC 27002:2013 information security reduces organizational risks by implementing a suitable set of controls, including policies, processes, procedures and structures that deal with the people and process side of risk management.



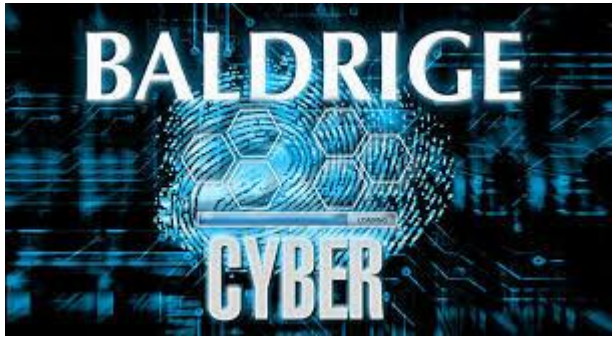
ISO 27002 Controls Mapping to the NIST Cybersecurity Framework:

		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 NIST CSF Controls (cont.)

- The Risk Management Controls
  - 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.

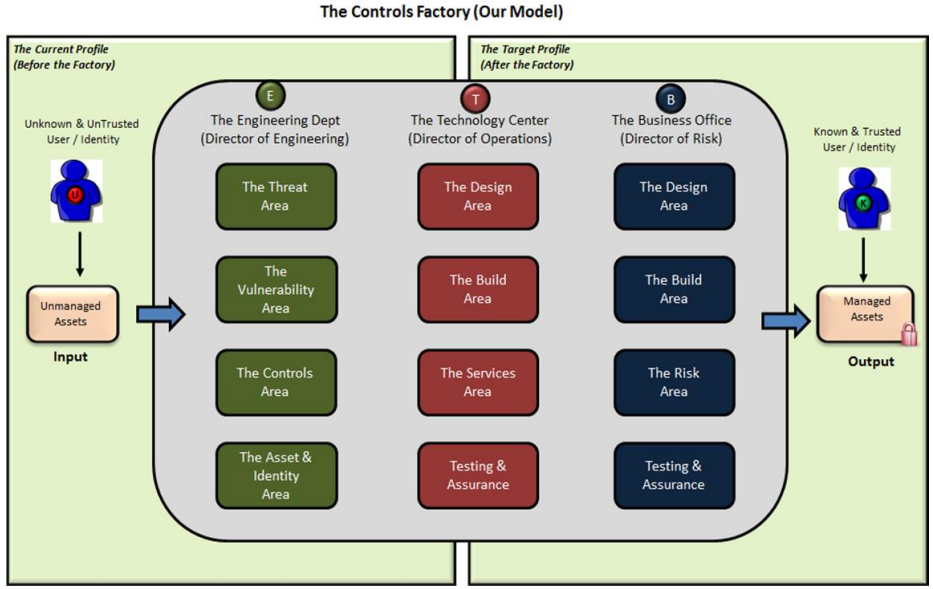
- Using this self-assessment tool, organizations can
  - Determine cybersecurity-related activities important to your business strategy and critical service delivery;
  - Prioritize your investments in managing cybersecurity risk;
  - Determine how best to enable your workforce, customers, suppliers, 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.



The UMASS Controls Factory

Operationalizing the NIST CSF Across an Enterprise and its Supply Chain

- The controls factory concept is used to help organize the engineering, technical and business functions of a NIST CSF 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.
- An 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.



NISTCSF.com Programs

- **Online or In-Class Training Programs on How Too Design, Build and Manage a NIST Cybersecurity Program –** This program teaches enterprises how to design, implement and manage a cyber security program based on the UMASS NIST Cybersecurity controls factory model.

- **Online NIST Cybersecurity Workforce Framework Career Pathway Trainings –** These programs teach students the knowledge and skills to sit for the professional examinations outlined in the NIST Cybersecurity Workforce Framework. Certification programs include CISSP, SSCP CISA, CISM, SECURITY+, CASP, A+ and Network+ certification.

- **Online NIST Cybersecurity Employee Awareness Training using the Axelos RESILIA™ portfolio of Games, Animations and Simulation -** The RESILIA employee cybersecurity awareness training program includes online modules covering topics in phishing, social engineering, online safety, social media, BYOD (Bring Your Own Device), removable media, password safety, personal information etc.

NISTCSF.com Programs (cont.)

- **NIST Cybersecurity Consulting Services –** NIST Cybersecurity Consulting Solutions provide enterprises with the option to learn the knowledge and skills to perform its own NIST CSF assessment or outsource that responsibility to UMASS or one of its licensed partners.

- **NIST Cybersecurity Testing & Continuous Monitoring Services –** NIST Cybersecurity Testing & Monitoring Solutions provide enterprises with the option to learn the knowledge and skills to build their own continuous monitoring program or outsource that responsibility to UMASS or one of its licensed partners.

Questions & Answers