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

A Business Case

Agenda and Objectives

- The Digital Innovation Economy
- The Cyber Security Problem
- The Cyber Security Solution
- The UMASS Controls Factory
- UMASS Cybersecurity Services
  - Training & Mentoring Services
  - Assessment Services
  - Managed Services

The Digital Innovation Economy

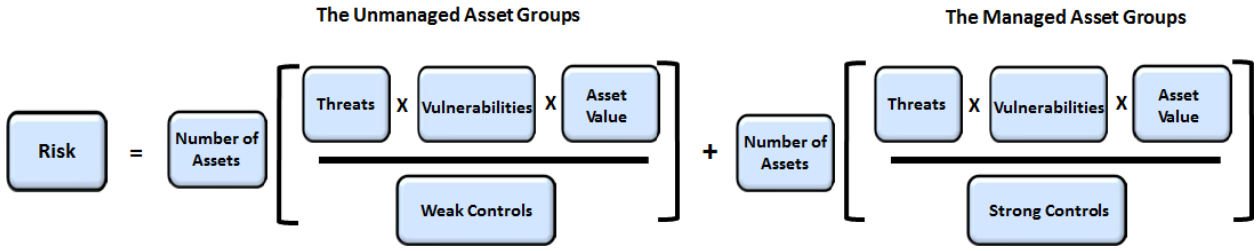
- Three things are certain in today's business world: first, digital services are now at the center of all businesses; second, business is a moving target and third businesses are under attack from those trying to steal the critical information companies rely on for daily business operations and revenue 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 digital innovation economy, an enterprise must ensure that it can build and maintain a reliable, resilient, secure and trusted digital infrastructure.

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
- An effective cybersecurity program involves a thorough understanding these risk components and how they are secured and managed within an organization
- The equation for risk, which identifies the key components of risk is shown below



The Cyber Security Solution

NIST Cybersecurity Framework

- Recognizing the national and economic security of the United States depends on the reliable function of critical infrastructure, the President issued Executive Order (EO) 13636 in February 2013.

- The Order directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure.

- Standards, guidelines and practices include – ISO 27001, Cobit, CCS CSC, NIST 800-53, 800-171 etc.

- The program focuses on the 16 critical infrastructure sectors as defined by the Department of Homeland Security but has now extended its reach across other sectors, countries and governments

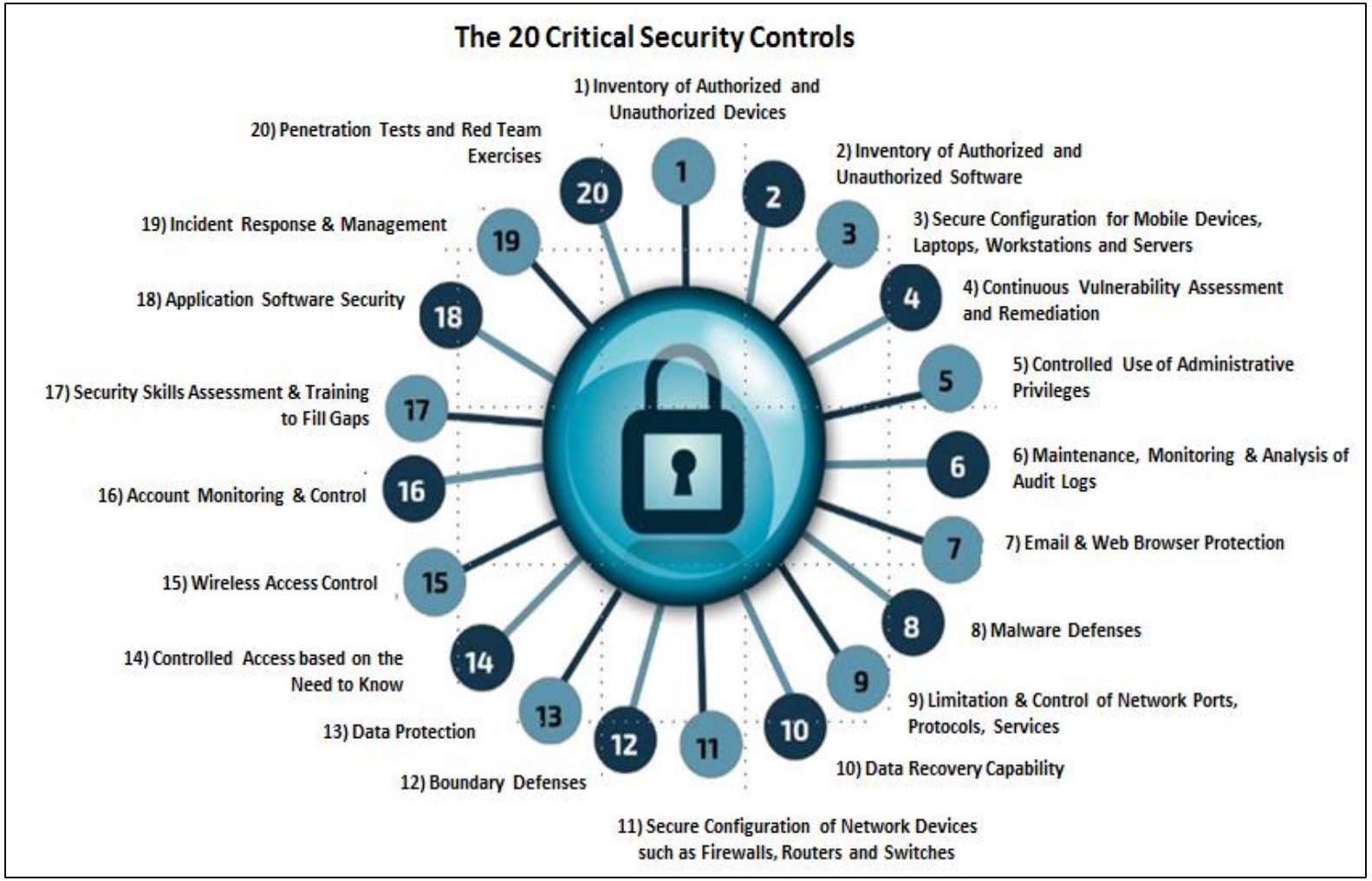
The NIST CSF Technical Controls

- 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

- 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 85 percent. Implementing all 20 CIS Controls increases the risk reduction to 94 percent

CIS Critical Security Controls



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 Business Controls

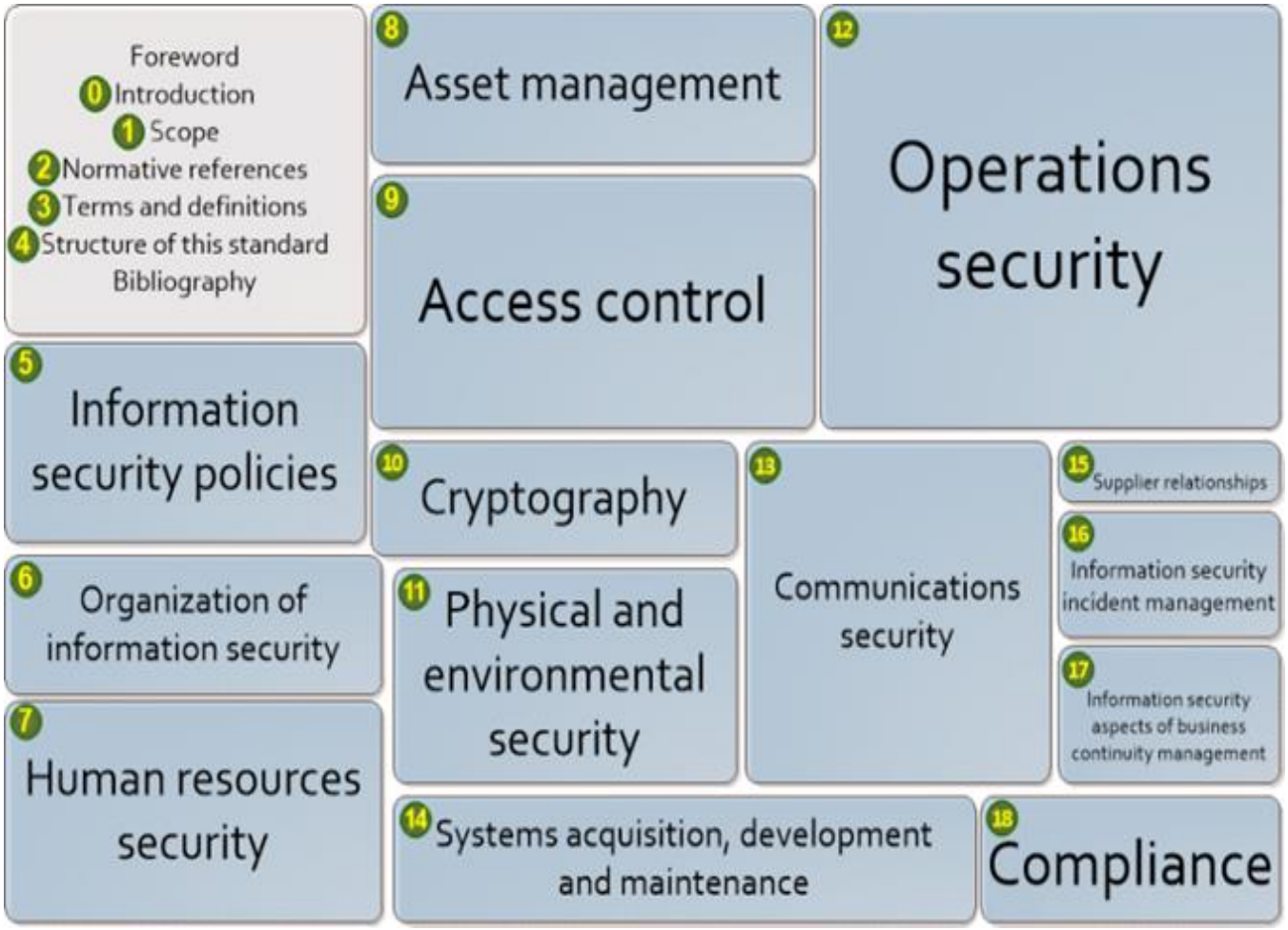
- Organizational assets are subject to both deliberate and accidental threats as the related processes, systems, networks and people that use and support them have inherent vulnerabilities

- Changes to business processes and systems or other external changes (such as new laws and regulations) may create new information security risks

- Effective information security reduces these risks by implementing a suitable set of controls, including policies, processes, procedures and organizational structures that deal with the people and process side of risk management.

- ISO/IEC 27002:2013 provides guidelines for organizational information security standards and information security management practices including taking into consideration the organization's people and process risk environment(s)

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 NIST CSF 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.

Baldrige Cybersecurity Excellence Builder

- **Senior and Cybersecurity Leadership**: How do your senior leaders lead cybersecurity policies and operations?
- **Governance and Societal Responsibilities**: How do you govern cybersecurity policies and operations and fulfill your organization's societal responsibilities?
- **Strategy Development:** How do you develop your cybersecurity strategy?
- **Strategy Implementation**: How do you implement your cybersecurity strategy?
- **Voice of the Customer**: How do you obtain information from your customers?
- **Customer Engagement**: How do you engage customers by serving their needs and building relationships?
- **Measurement, Analysis, and Improvement of Performance**: How do you measure, analyze, and then improve cybersecurity-related performance?
- **Knowledge Management**: How do you manage your organization's cybersecurity related knowledge assets?
- **Workforce Environment**: How do you build an effective and supportive workforce environment to achieve your cybersecurity goals?

Baldrige Cybersecurity Excellence Builder (cont.)

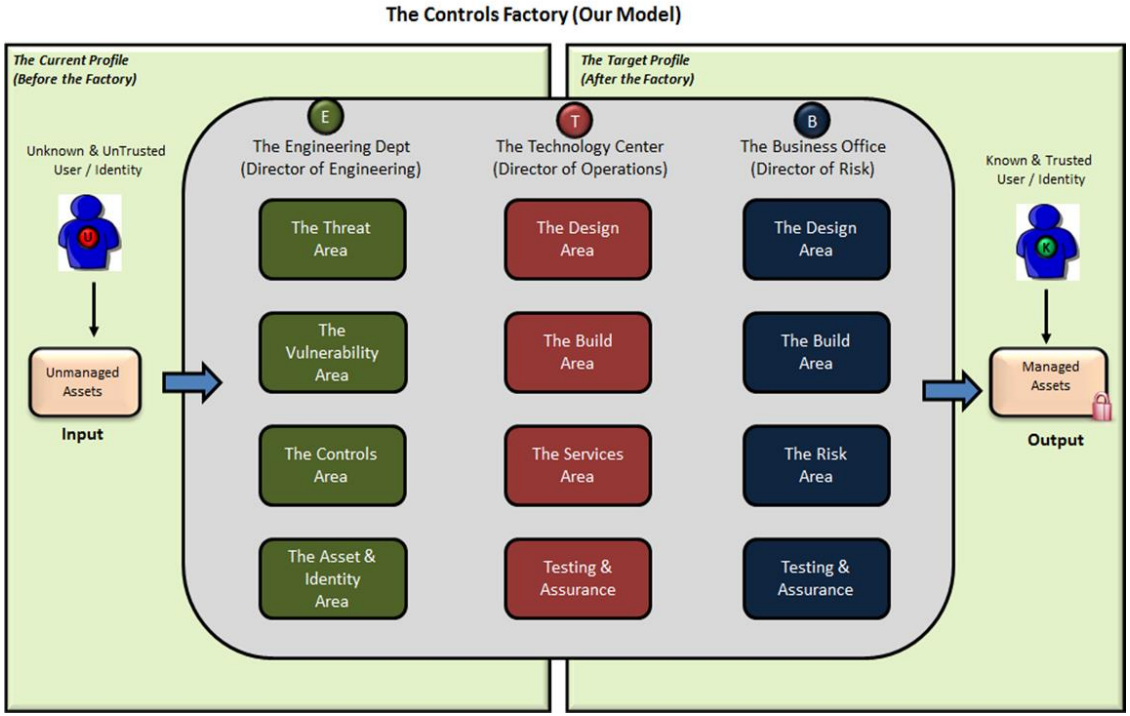
- **Workforce Engagement:** How do you engage your workforce to achieve a high performance work environment in support of cybersecurity policies and operations?
- **Work Processes:** How do you design, manage, and improve your key cybersecurity work processes?
- **Operational Effectiveness:** How do you ensure effective management of your cybersecurity operations?
- **Process Results:** What are your cybersecurity performance and process effectiveness results?
- **Customer Results**: What are your customer-focused cybersecurity performance results?
- **Workforce Results:** What are your workforce-focused cybersecurity performance results?
- **Leadership and Governance Results**: What are your cybersecurity leadership and governance results?
- **Financial Results**: What are your financial performance results for your cybersecurity operations?

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 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.



The UMASS Controls Factory Model

- The Engineering Department organizes all of the engineering functions 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 and assurance functions
- The Business Office organizes business functions focused on people, process and policy design (based on ISO 27002)
- The control factory capabilities are modular and therefore can work with any framework or standard. 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

UMASS NIST CSF Cyber Security Services

- UMASS Cybersecurity Services was launched in May 2015, when the UMass CISO was approached by The Boston Consortium with a request to provide NIST Cybersecurity Services to under-resourced academic institutions in New England

- After a detailed discussion and review of the key UMass capabilities, a pilot program was launched and now provides cybersecurity services based on the NIST Cyber Security Framework to six universities within Massachusetts

- The pilot program has since expanded to become a global offering via licensed partnerships with other universities and private corporations. Programs include:

  - **NIST CSF Training & Mentoring Services** that teach enterprises how to design, implement and manage a cyber security program based on the NIST Cybersecurity Framework.

  - **NIST CSF Assessment Services** so the enterprise can identify and prioritize the threats and vulnerabilities the organization needs to deal with.

  - **NIST CSF Managed Services** where the university team or one if its licensed partners designs, implements and manages for the client a cyber security program based on the NIST Cybersecurity Framework.

NIST CSF Training
& Mentoring Services

- **NIST 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

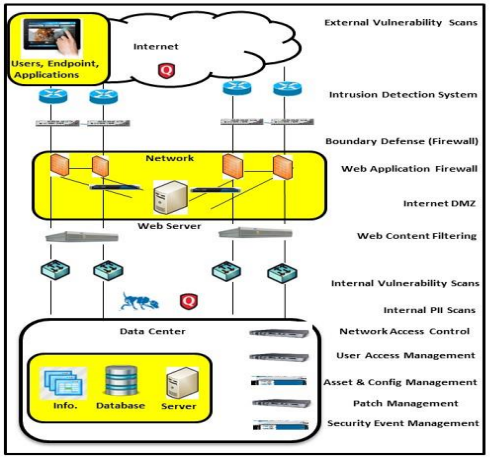
NIST CSF Assessment Services

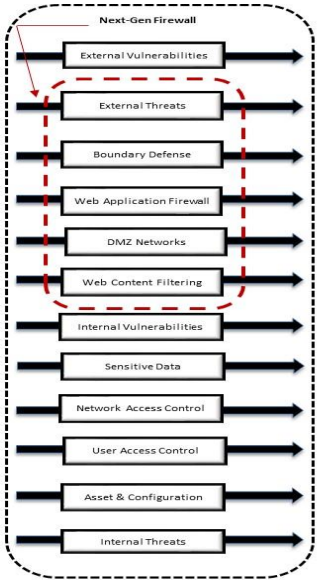
- Once the education program has been completed, the enterprise staff has the option to perform the assessment itself or outsource that responsibility to the UMASS team

- NIST CSF Assessment Services Cost - $

NIST CSF Managed Services

- 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 for the Security Architecture Diagram listed below
- NIST CSF Do IT Yourself Mentoring Cost - $





External vulnerability scanning
- Systems and networks vulnerable to external attacks
- Identify missing patches or system misconfigurations

External threat mitigation
- Actively block threats from Internet
- Includes DDoS mitigation, content filtering, suspicioustraffic

Network firewall policy analysis
- Separate trusted network from untrusted Internet
- Reports produced for high-risk firewall policies

Web Application Firewalls
- Focus on application level threats (OWASP Top 10)
- Mitigate known attack vectors

DMZ for web-facing applications
- Semi-trusted security zone for controlled access
- Separate security zones for isolating applications

Web Content Filtering
- Continuous website monitoring for malicious code
- Web reputation & block access to suspicious websites

Internal vulnerability scanning
- Systems and networks vulnerable to internal attacks
- Identify missing patches or system misconfigurations

Internal PII Scanning
- Scan for sensitive data on desktops/laptops and share drives
- Discover sensitive data on websites, databases, e-mail, ...

Network Access Control (NAC)
- NAC validates devices based on MAC filtering.
- Ensures device is patched and secure before allowing access

User Access Management
- **Control User Access (AuthN and AuthZ)**

Continuous management of university assets & configurations
- Assets – servers, desktops/laptops, networks
- Configuration – University standard configurations

Continuous monitoring / alerting for internal threats
- Alert for privileged user account creation & deletion
- Alert for log-on failures and account lockouts

Database security technologies

NIST CSF Managed Services (cont.)

- For the UMASS managed option, UMASS delivers both staffing and technology for your cyber security program.

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

- Technologies Include
  - 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 - $

Questions & Answers