Improving Cybersecurity through the use of the Cybersecurity Framework

March 11, 2015

Tom Conkle
G2, Inc.

Agenda

- Cybersecurity Framework
  - Why it was created
  - What is it
  - Why it matters
  - How do you use it

Cybersecurity spending is increasing, but companies are still being breached

- POS listed as one of the top nine data breach patterns in 2013
- $46 billion in Cybersecurity spending in 2013
- Cybersecurity spending increased by 10% in 2013
- SEC performing an audit of 50 financial institutions

Executive Order 13636 asked for the creation of a Cybersecurity Framework applicable to all sectors

- Executive Order
  - Be Flexible
  - Be non-prescriptive
  - Leverage existing approaches, standards, practices
  - Be globally applicable
  - Focus on risk management vs. rote compliance
- Framework for Improving Critical Infrastructure Cybersecurity
  - Referred to as "The Framework"
  - Issued by NIST on February 12, 2014.

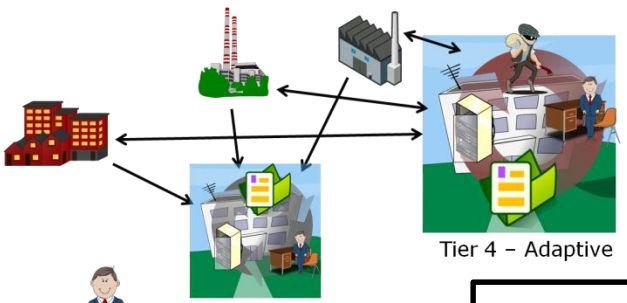
The Framework established three primary components used to develop a holistic cybersecurity program

ILLUSTRATIVE

Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established	· COBIT 5 APO01.03, EDM01.01, EDM01.02 · ISA 62443-2-1:2009 4.3.2.6 · ISO/IEC 27001:2013 A.5.1.1 · NIST SP 800-53 Rev. 4 -1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	· COBIT 5 APO13.12 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 · NIST SP 800-53 Rev. 4 PM-1, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· COBIT 5
PROTECT (PR)	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users	· CCS CSC · COBIT 5 · ISA 62443 · ISA 62443 1.8, SR 1.9 · ISO/IEC · NIST SP
		PR.AC-2: Physical access to assets is managed and protected	· COBIT 5 · ISA 62443 · ISO/IEC · NIST SP
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	· COBIT 5 · ISA 62443 · NIST SP
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	· ISA 62443 · ISA 62443 SR. 6.1, SR. 6.2 · ISO/IEC · NIST SP
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	· ISA 62443 · NIST SP
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event	· COBIT 5 · CCS CSC · ISA 62443 · ISO/IEC · NIST SP
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	· COBIT 5 · ISA 62443 · ISO/IEC · NIST SP
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	· CCS CSC · COBIT 5 · ISO/IEC · NIST SP
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	· COBIT 5 · ISA 62443 · NIST SP
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed	· COBIT 5
		RC.CO-2: Reputation after an event is repaired	· COBIT 5
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	· NIST SP

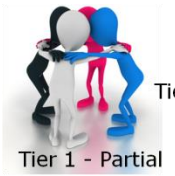
Implementation Tiers



Tier 4 – Adaptive

Tier 3 – Repeatable

Tier 2 – Risk Informed



Tier 1 - Partial

Framework Profiles

Function	Category	Subcategory	Priority	Org Policy	Org Practices	Status	Comments / Evidence
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy	ID.AM-1: Physical devices and systems within the organization are inventoried	M				
		ID.AM-2: Software platforms and applications within the organization are inventoried	L				
		ID.AM-3: Organizational communication and data flows are mapped	H				
		ID.AM-4: External information systems are catalogued	M				
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on	M				
		ID.AM-6: Cybersecurity roles and responsibilities for the entire	H				

The Framework Core establishes a common language for describing a cybersecurity program

- A set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.

- Consists of 5 Functions —Identify, Protect, Detect, Respond, Recover. These provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

- Categories and Subcategories for each Function, matched with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

Framework Core

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

The subcategories describe expected outcomes

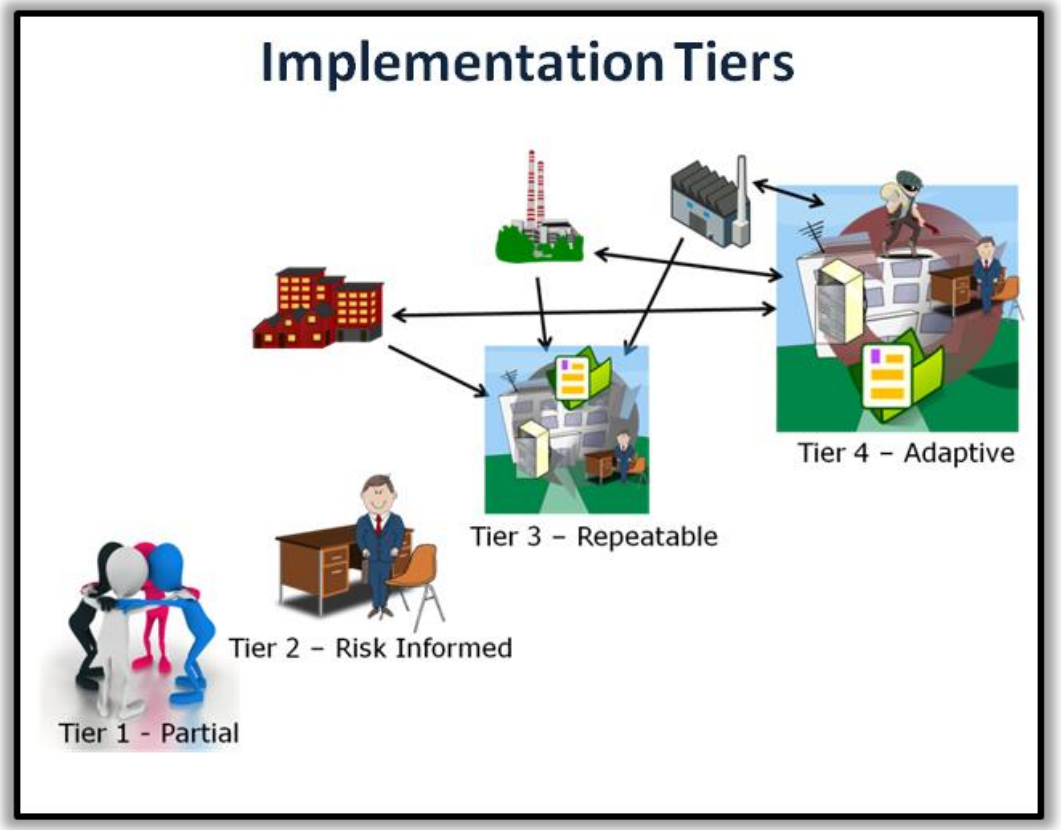
EXAMPLE

Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9

Organizations select an Implementation Tier based on their risk threshold

- **Three attributes of Tiers:**
  - Risk Management Process
  - Integrated Risk Management Program
  - External Participation



Tier 4 may not always be the goal

Current and Target state profiles help organizations capture their cybersecurity program

Function	Category	Subcategory	Priority	Org Policy	Org Practices	Status	Comments / Evidence
IDENTIFY (ID)	**Asset Management**: data, personnel, de… and facilities th… organization to a… purposes are identified and … consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	M				
		ID.AM-4: External information systems are catalogued					
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on	M				
		ID.AM-6: Cybersecurity roles and responsibilities for the entire … for … and third-par…	H				

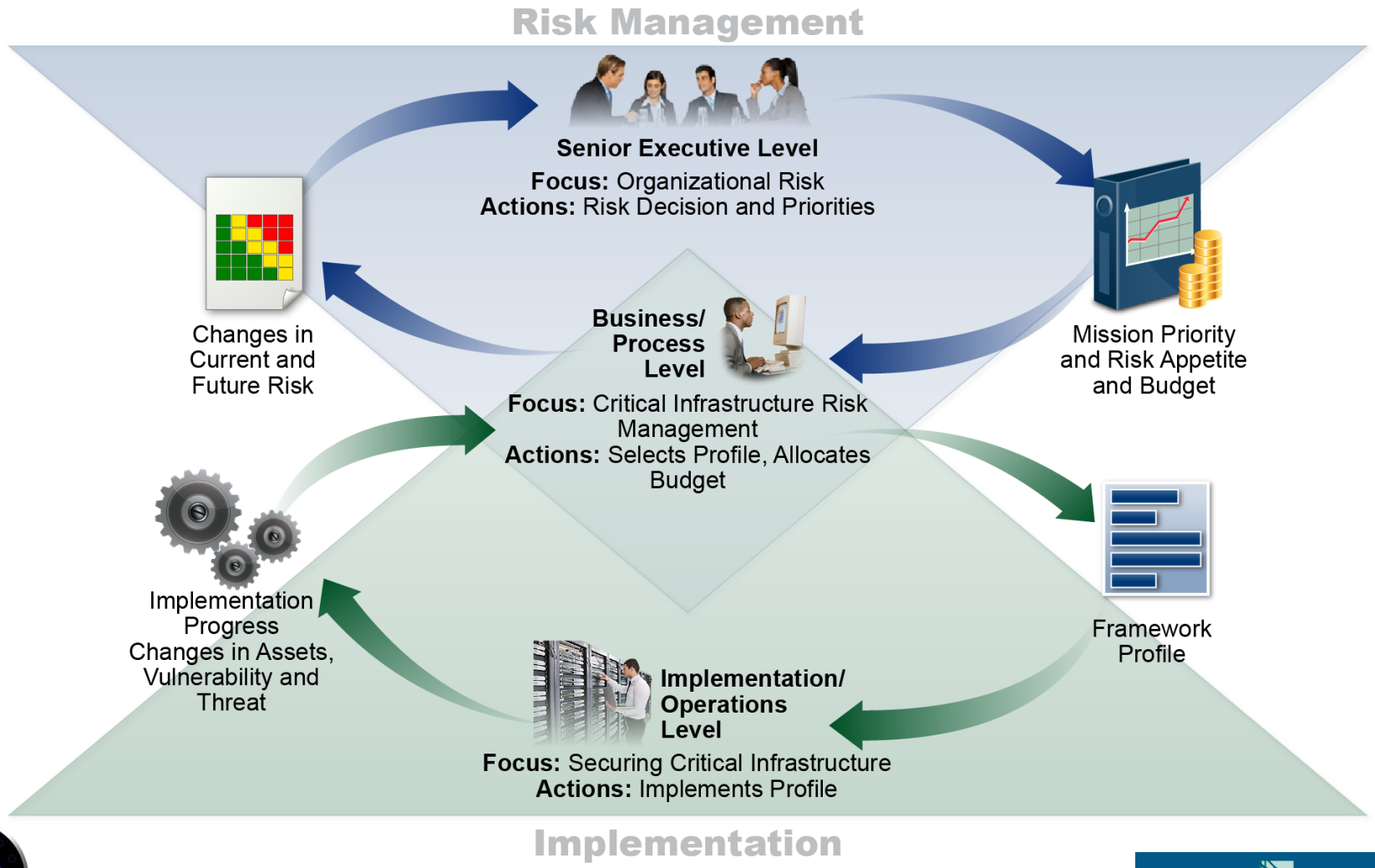
CURRENT PROFILE EXAMPLE

Why Use the Cybersecurity Framework?

- Common Language
- Collaboration Opportunities
- Ability to Demonstrate Due Care
- Easily Maintain Compliance
- Secure Supply Chain
- Cost Efficiency

Compliance ⊜ Secure

The Framework clarifies communications within an organization and with external partners



The Framework identifies seven steps for improving or developing a risk informed cybersecurity program

- Step 1: Prioritize and Scope
- Step 2: Orient
- Step 3: Create a Current Profile
- Step 4: Conduct a Risk Assessment
- Step 5: Create a Target Profile
- Step 6: Determine, Analyze, and Prioritize Gaps
- Step 7: Implement Action Plan (Build a Roadmap)

We are available to answer any additional questions

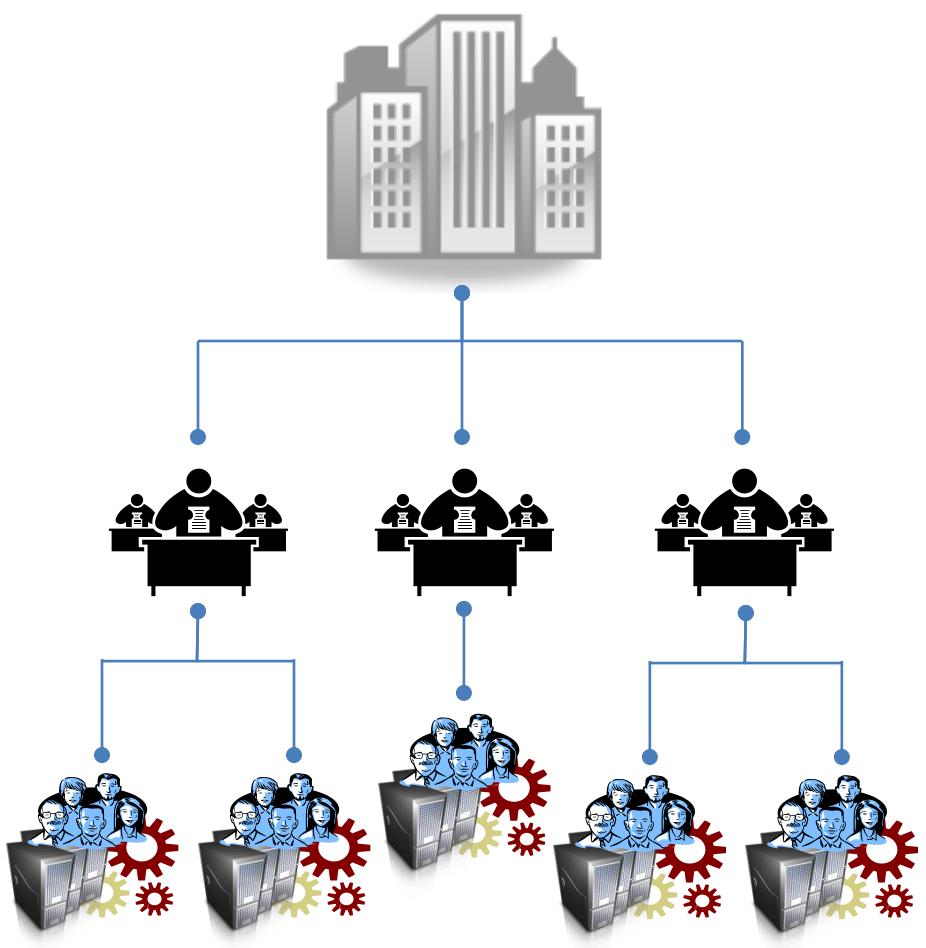
Tom Conkle
Cybersecurity Engineer
tom.conkle@g2-inc.com
(301) 575-5139

American Association of Port Authorities
Alliance of the Ports of Canada, the Caribbean, Latin America and the United States

Backup

Organizations identify their business and mission objectives to initiate the process

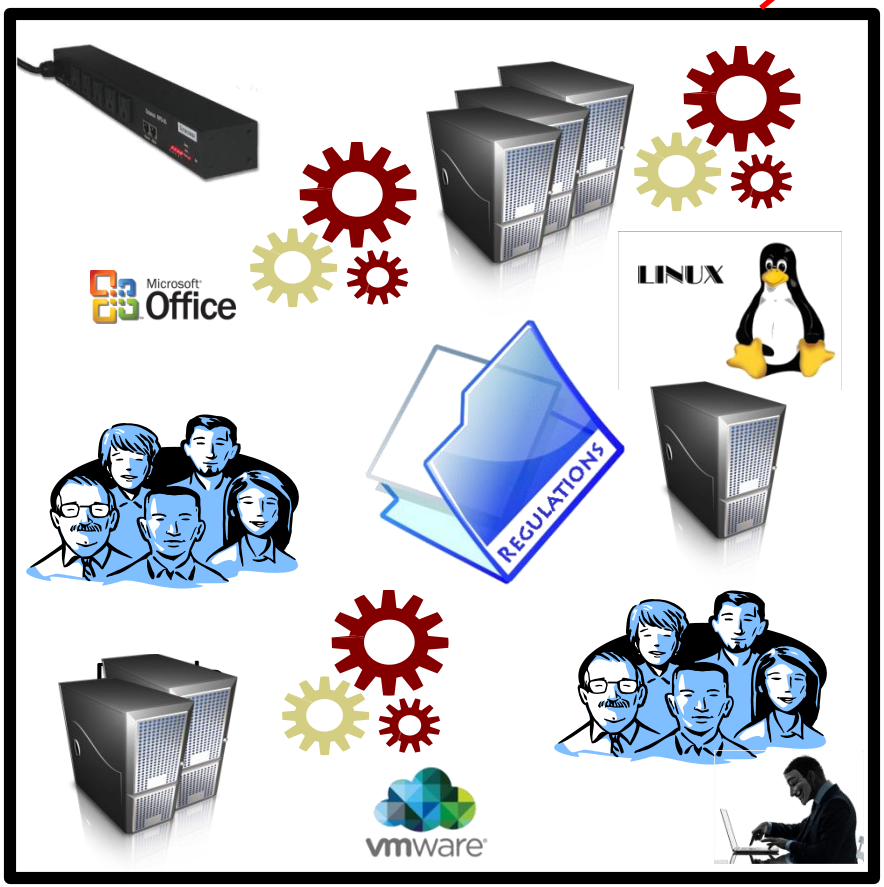
STEP 1:
PRIORITIZE AND SCOPE



The orient step aligns the business goals, assets, systems, and regulatory requirements for the program

STEP 2:
ORIENT

Risk Thresholds

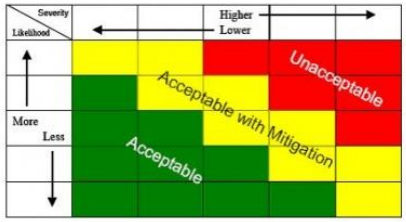


Next organization assess their current and target cybersecurity programs to identify gaps

STEP 3:
CREATE A CURRENT PROFILE

Function	Category	Subcategory	Priority	Org Policy	Org Practices	Status	Comments / Evidence
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	M				
		ID.AM-2: Software platforms and applications within the organization are inventoried	L				
		ID.AM-3: Organizational communication and data flows are mapped	H				
		ID.AM-4: External information systems are catalogued	M				
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on	M				
		ID.AM-6: Cybersecurity roles and responsibilities for the entire	H				

STEP 4:
CONDUCT A RISK ASSESSMENT



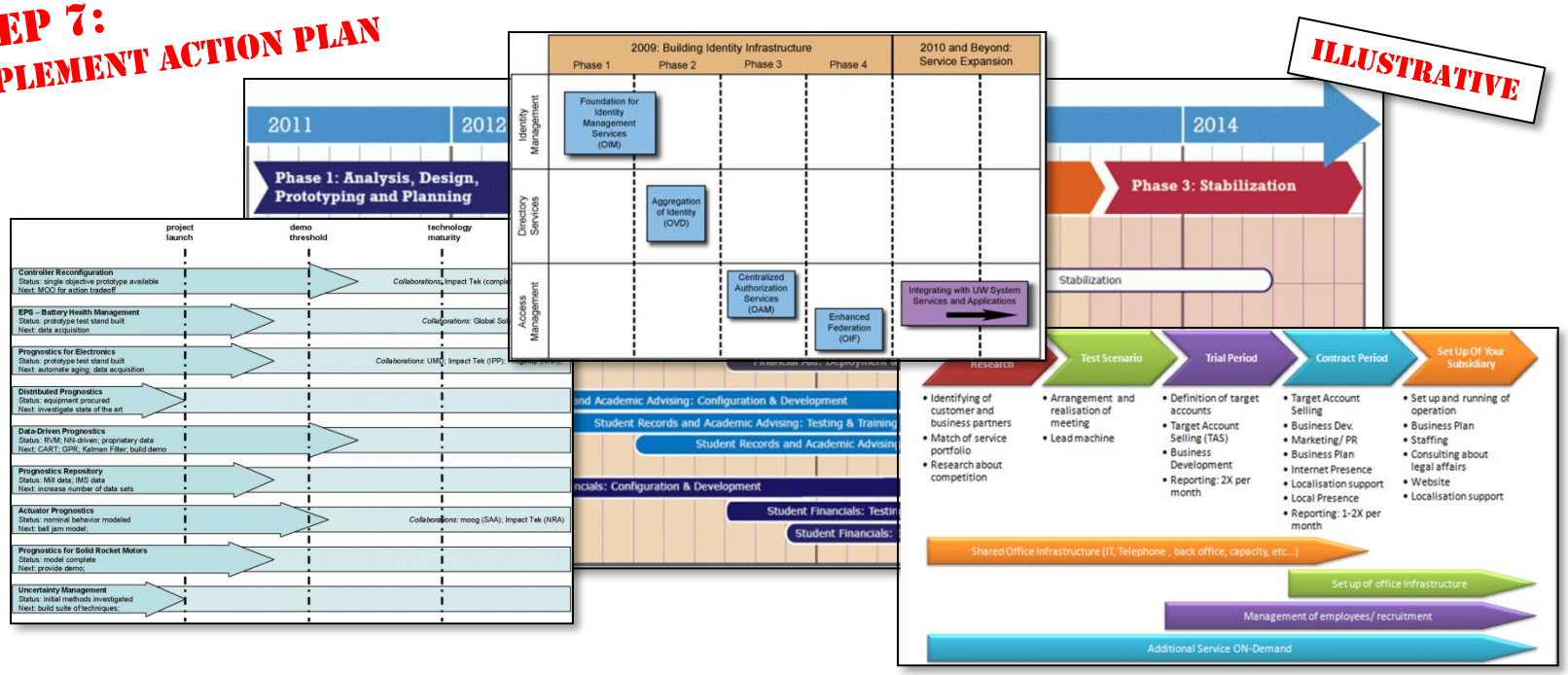
STEP 5:
CREATE A TARGET PROFILE

Function	Category	Subcategory	Priority	Org Policy	POCs	Resources	Comments / Evidence
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	M				
		ID.AM-2: Software platforms and applications within the organization are inventoried	L				
		ID.AM-3: Organizational communication and data flows are mapped	H				
		ID.AM-4: External information systems are catalogued	M				
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on	M				
		ID.AM-6: Cybersecurity roles and responsibilities for the entire	H				

STEP 6:
DETERMINE, ANALYZE, AND PRIORITIZE GAPS

The final step is to implement and monitor an action plan to close identified gaps

STEP 7:
IMPLEMENT ACTION PLAN



Stakeholders

Milestones

Status

Completion Date

Priority

Specific Action

Resources

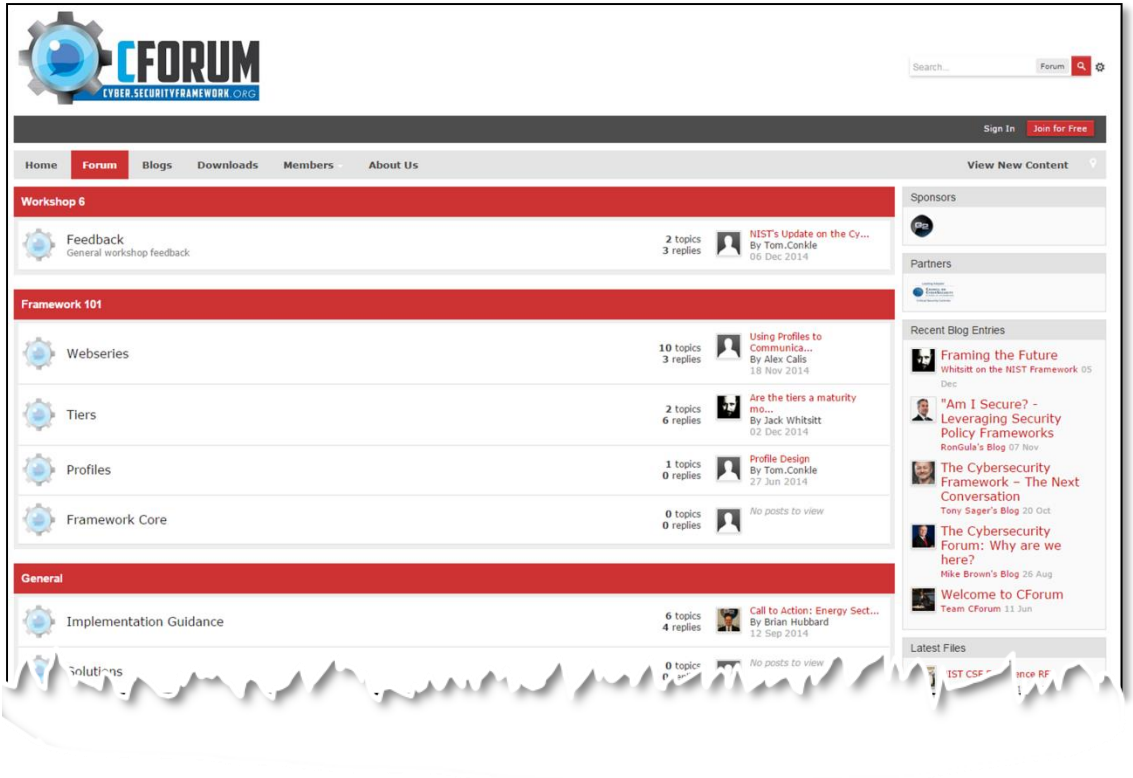
Owner

Rationale

Action Identifier

Dependencies

CForum is an online community focused on continuing the discussion started by the Framework development process



- Located at: Cyber.securityFramework.org
- Free for users to share best practices and lessons Learned
- Enables ongoing support for improving cybersecurity protections

CFORUM
WWW.CYBER.SECURITYFRAMEWORK.ORG

NIST has several resources available to organizations wanting to understand and use the Framework

- http://www.nist.gov/cyberframework/cybersecurity-framework-industry-resources.cfm