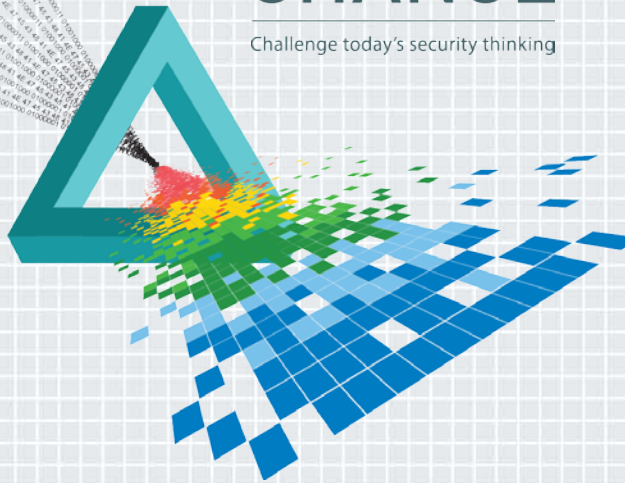
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: GRC-W04

70% of US Business Will Be Impacted by the Cybersecurity Framework: Are You Ready?

Tom Conkle
Cybersecurity Engineer
G2, Inc.
@TomConkle

Greg Witte
Senior Security Engineer
G2, Inc.
@thenetworkguy

Compliance standards have historically defined risk thresholds for organizations

HIPAA
Health Insurance Portability and Accountability Act

NERC CIP v5

FedRAMP SM

NIST
National Institute of Standards and Technology

Information Security Management System ISO 27001 Certified

PCI COMPLIANT PCI

G2

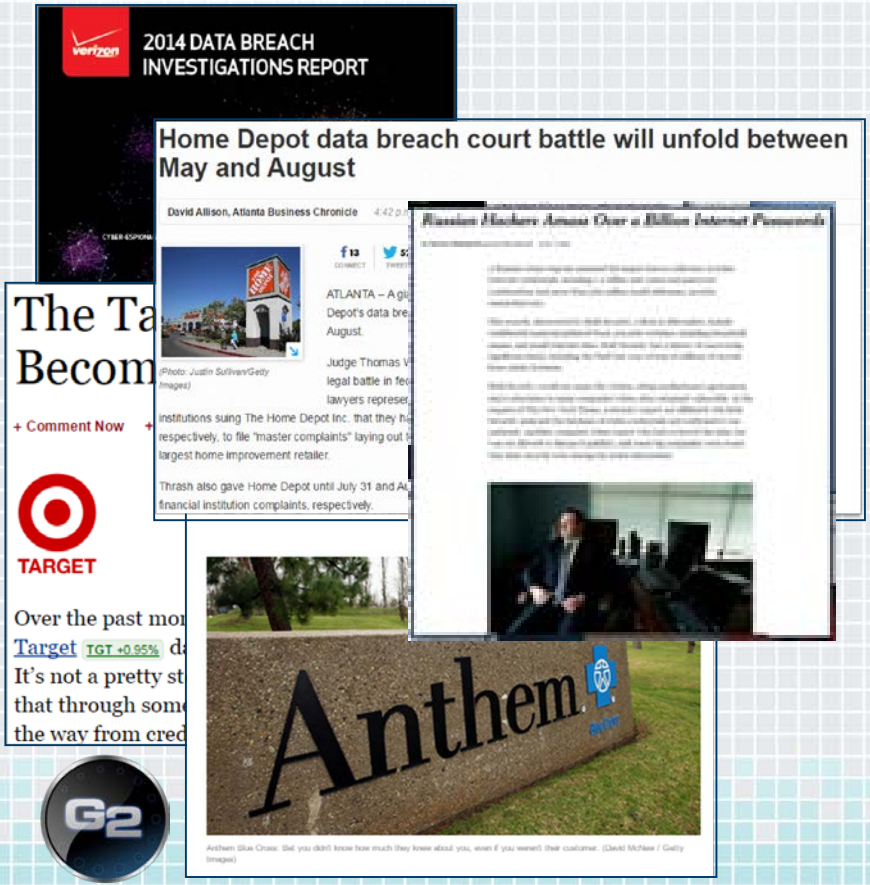
Compliant does not always mean secure

Security should be commensurate with risk

Agenda

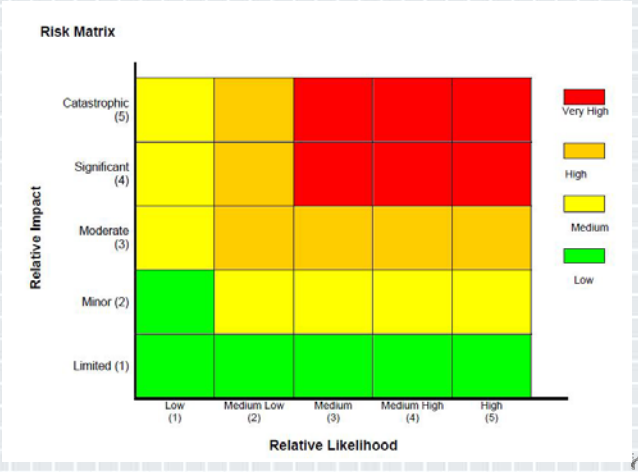
- Why the Cybersecurity Framework was needed
- What is the Cybersecurity Framework
- Why you should care about the Cybersecurity Framework
- Preparing for using the Cybersecurity Framework

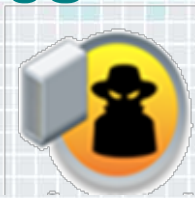
More breaches every day despite increased compliance requirements and billions in spending



- $46 billion in Cybersecurity spending in 2013
- Cybersecurity spending increased by 10% in 2013
- $3.5M average cost of data breach – Up 15%

Communicating cybersecurity risk enables appropriate spending

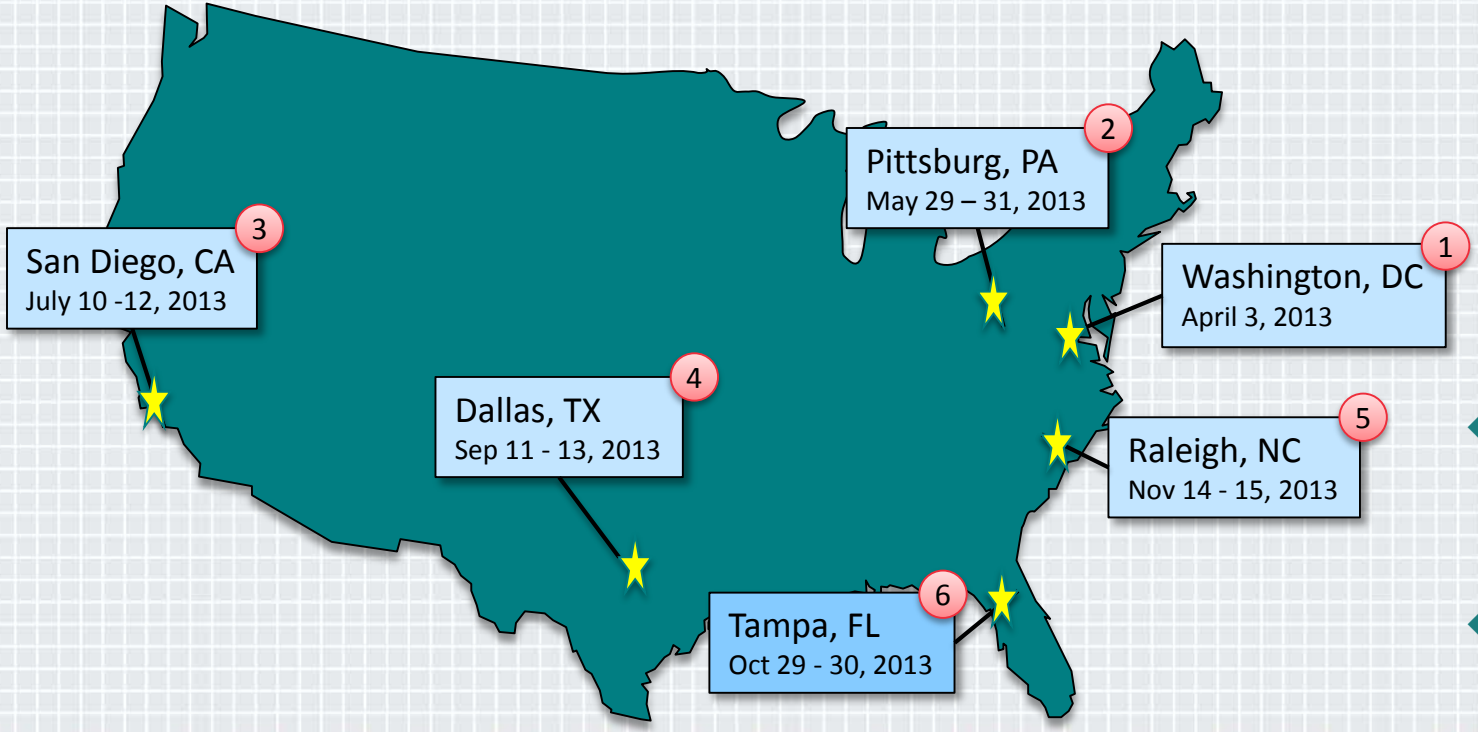




Executive Order 13636 asked for the creation of a Cybersecurity Framework applicable to all sectors

- Executive Order Requirements
  - 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 was developed in partnership among industry, academia and government



- NIST Conducted 5 workshops
- Released 2 RFIs

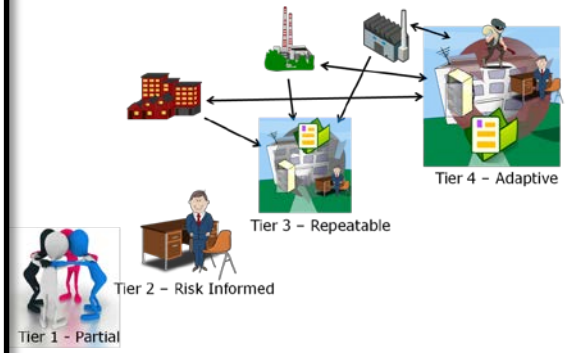
The Framework establishes three primary components

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 MEA03.01, MEA03.04 ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1 NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
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 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
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 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	ISA 62443-2-1:2009 4.2.3.10, 4.4.3.7, 4.4.4.5 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	ISA 62443-3-3:2013 SR 6.1 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
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 BAI01.10 CCS CSC 18 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	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 BAI01.13 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
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 8 COBIT 5 DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	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 BAI07.08 ISA 62443-2-1:4.4.3.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	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 EDM03.02
		RC.CO-2: Reputation after an event is repaired	COBIT 5 MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	NIST SP 800-53 Rev. 4 CP-2, IR-4

Implementation Tiers



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

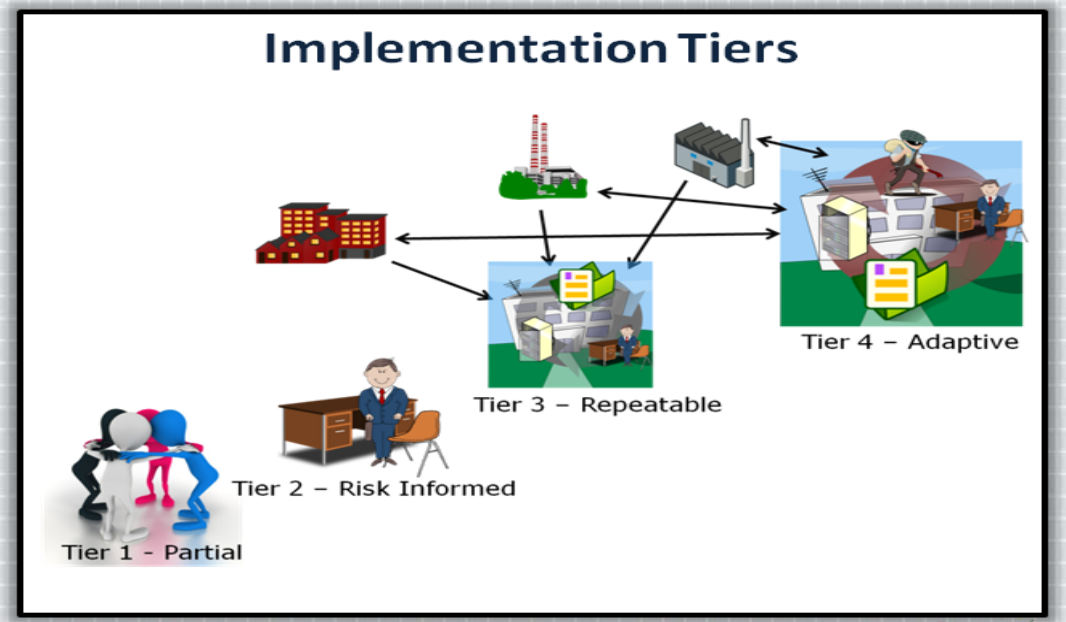
EXAMPLE

Framework Core

	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



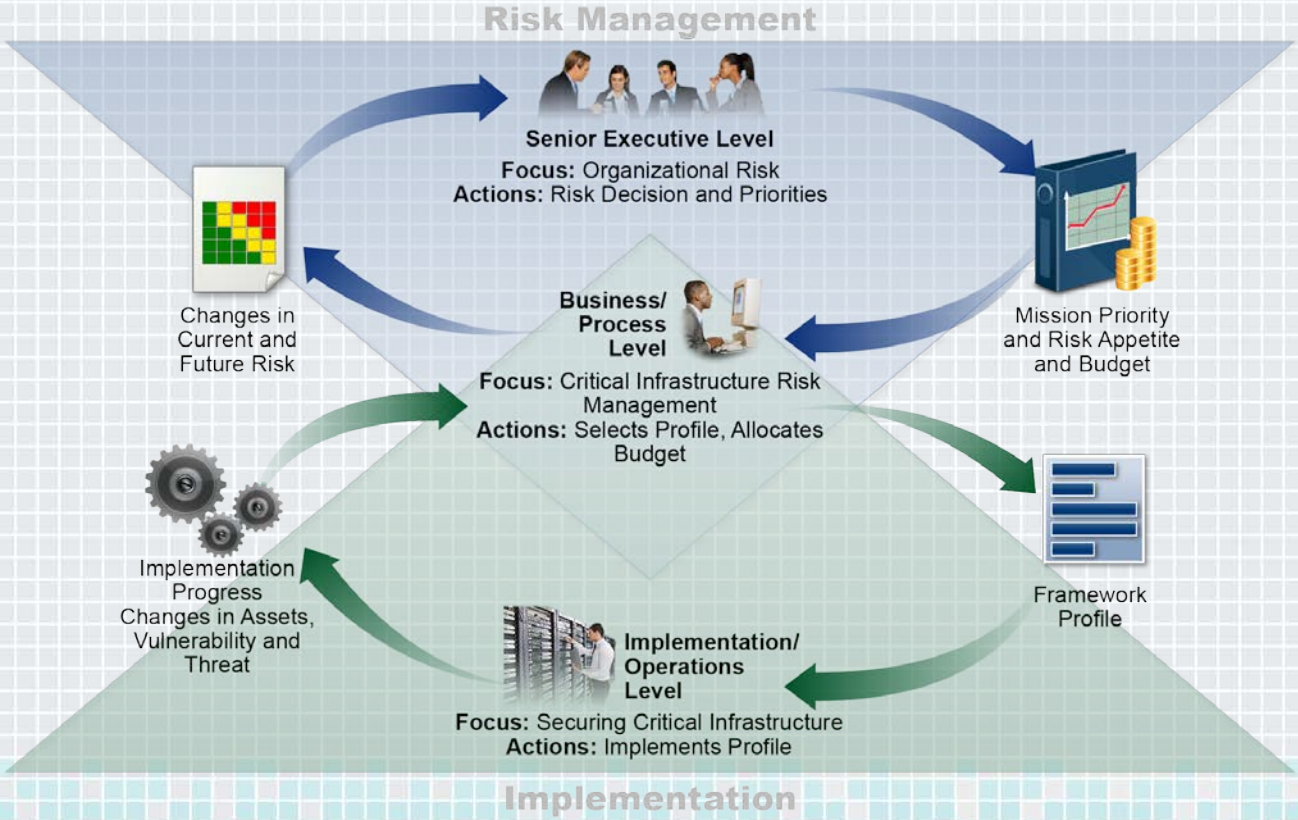
Tier 4 may not always be the goal

Current and Target state profiles help organizations capture their cybersecurity program

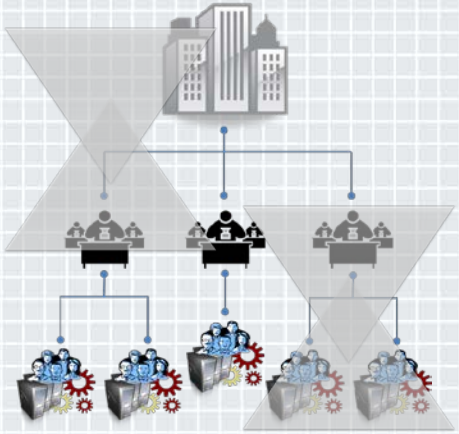
Function	Category	Subcategory	Priority	Org Policy	Org Practices	Status	Comments / Evidence
IDENTIFY (ID)	**Asset Management**: data, personnel, de… and facilities th… organization to a… purposes are identi… consistent with the… importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are	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 en…	H				

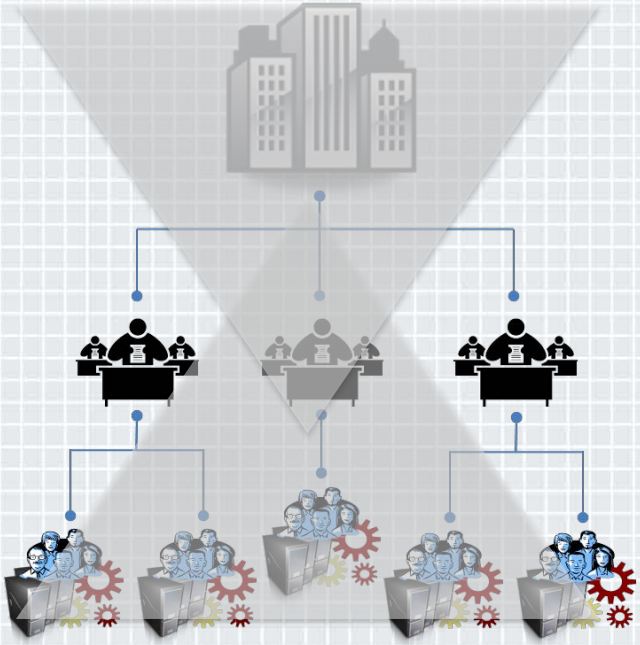
CURRENT PROFILE EXAMPLE

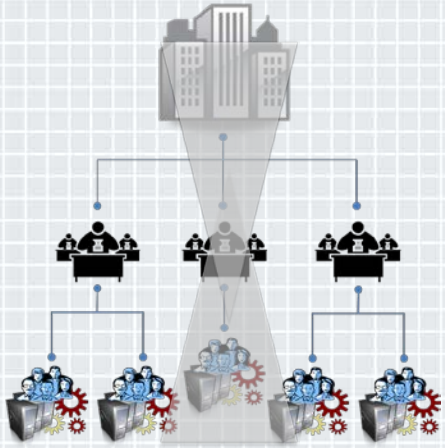
The Framework establishes a common language for cybersecurity



Communications can occur at all levels within an organization using the Framework







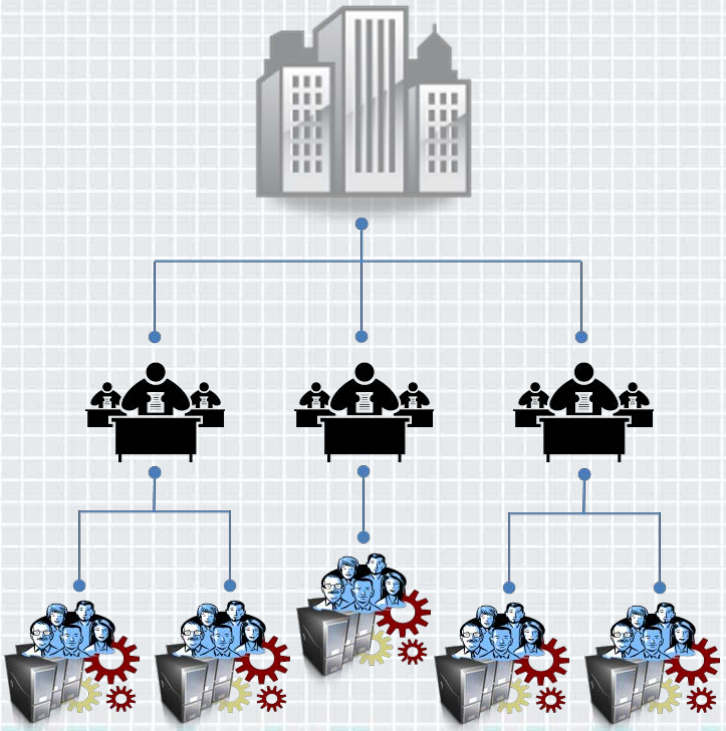
The Framework identifies seven steps for developing/improving a cybersecurity program

- 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)

Organizations identify their business and mission objectives to initiate the process

STEP 1: PRIORITIZE AND SCOPE

- Organizational Structure
- Mission Goals
- Business Drivers
- Regulatory Requirements
- Existing Policies
- Priorities
- Budget



The orient step aligns the business goals, assets, 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

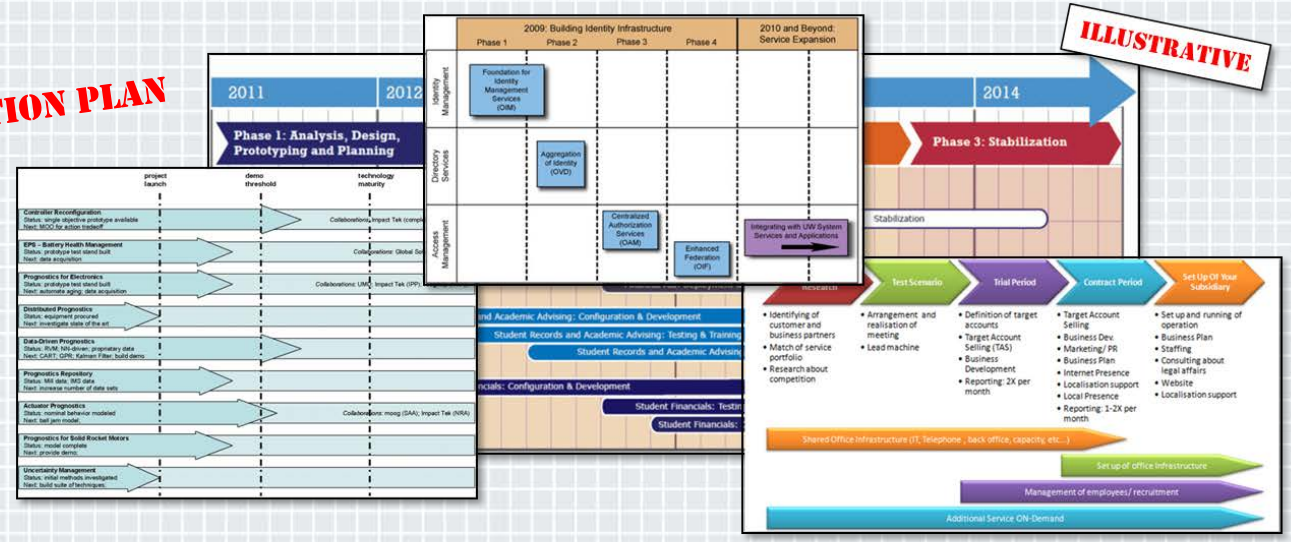
STEP 5: CREATE A TARGET PROFILE

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.,					

STEP 6: DETERMINE, ANALYZE, AND PRIORITIZE GAPS

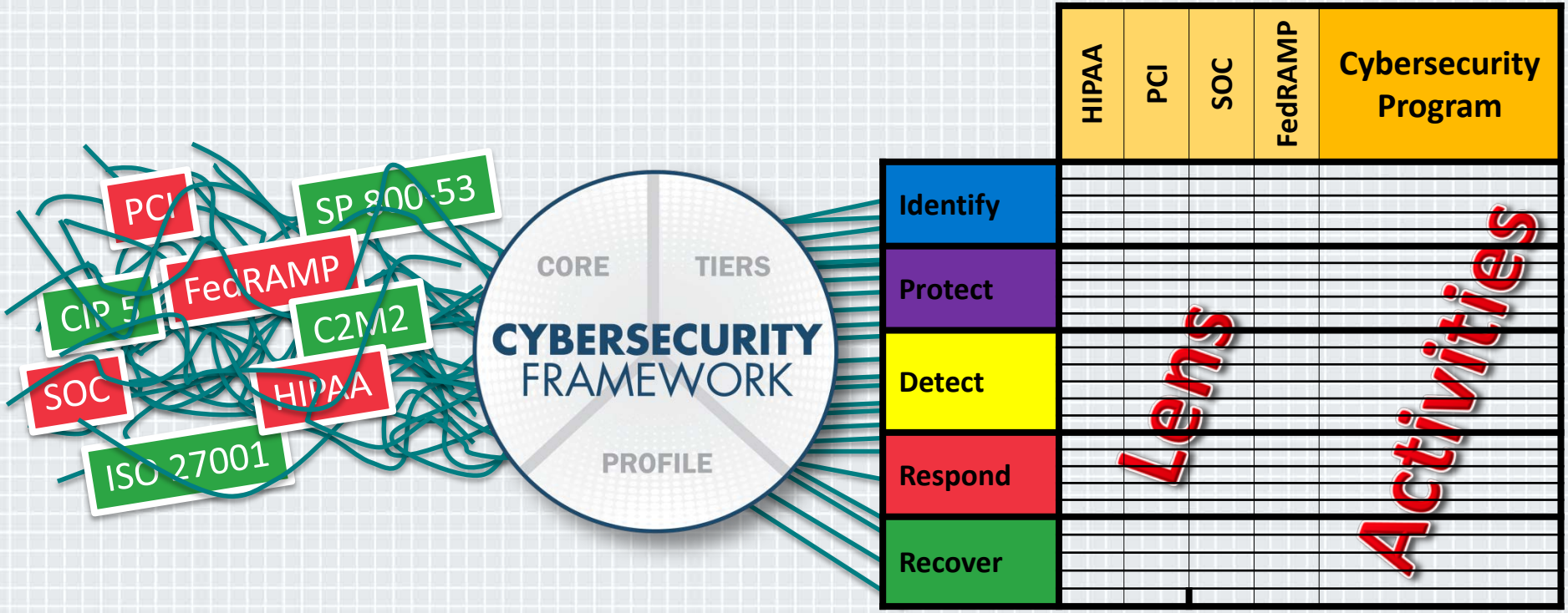
The final step is to implement and monitor an action plan to close identified gaps

STEP 7:
IMPLEMENT ACTION PLAN



Stakeholders
Milestones
Status
Completion Date
Priority
Specific Action
Resources
Owner
Action Identifier
Dependencies
Rationale

Using the Framework improves communications and eases compliance



Regulators are using the Framework to increase efficiencies and decrease redundancy

- The Framework has been mapped to industry leading regulations
  - HIPAA
  - PCI
  - CIP 5
  - etc
- Organization not voluntarily aligning to the Framework may see increased burden demonstrating compliance

There are several resources available to help you use the Framework

- Government Programs
  - Department of Homeland Security's C3 Voluntary Program
  - NIST Industry Resources
- Internet Resource Centers
  - Cybersecurity Framework (CForum)

Apply: 70%+ of organizations can benefit from using the Framework

- Next week you should:
  - Prioritize and scope your organizations cybersecurity program
- In the first three months following this presentation you should:
  - Initiate a pilot implementation of the cybersecurity Framework
  - Understand areas of improvement within your organization
- Within six months you should:
  - Begin addressing the roadmap items
  - Expand on the pilot program throughout your organization

Q&A

Tom Conkle
Cybersecurity Engineer
G2, Inc.
@TomConkle

Greg Witte
Sr. Security Engineer
G2, Inc.
@thenetworkguy