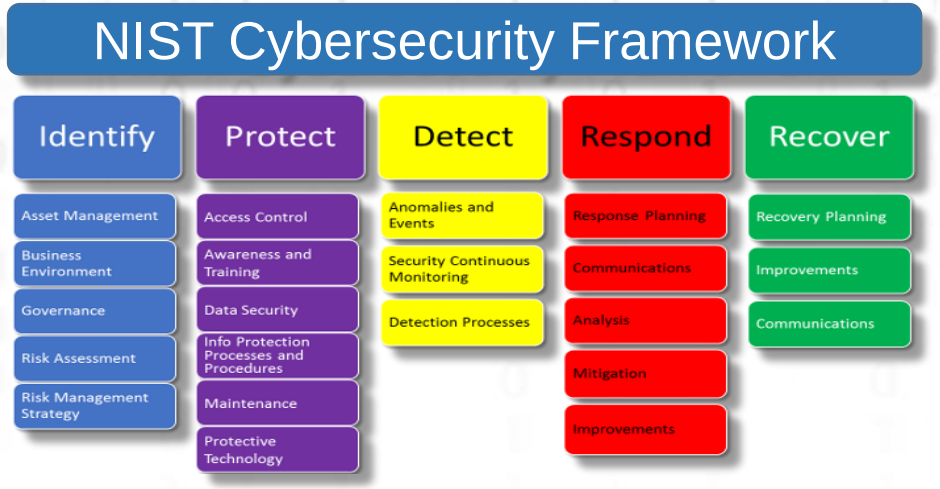
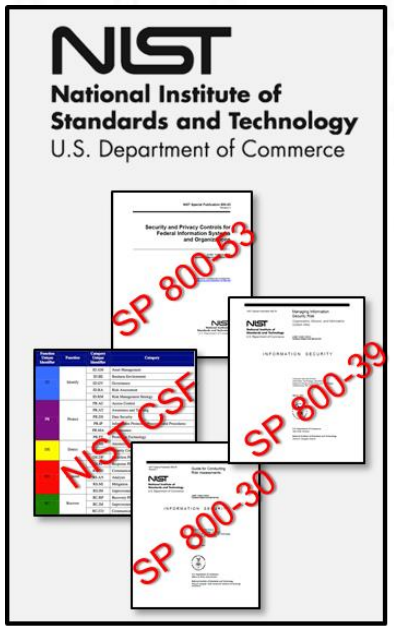
Cybersecurity Risk Management

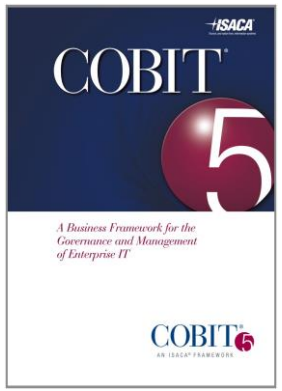
Through the Cybersecurity Framework

March 2018

There are hundreds if not thousands of controls and standards for implementing cybersecurity







Defining cybersecurity programs is typically done through compliance

G2 COMMERCIAL

HIPAA
Health Insurance Portability and Accountability Act

NIST
National Institute of Standards and Technology

NERC CIP v5

FedRAMP℠

Information Security Management System ISO 27001 Certified

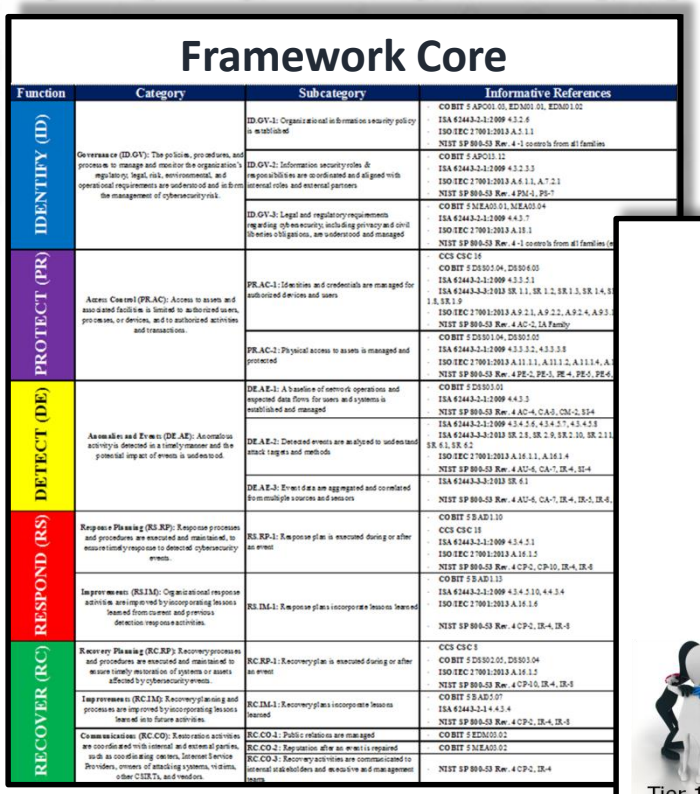
AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports ®

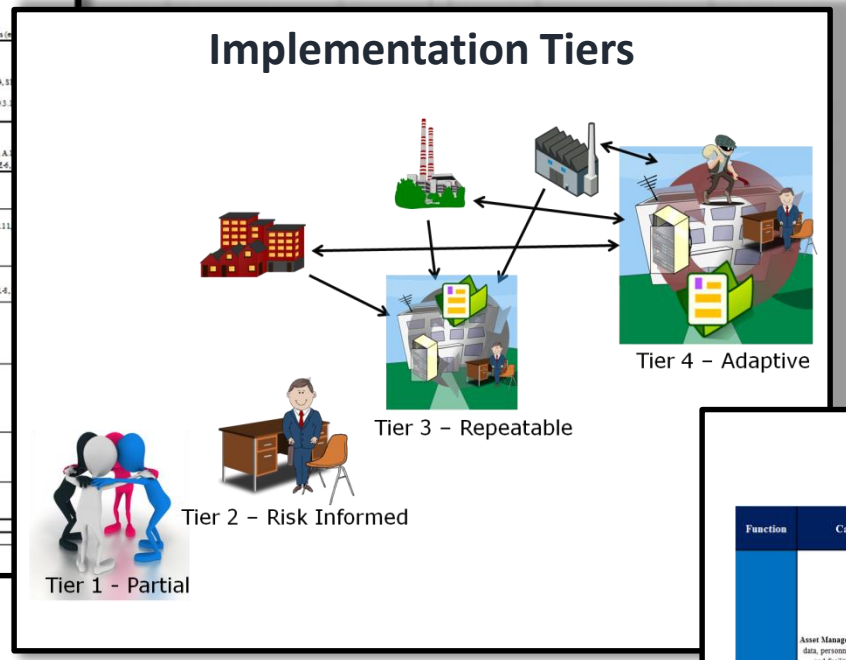
PCI COMPLIANT

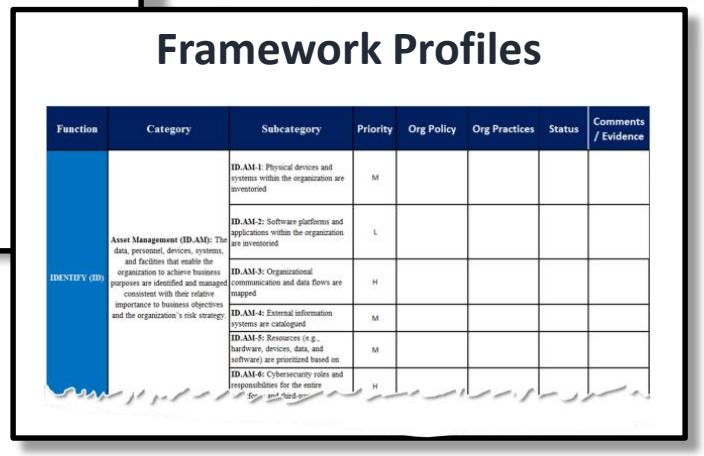
Compliance does not always mean secure

Other times security is not commensurate with the risk

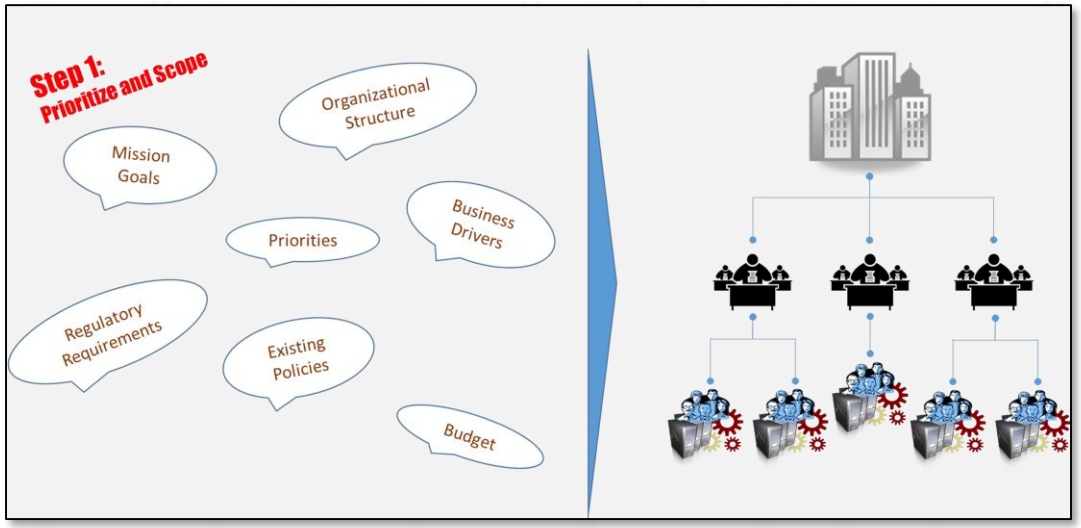
Our Cybersecurity Framework assessments uses all three components of the Framework

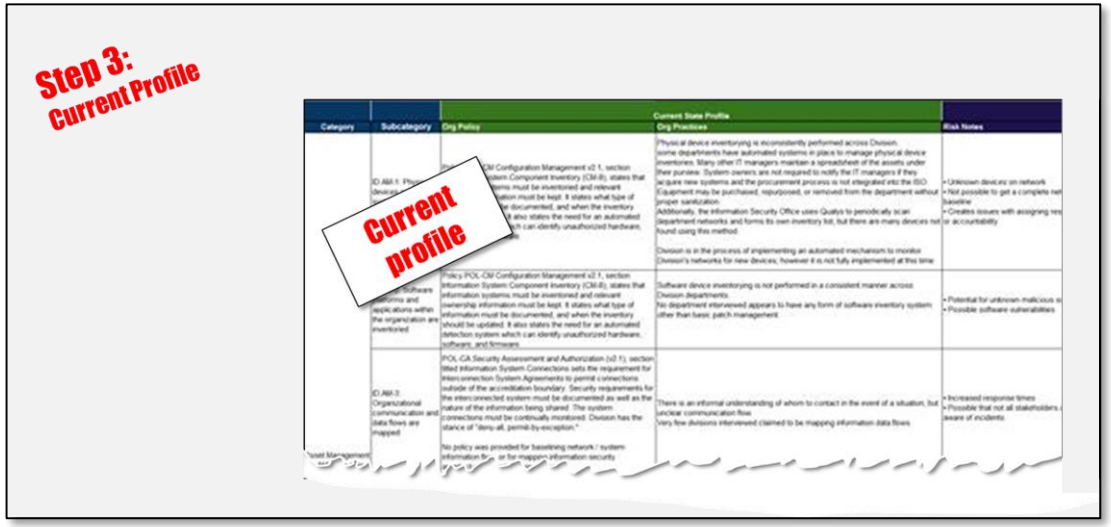






The Cybersecurity Framework defines a seven step implementation process





The risk register ensures proper cybersecurity considerations are prioritized and defined

STEP 4:
CONDUCT A RISK ASSESSMENT

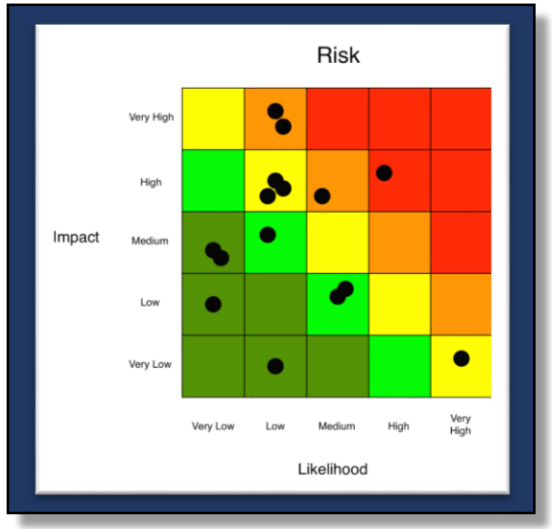
Risk #	Example Actor/Source	Risk Area	Risk Event	Likelihood	Impact	Notes
1	Internal (accidental, e.g., hw/software failure), Internal (deliberate), External (deliberate, e.g., malware,ransomware), 3rd Party (accidental), 3rd Party (deliberate)	Sensitive privacy-related electronic data	is wrongly disclosed			
2			is corrupted or modified without authorization			
3			is deleted without authorization			
4	Internal (accidental, e.g., hw/software failure), Internal (deliberate), External (deliberate, e.g., malware,ransomware), 3rd Party (accidental), 3rd Party (deliberate)	Sensitive research data	is wrongly disclosed			
5			is corrupted or modified without authorization			
6			is deleted without authorization			
7	Internal (accidental), Internal (deliberate), 3rd Party (accidental), 3rd Party (deliberate)	Staff member(s) or 3rd Party Provider(s) fail to comply with legal, contractual or regulatory requirements				

Likelihood – Identifies how often the threat is expected to act on resources

Impact – Assesses the effect the security risk will have on business functions and operations

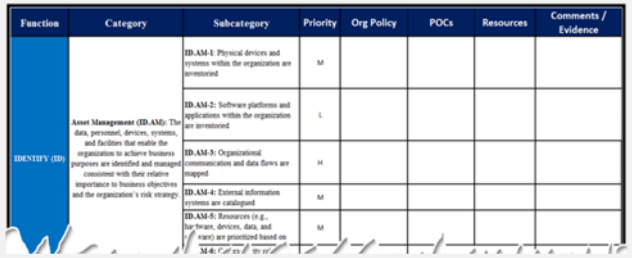
Security Risks are prioritized in the register

- Business objectives are addressed timely
- Properly define security countermeasures



The implementation steps conclude with an action plan for improving the cybersecurity program

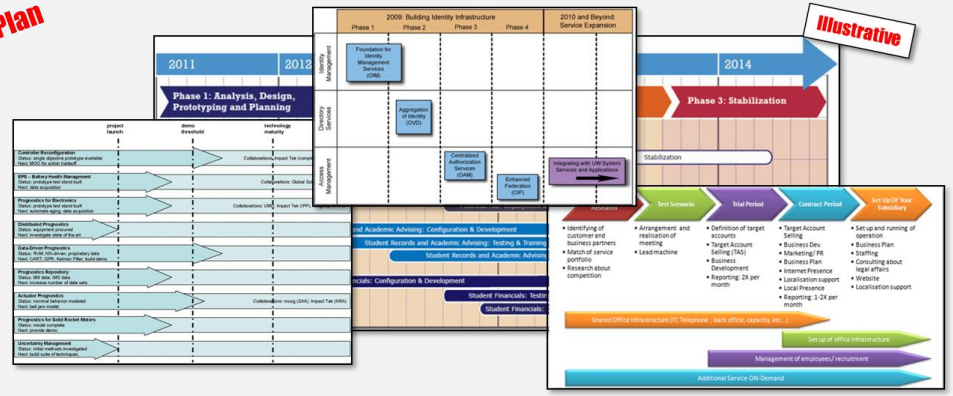
Step 5:
Create a Target Profile



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				

Step 6:
Determine, Analyze, and Prioritize Gaps

Step 7:
Implement Action Plan



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

Now your ready to successfully use the Framework to improve your cybersecurity program

Questions?

Tom Conkle
Cybersecurity Engineer
Tom.Conkle@G2-inc.com
(443) 292-6679