

Cybersecurity Risk Management

Through the Cybersecurity Framework

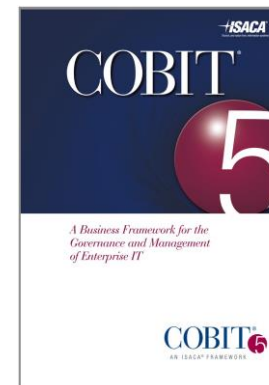
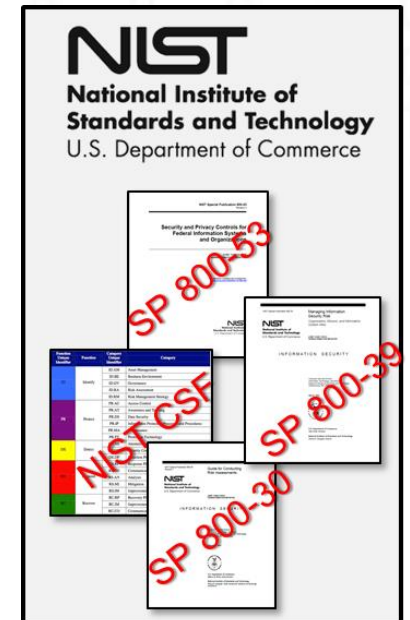
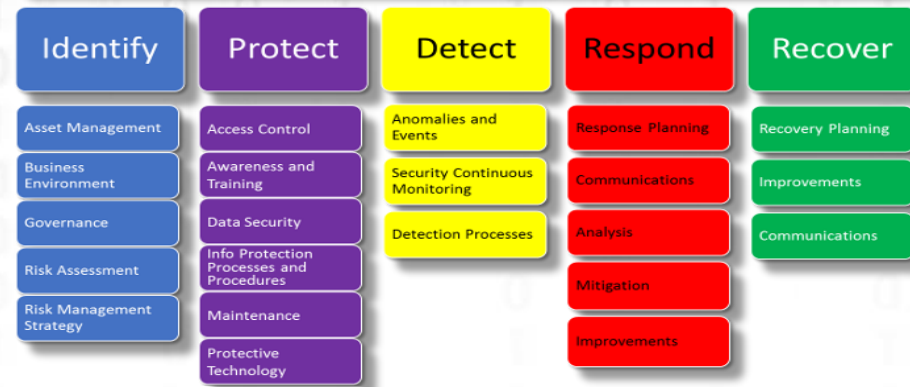
March 2018



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



NIST Cybersecurity Framework



Defining cybersecurity programs is typically done through compliance



NERC CIP v5



Compliance does not always mean secure



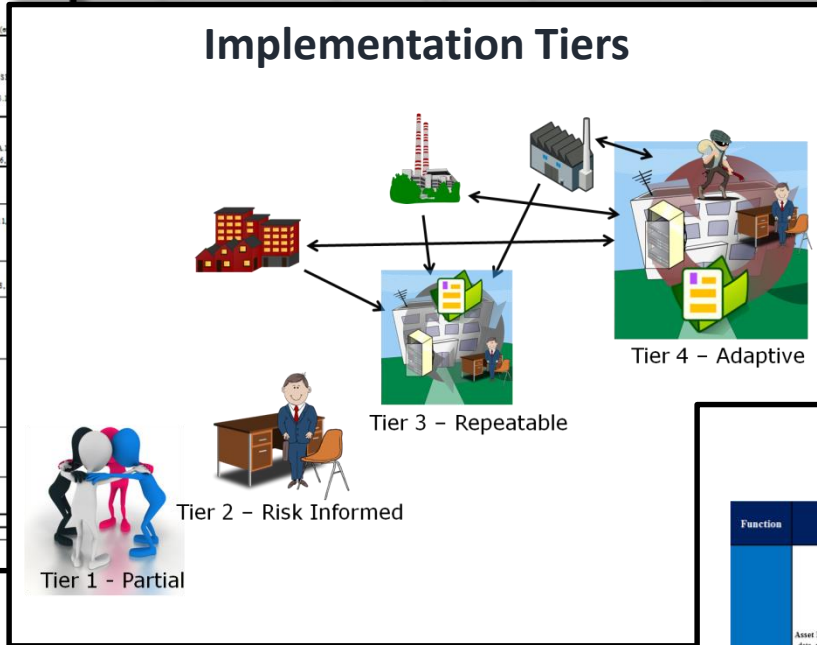
Other times security is not commensurate with the risk



Our Cybersecurity Framework assessments uses all three components of the Framework



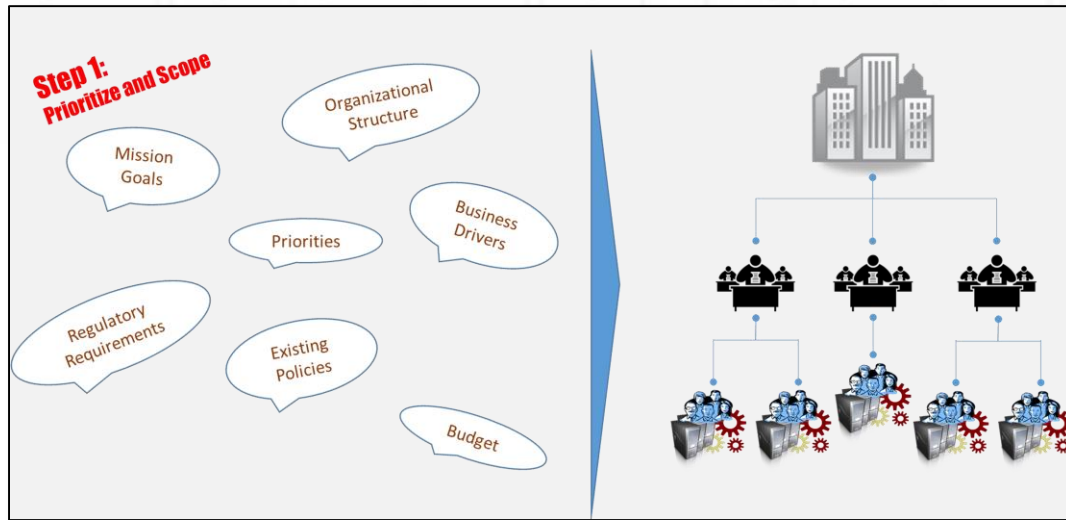
Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity.	ID.GV-1: Organizational information security policy is established	COBIT 5 APO10.01, ED2010.01, ED2010.02 ISA 63443-3-2:2009 4.3.2.4 ISO IEC 27001:2013 A.1.1.1 NIST SP 800-53 Rev. 4-1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with formal roles and external partners	COBIT 5 APO10.02 ISA 63443-3-2:2009 4.3.2.3.3 ISO IEC 27001:2013 A.6.1.1, A.7.2.1 NIST SP 800-53 Rev. 4 P24.4, P5-7
PROTECT (PR)	Access Controls (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: Identifiers and credentials are managed for authorized devices and users	COBIT 5 D0501.04, D0501.05 ISA 63443-3-2:2009 4.3.3.1.1 ISA 63443-3-2:2013 SR.11, SR.1.2, SR.1.3, SR.1.4, SR.1.5, SR.1.9 ISO IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3 NIST SP 800-53 Rev. 4 AC-2, IA Family
		PR.AC.2: Physical access to assets is managed and protected	COBIT 5 D0501.04, D0501.05 ISA 63443-3-2:2009 4.3.3.2, 4.3.3.3 ISO IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.5 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE.4, PE.5, PE.6
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity detected is a timely reason and the potential impact of events is understood.	DE.AE.1: A baseline of network operations and reported data flows for users and systems is established and managed	COBIT 5 D0501.01 ISA 63443-3-2:2009 4.4.3.3 NIST SP 800-53 Rev. 4 AC-CA.3, CM-2, IS.4 ISA 63443-3-2:2009 4.3.4.2.4, 4.3.4.3, 4.3.4.3.3 ISA 63443-3-2:2013 SR.2.3, SR.2.6, SR.2.10, SR.2.11, 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-4, CA-7, IX-4, IX-4
		DE.AE.2: Detected events are analyzed to understand attack targets and methods	COBIT 5 D0501.01 ISA 63443-3-2:2009 4.4.3.3 NIST SP 800-53 Rev. 4 AC-CA.3, CM-2, IS.4 ISA 63443-3-2:2013 SR.2.3, SR.2.6, SR.2.10, SR.2.11, 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-4, CA-7, IX-4, IX-4
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to assure timely response to detected cybersecurity events.	RS.RP.1: Response plan is executed during or after an event	COBIT 5 D0501.10 CCS CSC 15 ISA 63443-3-2:2009 4.5.4.1.1 ISO IEC 27001:2013 A.16.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-10, IX-4, IX-6
		RS.RP.2: Response plan is updated and maintained, to assure timely response to detected cybersecurity events	COBIT 5 D0501.11 ISA 63443-3-2:2009 4.5.4.2.10, 4.4.3.4 ISO IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IX-4, IX-6
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	COBIT 5 D0501.13 ISA 63443-3-2:2009 4.5.4.3.10, 4.4.3.4 ISO IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IX-4, IX-6
		RC.RP.2: Recovery plan is updated and maintained, to ensure timely restoration of systems or assets affected by cybersecurity events	COBIT 5 D0501.13 ISA 63443-3-2:2009 4.5.4.3.10, 4.4.3.4 ISO IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IX-4, IX-6
RECOVER (RC)	Communication (RC.CO): Two-way activities are coordinated with external stakeholders, 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 D0501.02 NIST SP 800-53 Rev. 4 CP-2, IX-4
		RC.CO.2: Responses after an event is reported	COBIT 5 D0501.02 NIST SP 800-53 Rev. 4 CP-2, IX-4
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	COBIT 5 D0501.10 CCS CSC 15 ISA 63443-3-2:2009 4.5.4.1.1 ISO IEC 27001:2013 A.16.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-10, IX-4, IX-6
		RC.RP.2: Response plan is updated and maintained, to assure timely response to detected cybersecurity events	COBIT 5 D0501.11 ISA 63443-3-2:2009 4.5.4.2.10, 4.4.3.4 ISO IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IX-4, IX-6



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 cataloged	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 organization are established	H				

The Cybersecurity Framework defines a seven step implementation process



Step 3: Current Profile

Category	Subcategory	Org Policy	Current State Profile	Risk Notes
Asset Management	ICM-1: Physical Devices	ICM-1: Physical Devices (ICM-1) states that equipment must be inventoried and when the inventory should be updated. It also states the need for an automated detection system which can identify unauthorized hardware.	Physical device inventorying is inconsistently performed across Division. Some departments have automated systems in place to manage physical device inventories. Many other IT managers maintain a spreadsheet of the assets under their purview. System owners are not required to notify the IT managers if they acquire new systems and the procurement process is not integrated into the ICM. Equipment may be purchased, repositioned, or removed from the department without proper justification. Additionally, the Information Security Office uses Qualtrics to periodically scan department networks and forms its own inventory list, but there are many devices not found using this method.	<ul style="list-style-type: none"> Division devices on network Not possible to get a complete net baseline Creates issues with assigning res or accountability
	ICM-2: Software	ICM-2: Software (ICM-2) states that information systems must be inventoried and relevant ownership information must be kept. It states what type of information must be documented, and when the inventory should be updated. It also states the need for an automated detection system which can identify unauthorized hardware, software, and firmware.	Software device inventorying is not performed in a consistent manner across Division departments. The department interviewed appears to have any form of software inventory system other than basic patch management.	<ul style="list-style-type: none"> Potential for unknown malicious Possible software vulnerabilities
	ICM-3: Organizational Communication and Data Flows are mapped	ICM-3: Organizational Communication and Data Flows are mapped (ICM-3) states that information system connections to permit connections outside of the accreditation boundary. Security requirements for the interconnected system must be documented as well as the nature of the information being shared. The system connections must be continuously monitored. Division has the stance of "deny all, permit by exception."	There is an informal understanding of whom to contact in the event of a situation, but unclear communication flow. Very few divisions interviewed claimed to be mapping information data flows.	<ul style="list-style-type: none"> Increased response times Possible that not all stakeholders aware of incidents

Current profile

The risk register ensures proper cybersecurity considerations are prioritized and defined



**STEP 4:
CONDUCT A RISK ASSESSMENT**

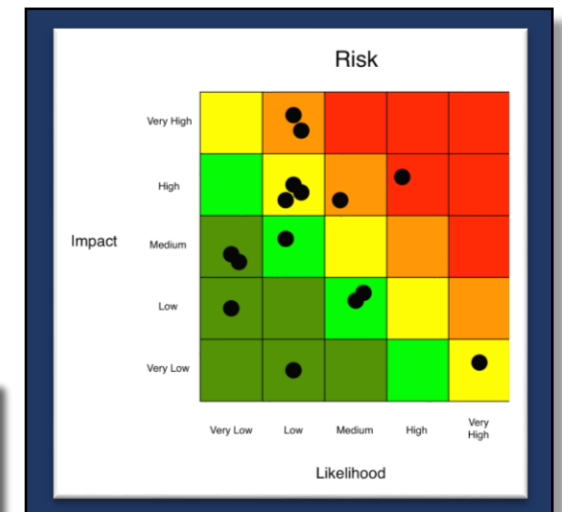
Risk #	Example Actor/Source	Risk Area	Risk Event	Likelihood	Impact	Notes
1	Internal (accidental, e.g., hw/software failure), Internal (deliberate),	Sensitive privacy-related electronic data	is wrongly disclosed			
2	External (deliberate, e.g., malware,ransomware), 3rd Party (accidental), 3rd Party (deliberate)		is corrupted or modified without authorization			
3			is deleted without authorization			
4	Internal (accidental, e.g., hw/software failure), Internal (deliberate),	Sensitive research data	is wrongly disclosed			
5	External (deliberate, e.g., malware,ransomware), 3rd Party (accidental), 3rd Party (deliberate)		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				

Security Risks are prioritized in the register

- Business objectives are addressed timely
- Properly define security countermeasures

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



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



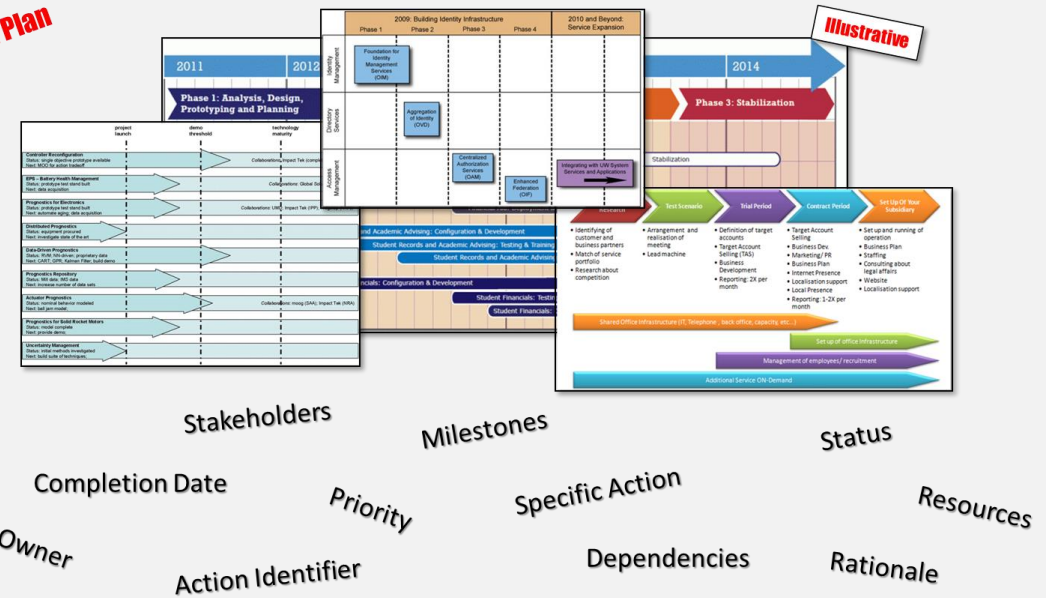
Step 5: Create a Target Profile

Function	Category	Subcategory	Priority	Org Policy	POCs	Resources	Comments / Evidence
IDENTITY (ID)	Asset Management (IDAM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed in accordance with their relative importance to business objectives and the organization's risk strategy.	IDAM 1: Physical devices and systems within the organization are inventoried.	M				
		IDAM 2: Software platforms and applications within the organization are inventoried.	L				
		IDAM 3: Organizational communication and data flows are mapped.	H				
		IDAM 4: External information systems are cataloged.	M				
		IDAM 5: Resources (e.g., the device, device, data, and IP) are inventoried based on M4: Criticality of assets.	M				

Step 6: Determine, Analyze, and Prioritize Gaps



Step 7: Implement Action Plan



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