Experis™
Finance
ManpowerGroup

Assessing Cyber Risk

Challenges and Solutions

Stephen Head | Director | Experis Finance

Meet Our Presenter

Stephen Head, CISSP, CISM, CISA

Director, IT Risk Advisory Services
Experis Finance

Agenda

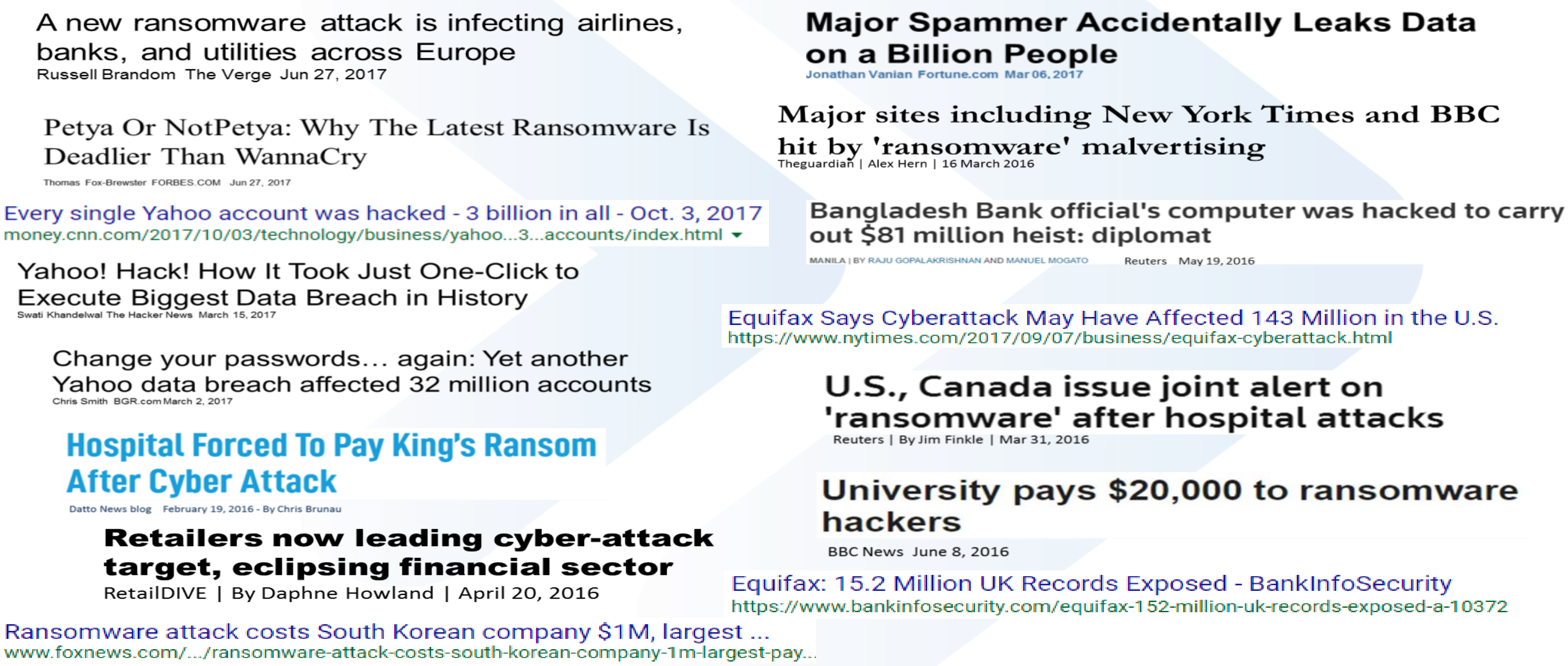
- Threats and Root Causes of Breaches
- The Changing Regulatory Landscape
- Security Frameworks and Tools
- Practical Ways to Assess your Risk and Organizational Exposure
- Key Elements of a Successful Cyber Risk Management Program

Threats and Root Causes of Breaches

Why is Cyber Risk Important?

- Financial risk / loss
- Business interruption
- Reputational / brand risk
- Regulatory risk / requirements
- Liability of Board / Management
- Technology proliferation / Internet of Things (IoT)
  - Third-party / outsourced service providers
  - Sensor proliferation
  - Drone technologies
  - Alternative payment systems
  - Use of contractors

Headlines Highlight Increased Cyber Risk



A new ransomware attack is infecting airlines, banks, and utilities across Europe
Russell Brandom The Verge Jun 27, 2017

Petya Or NotPetya: Why The Latest Ransomware Is Deadlier Than WannaCry
Thomas Fox-Brewster FORBES.COM Jun 27, 2017

Every single Yahoo account was hacked - 3 billion in all - Oct. 3, 2017
money.cnn.com/2017/10/03/technology/business/yahoo...3...accounts/index.html ▾

Yahoo! Hack! How It Took Just One-Click to Execute Biggest Data Breach in History
Swati Khandelwal The Hacker News March 15, 2017

Change your passwords… again: Yet another Yahoo data breach affected 32 million accounts
Chris Smith BGR.com March 2, 2017

Hospital Forced To Pay King's Ransom After Cyber Attack
Datto News blog February 19, 2016 - By Chris Brunau

Retailers now leading cyber-attack target, eclipsing financial sector
RetailDIVE | By Daphne Howland | April 20, 2016

Ransomware attack costs South Korean company $1M, largest ...
www.foxnews.com/.../ransomware-attack-costs-south-korean-company-1m-largest-pay...

Major Spammer Accidentally Leaks Data on a Billion People
Jonathan Vanian Fortune.com Mar 06, 2017

Major sites including New York Times and BBC hit by 'ransomware' malvertising
Theguardian | Alex Hern | 16 March 2016

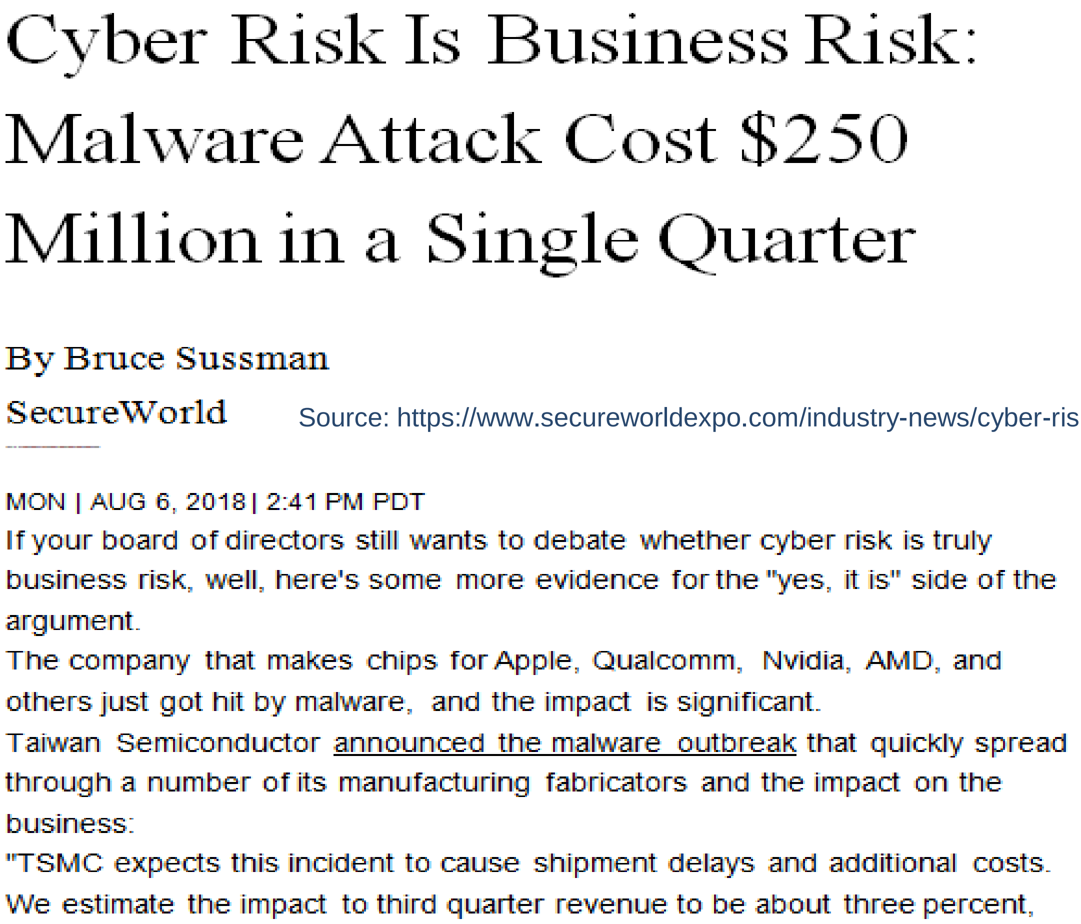
Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat
MANILA | BY RAJU GOPALAKRISHNAN AND MANUEL MOGATO Reuters May 19, 2016

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.
https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

U.S., Canada issue joint alert on 'ransomware' after hospital attacks
Reuters | By Jim Finkle | Mar 31, 2016

University pays $20,000 to ransomware hackers
BBC News June 8, 2016

Equifax: 15.2 Million UK Records Exposed - BankInfoSecurity
https://www.bankinfosecurity.com/equifax-152-million-uk-records-exposed-a-10372



Cyber Risk Is Business Risk: Malware Attack Cost $250 Million in a Single Quarter

By Bruce Sussman

SecureWorld

Source: https://www.secureworldexpo.com/industry-news/cyber-risk-is-business-risk

MON | AUG 6, 2018 | 2:41 PM PDT

If your board of directors still wants to debate whether cyber risk is truly business risk, well, here's some more evidence for the "yes, it is" side of the argument.

The company that makes chips for Apple, Qualcomm, Nvidia, AMD, and others just got hit by malware, and the impact is significant.

Taiwan Semiconductor announced the malware outbreak that quickly spread through a number of its manufacturing fabricators and the impact on the business:

"TSMC expects this incident to cause shipment delays and additional costs. We estimate the impact to third quarter revenue to be about three percent,

Not IF, but WHEN You Will Be Attacked

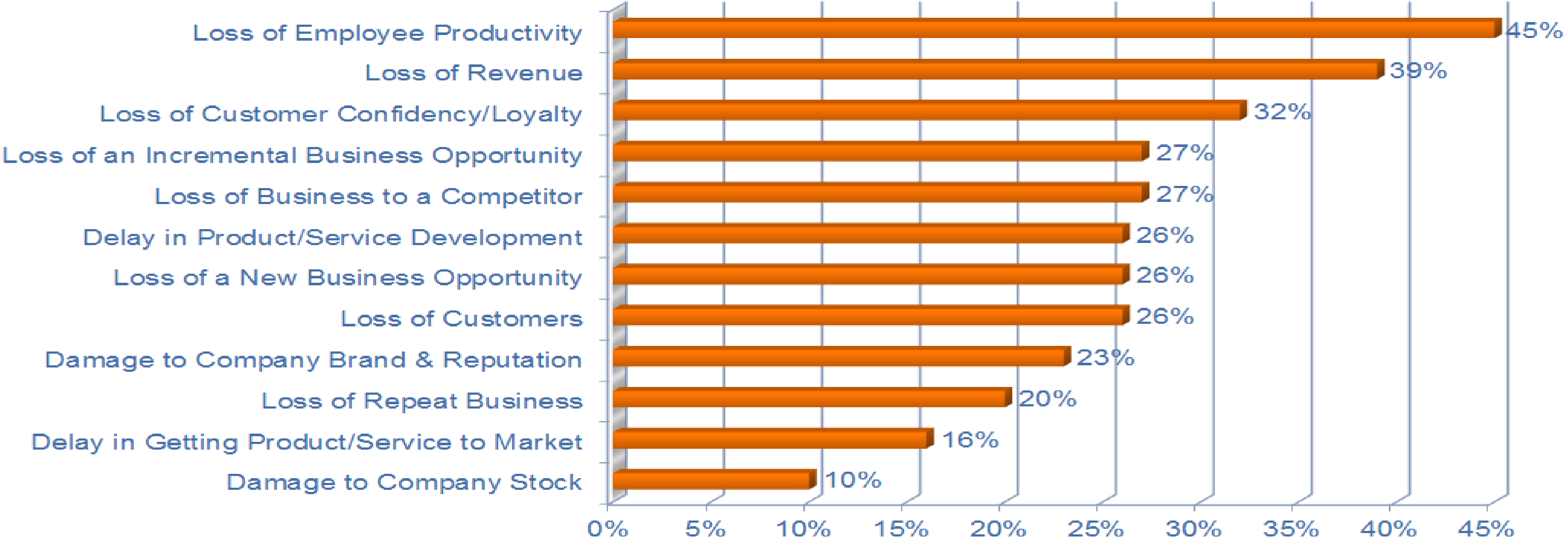
Pundits extoll the costs of breaches and cyber attacks, but few offer anything beyond anecdotal data collected through surveys. According to the Ponemon Institute, as of 2018:

- $3.86 million is the average total cost of a data breach
- 6.4% increase in the total cost of a data breach since 2017
- $148 is the average cost per lost or stolen record

The only cost that truly matters is the one your organization must deal with!

Source: Ponemon Institute

Data Losses Are Only One Aspect of a Broader Issue



Source: http://www.emc.com/collateral/other/emc-trust-curve-es.pdf

Attackers, Targets and Motivations are Evolving

Threat Actors	Motives	Attack Targets	Risks
Nation State	• Political Agenda • Military Agenda • Economic Harm	• Intellectual Property • Sensationalism • Critical Infrastructure	• Competitive Impact • Service Disruptions • Design Disclosure
Criminal Underground	• Theft • Fraud • Ransom	• Personal Information • Credit Card Data • Device Manipulation	• Regulatory Sanctions • Lawsuits • Loss of Reputation
Hactivists	• Political Agenda • Personal Agenda • Social Change	• Corporate Sensitive • Key Employee Information	• Brand Damage • Business Disruption • Loss of Reputation
Lone Wolves	• Thrill Seeking • Personal Gain • Social Status	• Device Control • Vandalism • Harassment	• Business Disruption • Brand Damage • Personal Safety
Insiders	• Financial Gain • Social/Political Gain • Revenge	• Device Control • Vandalism • Harassment	• Competitive Impact • Business Disruption • Loss of Reputation

Anatomy of an Attack

Each attack type is unique, but most have a similar structure

	Planning/Information Gathering	Initial Attack and Breach	Establish Command and Control	Additional Exploitation	Data Exfiltration and Persistence
Phases	Information available on the internet Information coerced via various means	Identify vulnerable systems, services, processes Gain access to internal network or systems	Establish a means of controlling "base" for gathering more network details and exploitation Malware takes effect	Search for information sources Additional credentials/ authorizations Attempt additional exploits	Remove or extract data obtained Avoid discovery
Example	Identify Employees and Contact Information	Create a spoofed web site Send malicious link Wait for results	Test for access, connectivity, conduct scans, identify resources	Identify additional vulnerabilities, execute exploits, collect information	Identify additional vulnerabilities

The right sensors ***when monitored and acted upon*** *can prevent or detect attacks at each critical phase*

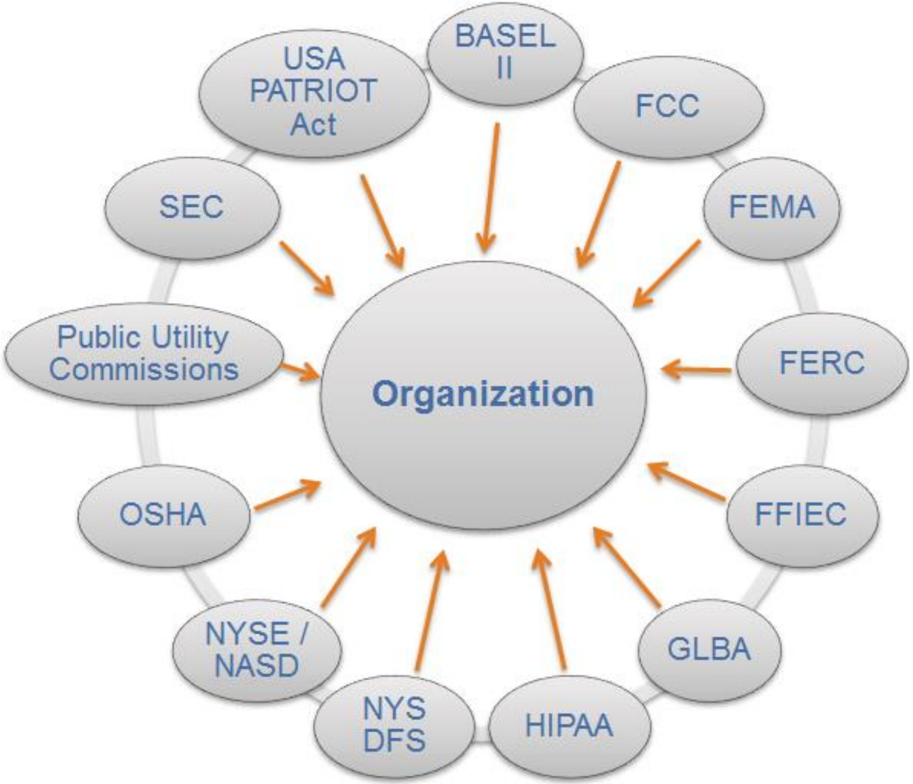
The Changing Regulatory Landscape

What Regulators are Saying

- Cybercriminals can cause significant financial losses for regulated entities as well as for consumers whose private information may be revealed and/or stolen for illicit purposes.
- The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark.
- Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted.

Source: New York State DFS 23 NYCRR 500

Regulatory Risk / Requirements



GDPR

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for individuals in the EU and the European Economic Area. Critical compliance and regulatory changes it entails are:

- Clear consent required to collect and use data.
- Limitations on automated data processing for decision making.
- Right to rectify and restrict data usage, and the right to be forgotten.
- Transparency and accountability about processing.
- ‘Right to portability’, to migrate data between service providers.
- Data access denial procedures to be as simple as data collection.
- ‘Right to notification’ if data is compromised.
- Stricter safeguards for transfers of personal data outside the EU.

Security Frameworks and Tools

NIST

- National Institute of Standards and Technology
- Part of the U.S. Department of Commerce
- NIST’s mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.
- 3,000 employees
- 2,700 guest researchers
- Two main locations: Gaithersburg, MD and Boulder, CO

NIST Priority Research Areas

Advanced Manufacturing

IT and Cybersecurity

Healthcare

Forensic Science

Disaster Resilience

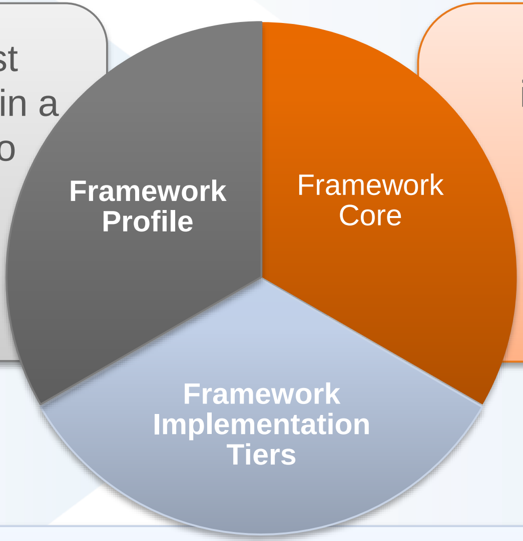
Cyber-physical Systems

Advanced Communications

NIST Framework Components

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs



Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

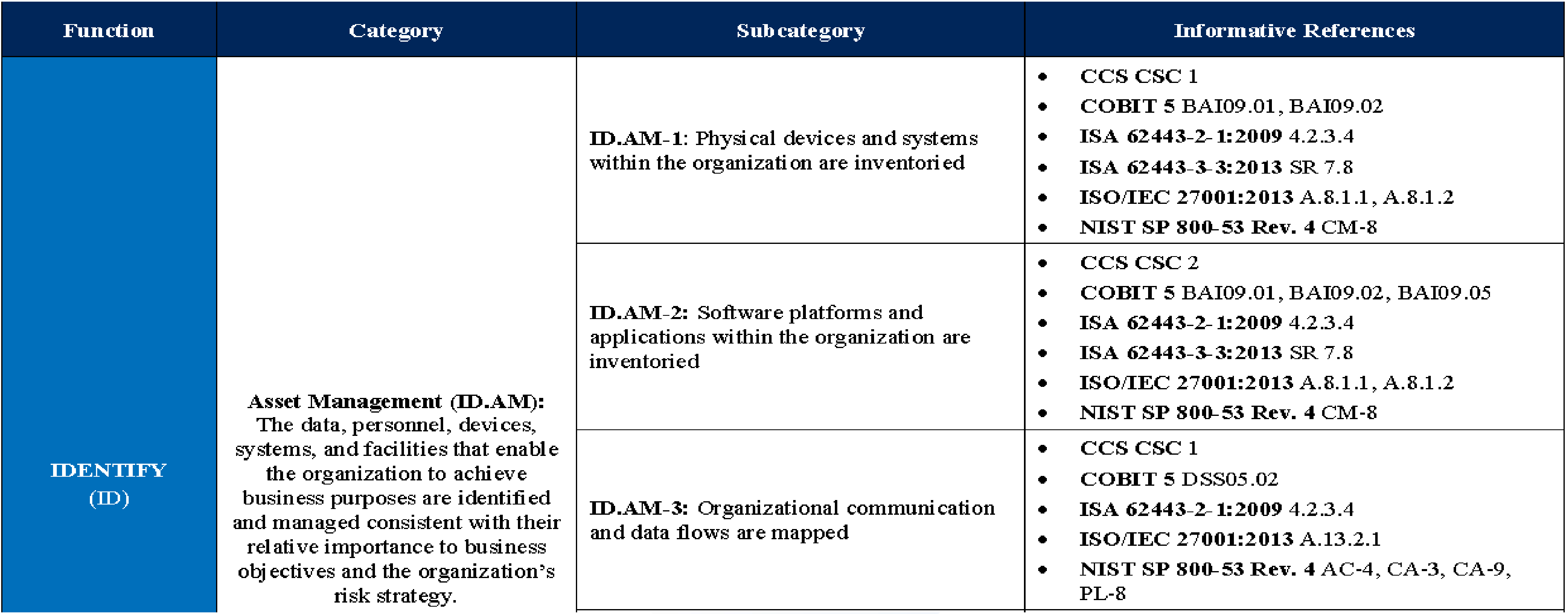
Source: NIST Cybersecurity Framework

NIST Cybersecurity Framework

Each NIST function has multiple categories subdividing the cybersecurity requirements into more detailed groups of activities. These categories are further divided into over 100 subcategories.

Identify	Protect	Detect	Respond	Recover
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Supply Chain Risk Management	• Identity Management & Access Control • Awareness & Training • Data Security • Information Protection Processes & Procedures • Maintenance • Protective Technology	• Anomalies & Events • Security Continuous Monitoring • Detection Processes	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvements • Communications
What assets need protection?	What safeguards are available?	What techniques can identify incidents?	What techniques can contain the impact of incidents?	What techniques can restore capabilities?

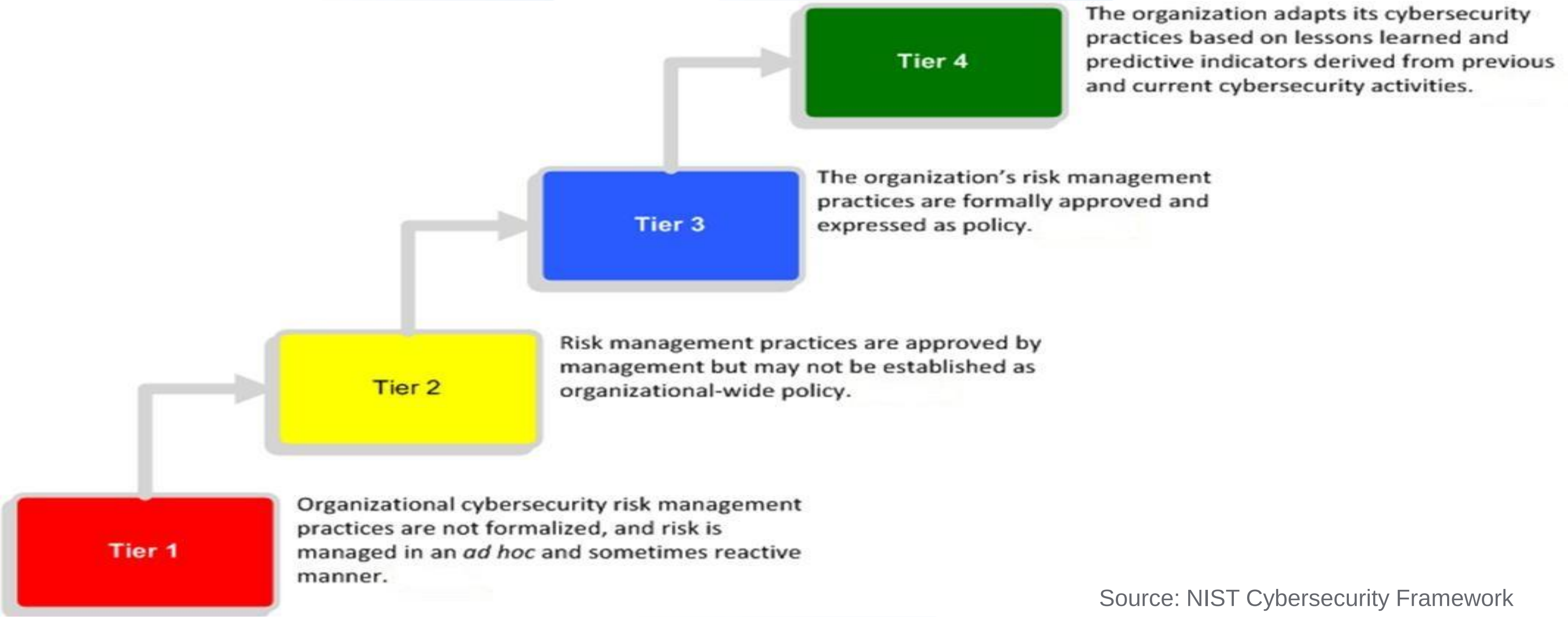
NIST Framework Core Excerpt



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

Source: NIST Cybersecurity Framework

NIST Implementation Tiers



Tier 4

The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.

Tier 3

The organization's risk management practices are formally approved and expressed as policy.

Tier 2

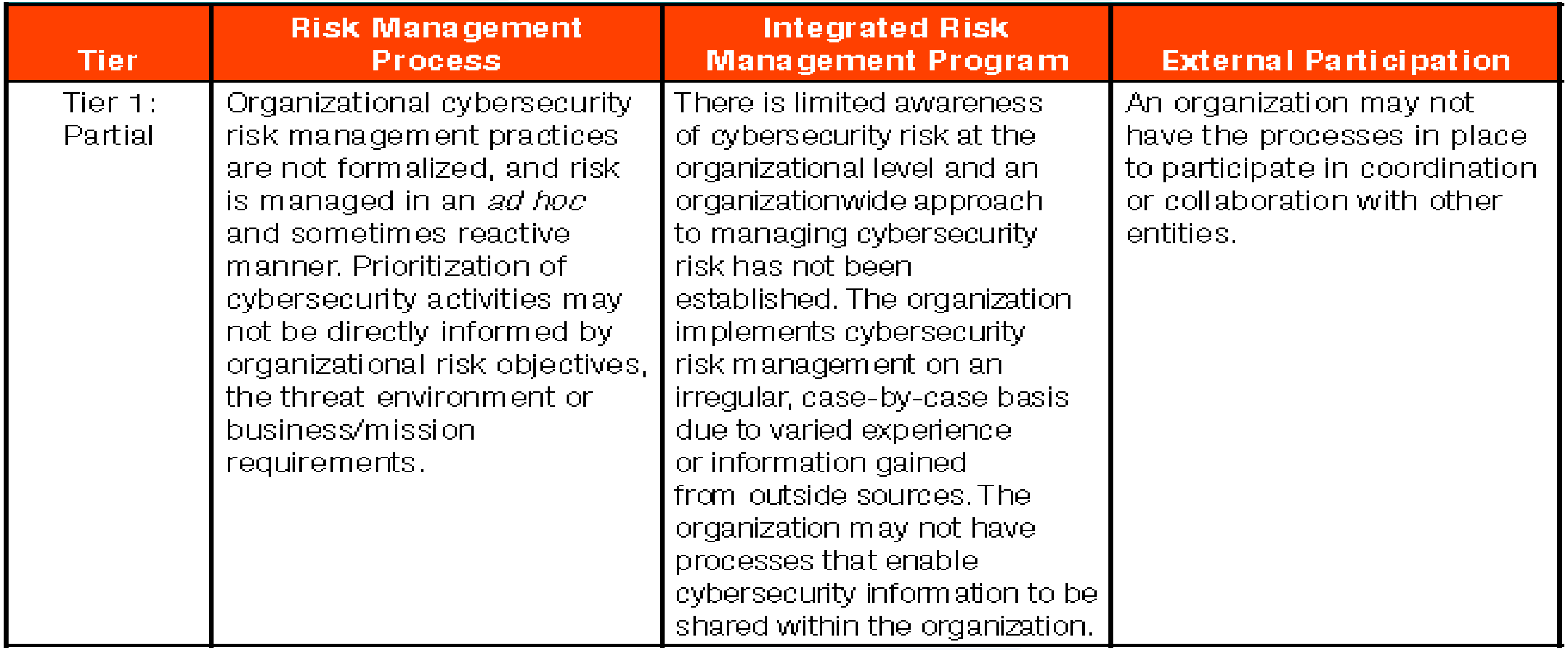
Risk management practices are approved by management but may not be established as organizational-wide policy.

Tier 1

Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner.

Source: NIST Cybersecurity Framework

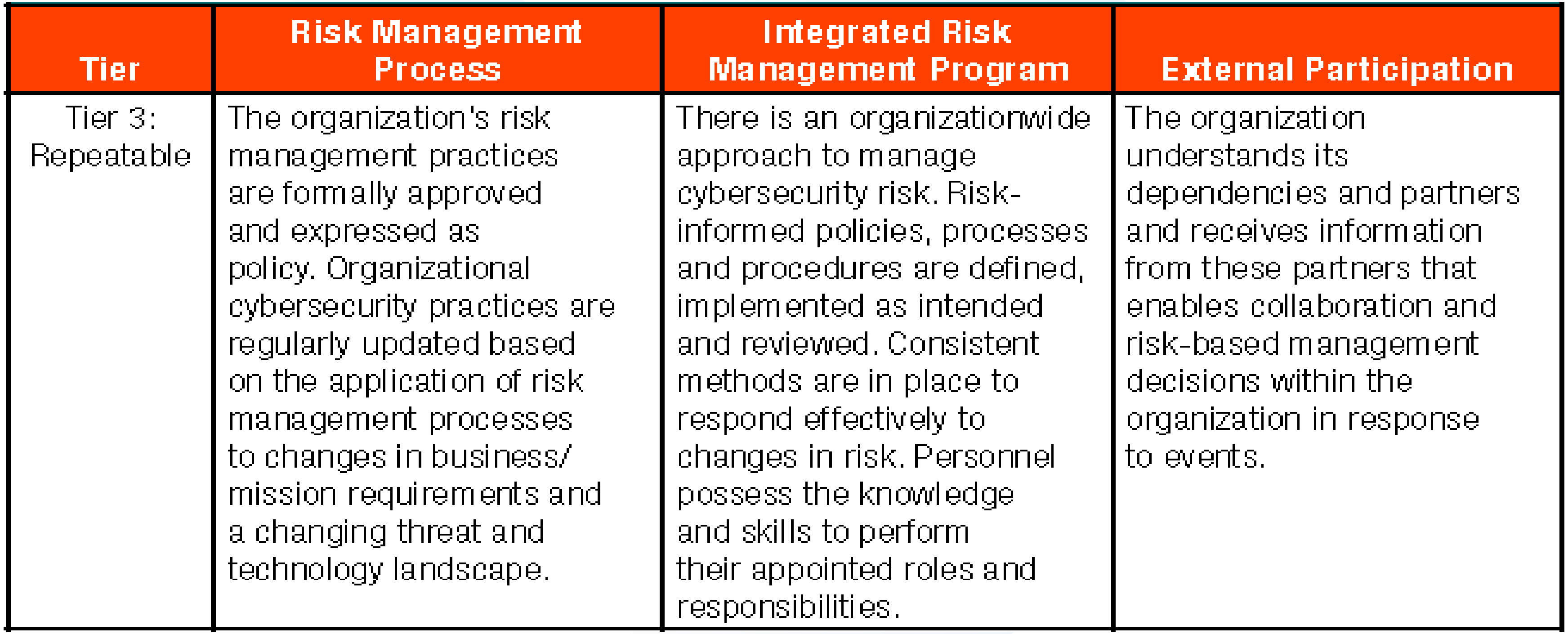
Criteria for Tier 1



Tier	Risk Management Process	Integrated Risk Management Program	External Participation
Tier 1: Partial	Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment or business/mission requirements.	There is limited awareness of cybersecurity risk at the organizational level and an organizationwide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.	An organization may not have the processes in place to participate in coordination or collaboration with other entities.

Source: NIST Cybersecurity Framework

Criteria for Tier 3



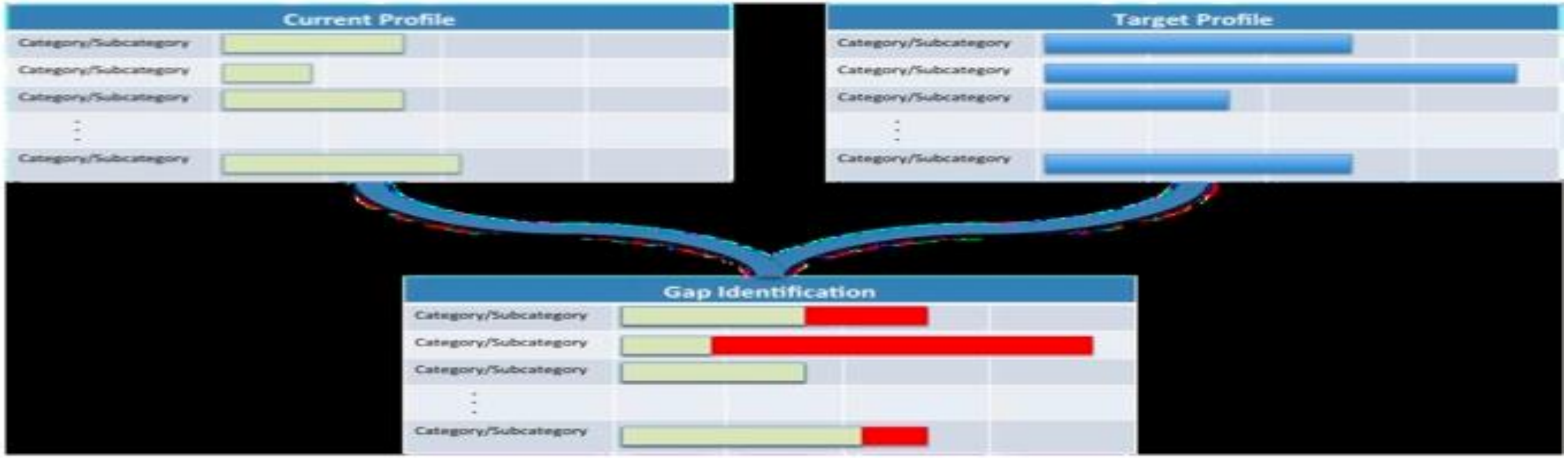
Tier	Risk Management Process	Integrated Risk Management Program	External Participation
Tier 3: Repeatable	The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/ mission requirements and a changing threat and technology landscape.	There is an organizationwide approach to manage cybersecurity risk. Risk-informed policies, processes and procedures are defined, implemented as intended and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.	The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

Source: NIST Cybersecurity Framework

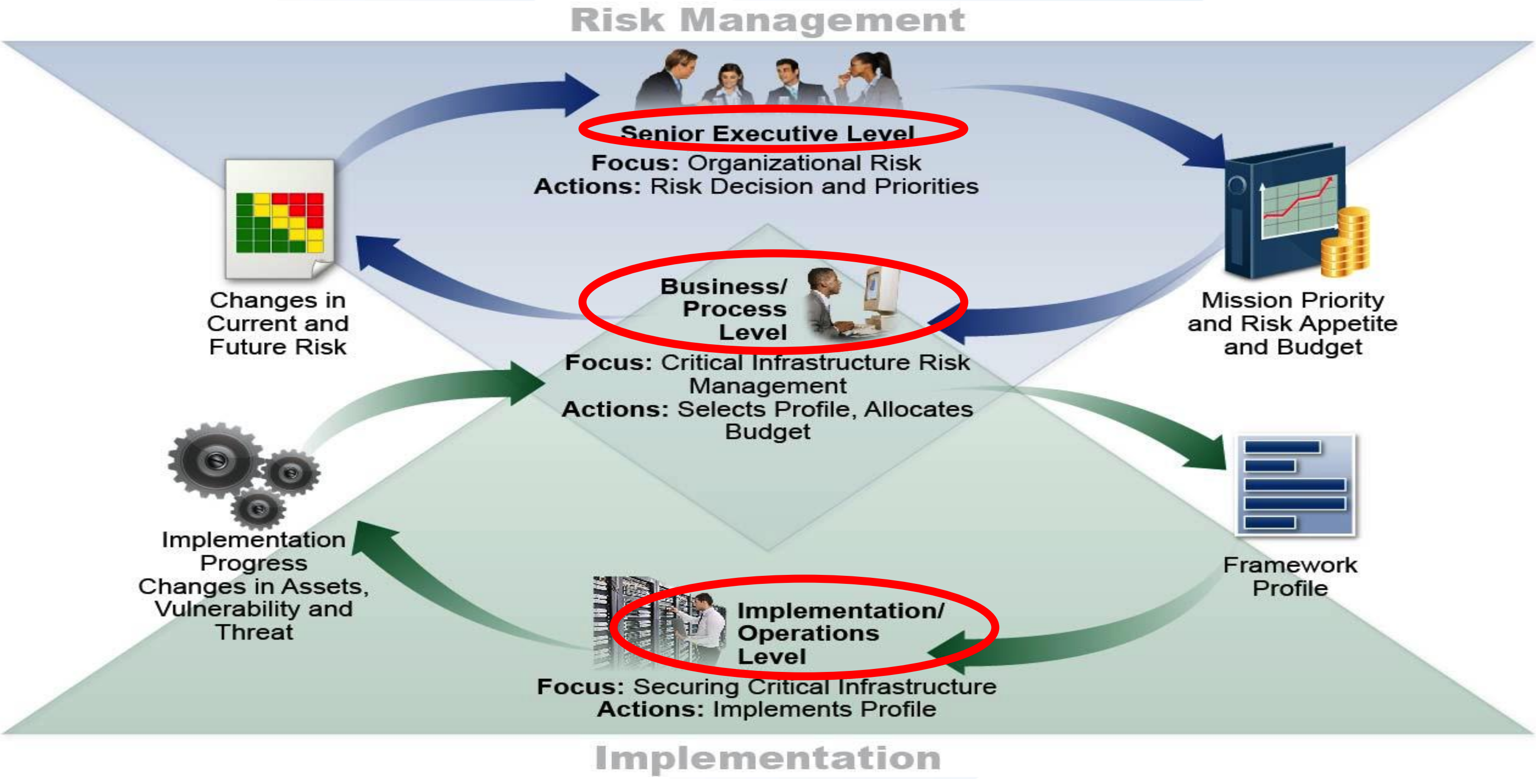
NIST Framework Profile

- Enables organizations to **establish a roadmap for reducing cybersecurity risk** that is aligned with organizational goals, considers legal/regulatory requirements and industry best practices, and reflects the risk management priorities of the organization

- Used to describe **current state and the desired target state** of cybersecurity activities



Framework Scope: Executives to Operations


Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Risk Decision and Priorities
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profile
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

Why Adopt the NIST Framework?

Benefits	Features
• Reduces time and expense of starting an information security program • Reduces risk within current information security programs by identifying areas for improvement • Increases efficiencies and reduce the possibility of miscommunication within your information security program and with other organizations such as partners, suppliers, regulators, and auditors	• Organizes reconciliation and reducing conflicts between legislation, regulation, policy, and industry best practice (Core) • Guides organization and management of and information security program (Core) • Measures current state and expresses desired state (Profile) • Provides justification for investment decisions to address gaps in current state (Profile) • Communicates cybersecurity requirements with stakeholders, including partners and suppliers (Profile) • Enables informed trade-off analysis of expenditure versus risk (Tiers)

What is the FFIEC CAT?

- The Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool (Assessment) to help institutions identify their risks and determine their cybersecurity maturity. The methodology provides a repeatable process to measure your cybersecurity preparedness over time
- The FFIEC Assessment is much more detailed than NIST. The NIST Framework only looks at 100+ controls, while the FFIEC Assessment looks at 494 different controls, which they refer to as declarative statements.

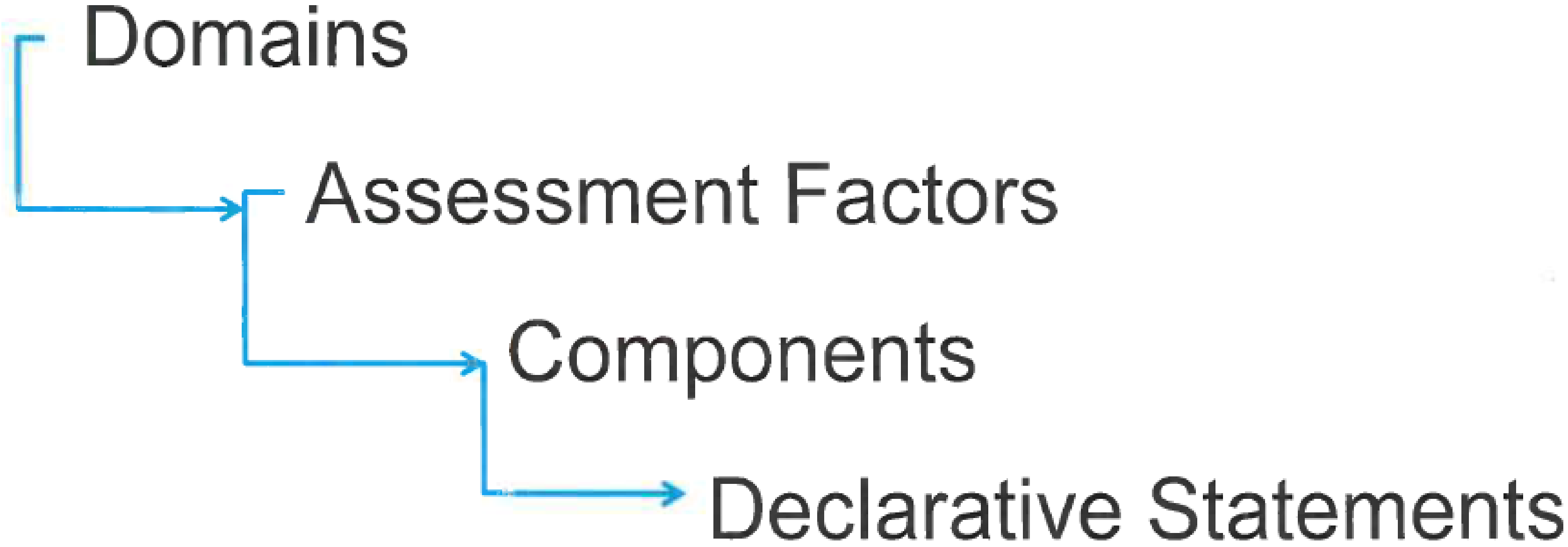
The FFIEC Tool Has Two Components

- **Inherent Risk Profile**
  - What is your organization’s degree of exposure to cyber risks (based on type, volume, an complexity of operations)?
- **Cybersecurity Maturity**
  - Based on the inherent risk profile, what level of control is needed?
  - Organizations subject to higher risk require more sophisticated control mechanisms.

FFIEC Risk/Maturity Relationship

		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level for Each Domain	Innovative				🟦	🟦
	Advanced			🟦	🟦	🟦
	Intermediate		🟦	🟦	🟦	
	Evolving	🟦	🟦	🟦		
	Baseline	🟦	🟦			

FFIEC Cybersecurity Assessment Structure



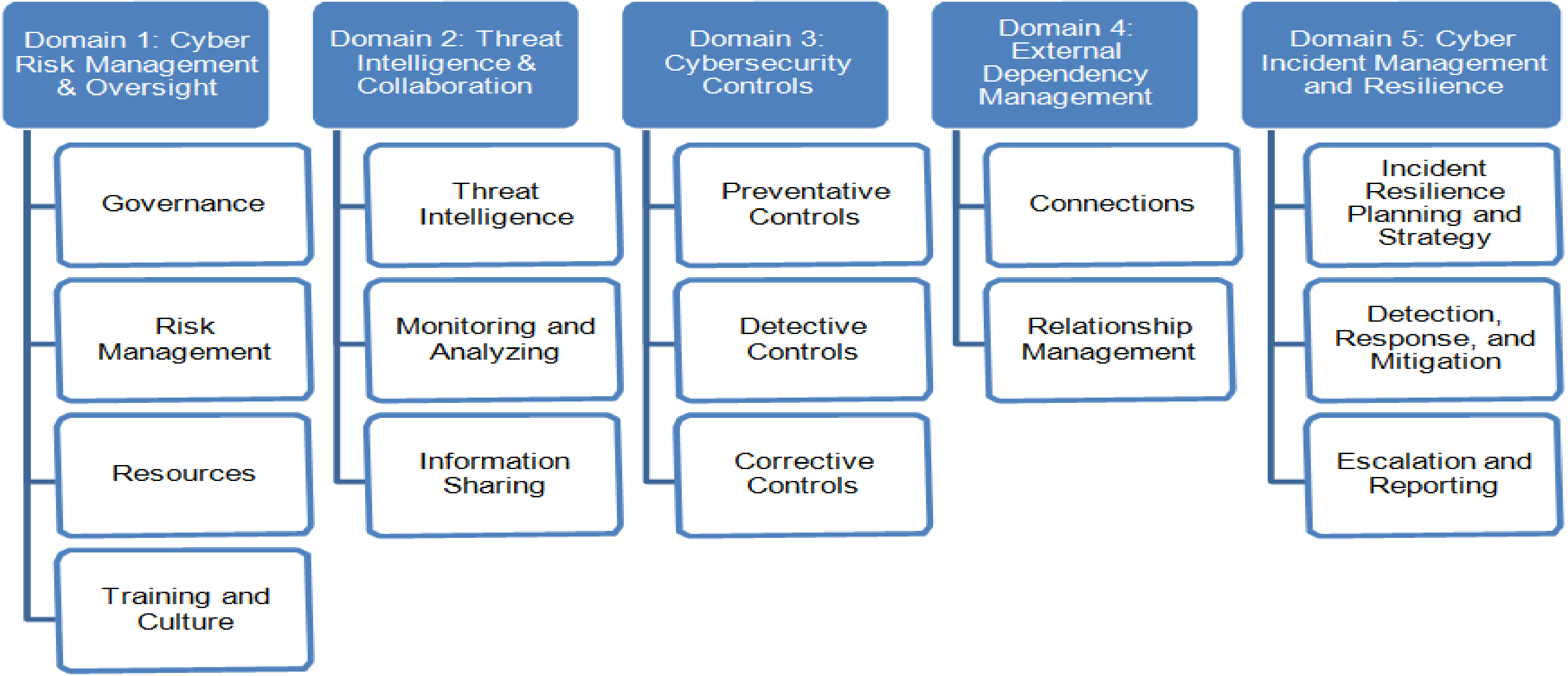
Domains

Assessment Factors

Components

Declarative Statements

Domains and Assessment Factors



Domain 1: Cyber Risk Management & Oversight
- Governance
- Risk Management
- Resources
- Training and Culture

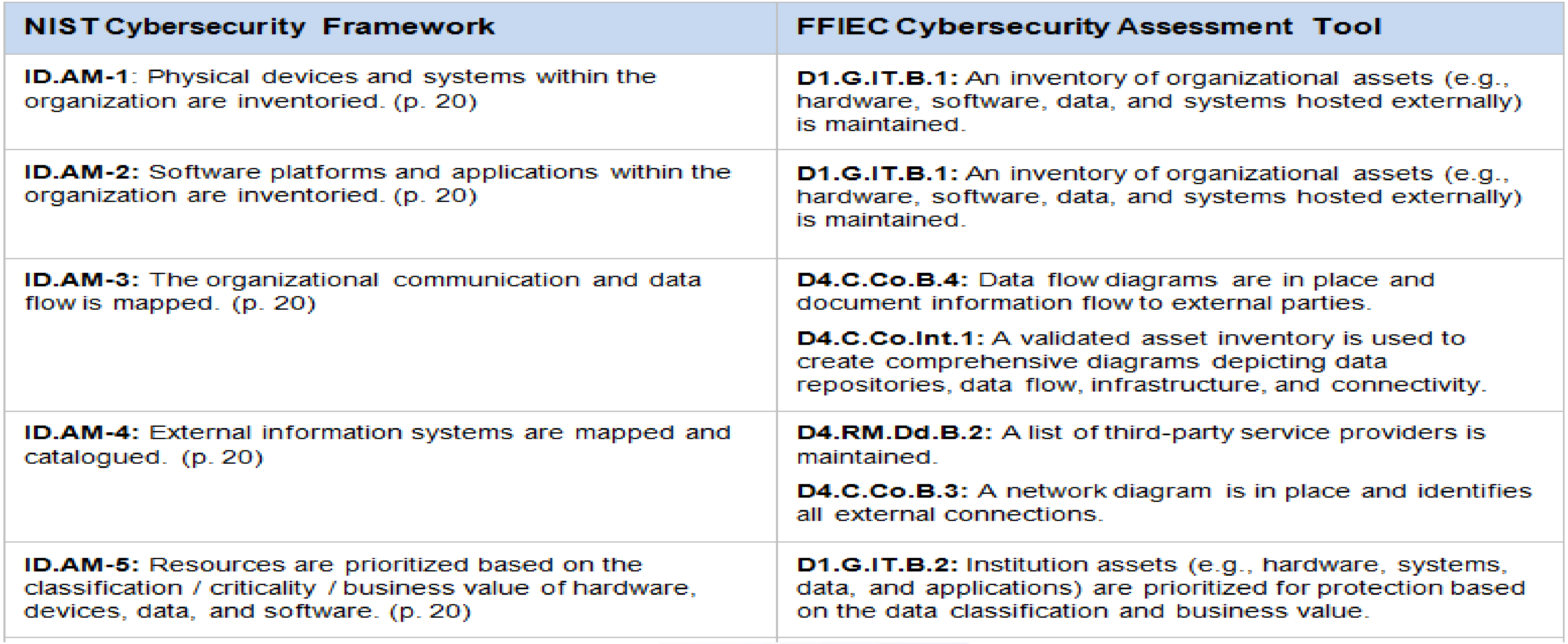
Domain 2: Threat Intelligence & Collaboration
- Threat Intelligence
- Monitoring and Analyzing
- Information Sharing

Domain 3: Cybersecurity Controls
- Preventative Controls
- Detective Controls
- Corrective Controls

Domain 4: External Dependency Management
- Connections
- Relationship Management

Domain 5: Cyber Incident Management and Resilience
- Incident Resilience Planning and Strategy
- Detection, Response, and Mitigation
- Escalation and Reporting

Mapping NIST to the FFIEC Assessment Tool



NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
ID.AM-1: Physical devices and systems within the organization are inventoried. (p. 20)	**D1.G.IT.B.1:** An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained.
ID.AM-2: Software platforms and applications within the organization are inventoried. (p. 20)	**D1.G.IT.B.1:** An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained.
ID.AM-3: The organizational communication and data flow is mapped. (p. 20)	**D4.C.Co.B.4:** Data flow diagrams are in place and document information flow to external parties. **D4.C.Co.Int.1:** A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.
ID.AM-4: External information systems are mapped and catalogued. (p. 20)	**D4.RM.Dd.B.2:** A list of third-party service providers is maintained. **D4.C.Co.B.3:** A network diagram is in place and identifies all external connections.
ID.AM-5: Resources are prioritized based on the classification / criticality / business value of hardware, devices, data, and software. (p. 20)	**D1.G.IT.B.2:** Institution assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.

Source: FFIEC CAT Document - Appendix B

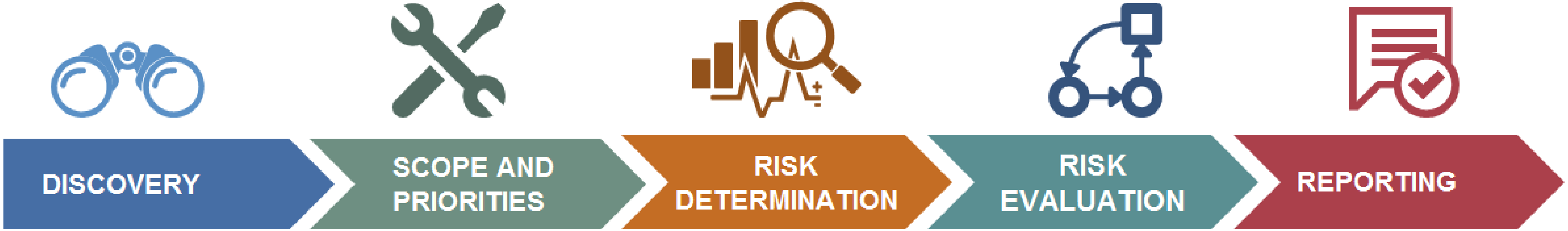
Practical Ways to Assess your Risk and Organizational Exposure

What is a Cyber Risk Assessment?

A Cyber Risk Assessment is a comprehensive evaluation of your cybersecurity program and overall security posture. It identifies key risks that can impact the availability, integrity, and confidentiality of your information assets, determines where your strengths are, and zeroes in on weaknesses that present the greatest threats to the organization.

It is a deep dive into the layers of protection that separate sensitive and critical data from sophisticated attackers. It gives you the necessary information to close gaps in your defenses, and provides the needed detail on how to do so in a cost effective manner.

Assessment Process



DISCOVERY

- **Business Environment**
  - Services
  - Processes
  - Systems
- **Documentation**
  - Policy Portfolio
  - Metrics Portfolio
  - Strategic Goals
  - Security Initiatives
  - Past Risk Assessments

SCOPE AND PRIORITIES

- **Needs Identification**
  - Business Stakeholders
  - Operations Stakeholders
  - Oversight Stakeholders
- **Security Priorities**
  - Management Priorities
  - Critical Processes
  - Key Information Assets
  - Regulatory Priorities
  - Third Party Obligations

RISK DETERMINATION

- **Risk Drivers**
  - Threats
  - Vulnerabilities
  - Attack Vectors
- **Determine Risks**
  - Probability
  - Impact
  - Inherent Risk
  - B2B Risk
  - Customer Risk

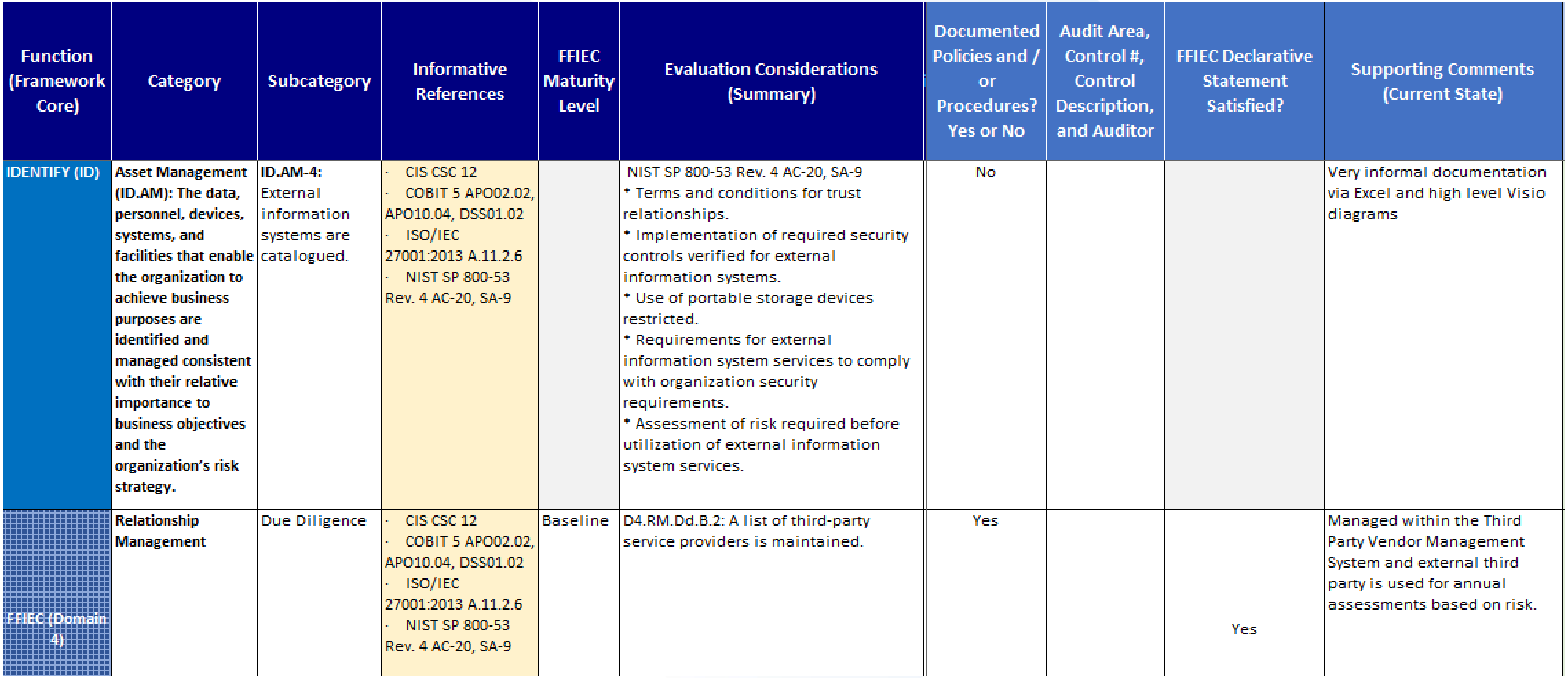
RISK EVALUATION

- **Capabilities Review**
  - Control Maturity
  - Audit Capability
  - Probable Impacts
- **Analysis**
  - Residual Risk Level
  - Mitigation Considerations
  - Aggregated Risks
  - Control Deficiencies

REPORTING

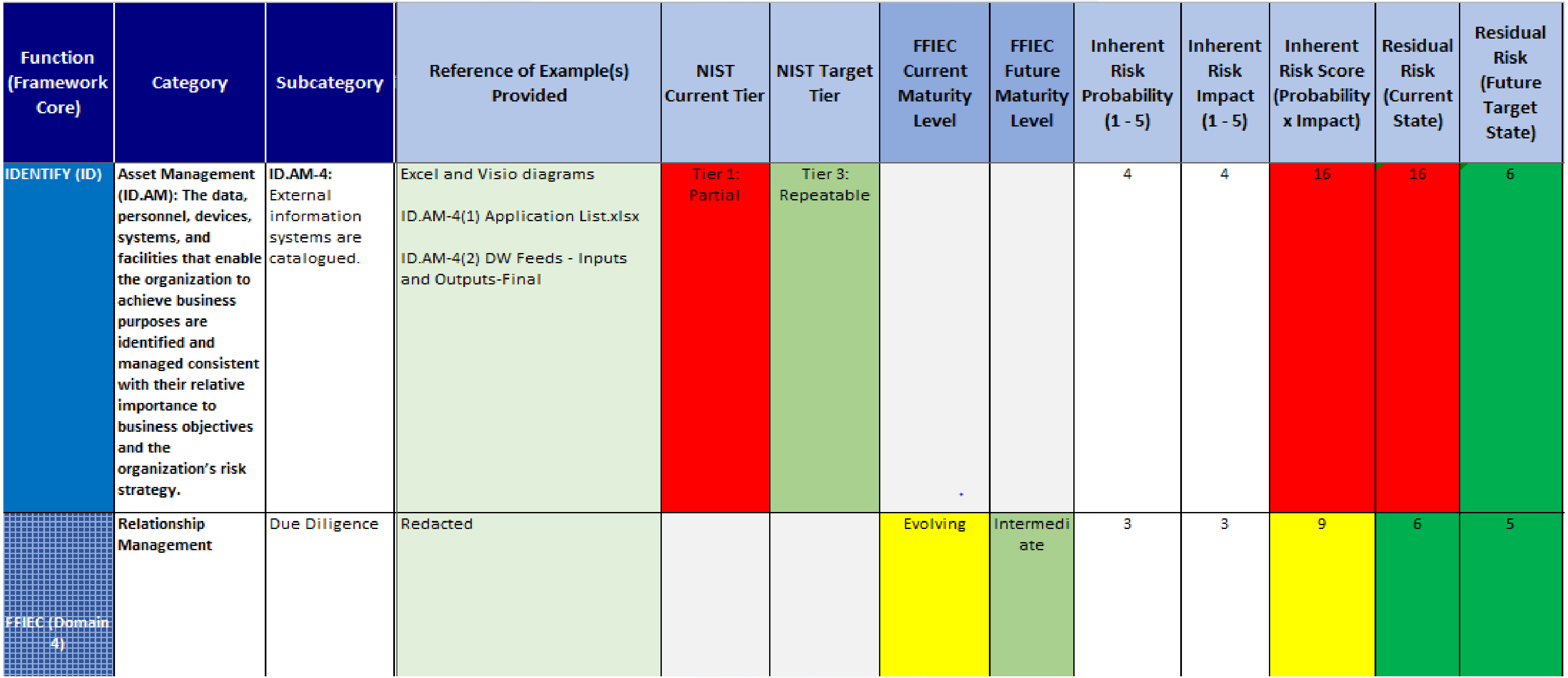
- **Report**
  - Current Strengths
  - Critical Control Gaps
  - Key Opportunities
  - Remediation Recommendations
  - Prioritized Actions Roadmap

Assessment Tool



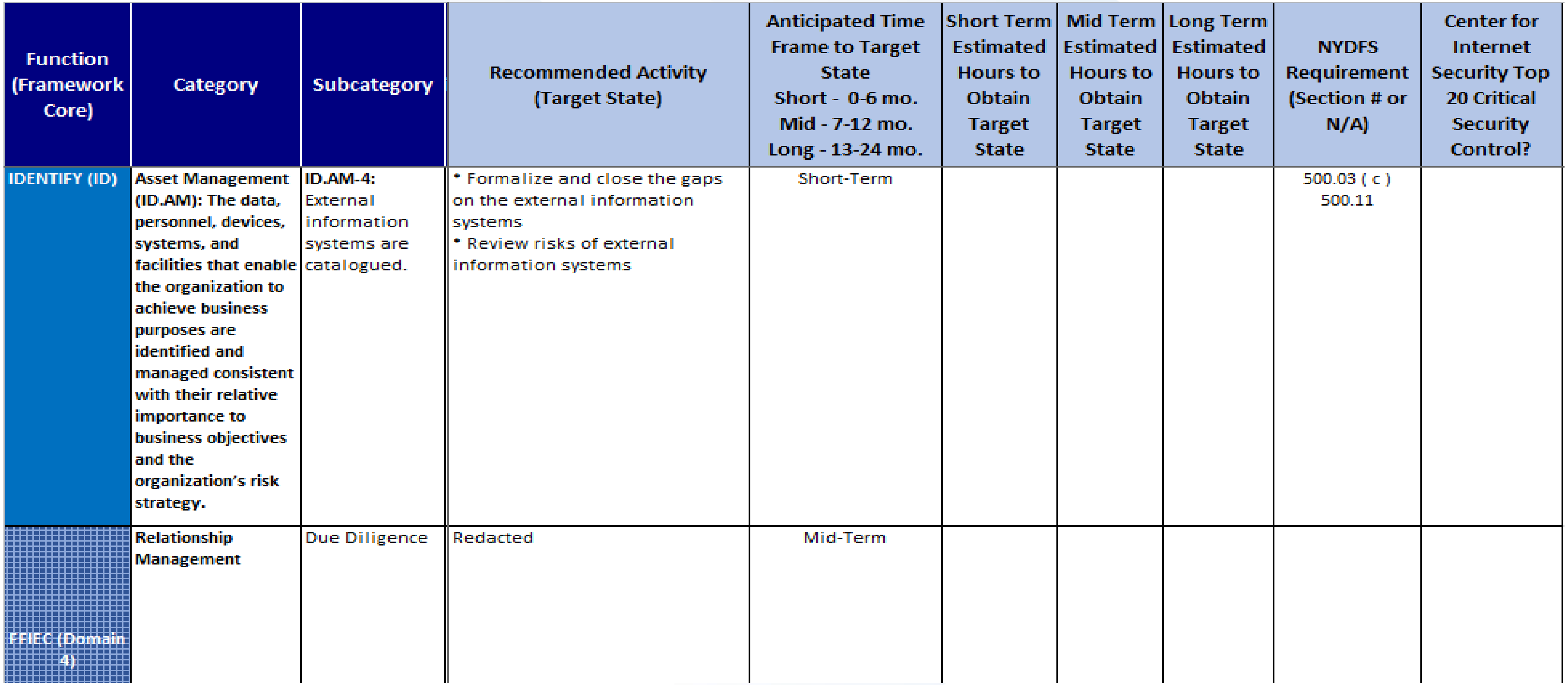
Function (Framework Core)	Category	Subcategory	Informative References	FFIEC Maturity Level	Evaluation Considerations (Summary)	Documented Policies and / or Procedures? Yes or No	Audit Area, Control #, Control Description, and Auditor	FFIEC Declarative Statement Satisfied?	Supporting Comments (Current State)
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-4:** External information systems are catalogued.	· CIS CSC 12 · COBIT 5 APO02.02, APO10.04, DSS01.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9		NIST SP 800-53 Rev. 4 AC-20, SA-9 * Terms and conditions for trust relationships. * Implementation of required security controls verified for external information systems. * Use of portable storage devices restricted. * Requirements for external information system services to comply with organization security requirements. * Assessment of risk required before utilization of external information system services.	No			Very informal documentation via Excel and high level Visio diagrams
FFIEC (Domain 4)	**Relationship Management**	Due Diligence	· CIS CSC 12 · COBIT 5 APO02.02, APO10.04, DSS01.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9	Baseline	D4.RM.Dd.B.2: A list of third-party service providers is maintained.	Yes		Yes	Managed within the Third Party Vendor Management System and external third party is used for annual assessments based on risk.

Assessment Tool



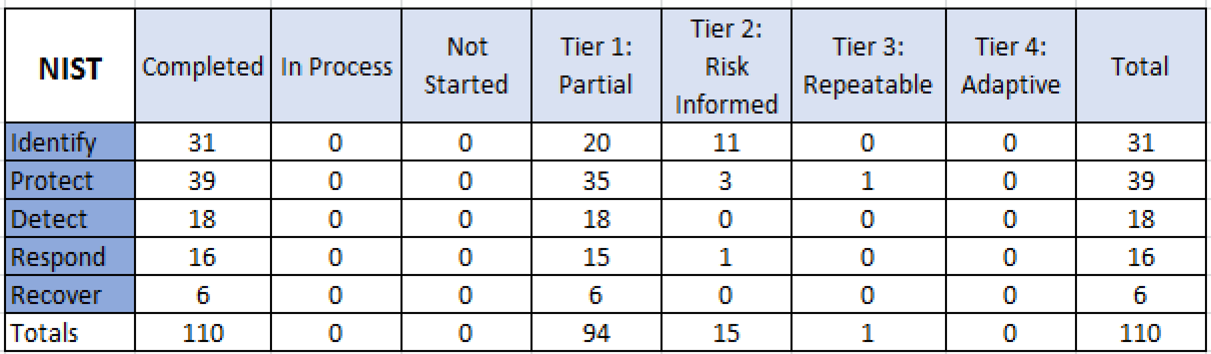
Function (Framework Core)	Category	Subcategory	Reference of Example(s) Provided	NIST Current Tier	NIST Target Tier	FFIEC Current Maturity Level	FFIEC Future Maturity Level	Inherent Risk Probability (1 - 5)	Inherent Risk Impact (1 - 5)	Inherent Risk Score (Probability x Impact)	Residual Risk (Current State)	Residual Risk (Future Target State)
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-4: External information systems are catalogued.	Excel and Visio diagrams ID.AM-4(1) Application List.xlsx ID.AM-4(2) DW Feeds - Inputs and Outputs-Final	Tier 1: Partial	Tier 3: Repeatable			4	4	16	16	6
FFIEC (Domain 4)	Relationship Management	Due Diligence	Redacted			Evolving	Intermediate	3	3	9	6	5

Assessment Tool

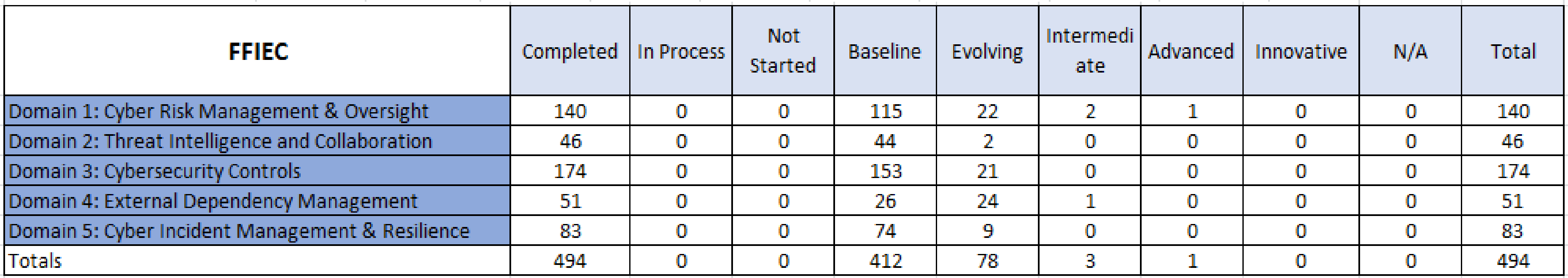


Function (Framework Core)	Category	Subcategory	Recommended Activity (Target State)	Anticipated Time Frame to Target State Short - 0-6 mo. Mid - 7-12 mo. Long - 13-24 mo.	Short Term Estimated Hours to Obtain Target State	Mid Term Estimated Hours to Obtain Target State	Long Term Estimated Hours to Obtain Target State	NYDFS Requirement (Section # or N/A)	Center for Internet Security Top 20 Critical Security Control?
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-4: External information systems are catalogued.	* Formalize and close the gaps on the external information systems * Review risks of external information systems	Short-Term				500.03 (c) 500.11	
FFIEC (Domain 4)	Relationship Management	Due Diligence	Redacted	Mid-Term					

Assessment Tool

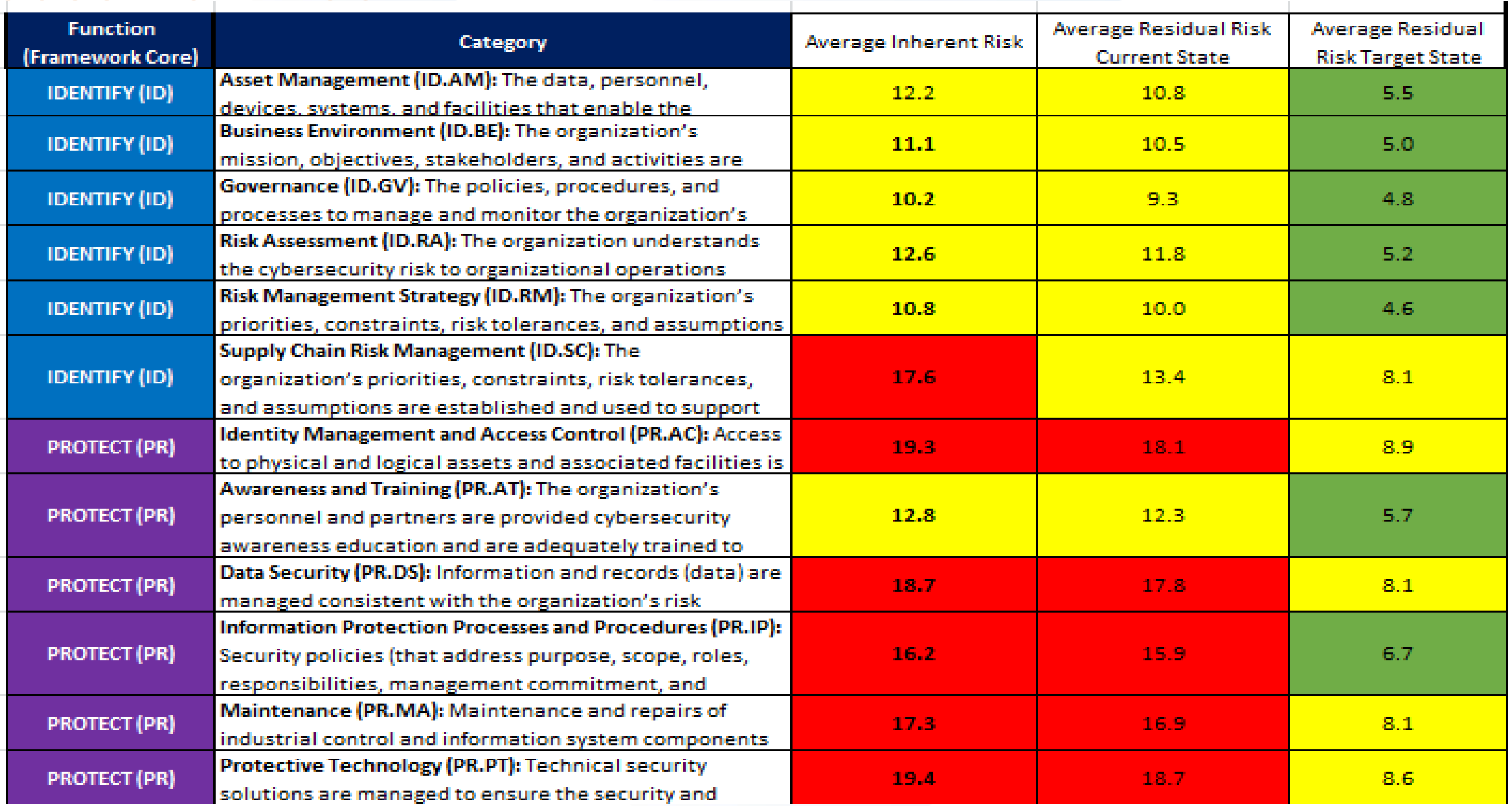


NIST	Completed	In Process	Not Started	Tier 1: Partial	Tier 2: Risk Informed	Tier 3: Repeatable	Tier 4: Adaptive	Total
Identify	31	0	0	20	11	0	0	31
Protect	39	0	0	35	3	1	0	39
Detect	18	0	0	18	0	0	0	18
Respond	16	0	0	15	1	0	0	16
Recover	6	0	0	6	0	0	0	6
Totals	110	0	0	94	15	1	0	110



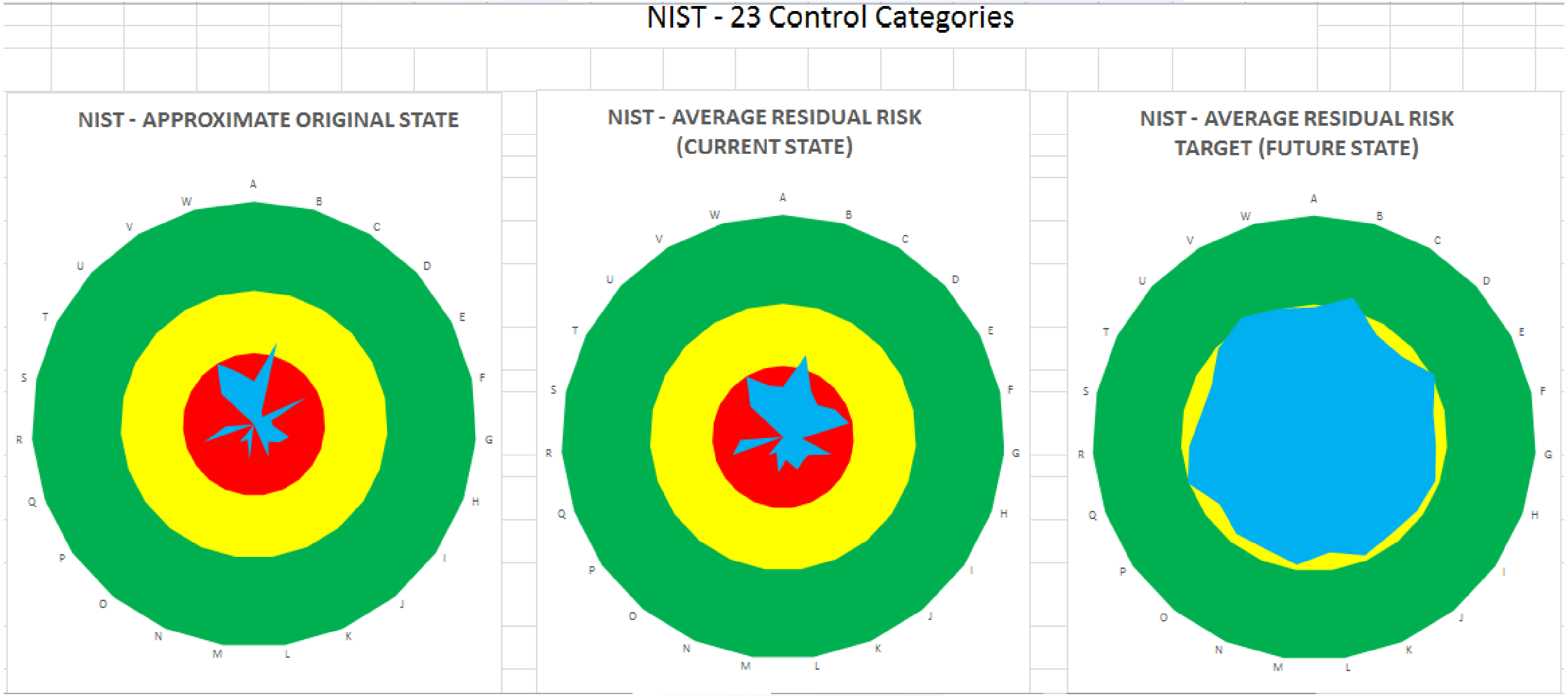
FFIEC	Completed	In Process	Not Started	Baseline	Evolving	Intermediate	Advanced	Innovative	N/A	Total
Domain 1: Cyber Risk Management & Oversight	140	0	0	115	22	2	1	0	0	140
Domain 2: Threat Intelligence and Collaboration	46	0	0	44	2	0	0	0	0	46
Domain 3: Cybersecurity Controls	174	0	0	153	21	0	0	0	0	174
Domain 4: External Dependency Management	51	0	0	26	24	1	0	0	0	51
Domain 5: Cyber Incident Management & Resilience	83	0	0	74	9	0	0	0	0	83
Totals	494	0	0	412	78	3	1	0	0	494

Assessment Tool



Function (Framework Core)	Category	Average Inherent Risk	Average Residual Risk Current State	Average Residual Risk Target State
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the	12.2	10.8	5.5
IDENTIFY (ID)	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are	11.1	10.5	5.0
IDENTIFY (ID)	**Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's	10.2	9.3	4.8
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations	12.6	11.8	5.2
IDENTIFY (ID)	**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions	10.8	10.0	4.6
IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support	17.6	13.4	8.1
PROTECT (PR)	**Identity Management and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is	19.3	18.1	8.9
PROTECT (PR)	**Awareness and Training (PR.AT):** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to	12.8	12.3	5.7
PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk	18.7	17.8	8.1
PROTECT (PR)	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and	16.2	15.9	6.7
PROTECT (PR)	**Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components	17.3	16.9	8.1
PROTECT (PR)	**Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and	19.4	18.7	8.6

Assessment Tool



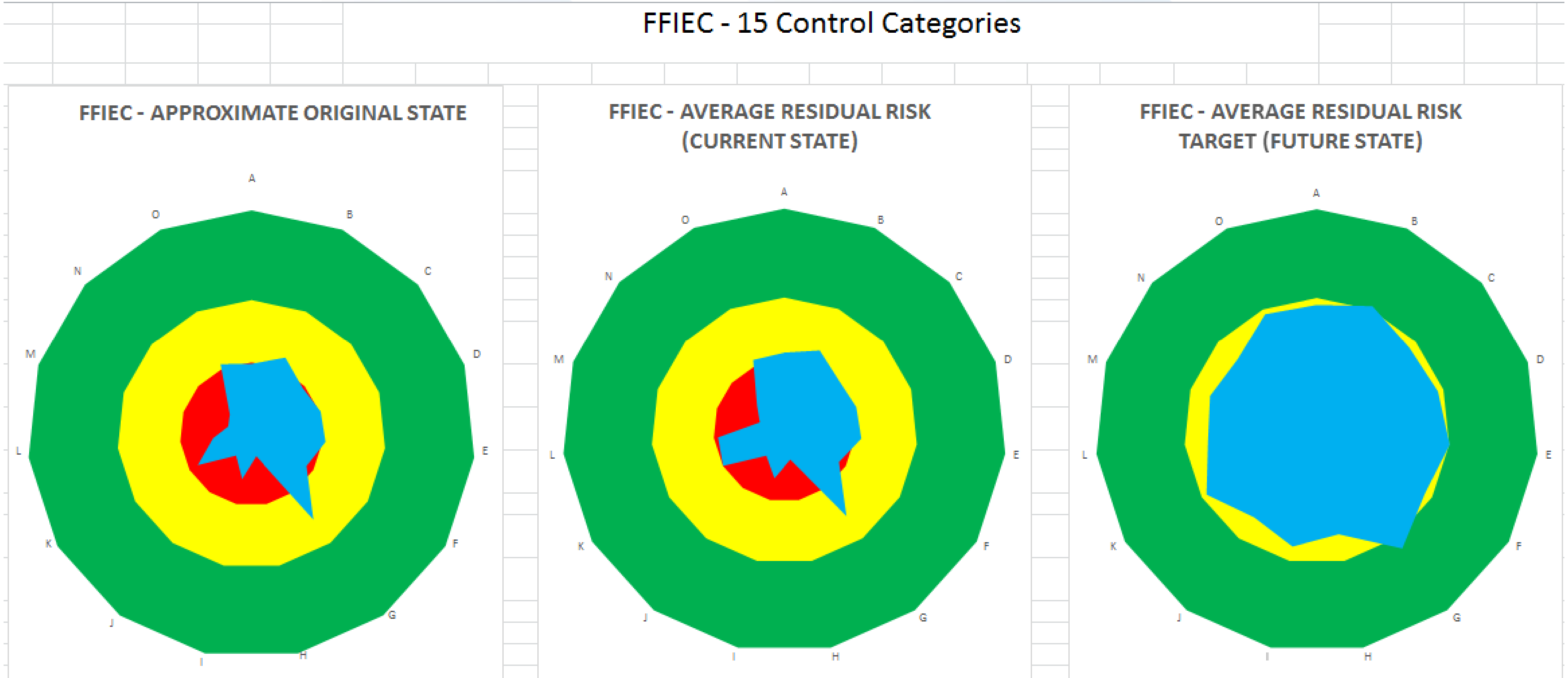
NIST - 23 Control Categories

NIST - APPROXIMATE ORIGINAL STATE

NIST - AVERAGE RESIDUAL RISK (CURRENT STATE)

NIST - AVERAGE RESIDUAL RISK TARGET (FUTURE STATE)

Assessment Tool



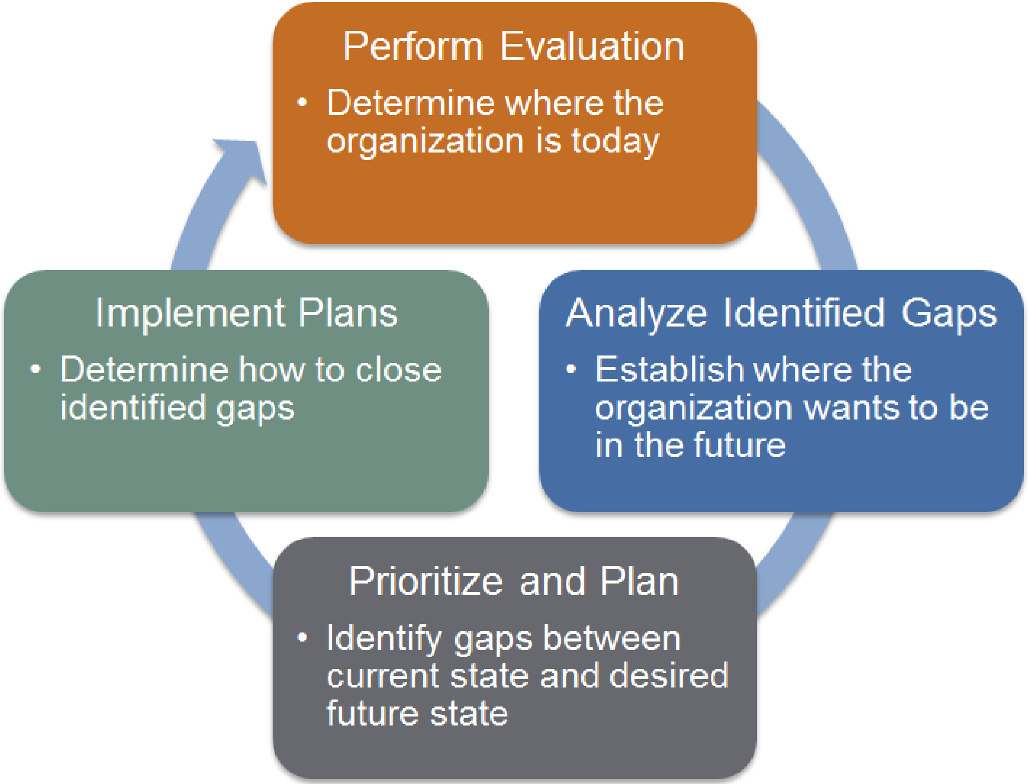
FFIEC - 15 Control Categories

FFIEC - APPROXIMATE ORIGINAL STATE

FFIEC - AVERAGE RESIDUAL RISK (CURRENT STATE)

FFIEC - AVERAGE RESIDUAL RISK TARGET (FUTURE STATE)

Ongoing Process



Perform Evaluation

- Determine where the organization is today

Analyze Identified Gaps

- Establish where the organization wants to be in the future

Prioritize and Plan

- Identify gaps between current state and desired future state

Implement Plans

- Determine how to close identified gaps

Key Elements of a Cyber Risk Management Program

What Key Elements Are Often Overlooked?

- **Asset Management** – we find that many clients lack clear information on how many servers they have, what other devices reside on their network, what O/S each is running, etc.
- **Controls Management** – many organizations lack continuous monitoring of controls, limiting their focus to what is necessary to meet regulatory requirements
- **Configuration and Change Management** – configuration changes often focus on getting the application up-and-running, not minimizing the attack surface
- **Vulnerability Management** – we see many cases where vulnerability management may take 6 to 8 weeks to close a vulnerability. This is 6 to 8 weeks during which the organization is at an increased level of risk
- **Incident Management** – we see a need for much greater coordination and communication between the information security group and the business units

What Key Elements Are Often Overlooked?

- **Service Continuity Management** – many organizations focus on traditional threats and have not performed tabletop or simulated tests involving a cyber attack
- **Risk Management** – we have noted many cases where risk management is assessing the risks posed by cyber attacks as they existed 10-15 years ago, failing to take into account how these risks have evolved in recent years
- **External Dependencies Management** – organizations are in many cases failing to fully evaluate the impact of a cyber attack against critical service providers, the communications links with them, and what the downstream impact will be
- **Training and Awareness** – many organizations ignore cross-functional training, whereas true resiliency requires a multi-disciplinary approach to training and awareness
- **Situational Awareness** – a number of organizations lack the tools and technical training to quickly identify, contain, and recover from cyberattacks

Essential Cyber Risk Management Practices

- Periodic risk assessment to evaluate IT cyber risk posture
- Comprehensive security policies that are reviewed annually
- Appointment of CISO with enterprise-wide responsibility
- Annual report by CISO to senior management covering cyber risks
- Risk personnel who understand how cyber risks affect business risks
- Training and awareness activities including testing
- Incident response management plan that is holistic
- Metrics to evaluate the efficiency and effectiveness of cyber operations
- Monitoring of business partners, vendors, third-parties
- Adherence to standardized framework requirements (NIST, etc.)

Q&A / Contact Information

Contact Information

Stephen Head, CISSP, CISM, CISA
Director, Experis Finance IT Risk Advisory Services
Mobile: 704.953.6688
Email: stephen.head@experis.com

Thank You!