SECURITY FRAMEWORKS: NIST CSF AS AN ENABLER

May, 2020

AGENDA

- Quick Introduction to Security Frameworks
- Review of the NIST CSF Framework
- Focus on Using CSF for Incident Response

WHAT IS AN IT SECURITY FRAMEWORK?

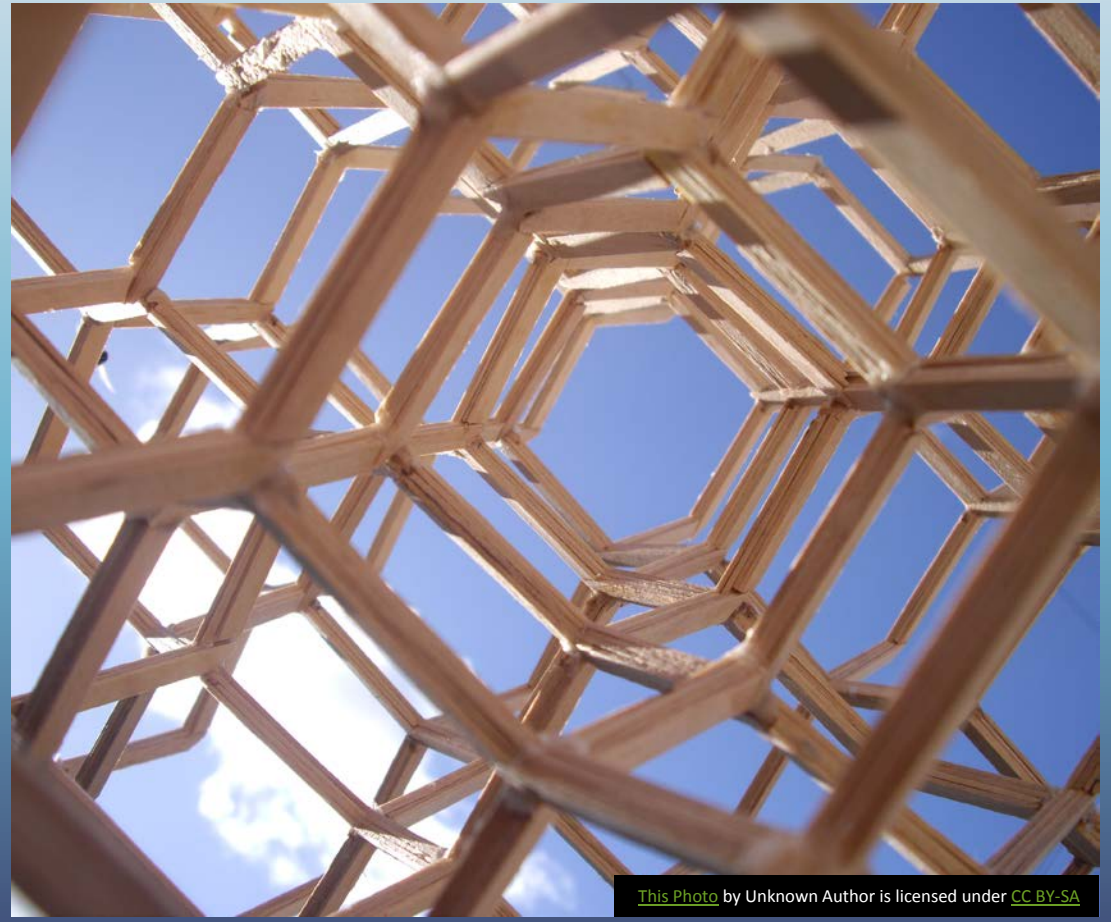
At the core a security framework is a series of documented processes used to define process and procedures and set objectives or outcomes.

- A model to build and measure the information security program and information security risks.
- Used to define and prioritize the tasks to execute security functions

Effective Frameworks are adapted to the business's needs and objectives.

IT SECURITY FRAMEWORKS SHOULD BE CUSTOMIZED

- Frameworks may present options that do not fit the intent of the business
- Spending effort where it is not needed is not productive to managing a realistic information security program
- Customization should be done based upon the business or regulatory drivers, cost and level of effort and expected impact on the risk profile of the business.
- Multiple frameworks can work together as they often have different goals or focus areas.



A COMMON TAXONOMY

Current State	Describe the current cybersecurity posture
Target State	Describe the target state for cybersecurity
Identify and prioritize	Identify and prioritize opportunities for improvement – focusing on continuous, repeatable processes
Assess	Assess progress toward the target state
Communicate	Communicate to internal and external stakeholders about cybersecurity risk in a consistent manner

Framework	Industry Recognized	Internal Business Drivers	Statutory Requirements	Regulatory Requirements	Contractual Requirements	Internal Compliance	Flexibility & Adaptability	Ease of Governance	Ease of Management	Business Alignment	Value Proposition	Scalability	Risk Driven	Auditable
COBIT 2019	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ISO/IEC 27001:2013	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
NIST Cybersecurity Framework (CSF)	✓	--	✓	--	--	--	✓	--	--	✓	✓	✓	✓	✓
CIS Top 20 CSC	✓	--	--	--	--	--	✓	--	✓	--	--	✓	--	✓

FRAMEWORKS CONSIDERED & COMPARED

Framework	Focus Area	Industry Body	Orientation
COBIT 2019	Governance & Management of Information & Technology	Information Systems Audit and Control Association (ISACA)	Business Process
ISO/IEC 27001:2013	Information Security Management	International Organization of Standards (ISO/IEC)	Business Process
CIS CSC	Critical Security Controls to Prevent Data Breach	Center for Internet Security (CIS)	Technical Controls
NIST Cyber Security Framework	Civilian Critical Infrastructure	National Institute of Standards and Technology (NIST)	Technical Controls

WHAT COBIT IS

COBIT is a framework for the governance and management of enterprise information and technology.

COBIT is aimed at the whole enterprise.

COBIT makes a clear distinction between governance and management.

COBIT defines the components to build and sustain a governance system.

COBIT defines the design factors that should be considered by the enterprise to build a best-fit governance system.

COBIT addresses governance issues by grouping relevant governance components into governance and management objectives that can be managed to the required capability levels.

Reference: COBIT 2019 Framework: Introduction and Methodology Chapter 1 Introduction

WHAT COBIT IS NOT

COBIT is not a full description of the whole IT environment of an enterprise.

COBIT is not a framework to organize business processes.

COBIT is not an (IT-)technical framework to manage all technology.

COBIT does not make or prescribe any IT-related decisions.

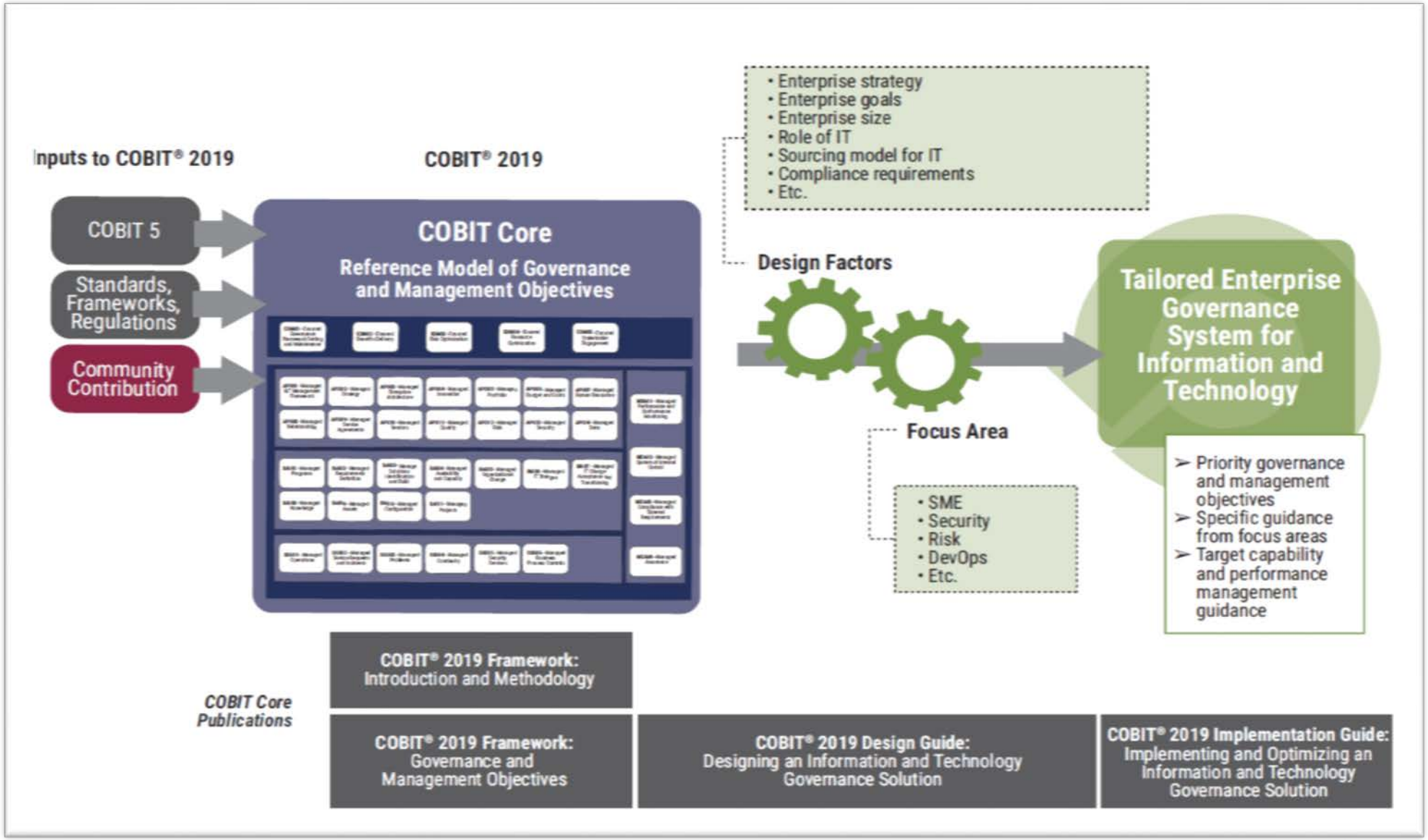
Reference: COBIT 2019 Framework: Introduction and Methodology Chapter 1 Introduction

COBIT AND OTHER STANDARDS

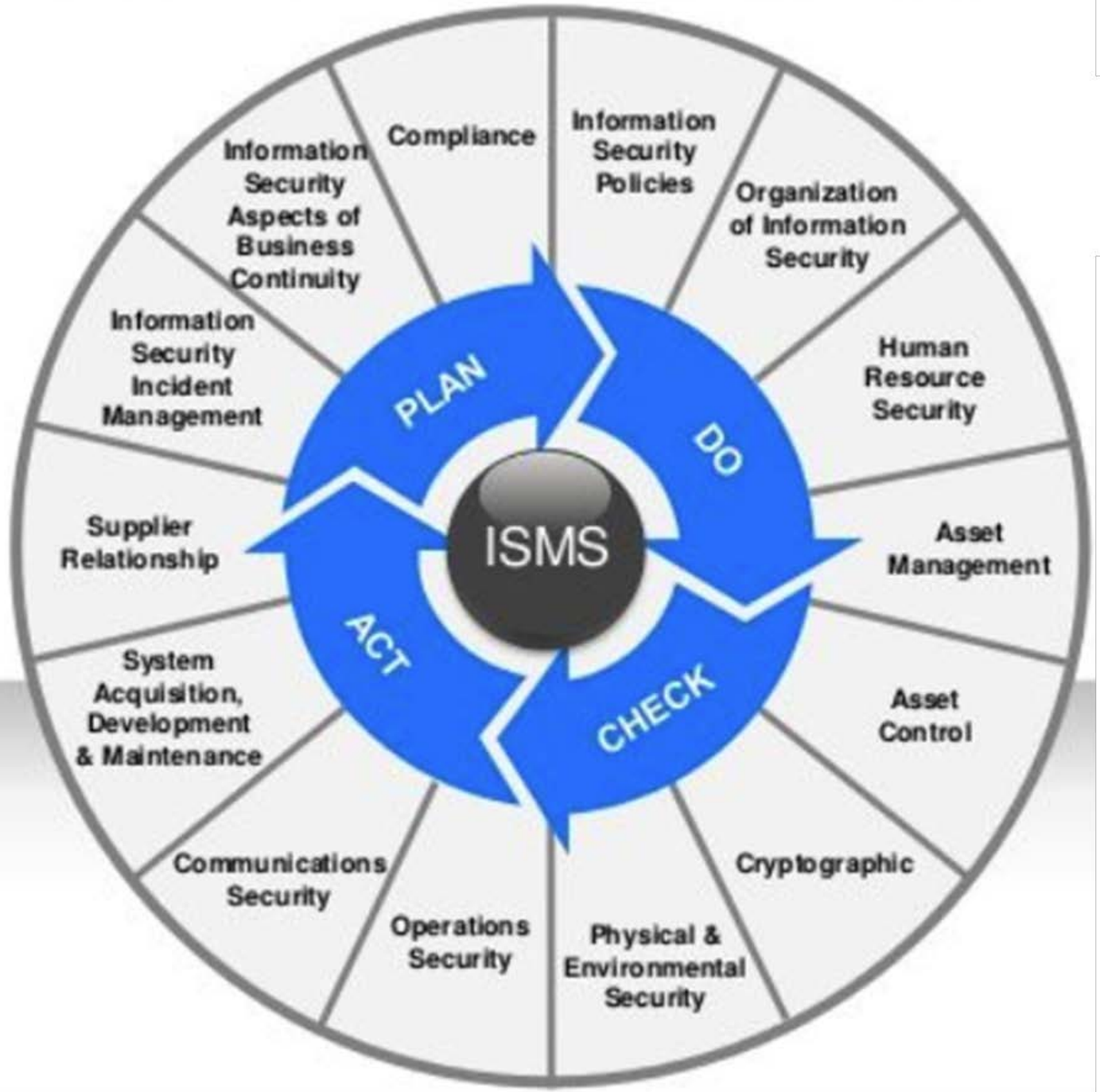
- One of the guiding principles applied throughout the development of COBIT 2019 was to maintain the positioning of COBIT as an umbrella framework.
- This means that COBIT 2019 continues to align with a number of relevant standards, frameworks and/or regulations.
  - COBIT does not contradict any guidance in the related standards.
  - COBIT does not copy the contents of these related standards.
  - COBIT provides equivalent statements or references to related guidance.

Reference: COBIT 2019 Framework: Introduction and Methodology Chapter 10 COBIT and Other Standards

COBIT OVERVIEW AND PRODUCT ARCHITECTURE



Reference: COBIT 2019 Framework: Introduction and Methodology Chapter 4 Basic Concepts



ISO 27001: 2013 FRAMEWORK

- Risk-based approach – Risk Assessment required to build and maintain
- Objectives are broken into 14 control areas
- What you do is based on the controls you adopt – modular approach
- Can be certified against – internationally recognized

CIS CSC 7.1

- Tiered Control Framework
- First 6 controls have most return for effort in stopping incidents
- Vetted and Selected by Practitioners
- Tactical Focus
- Doesn’t meet most Audit standards for compliance – no governance or policy elements

Basic CIS Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational CIS Controls

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

NIST CYBERSECURITY FRAMEWORK OVERVIEW

NIST CYBERSECURITY FRAMEWORK – 3 GOALS

- The Framework is **guidance** not mandate
- Developed as a “lightweight” approach
- No Formal Assessment program
- The Framework is not a one-size-fits-all approach to managing cybersecurity risk

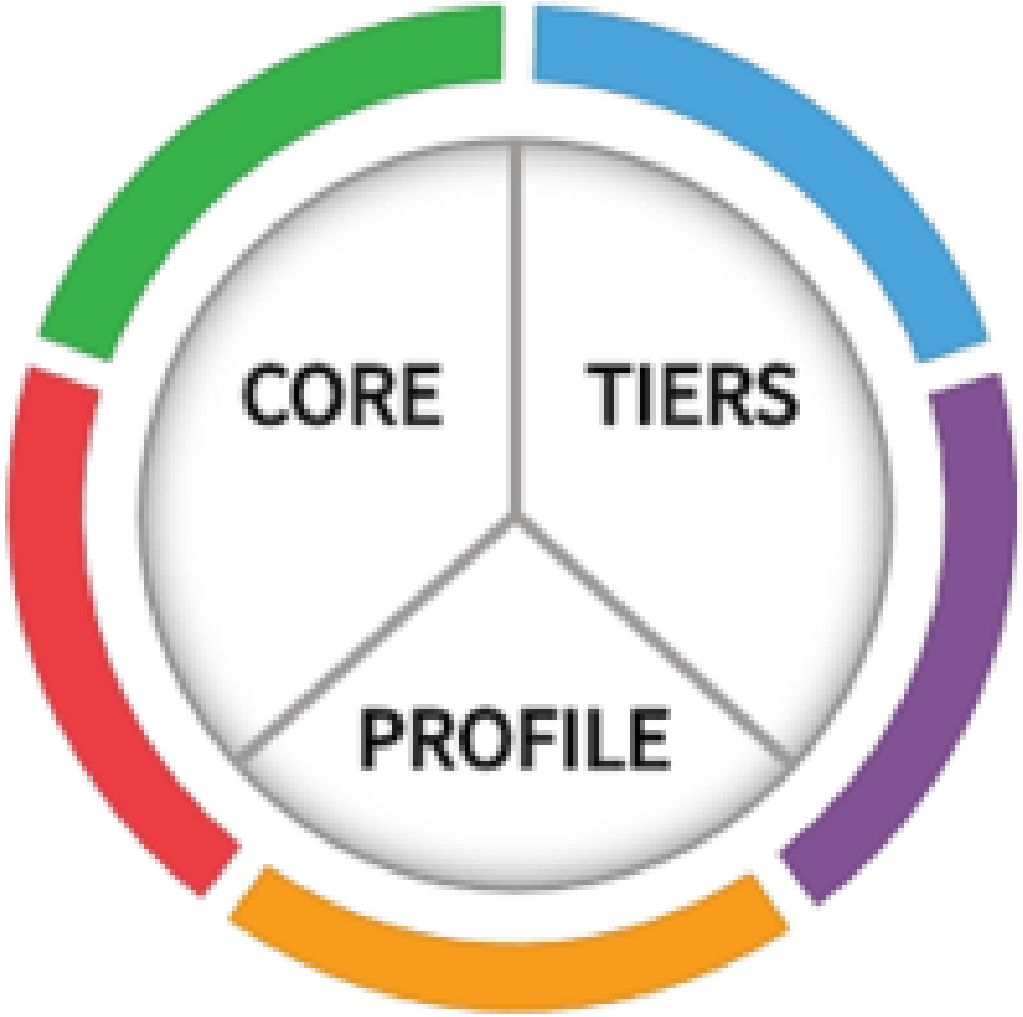
Help Organizations Manage Cyber Risks

Provide Common language to Discuss Cyber Risks

Create, Guide, Assess or Improve Cybersecurity Programs

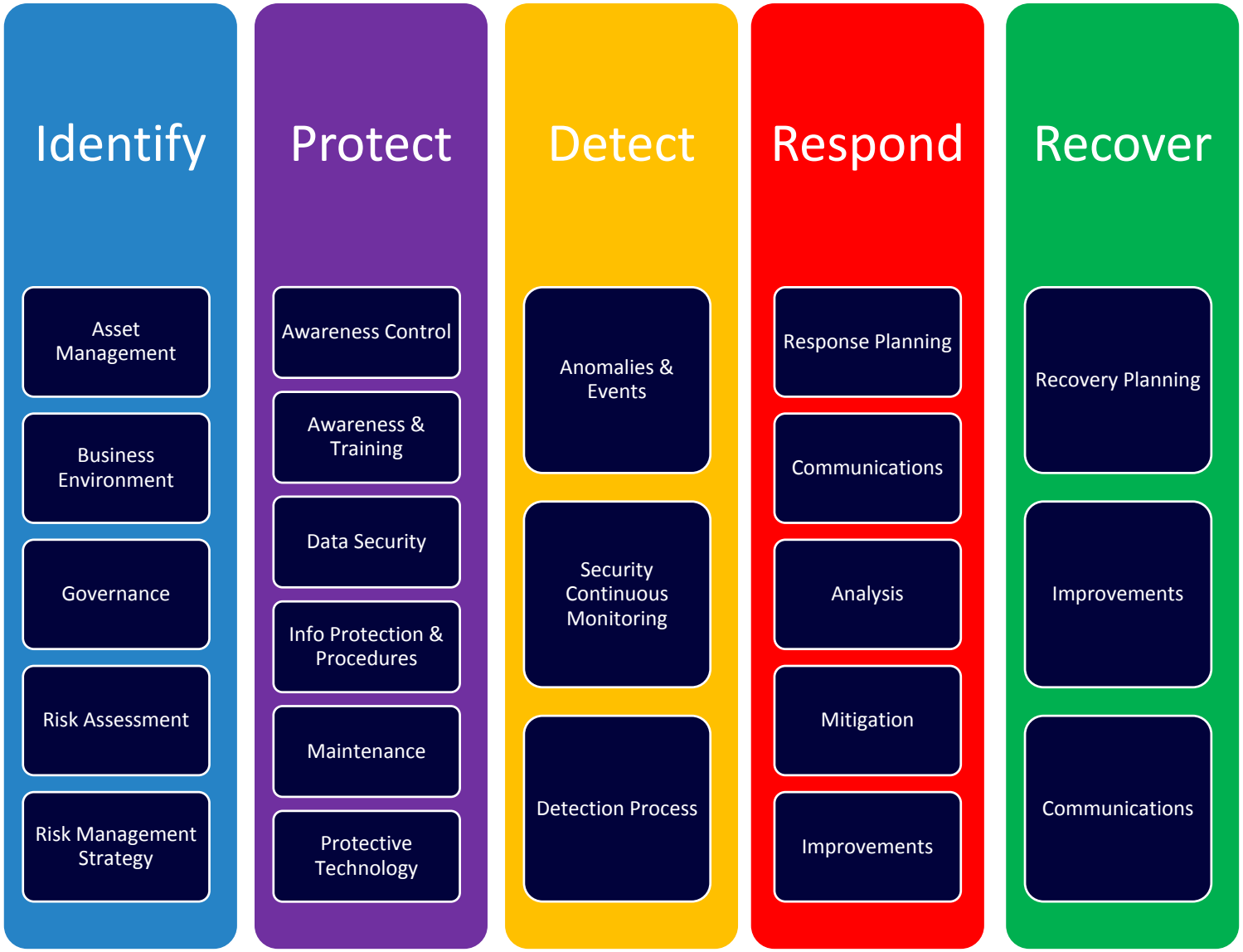
NIST CYBERSECURITY FRAMEWORK V 1.1

- Three Pieces:
  - Core: Cybersecurity activities, desired outcomes and applicable references
  - Tiers: Risk Context of the organization – Rated 1 to 4 in increasing Rigor
  - Profile: Business defined outcomes – “as is” and “to be” states are profiles

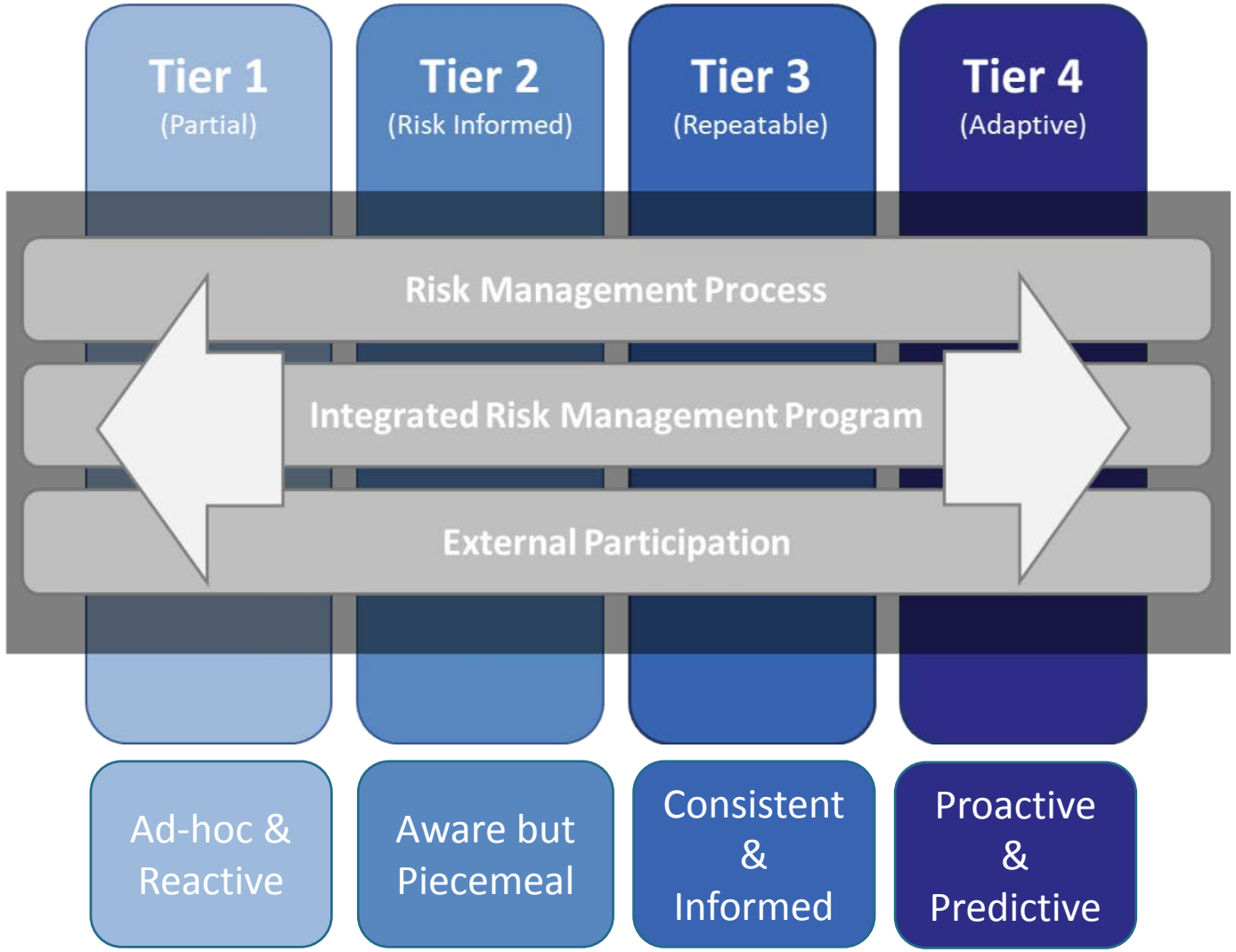


FRAMEWORK CORE

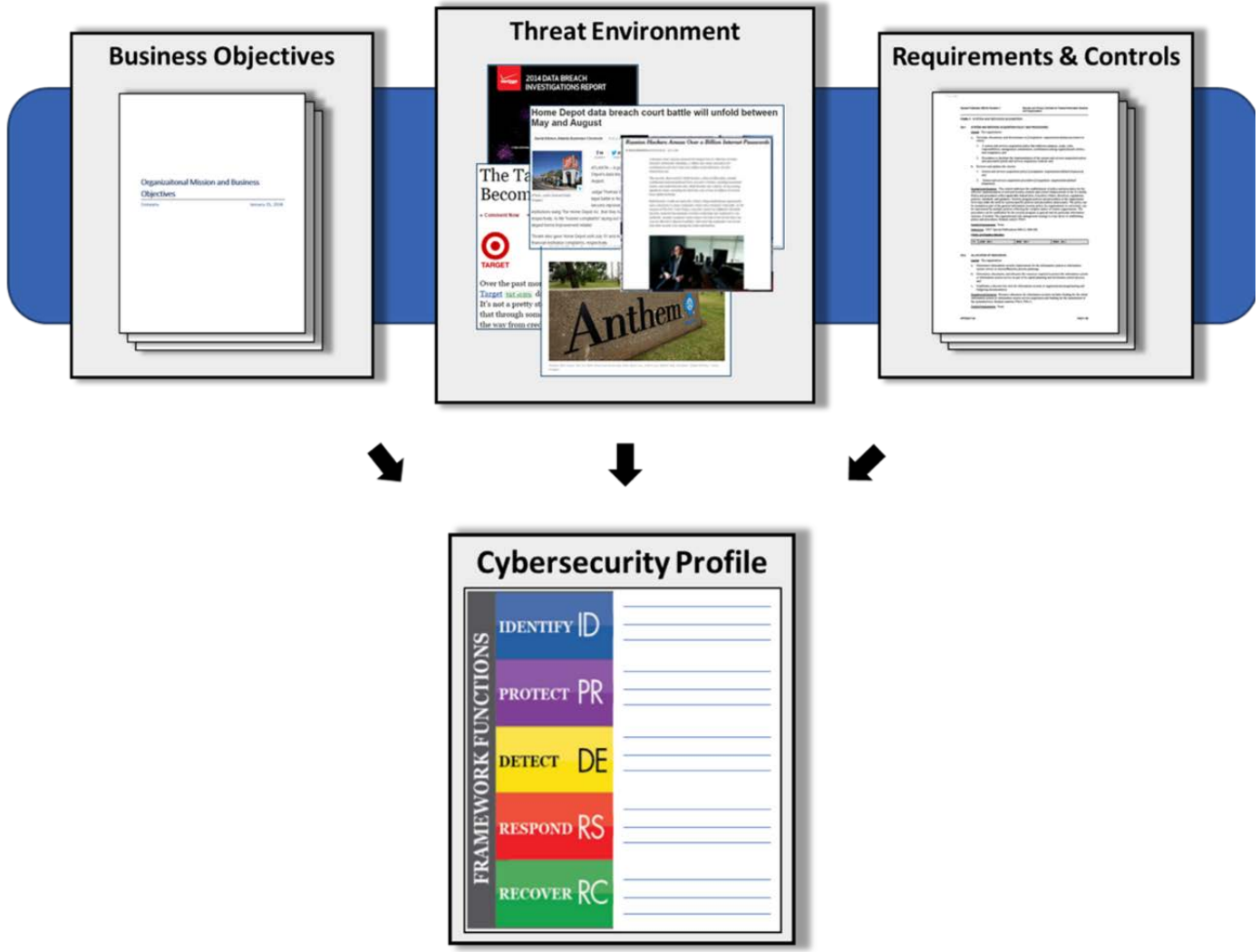
- Consists of:
  - 5 Concurrent and Continuous Functions
  - 23 categories
  - 108 subcategories



FRAMEWORK TIERS



ORGANIZATION CYBERSECURITY PROFILE



KEY STEPS TO ADOPTING NIST CSF

Identify and align

Identify and align the program with organizational business objectives

Review

Review controls already in place to identify your primary controls and establish enhancement or maturity tasks for later growth.

Consider

Consider using NIST SP 800-171 as a “first step” to building key controls

Ensure

Ensure you consider all the functions equally

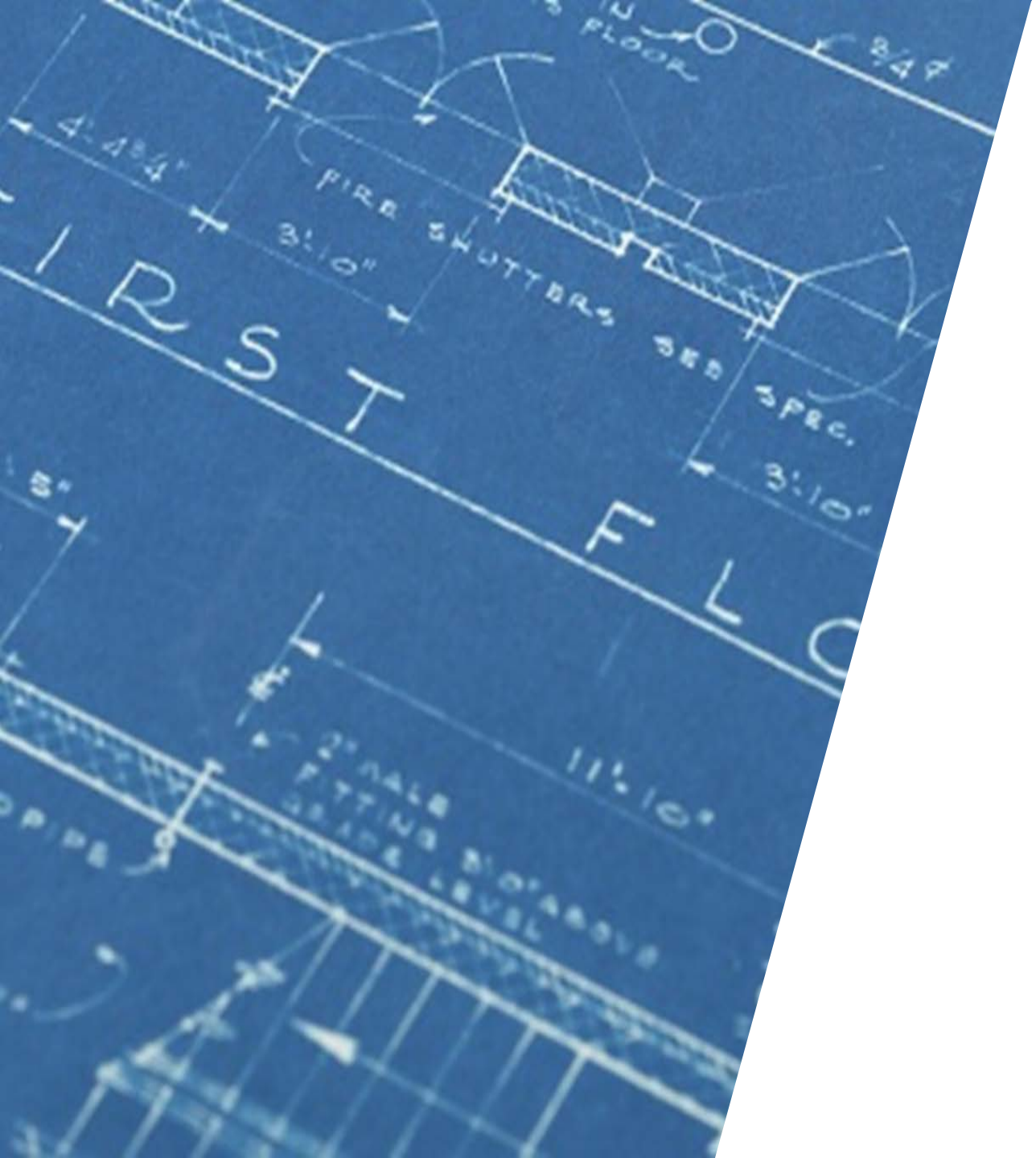
Involve

Involve key areas of the business – educate and delegate controls to the business areas

FRAMEWORK ROADMAP

14 High-Priority Areas

- Confidence Mechanisms
- Cyber-Attack Lifecycle
- Cybersecurity Workforce
- Cyber Supply Chain Risk Management
- Federal Agency Cybersecurity Alignment
- Governance and Enterprise Risk Management
- Identity Management
- International Aspects, Impacts, and Alignment
- Measuring Cybersecurity
- Privacy Engineering
- Referencing Techniques
- Small Business Awareness and Resources
- Internet of Things (IoT)
- Secure Software Development



FOCUS ON RESPONSE

PRACTICAL CONCERNS

You have limited budget and time, your adversary has infinite supplies of both

Training is easy, practicing is hard

RESPOND

Ensuring Response Planning process are executed during and after an incident

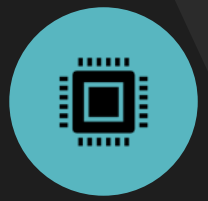
Managing Communications during and after an event with stakeholders, law enforcement, external stakeholders as appropriate

Analysis is conducted to ensure effective response and support recovery activities including forensic analysis, and determining the impact of incidents

Mitigation activities are performed to prevent expansion of an event and to resolve the incident

The organization implements Improvements by incorporating lessons learned from current and previous detection / response activities

RESPOND DOESN'T WORK WITHOUT DETECT



Does your organization have the sensors, processes and practices to identify a cybersecurity event?

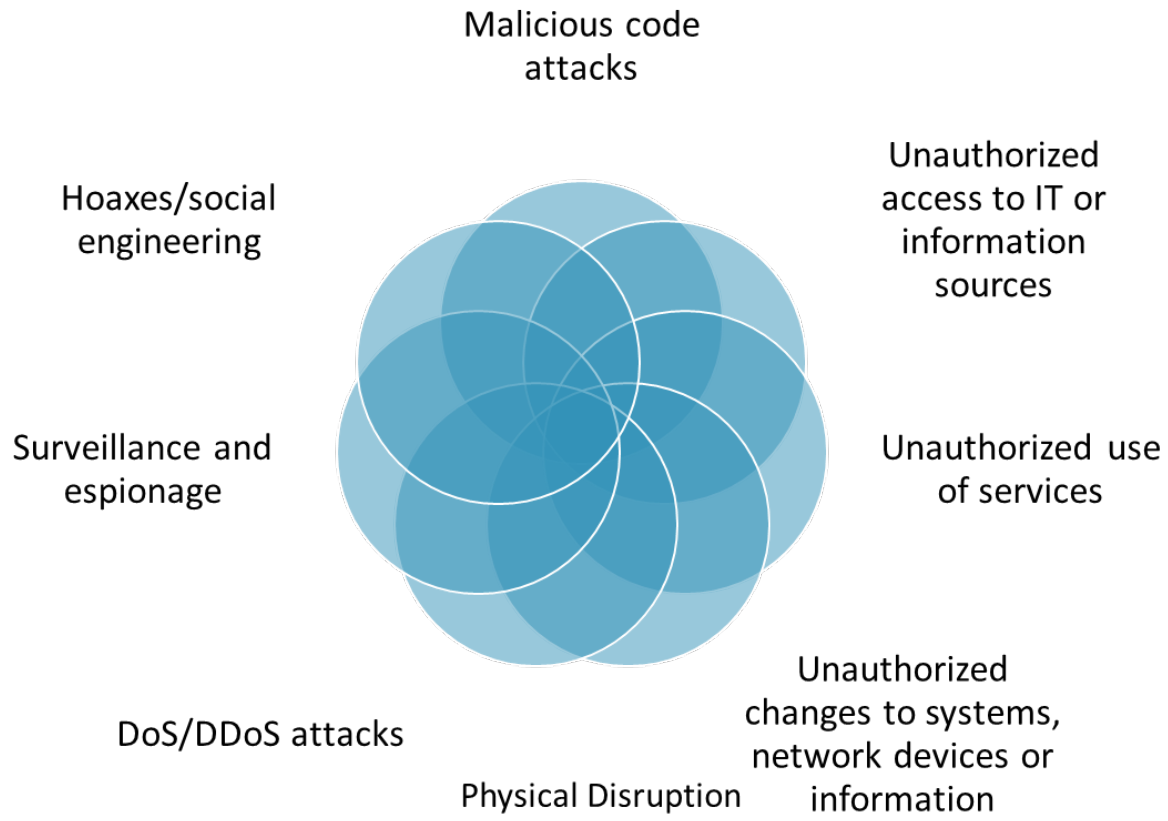
Are your existing detection means effective? How much can they see?

Do you have the right people looking at the details?

How often are you looking for events?

What details are you provided to get context?

Can you even define a "normal" event?



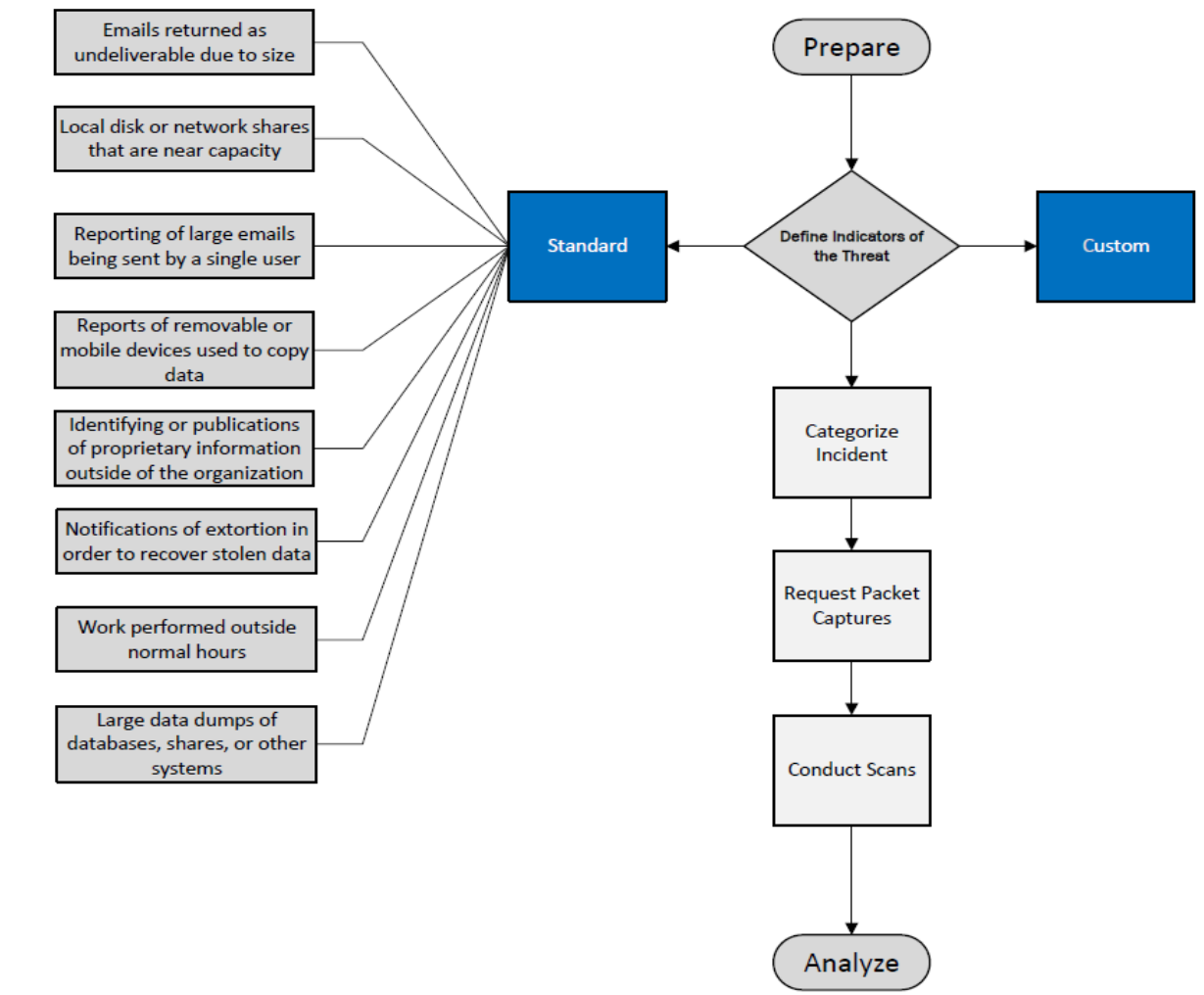
COMMON INCIDENT TYPES

RESPONSE

Response Planning	Communications	Analysis	Mitigation	Improvement
Prepare before and respond appropriately	Know who needs information, when and how	Ensure you understand the event and can design a recovery that's effective	Limit the scope and impact as you resolve the event	Review the event to strengthen your current capabilities
Deliverable: Incident Response Plan	Deliverable: Incident/Crisis Communication Plan	Deliverable: Incident Checklist and Playbook	Deliverable: Incident Containment Plan	Deliverable: Root Cause/After Action Analysis (5 Why's)

IR POLICY & PLAYBOOK

- Need to outline who is involved
  - Legal
  - HR
  - PR
  - Executives
  - IT
- Need to establish repeatable practices
  - Playbook & Checklists – information gathering; evidence collection; reporting



CHECKLISTS

- Well developed checklists guide the investigation; collect information and assist in reporting
- Checklists should be practiced before incidents

ase No.:_____

ation

cident scope? ☐ Local ☐ Regional ☐ Enterprise-wide

es:_____

7 Who reported the incident?_____

8 Which users are impacted?_____

9 What systems are involved?_____

10 What evidence do we have?_____

☐ Document Means of Incident

11 System Common Name:_____
12 System Asset ID:_____
13 System Serial Number:_____
14 Network Address :(IP, MAC, etc.)_____
15 Physical Location:_____

16 Responsible Unit/Organization:_____

17 Support Contact :(e.g., Sysadmin, App, etc.):_____

18 System Role/Use:_____

19 Protected Data? ☐ PHI ☐ PII ☐Financial ☐ PCI ☐ IP ☐ other:_____

20 Important Applications or Services:_____

f data elements:_____

elease

Identify
- ☐ Recognize existe
- ☐ Gather Information
- ☐ Document Means of Incident
- ☐ Obtain Logs & Documents
- ☐ Identify Method of Incident
- ☐ Identify Initial Scope of the Incident
- ☐ Identify what led to Incident
- ☐ Notify Management
- ☐ Update IR Database & Track Costs
- ☐ Image the System & Preserve Relevant Data
- ☐ Respond to Incident

Containment
- ☐ Consult regarding isolation
- ☐ Isolate the System
- ☐ Identify Source of Incident
- ☐ Verify Integrity of Backups
- ☐ Review Accounts & Access
- ☐ Increase Network & System Monitoring
- ☐ Update IR Database & Track Costs

Eradication
- ☐ Disable Access & Services
- ☐ Rebuild the System from Base Image
- ☐ Patch System & Install Application Updates
- ☐ Review & Document System Configuration
- ☐ Scan the System for Vulnerabilities
- ☐ Update IR Database & Track Costs

Recovery
- ☐ Restore User & Application Data
- ☐ Restore Any Transactions from Redundant System
- ☐ Verify System Restoration Actions
- ☐ Reconnect System Access
- ☐ Return System to Production
- ☐ Monitor System for Repeated Attack
- ☐Update IR Database & Track Costs

Resolution
- ☐ Prepare Regulatory Incident Reports
- ☐ Schedule and Hold Incident Post-Mortem
- ☐ Document Control Failures & Vulnerabilities
- ☐ Document Policy, Control & Procedure Gaps
- ☐ Develop Resolution Plan
- ☐ Assign Resolution Plan Activities
- ☐ Implement Resolution Plan
- ☐ Close Incident in IR Database
- ☐ Finalize and Share Incident Costs

RUBIC

INCIDENT RESPONSE TEAMS (IRTS)

- Pre-designated teams help to quickly assemble people with useful skills.
  - Depending on the incident, specialized skills may be needed.
- IRTs may be centralized, distributed or a hybrid model.
- IRT structure should be reviewed and approved by senior management

WHO IS ON THE TEAM?

A typical IRT includes:

Information security manager

Steering committee/advisory board (governance position only)

Permanent/dedicated team members

Virtual/temporary team members

Other positions include:

Incident response manager

Incident handler

Investigator

IT security specialists

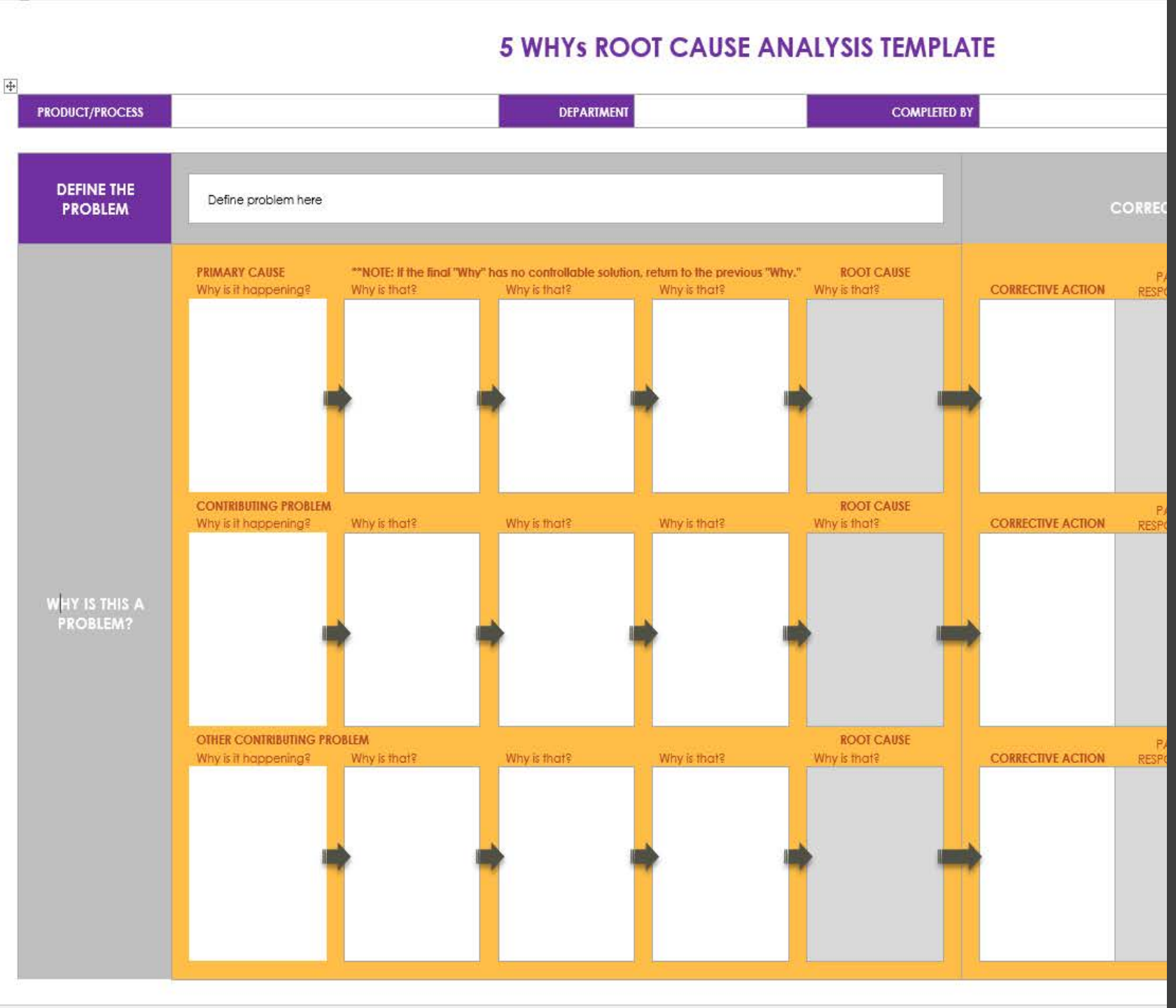
IT specialists/representatives

Business managers

Legal, HR, PR

Risk management specialist

Physical security/facilities manager



RECOVERY & IMPROVEMENT

- CSF expects continuous improvements
- Root Cause feeds into to enhancing your internal capabilities
- Helps prioritize spend and return on security investment after an event


QUESTIONS

RUBICON
ADVISORY GROUP

THANK YOU

Shawn Sines, CISSP, ITIL

shawn@therubiconadvisorygroup.com

https://www.therubiconadvisorygroup.com/