

# Cybersecurity Webinar Series

Part II - Cybersecurity Hazards: Threat, Assessment & Recovery

February 26, 2020



# Q&A

The screenshot shows a browser window displaying the Zoom website. The browser's address bar shows 'https://zoom.us'. A 'View Options' dropdown menu is open, showing 'Original Size' and 'Exit Full Screen'. The website header includes the Zoom logo, navigation links for 'SOLUTIONS', 'PLANS & PRICING', and 'CONTACT SALES', and user options for 'JOIN A MEETING', 'HOST A MEETING', and 'MY ACCOUNT'. The main content area features the headline 'One Consistent Enterprise Experience.' followed by six feature cards: Meetings, Video Webinar, Zoom Rooms, Business IM, H.323/SIP Connector, and Developer Platform. Each card includes a description and links to 'Watch Video' and 'Learn More'. A meeting overlay is visible at the bottom of the browser window, showing 'Audio Settings', 'Chat', 'Raise Hand', 'Q&A', and a 'Leave Meeting' button.

Zoom

SOLUTIONS PLANS & PRICING CONTACT SALES

JOIN A MEETING HOST A MEETING MY ACCOUNT

One Consistent Enterprise Experience.

- Meetings**  
Online Meetings, Training & Technical Support  
[Watch Video >](#)  
[Learn More >](#)
- Video Webinar**  
Marketing Events & Town Hall Meetings  
[Watch Video >](#)  
[Learn More >](#)
- Zoom Rooms**  
Build Collaboration-Enabled Conference Rooms  
[Watch Video >](#)  
[Learn More >](#)
- Business IM**  
Cross-Platform Messaging & File Sharing  
[Watch Video >](#)  
[Learn More >](#)
- H.323/SIP Connector**  
Bring H.323/SIP Video Systems to the Cloud  
[Watch Video >](#)  
[Learn More >](#)
- Developer Platform**  
Empower Your Apps With Video, Voice & Screen Sharing  
[Customer Spotlight >](#)  
[Learn More >](#)

Happiest Customers. Best Reviews.

Audio Settings ^

Chat Raise Hand Q&A

Leave Meeting

# Disclaimer

---

This is a NYS Health Center Controlled Network (NYS-HCCN) Activity  
A HRSA-Funded Project of the Community Health Care Association of New York State  
HCCN Grant Number: H2QCS30278

# Welcome

---



## Alex Lipovtsev

*Director – Health Center Support  
Emergency Management*



[alipovtsev@chcanys.org](mailto:alipovtsev@chcanys.org)



212-279-9686 x127



## Avery Epstein

*Program Manager  
Data & Technology*



[aepstein@chcanys.org](mailto:aepstein@chcanys.org)



212-279-9686 x109

# 2020 HCCN Webinar Series

The webinar series consists of 3 parts with the following schedule:

February 12

Part I - Emergency Management Planning for Cybersecurity

- *Introduction, general concepts of emergency management that would be important to consider for cybersecurity and protecting your data and systems.*

Today

February 26

Part II – Cybersecurity Hazards: Threat, Assessment & Recovery

- *Focus on cybersecurity as a specific hazard, assessment of vulnerabilities, making a robust plan and recovering quickly when affected.*

March 10

Part III – Cybersecurity through the lens of Business Continuity

- *Cybersecurity activities through the prism of the general organizational business continuity planning efforts*

# 2020 HCCN Webinar Series

Additionally, HITEQ will host the following webinars part of this HCCN series:

## March 24 Ransomware Guidance

*12:00 pm – 1:00 pm*

- TO JOIN -

<https://zoom.us/j/958917558?pwd=emZ2WXF1N3o2eU1YSjMzdmJOZFhkdz09>

Password: 290814

## April 7 Cybersecurity Breach Protection and Response

*11:30 am – 12:30 pm*

- TO JOIN -

<https://zoom.us/j/342999407?pwd=cEE4RUtMMTZ2dGRoSitRNW5Pd3Jldz09>

Password: 255076

# Today's Objectives

---

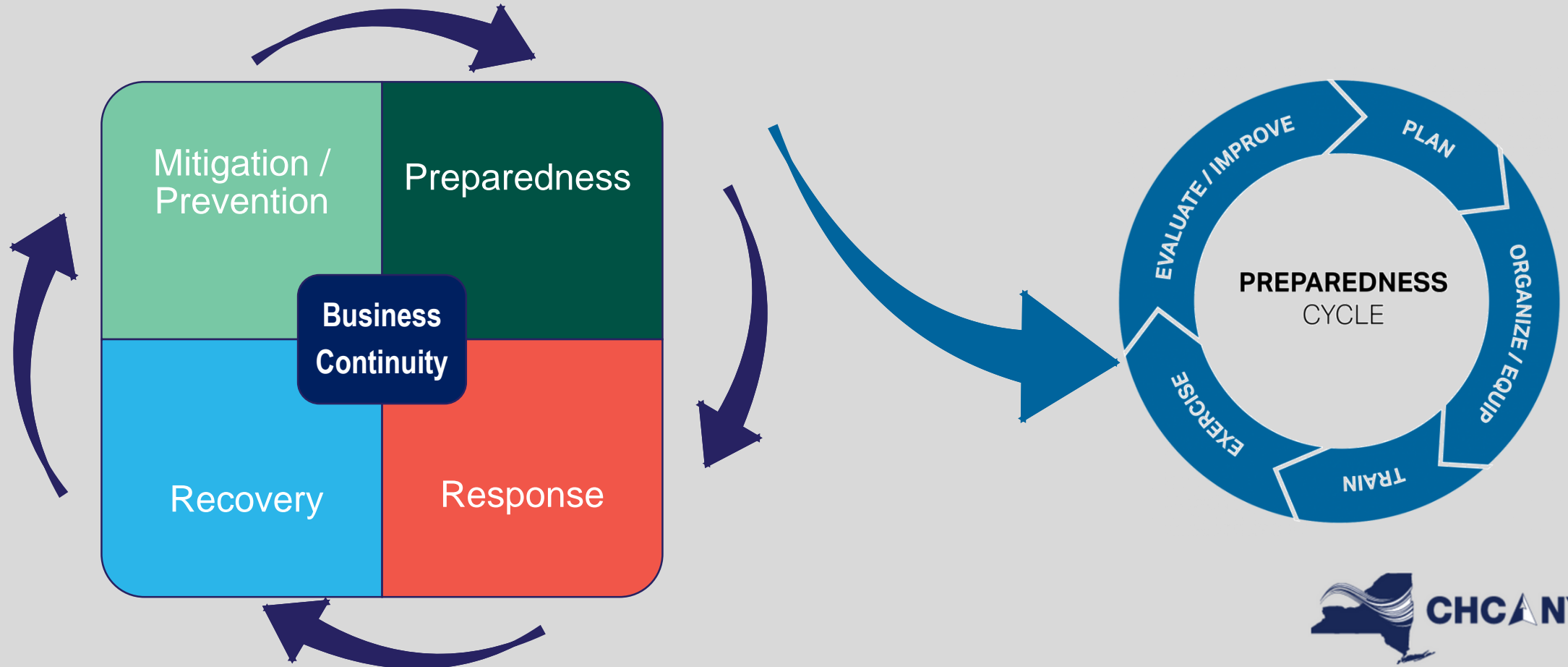
- Define structure of a hazard-specific plan
- Introduce the Cybersecurity Framework
- Define steps for setting up effective cybersecurity plans
- Provide relevant resources

# QUICK RECAP

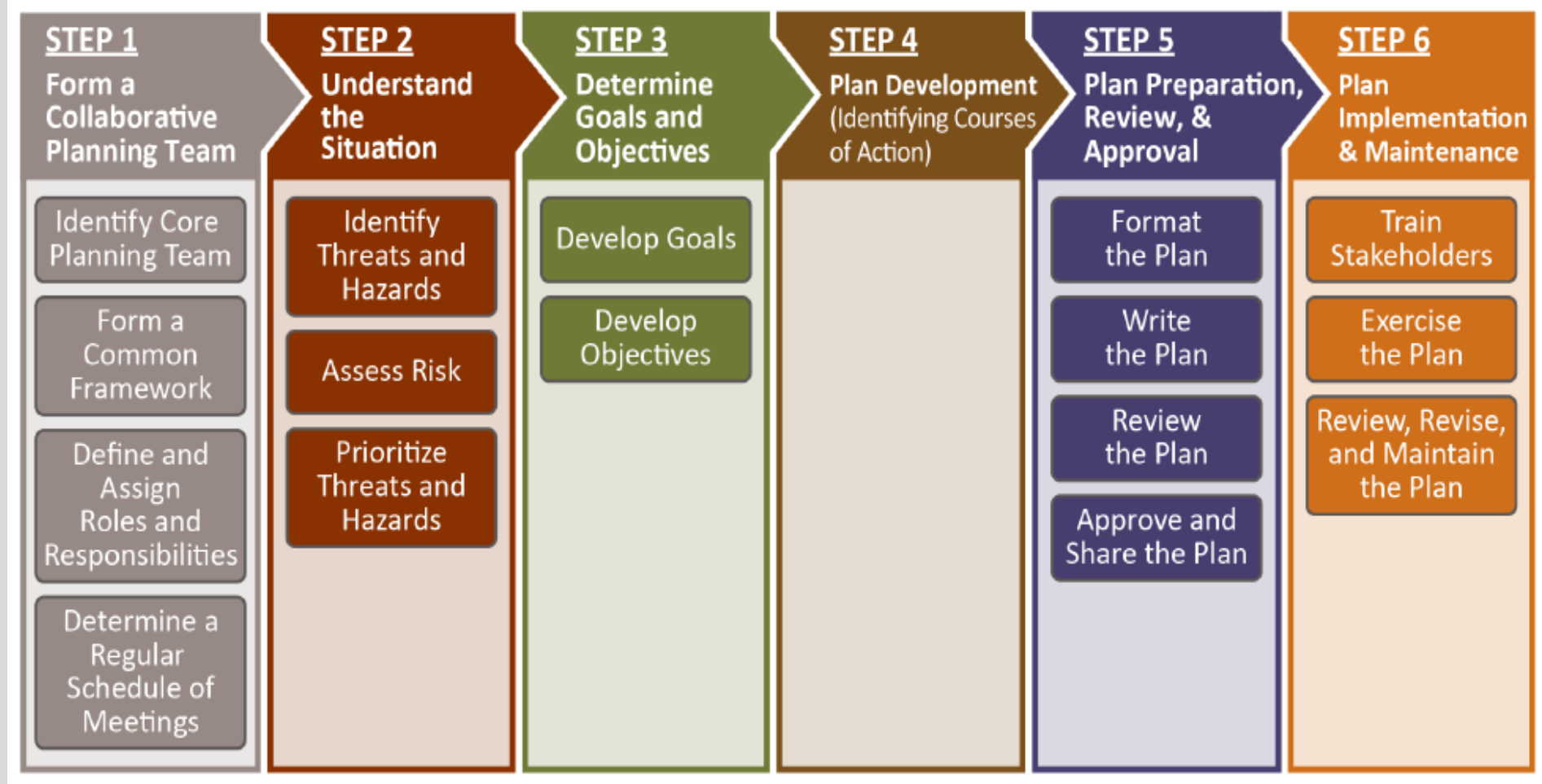


# The Emergency Management Cycle

Emergency Management Programs are based on the four phases of the Emergency Management cycle:



# Steps in the EM Planning Process



Source: FEMA

<https://www.fema.gov/media-library/assets/documents/25975>

# EOP Traditional Format

- **Base Plan**
  - *Intro, Purpose, Communications, Finance etc.*
- **Functional Annexes**
  - *Business Continuity, Volunteer Management, Evacuation, Fire Safety, etc.*
- **Hazard-, Threat-, or Incident- Specific Annexes**
  - *Coastal Storm, Infectious Disease, **Cyberattack**, Inclement Weather, Active Shooter, etc.*



## Developing and Maintaining Emergency Operations Plans

Comprehensive Preparedness Guide (CPG) 101

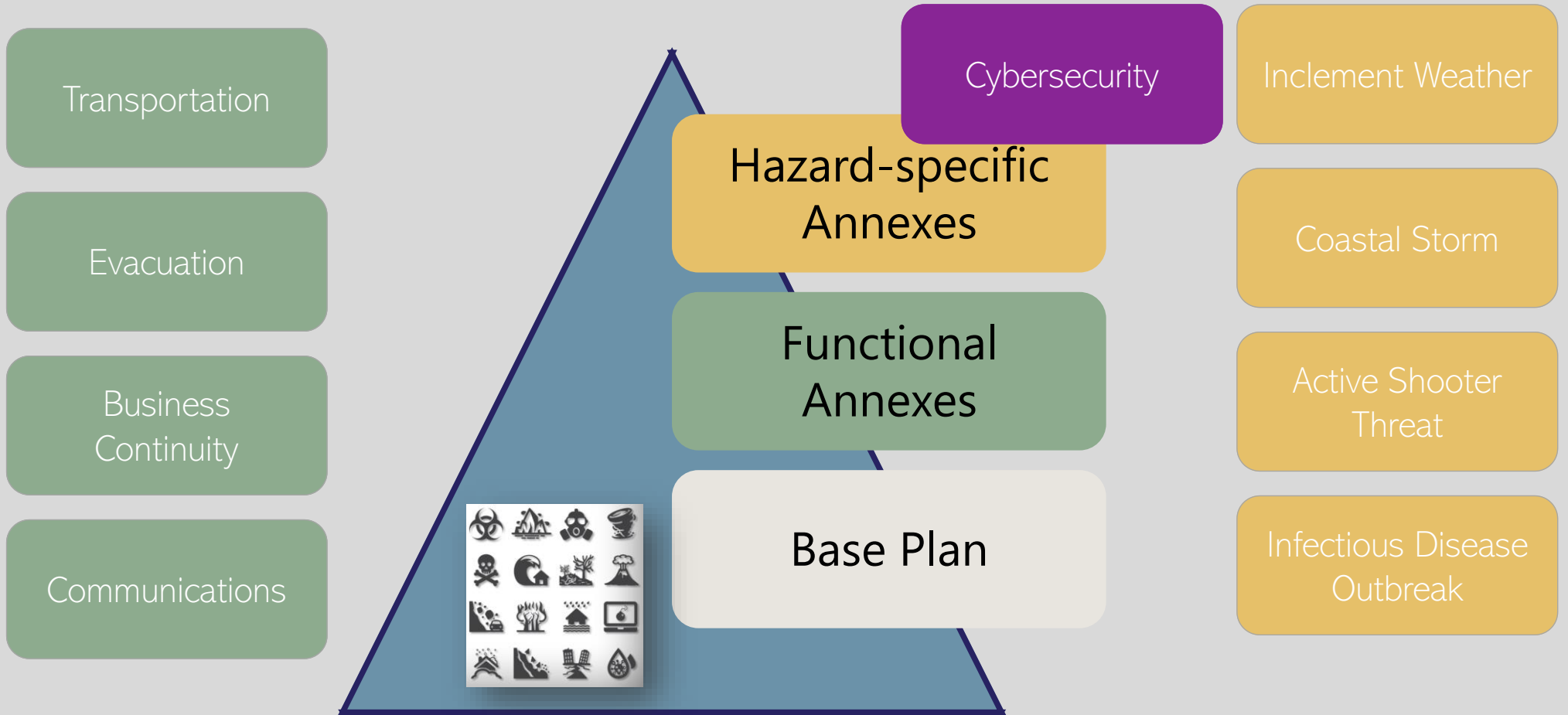
Version 2.0

November 2010



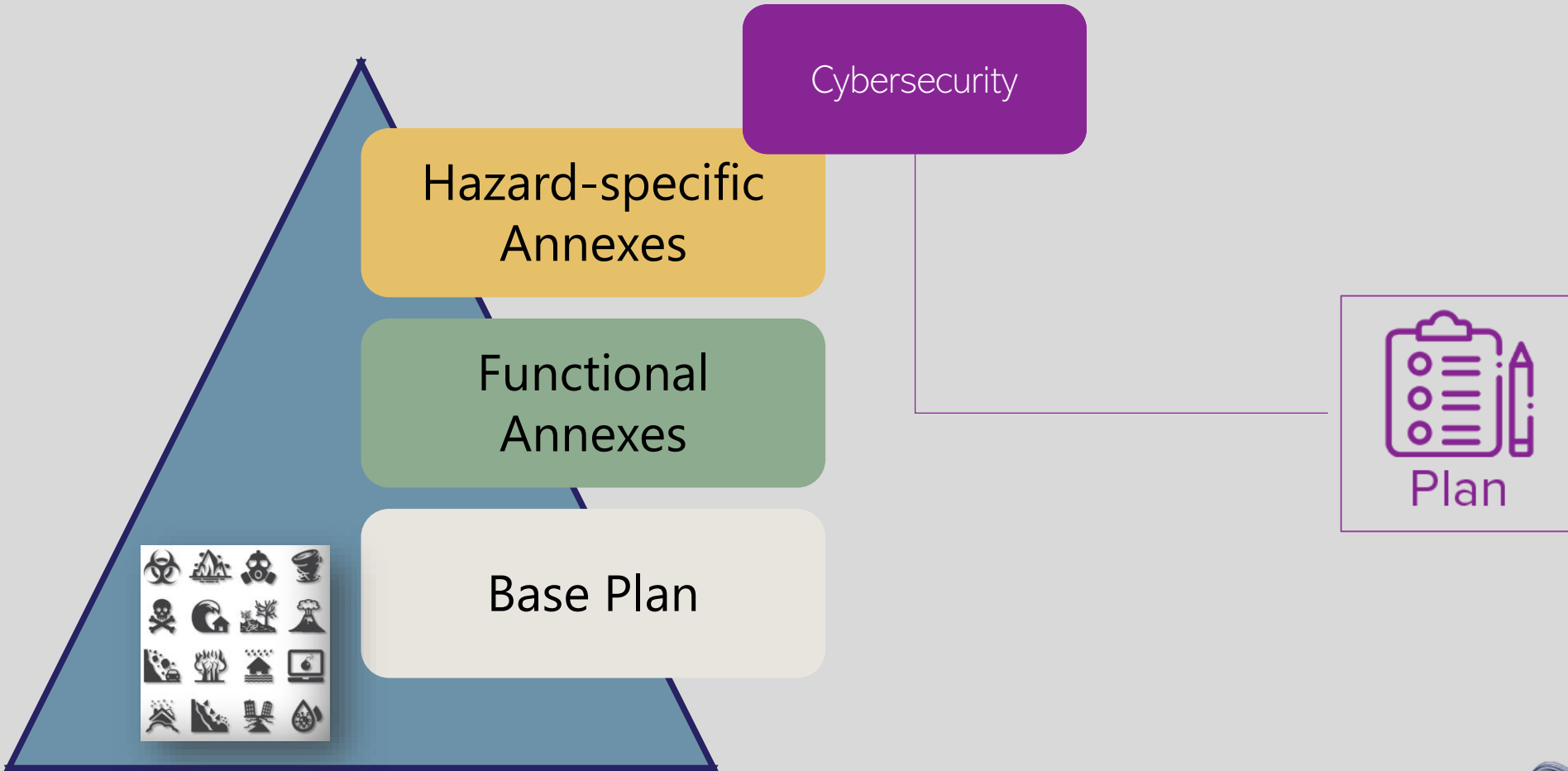
FEMA

# Traditional Format



# CYBERSECURITY HAZARD-SPECIFIC PLAN

# Hazard-Specific Annex for Cybersecurity



# Sample Cyber Security Plan Elements

## 1. Introduction

## 2. Purpose

A. *Scope*

B. *Planning Assumptions*

## 3. Policies and Agreements

- *Activation*

## 4. Situation and Assumptions

## 5. Roles and Responsibilities

## 6. Concept of Operations

- *Mitigation, Preparedness, Response, Recovery;*

## 7. Direction and Control

## 8. Plan Development

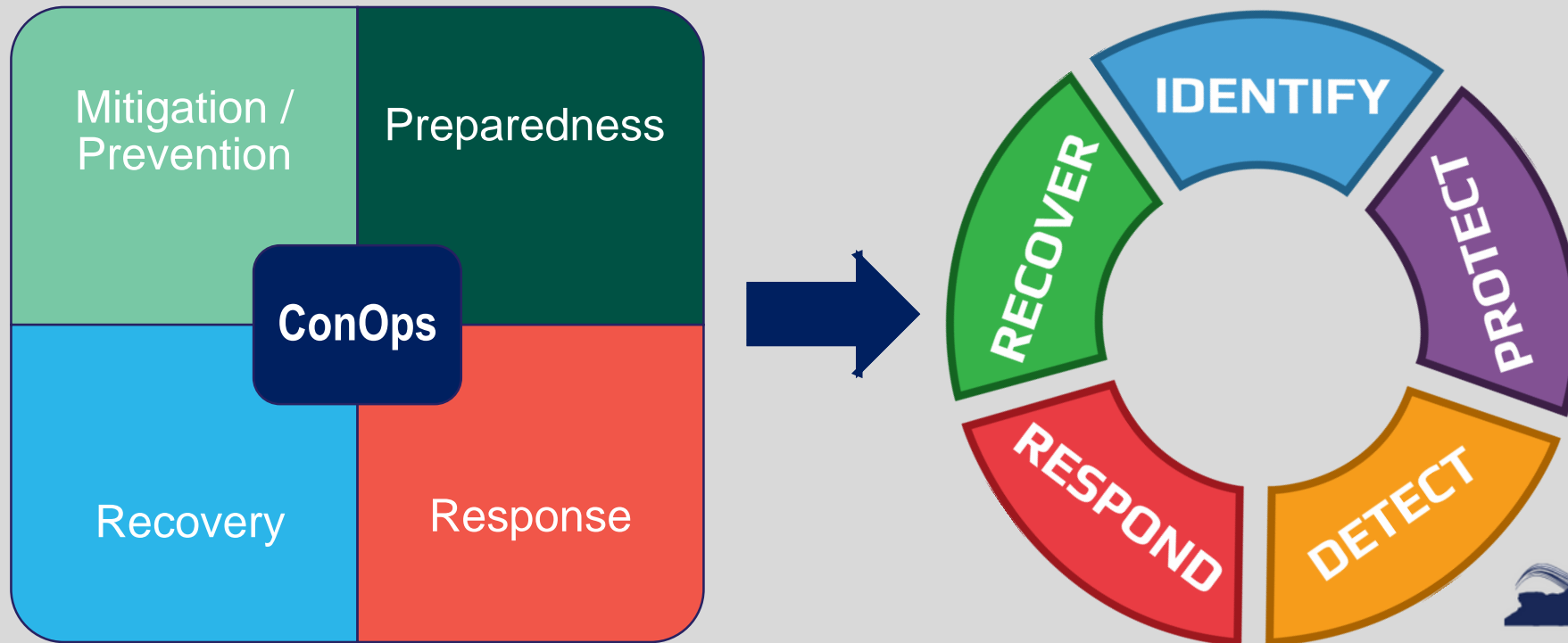
## 9. Standards, Regulations and Guidelines

## 10. Appendices

- *Appendix A - Glossary*

# Concept of Operations (CONOPS)

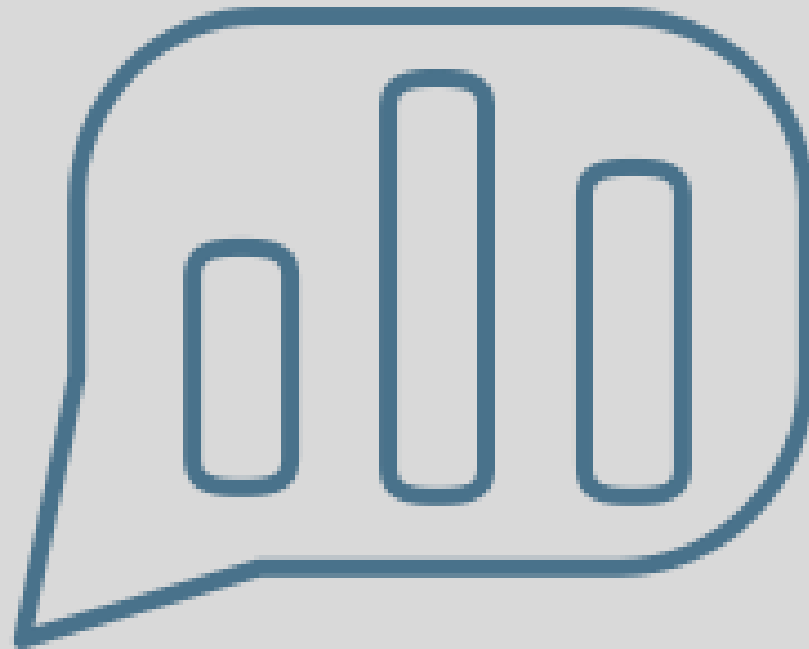
- The Concept of Operations (CONOPS) is a user-oriented document that “described systems characteristics for a proposed system from a user’s perspective.
- The CONOPS section explains, in **very broad terms**, the process and strategy involved in preparing, responding, recovering, and mitigating against the impacts of hazards that threaten the health center.





# Participant Poll 1

---



# THE CYBERSECURITY FRAMEWORK

# The Cybersecurity Framework

- Set forth by the *National Institute of Standards and Technology (NIST)* under the United States Commerce Department.
- NIST is responsible for developing information security standards for federal agencies.
- The **Cybersecurity Framework** is a set of guidelines for private sector companies to follow to be better prepared in identifying, detecting, and responding to cyber-attacks



<https://www.nist.gov/cyberframework>

# Three Primary Components

- **Core**

*Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls*

- **Profiles**

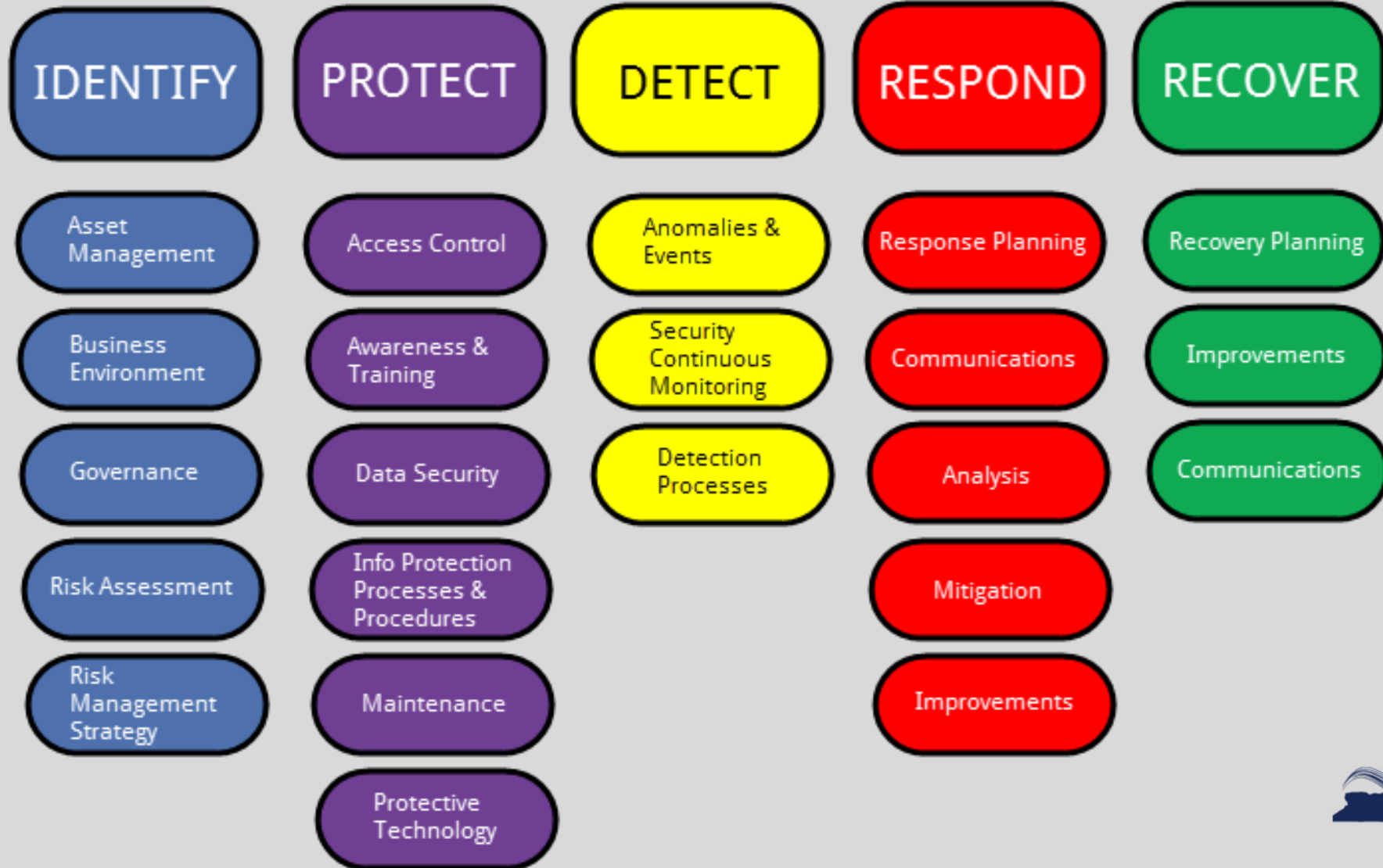
*Alignment of an organization's requirements and objectives, risk appetite and resources **using** the desired outcomes of the Framework Core*

- **Implementation Tiers**

*A qualitative measure of organizational cybersecurity risk management practices*



# NIST Cybersecurity Framework



# Framework Core Function

IDENTIFY

**Identify** - Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

- Examples of outcome Categories within this Function include:
  - *Asset Management*
  - *Business Environment*
  - *Governance*
  - *Risk Assessment\**
  - *Risk Management Strategy\**

# Reminder: HIPAA Security Rule Requirements

---

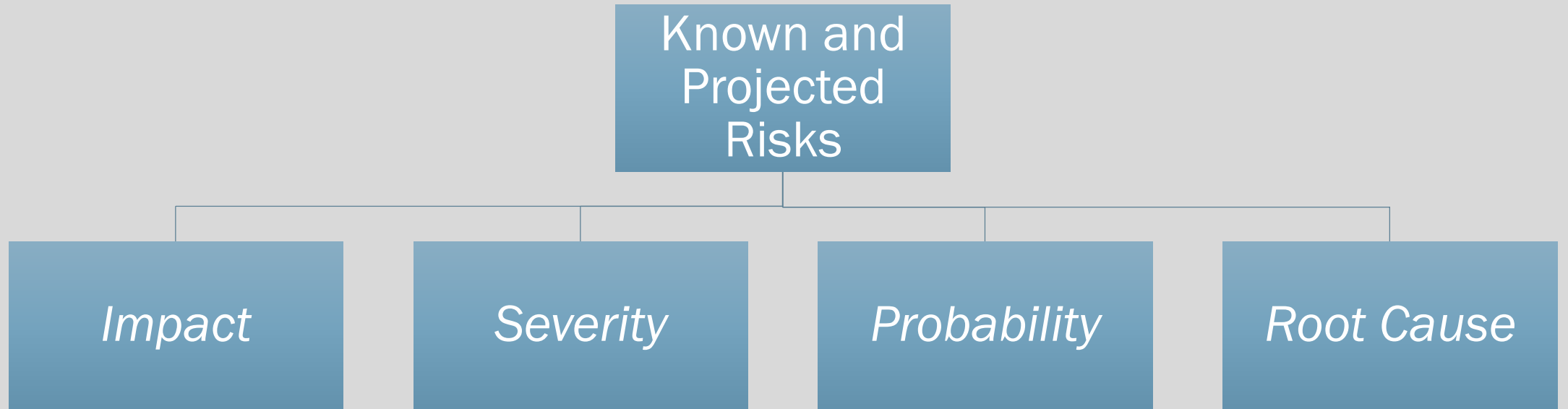
- The HIPAA Security Rule requires HIPAA covered entities and business associate to identify and respond to suspect or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. See **45 C.F.R. § 164.308(a)(6)**.
- The HIPAA Security Rule also requires HIPAA covered entities and business associates to establish and implement contingency plans, including data backup plans, disaster recovery plans, and emergency mode operation plans. See **45 C.F.R. § 164.308(a)(7)**.

<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf?language=es>



# Assessing Risk

---





# Resources for Assessing Risk

---

- Security Risk Assessment Tool from HealthIT.gov
  - <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool>
- HHS Guidance on Risk Analysis
  - <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>

# Risk Assessment: First Steps

---

- Identify stakeholders
- Hire a Chief Information Security Officer (CISO)
- Consider:
  - *How are you currently identifying risk?*
  - *What tools do you have?*
  - *Are near-misses captured?*

# Risk Assessment: Choosing a Vendor



## Spotlight

- Dynamic solutions
- Purpose Built Platforms
- Implementation: scope, timeline, budget

# Vendor Contracts & Business Associate Agreements (BAAs)

---

- Specific data security/protection issues to review include:
  - *Security and data protection expectations*
  - *Substantive notification obligations (e.g., information to be provided and shared by vendor)*
  - *Coordination of security incident response*
  - *Sharing of information regarding/performance of ongoing risk assessments and audits*
  - *Vendor data storage and data destruction practices*
  - *Level of customer data segregation*
  - *Termination/ unwinding/ transition requirements*
  - *Indemnification, limitation of liability, and insurance provisions*
- Ensure BAAs are negotiated in light of the scope of services being provided and the level of risk related to PHI.

# Homeland Security Cybersecurity Advisors

---

- The Department of Homeland Security's (DHS) Cybersecurity Advisor (CSA) Program offers cybersecurity assistance on a voluntary, no-cost basis to critical infrastructure organizations.
- The CSA Program maintains regional subject matter experts throughout DHS emergency management and protection regions. CSAs introduce organizations to various no-cost DHS cybersecurity products and services, along with other public and private resources, and act as liaisons to other DHS cyber programs and leadership.

## DHS Region II Cybersecurity Advisor (CSA)

R. S. Richard Jr.

[richard.richard@hq.dhs.gov](mailto:richard.richard@hq.dhs.gov)

(631) 241-3662



# Resource – Health Industry Cybersecurity Practices

---

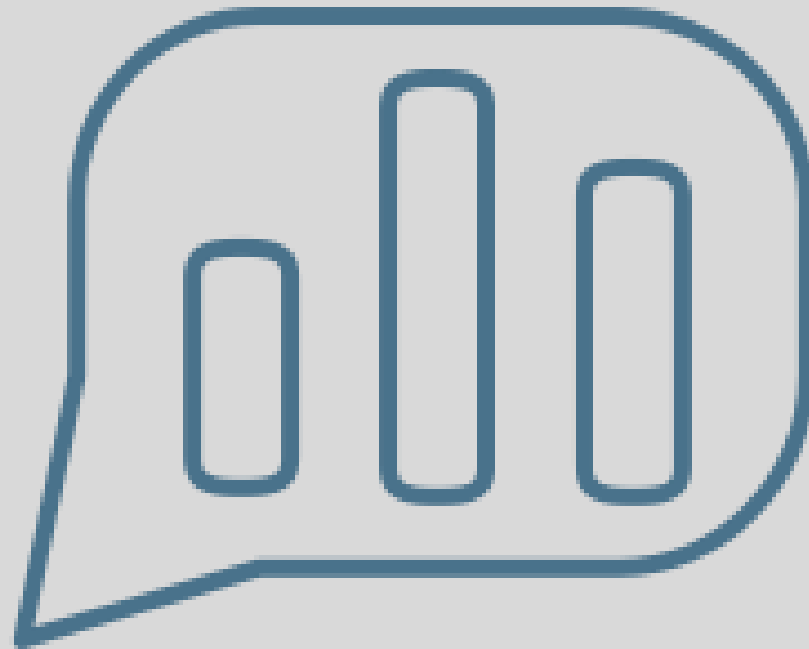
- Aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. It seeks to aid healthcare and public health organizations to develop meaningful cybersecurity objectives and outcomes.
  - *The **main document** examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores (5) current threats and presents (10) practices to mitigate those threats.*
  - ***Technical Volume 1** discusses these ten cybersecurity practices for small healthcare organizations*
  - ***Technical Volume 2** discusses these ten cybersecurity practices for medium and large healthcare organizations.*
  - ***Resources and Templates** volume provides additional cybersecurity resources and references*

SOURCE: [Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients](#)



# Participant Poll 2

---



# Framework Core Function

PROTECT

**Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.

- Examples of outcome Categories within this Function include:
  - *Identity Management and Access Control*
  - ***Awareness and Training\****
  - *Data Security*
  - *Information Protection Processes and Procedures*
  - *Maintenance*
  - *Protective Technology*



# Develop a Cybersecurity Training Program

---

- Consider conducting a tabletop exercise to simulate a cyber incident.
  - *Focus on incident management and response*
  - *Evaluate decision-making readiness*
  - *Review response plans, line up trusted providers*
  - *Prepare your message(s) to the public and key stakeholders*
  - *Identify and involve your counsel.*
- Determine if your organization outsources certain functions and identify involved stakeholders.
  - *Focus on "high risk" data*
  - *Not limited to IT department*

# Framework Core Function

DETECT

**Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

- Examples of outcome Categories within this Function include:
  - *Anomalies and Events*
  - *Security Continuous Monitoring*
  - *Detection Processes*

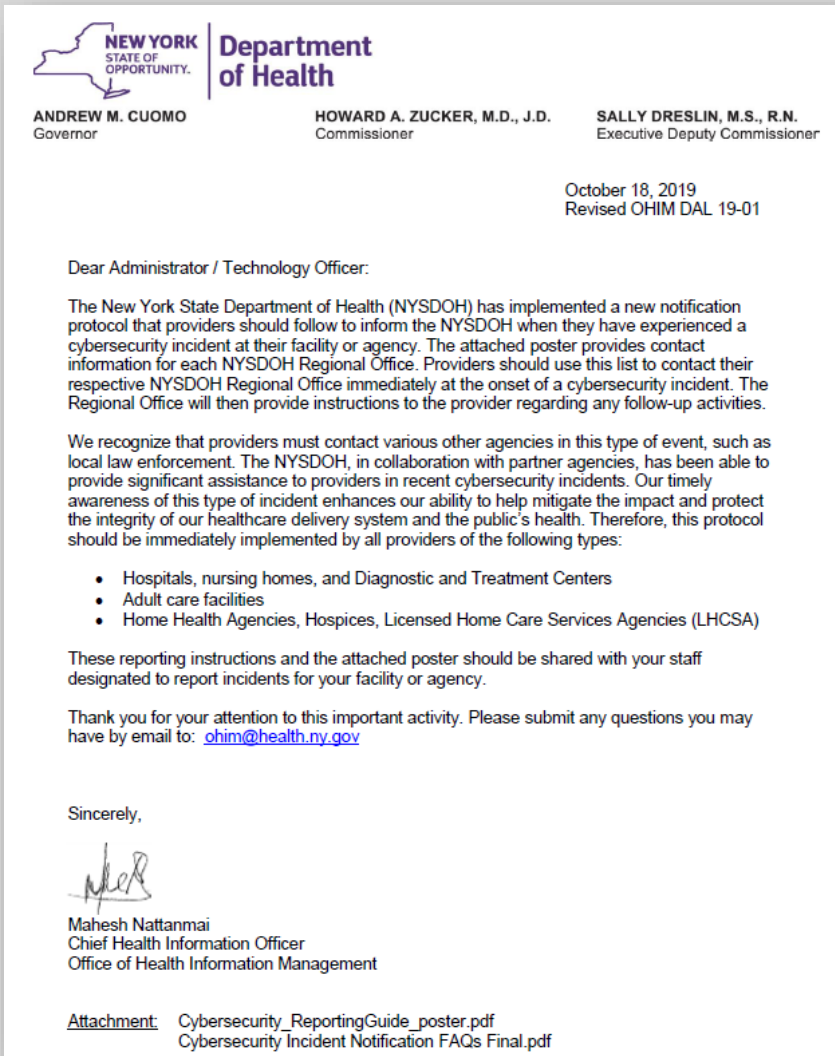
# Framework Core Function

RESPOND

**Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

- Examples of outcome Categories within this Function include:
  - *Response Planning*
  - ***Communications\****
  - *Analysis*
  - ***Mitigation\****
  - ***Improvements\****

# SDOH Cybersecurity Protocol



- State Department of Health (SDOH) notification protocol for when providers have experienced a **potential** cyber security incident at their facility or agency.
- Issued by Office of Health Information Management (OHIM DAL 19-01) on August 12, 2019 and in effect immediately.
- **Update** issued by Office of Health Information Management (Revised OHIM DAL 19-01) on October 18, 2019. Includes a FAQ sheet.
- Providers should contact their respective NYSDOH Regional Office immediately at the onset of a cybersecurity incident.
- For questions: Please send an e-mail to [ohim@health.ny.gov](mailto:ohim@health.ny.gov)



# SDOH Cybersecurity Protocol (cont.)

## Business Hours

8:30 am to 4:45 pm weekdays and non-holidays, unless noted

### Capital District

(518) 402-1036

Albany, Clinton, Columbia, Delaware, Essex, Franklin, Fulton, Greene, Hamilton, Montgomery, Otsego, Rensselaer, Saratoga, Schenectady, Schoharie, Warren and Washington

### Central New York

(315) 477-8400

Broome, Cayuga, Chenango, Cortland, Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence, Tioga and Tompkins

### Metropolitan Area

(212) 417-5550

9:00 am to 5:00 pm  
Bronx, Kings, New York, Queens and Richmond

### Central Islip

(631) 851-8050

9:00 am to 5:00 pm  
Nassau and Suffolk

### New Rochelle

(914) 654-7005

9:00 am to 5:00 pm  
Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster and Westchester

### Western Area

(716) 847-4505

Allegany, Cattaraugus, Chautauqua, Chemung, Erie, Genesee, Livingston, Monroe, Niagara, Orleans, Ontario, Schuyler, Seneca, Steuben, Wayne, Wyoming and Yates

## After Hours Emergencies

4:45 pm to 8:30 am weekdays. Available 24 hours a day on weekends and holidays.

### NYSDOH Duty Officer

(866) 881-2809

Select option #1 for reporting an emergency.

**CALL 911 if there is immediate threat to public health or safety.**

In all cases, the cybersecurity incident should be reported to law enforcement.

## You're the Key to Reporting a Cybersecurity Incident!

An incident is considered a reportable "cybersecurity incident" under the New York State Department of Health guideline, if it affects patient care, or represents a serious threat to patient safety, including intrusions whose intent appears to be breach or theft of protected health records. Examples include, but are not limited to:

- Successful intrusions into a health care provider's information technology system (including those that are contracted out by the health care provider), network infrastructure, and/or medical equipment/devices.
- Ransomware attacks that disable all or part of information technology operations including administrative systems such as payroll, billing, or appointment scheduling.
- Cybersecurity incidents that have the potential to spread through established connections to other health care networks or government systems. Examples include file transfer systems or data reporting interfaces.






# What is the Role of the State Health Department?

---

- Engage with the provider to learn and assess the impact of the cyber event to the larger public health landscape
- Facilitate communication with State, Federal and third-party resources as the need arises
- Advise providers of alternative methods of continuing critical aspects of their operations during an IT outage
- Collect and share general information on the cyber threats with other providers to prevent and protect other providers from similar vulnerabilities
- Establish and maintain a trusted collaboration with all types of providers, associations, other stakeholders
- Liaise with Health Information Technology community as needed
- Protect State IT resources as necessary

# GNYHA Guide to Cybersecurity Reporting

RESPOND: Based on the specifics of the attack on your facility, consider the following actions.			
CYBER ACTIVITY TYPE	RECOMMENDED ACTION	AGENCY/ GOVERNANCE	
Has the cyber activity impacted medical devices?	 Report cybersecurity incidents through the Food and Drug Administration's (FDA) "Medical Device Reporting" (MDR) system. User facilities are required to report device-related deaths to the FDA and the associated manufacturer within 10 working days of when they became aware of the incident.	FDA	<b>FBI</b>  <b>FBI New York Regional Cyber Branch</b> (New York City, Nassau, Suffolk, Westchester, Putnam, Orange, and Rockland counties) Phone: 212-384-2023  <b>Albany Regional Office</b> Phone: 518-465-7551  <b>Buffalo Regional Office</b> Phone: 716-865-7800  <b>Newark Regional Office</b> (Covers majority of New Jersey) Phone: 973-792-3015  <ul style="list-style-type: none"> <li>View additional <a href="#">regional FBI offices</a>.</li> <li>File a complaint with the <a href="#">FBI Internet Crime Complaint Center</a>.</li> </ul>
Was there a breach of protected health information or other private information?	 Refer to <a href="#">HIPAA Breach Notification Rule</a> , 45 CFR §§ 164.400-414 to determine if breach reporting is necessary per the Office for Civil Rights (OCR) guidance. <ul style="list-style-type: none"> <li><a href="#">OCR's most recent cyber guidance</a></li> <li><a href="#">OCR's most recent ransomware guidance</a></li> </ul>	OCR	
	 <a href="#">New York State Information Security Breach and Notification Act</a> comprised of <a href="#">section 208 of the State Technology Law</a> and <a href="#">section 899-aa of the General Business Law</a> stipulates breach reporting requirements to certain State agencies by faxing a <a href="#">data breach form</a> . The Act applies to breaches of "private information," defined as any personal information concerning a natural person in combination with any one or more of the following data elements: social security number, driver's license number, account number, or credit or debit card number in combination with any required security code.	New York State Police  New York State Attorney General's Office	
		New York State Department of State	



# Mitigate! Healthcare Sector Attacks Can Spread Very Quickly

---

- May cause major disruption of the healthcare delivery system in a city, county, region, involving thousands of providers, patients and residents:
  - *Interconnected/interdependent provider networks; communications between referring providers deliver multiple access points for attack;*
  - *disparity between organizations' ability to address cybersecurity issues;*  
*health care as a whole will only be as secure as the weakest link*
  - *locations not expecting to be a target can serve as doorways to other, more complex partners with greater cyber risks and rewards for the hacker*



# After-Action Report / Improvement Plan

[INSERT NAME OF ENTITY]  
DATE: [PROVIDE DATE]

## INCIDENT AFTER ACTION REPORT

### Appendix A: IMPROVEMENT PLAN

Objective	Issue/Area for Improvement	Corrective Action	Capability Element	Start Date	Completion Date
Objective 1: Increase cybersecurity awareness	1. More regional members involved/representation from other agencies	Current members and participants are encouraged to advocate for attendance and leadership buy-in at their agencies and those of their partners wherever able.	Planning, Organization	11/29/18	03/21/19
	2. More individual-agency collaboration with their IT personnel, end-users, and emergency management personnel.	Increase collaboration across organizational departments and divisions for a common understanding of the threat and how to mitigate it	Planning, Organization	11/29/18	03/21/19
Objective 2: Cybersecurity integration	1. More leadership/executive involvement (mayors, exec, directors).	Increase collaboration with leadership in the pursuit of organizational change and threat management	Planning	11/29/18	03/21/19
	2. Incorporate Continuity of Operations Planning (COOP) and Business Impact Analysis (BIA) with organizational cybersecurity	Collaboratively review existing COOP and BIAs for alignment with cybersecurity	Planning, Organization	11/29/18	03/21/19
Objective 3:	1. Lack of understanding and or				

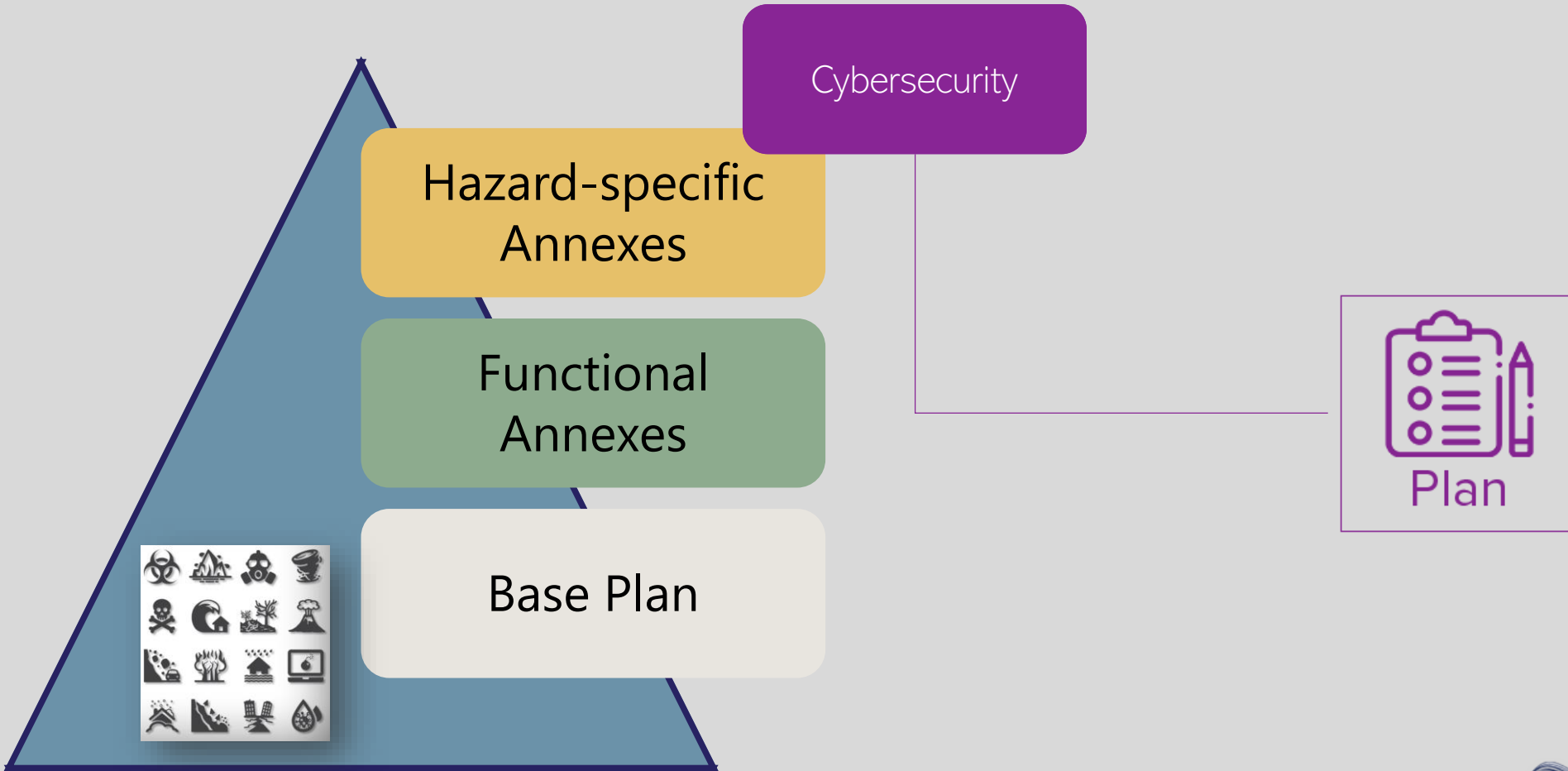
# Framework Core Function

RECOVER

**Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

- Examples of outcome Categories within this Function include:
  - *Recovery Planning*
  - *Improvements*
  - *Communications*

# Hazard-Specific Annex for Cybersecurity



# Healthcare Emergency Management & Business Continuity Framework

## Continuity | Response | Recovery

### Governance

**Emergency Operations Planning (EOP)**

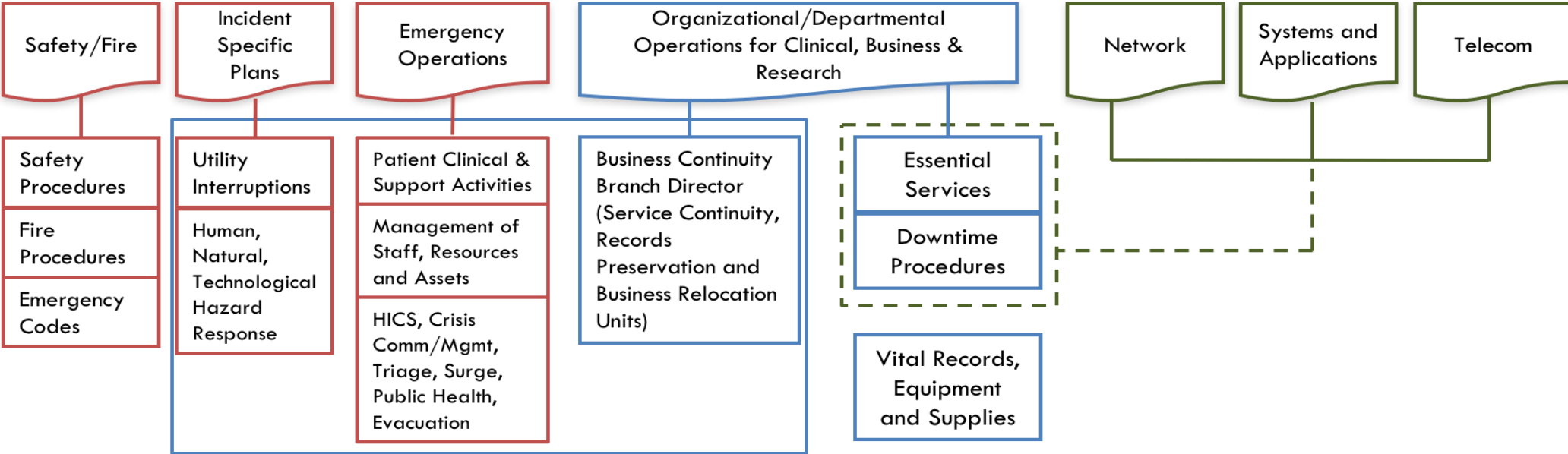
Plans, procedures and resources for all four emergency phases (mitigation, preparedness, response, and recovery), for all types of emergencies and disasters.

**Business Continuity Planning (BCP)**

Plans, procedures and resources to maintain and/or recover essential services and functions impacted by an event causing an interruption of normal operations.

**Disaster Recovery Planning (DRP)**

Plans, procedures and resources to maintain and/or recover the information technology systems, network, and telecommunications services.



An integrated, multi-disciplinary program focused on supporting and strengthening the organization's core mission

# Coming Up Next!

---

**March 10**

## Part III – Cybersecurity through the lens of Business Continuity

- *Cybersecurity activities through the prism of the general organizational business continuity planning efforts.*

[REGISTER HERE](#)

# Webinar Evaluation

---

We value your feedback!



# Questions?

---

**NYS HCCN**

[hccn@chcanys.org](mailto:hccn@chcanys.org)

