CYBERSECURITY FRAMEWORK ASSESSMENT AND IMPLEMENTATION

SRINI KOLATHUR

CISSP, CISA, CISM & MBA

Disclaimer

This webinar has been provided for educational and informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

WHO WE ARE …

EHR 2.0

SECURITY | COMPLIANCE | CERTIFICATION

We assist organizations and business associates develop and implement practices to secure sensitive data, and comply with regulations.

EDUCATION

Online Training, Webinars and Customized Workshop

DIY TOOLKIT

Assessment Portal, Training, Forms and more …

CONSULTING

Professional services to help you with your Compliance needs

ASSESSMENT SERVICES

Compliance, Certifications, Framework, Standards and Best practices

HIPAA/HITECH

Security, privacy and breach stds.

OSHA

Healthcare and Bloodborne Pathogens

CFR Part 11

Medical device security compliance

NIST Framework

800-53, 800-171 and more …

PCI DATA SECURITY

Payment card security

GDPR

European data security

ISO 27001

Security management program

Cybersecurity Framework

NIST Standards

AWS Security

AWS security setup

Azure Security

Microsoft Azure setup

Google Cloud

GCP Setup

SOC Certification

AICPA Service Organization Controls

SECURITY AND COMPLIANCE TOPICS WE SUPPORT

We’d love to hear from you if you need a customized service for your business needs

Srini Kolathur

CISSP, CISA, CISM, MBA

Director, EHR 2.0

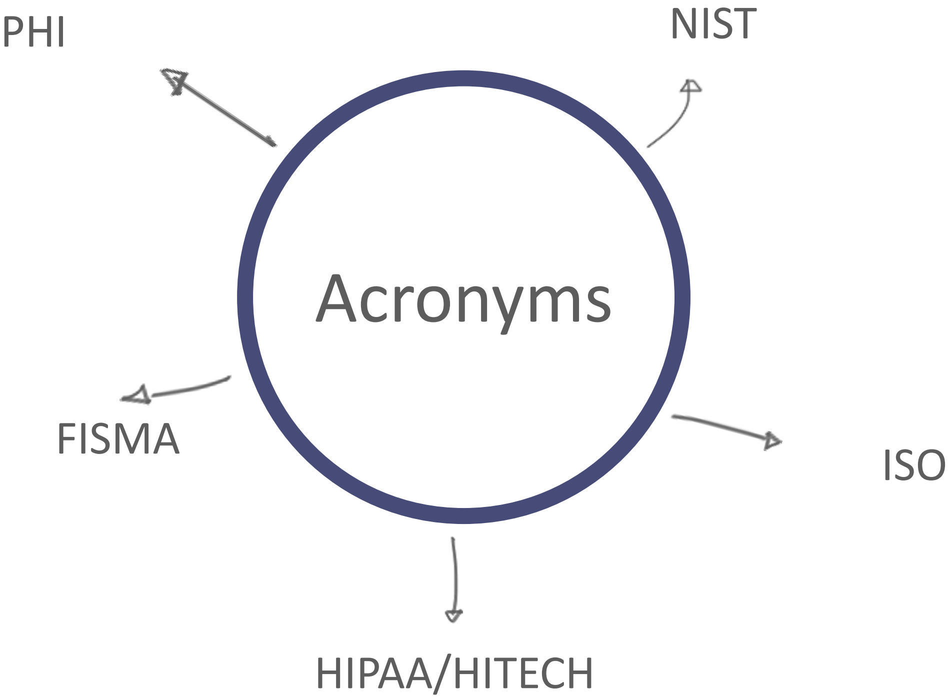
Srini's Background

- Security and Compliance
- Cisco IT Infrastructure
- HIPAA, PCI, Sarbanes-Oxley and ISO 27k Series
- A member of Rotary Club of Morrisville
- Interests: Running, healthy living and giving back

Agenda

- □ Cybersecurity Framework Overview
- □ The Five Functions
- □ Demo
- □ Summary

TERMS YOU MAY HEAR …



Acronyms

PHI

NIST

FISMA

ISO

HIPAA/HITECH

The Cybersecurity Framework...

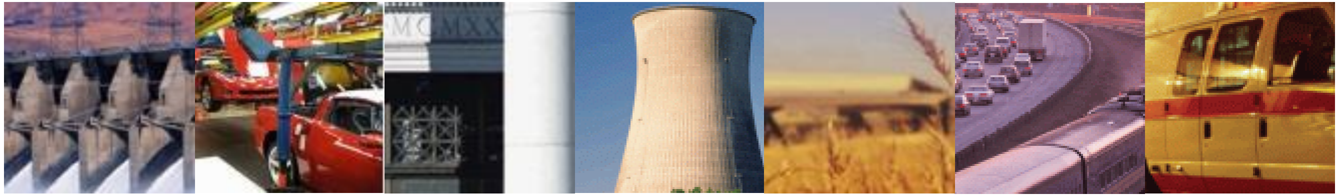
- Includes a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

- Provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.

- Identifies areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations.

- Is consistent with voluntary international standards.

The Framework is for Organizations…



- Of any size, in any sector in (and outside of) the critical infrastructure.
- That already have a mature cyber risk management and cybersecurity program.
- That don’t yet have a cyber risk management or cybersecurity program.
- Needing to keep up-to-date managing risks, facing business or societal threats.
- In the federal government, too…since it is compatible with FISMA requirements and goals.

Key Attributes

□ **It's a framework, not a prescriptive standard**

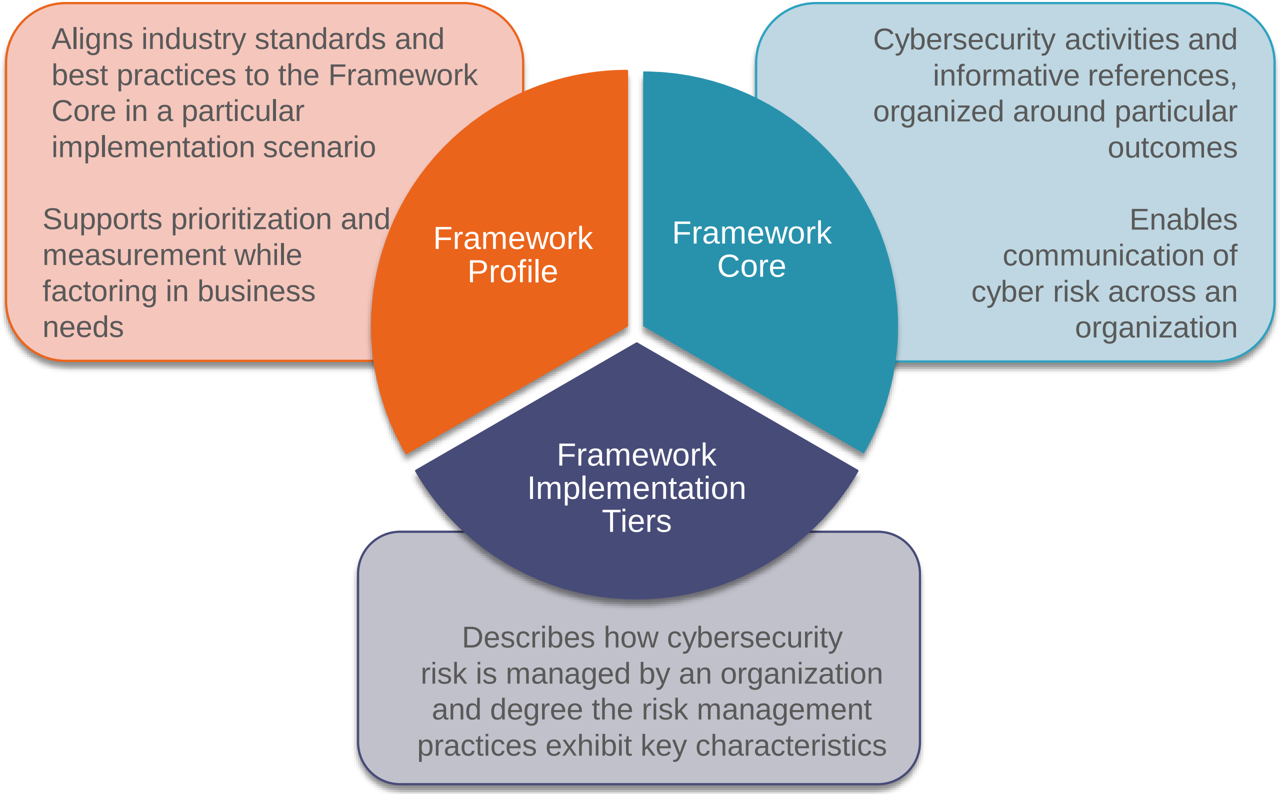
- Provides a common language and systematic methodology for managing cyber risk.
- Is meant to be adapted.
- Does not tell an organization ***how*** much cyber risk is tolerable, nor provide "the one and only" formula for cybersecurity.
- Enable best practices to become standard practices for everyone via common lexicon to enable action across diverse stakeholders.

□ **It's voluntary**

□ **It's a living document**

- It is intended to be updated as stakeholders learn from implementation, and as technology and risks change…more later.
- That's one reason why the Framework focuses on questions an organization needs to ask itself to manage its risk. While practices, technology, and standards will change over time—principles will not.

Cybersecurity 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

Implementation Tiers

	1	2	3	4
	Partial	Risk Informed	Repeatable	Adaptive
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization benefits my sharing or receiving information from outside parties			

Core

Cybersecurity Framework Component

	Function	Category	ID
What processes and assets need protection?	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
What safeguards are available?	Protect	Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes & Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
What techniques can identify incidents?	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
What techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
What techniques can restore capabilities?	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

Framework 7-Step Process

Step 1: Prioritize and Scope

Step 2: Orient

Step 3: Create a Current Profile

Step 4: Conduct a Risk Assessment

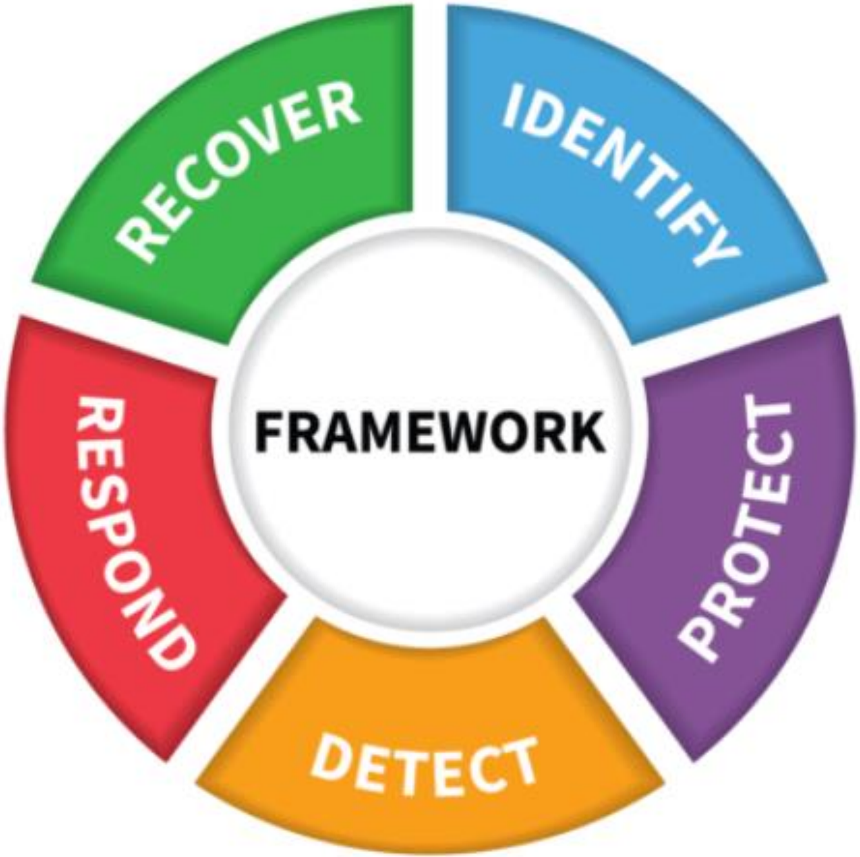
Step 5: Create a Target Profile

Step 6: Determine, Analyze, and Prioritize Gaps

Step 7: Implementation Action Plan

The Five Functions

- Highest level of abstraction in the core
- Represent five key pillars of a successful and wholistic cybersecurity program
- Aid organizations in expressing their management of cybersecurity risk at a high level

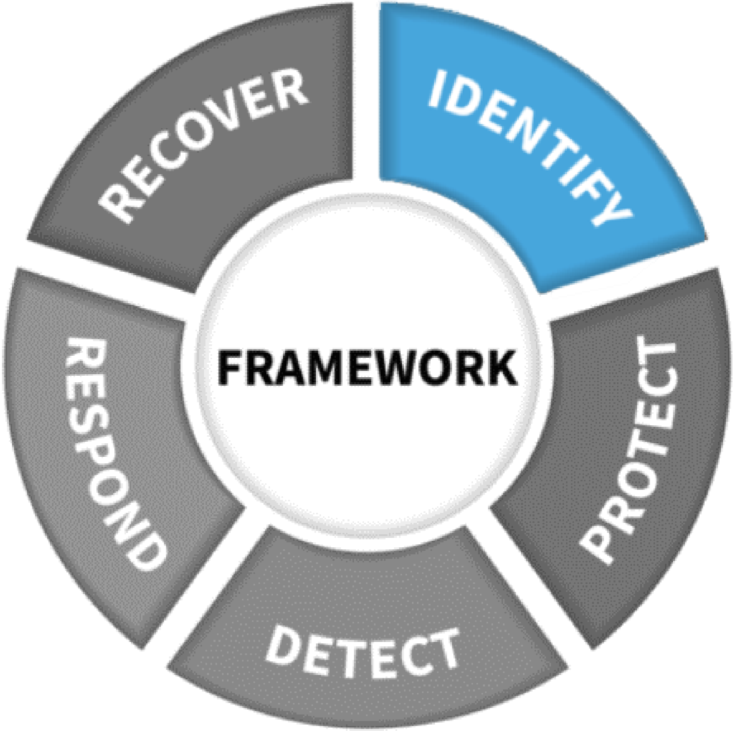


The Identify Function

The Identify Function assists in developing an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities

Example Outcomes:

- Identifying physical and software assets to establish an Asset Management program
- Identifying cybersecurity policies to define a Governance program
- Identifying a Risk Management Strategy for the organization

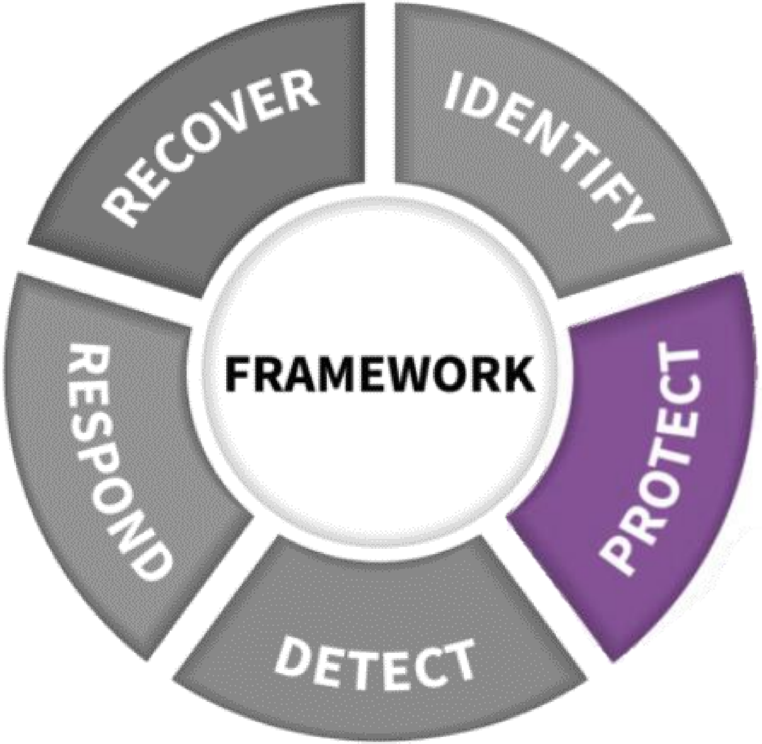


The Protect Function

The Protect Function supports the ability to limit or contain the impact of potential cybersecurity events and outlines safeguards for delivery of critical services

Example Outcomes:

- Establishing Data Security protection to protect the confidentiality, integrity, and availability
- Managing protective technology to ensure the security and resilience of systems and assists
- Empowering staff within the organization through awareness and training

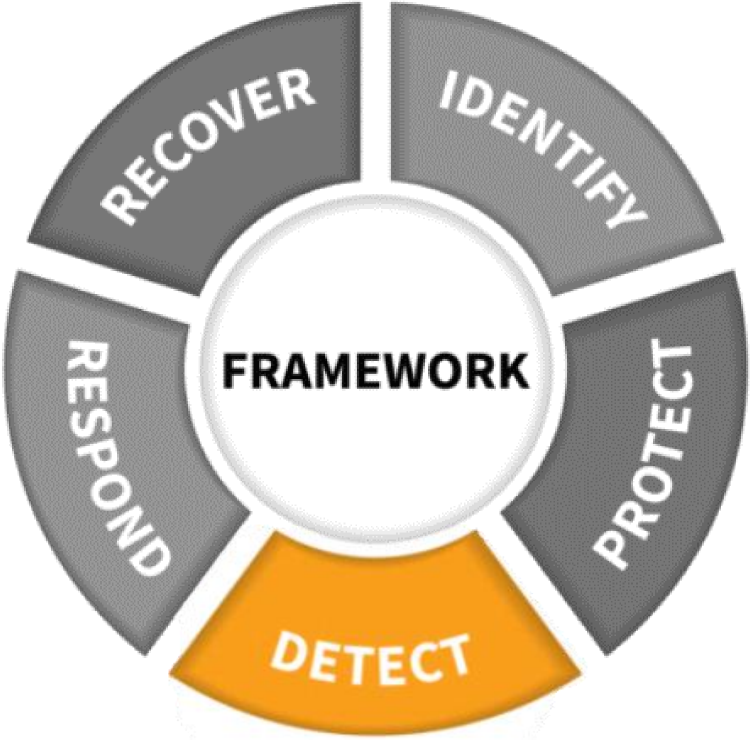


The Detect Function

The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner

Example Outcomes:

- Implementing security continuous monitoring capabilities to monitor cybersecurity events
- Ensuring anomalies and vvents are detected, and their potential impact is understood
- Verifying the effectiveness of protective measures

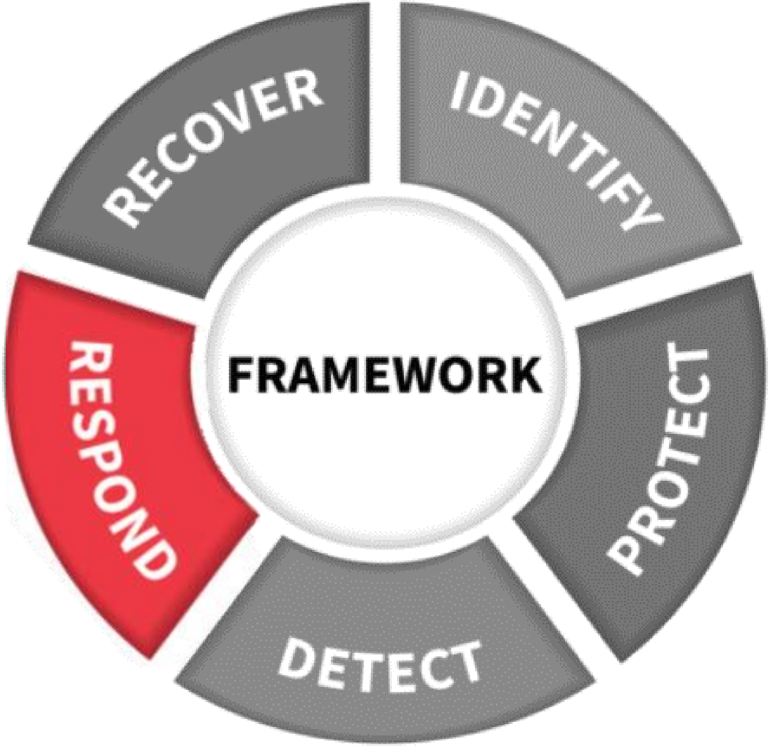


The Respond Function

The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident to minimize impact

Example Outcomes:

- Ensuring response planning processes are executed during and after an incident
- Managing communications during and after an event
- Analyzing effectiveness of response activities

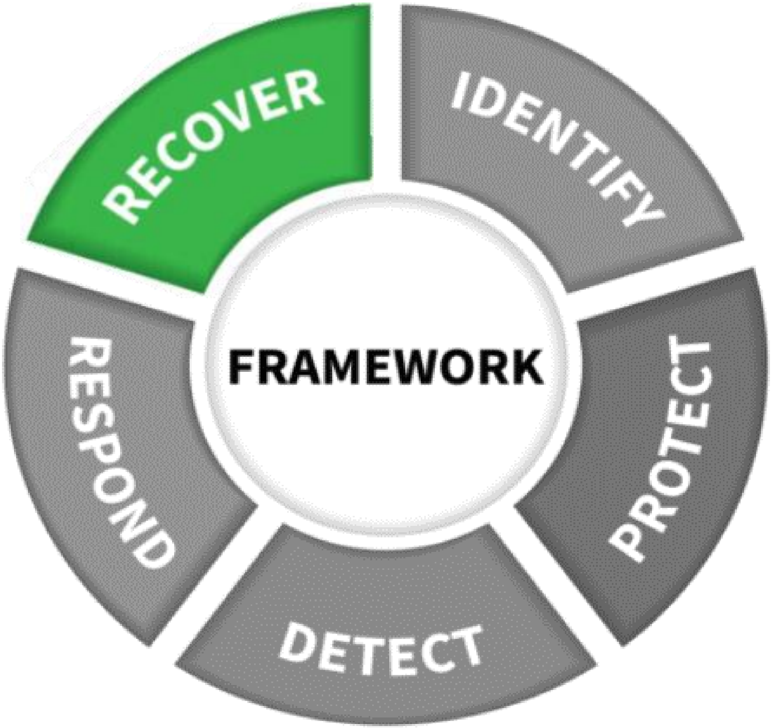


The Recover Function

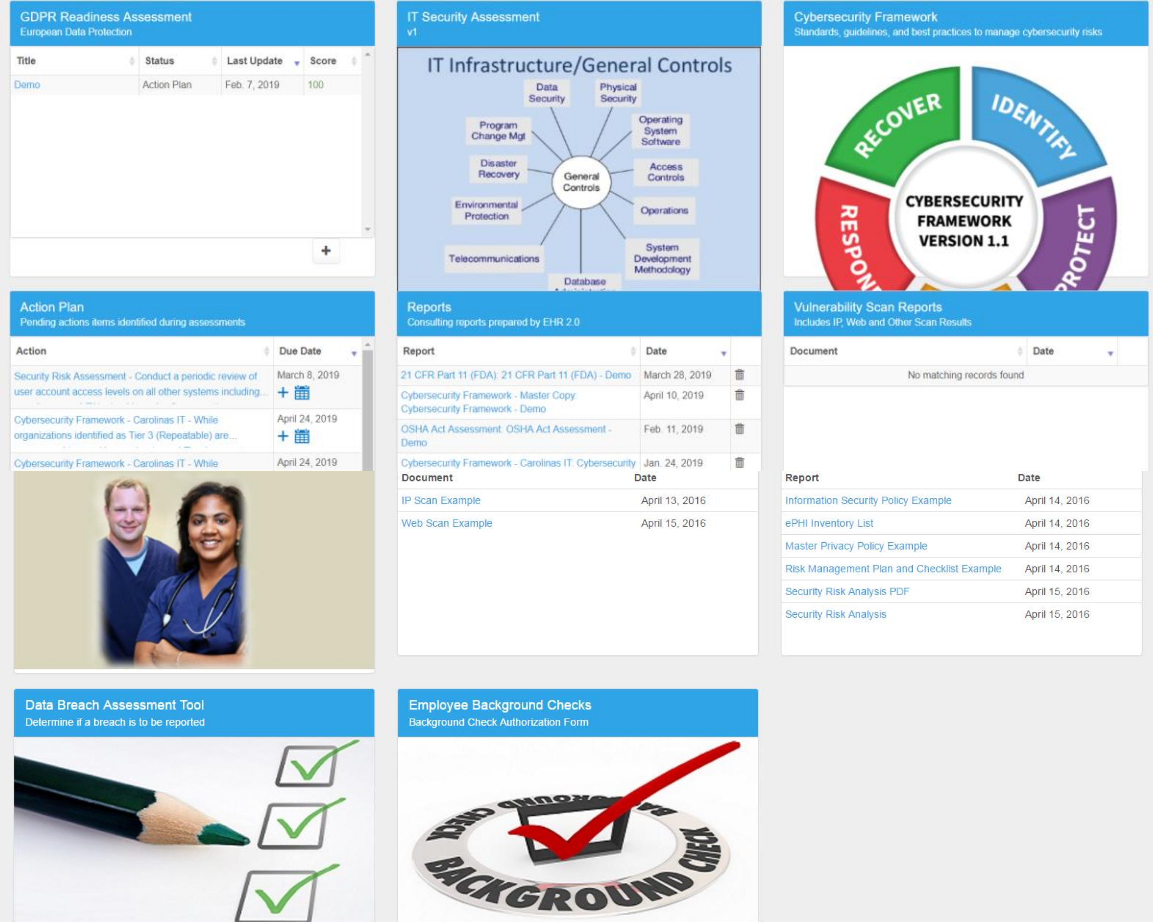
The Recover Function identifies appropriate activities to maintain plans for resilience and to restore services impaired during cybersecurity incidents

Example Outcomes:

- Ensuring the organization implements Recovery Planning processes and procedures
- Implementing improvements based on lessons learned
- Coordinating communications during recovery activities



EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION



GDPR Readiness Assessment
European Data Protection

Title	Status	Last Update	Score
Demo	Action Plan	Feb. 7, 2019	100

+

IT Security Assessment
v1

Cybersecurity Framework
Standards, guidelines, and best practices to manage cybersecurity risks

Action Plan
Pending actions items identified during assessments

Action	Due Date
Security Risk Assessment - Conduct a periodic review of user account access levels on all other systems including...	March 8, 2019
Cybersecurity Framework - Carolinas IT - While organizations identified as Tier 3 (Repeatable) are...	April 24, 2019
Cybersecurity Framework - Carolinas IT - While	April 24, 2019

Reports
Consulting reports prepared by EHR 2.0

Report	Date
21 CFR Part 11 (FDA): 21 CFR Part 11 (FDA) - Demo	March 28, 2019
Cybersecurity Framework - Master Copy: Cybersecurity Framework - Demo	April 10, 2019
OSHA Act Assessment: OSHA Act Assessment - Demo	Feb. 11, 2019
Cybersecurity Framework - Carolinas IT: Cybersecurity	Jan. 24, 2019

Vulnerability Scan Reports
Includes IP, Web and Other Scan Results

Document	Date
No matching records found	

Document	Date
IP Scan Example	April 13, 2016
Web Scan Example	April 15, 2016

Report	Date
Information Security Policy Example	April 14, 2016
ePHI Inventory List	April 14, 2016
Master Privacy Policy Example	April 14, 2016
Risk Management Plan and Checklist Example	April 14, 2016
Security Risk Analysis PDF	April 15, 2016
Security Risk Analysis	April 15, 2016

Data Breach Assessment Tool
Determine if a breach is to be reported

Employee Background Checks
Background Check Authorization Form

NEXT STEPS

1. 15-minute free consulting
2. DIY | Consulting | Managed Compliance
3. E-mail: info@ehr20.com

ⓘ **We provide audit support/guarantee for all our consulting and managed compliance customers**

Additional Resources

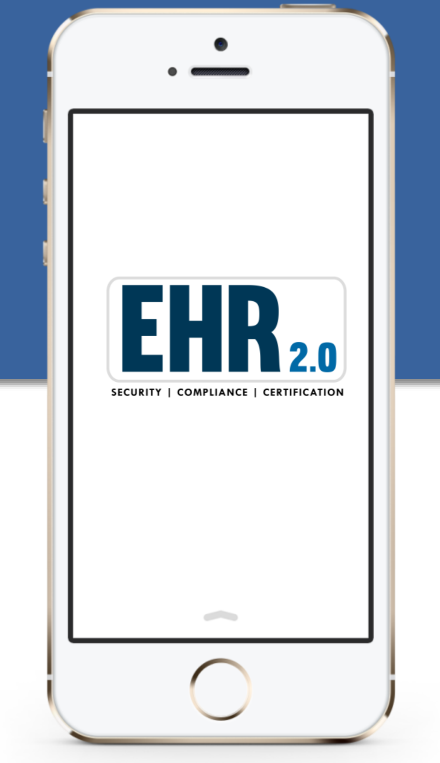
- □ NIST Cybersecurity Resources
- □ FAQ on Cybersecurity Assessment
- □ Small Business Information Security

Upcoming Events

- Become EHR 2.0 Partner – 4/25 @ 1 p.m. ET
- Open Source EMR – 5/15 @ 1 p.m. ET

Visit ehr20.com/webinars to learn more

FIND US



CALL US
866-276 8309

SERVICE
info@ehr20.com

LOCATION
150 Cornerstone Drive ,
#202
Cary, NC

SOCIALIZE
Facebook
Twitter

SECURITY | COMPLIANCE | CERTIFICATION

Questions?

E-mail: info@ehr20.com

Call: 866-276-8309

Thank you!