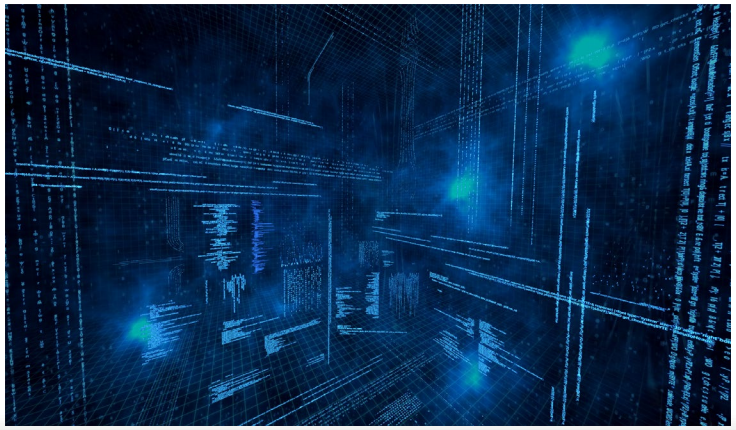


# CYBER & INFORMATION SECURITY EXECUTIVE UPDATE

## WHAT IS YOUR RISK PROFILE?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Sassan S. Hejazi, Ph.D.

JULY 2021

# Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide **confidentiality, integrity, and availability.**

# Current State of Cyber Security

- Pandemic accelerators
- Dark web considerations
- Bitcoin - They can get paid now
  - Exploit kits …help desk?
- Ransomware as a service
- Data breach privacy concerns
- Operational continuity issues
- Legal and branding concerns

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# High Value Target Assets

- Personally Identifiable Information (PII) such as employee and customer social security numbers, dates of birth, electronic protected health information (EPHI), email addresses, compensation and credit card numbers.
- Product and service intellectual property data, product design, engineering, manufacturing, marketing, regulatory and competitive data.
- Operational continuity and reliability capabilities, reputational and legal risk concerns.

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# Cyber Readiness Approaches

## Minimal

- Keeping up with latest patches and fixes at best
- Highly reactive in nature
- Lack of cyber related plans and budgets

## Traditional

- Having a formal cyber program in place
- Leveraging applicable industry methodologies
- Highly IT focused and driven

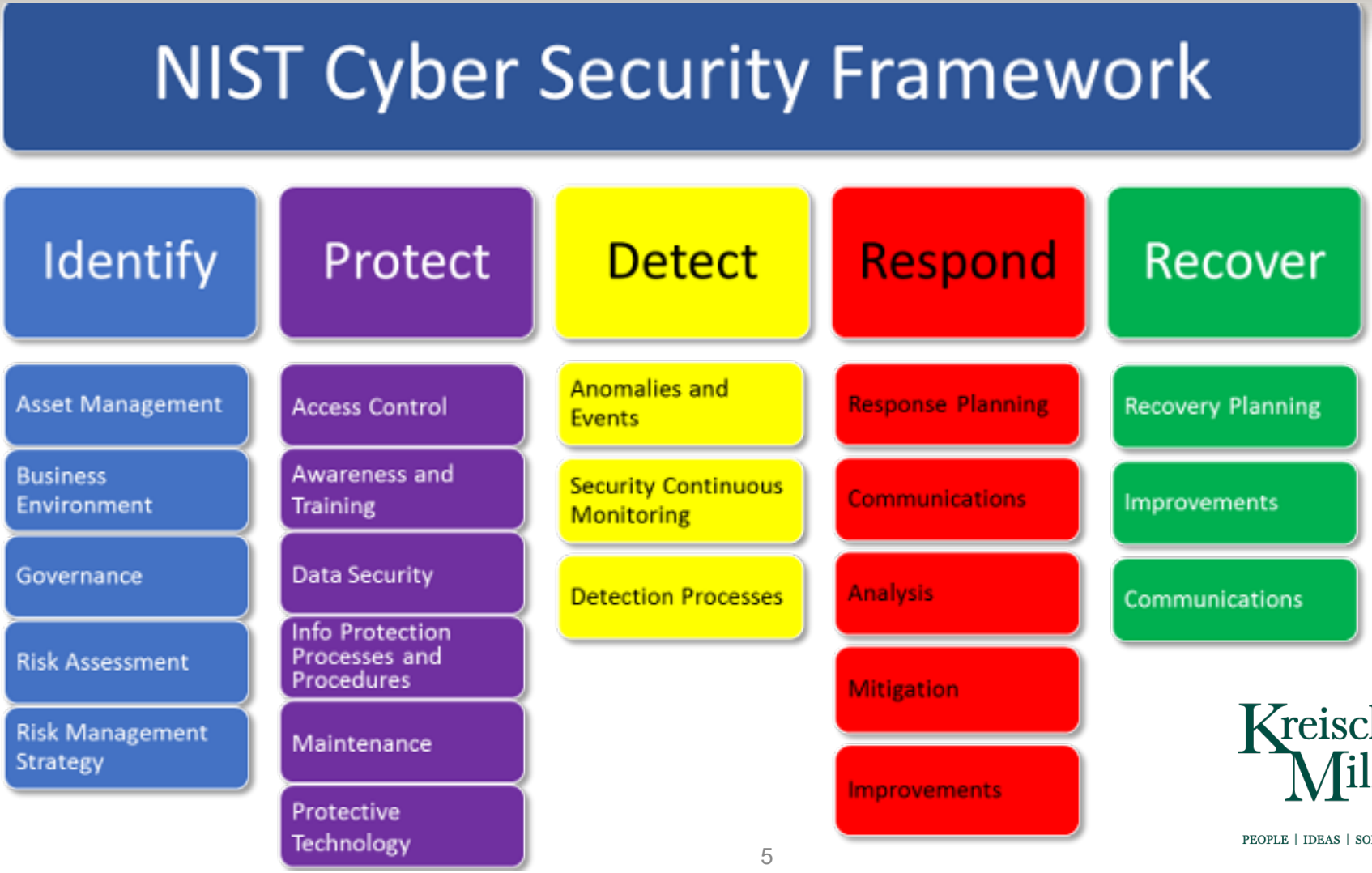
## Holistic

- Active cyber program in place
- Leveraging leading industry practices
- Close and active collaboration between IT and Management

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

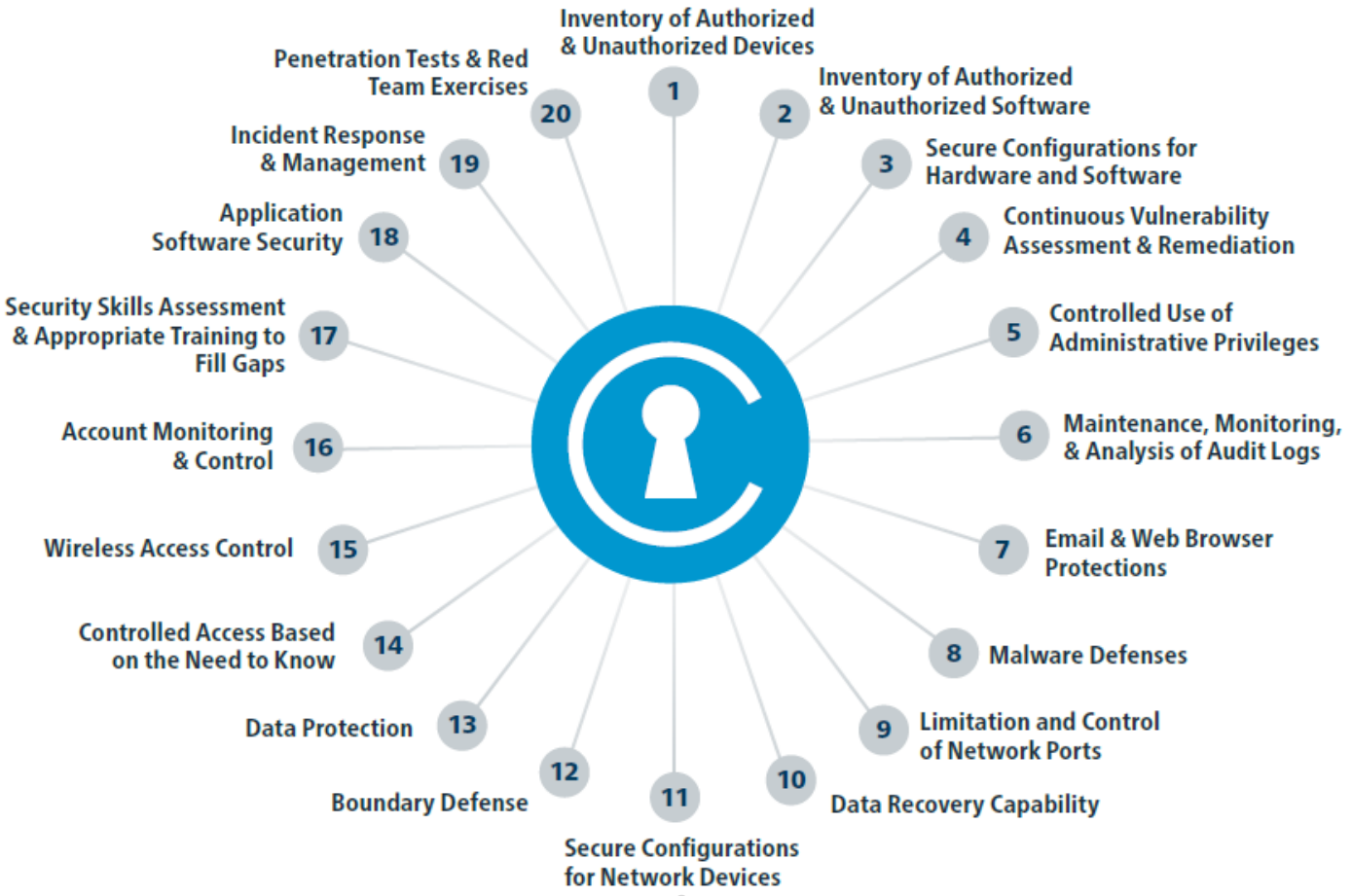
# Leveraging Frameworks



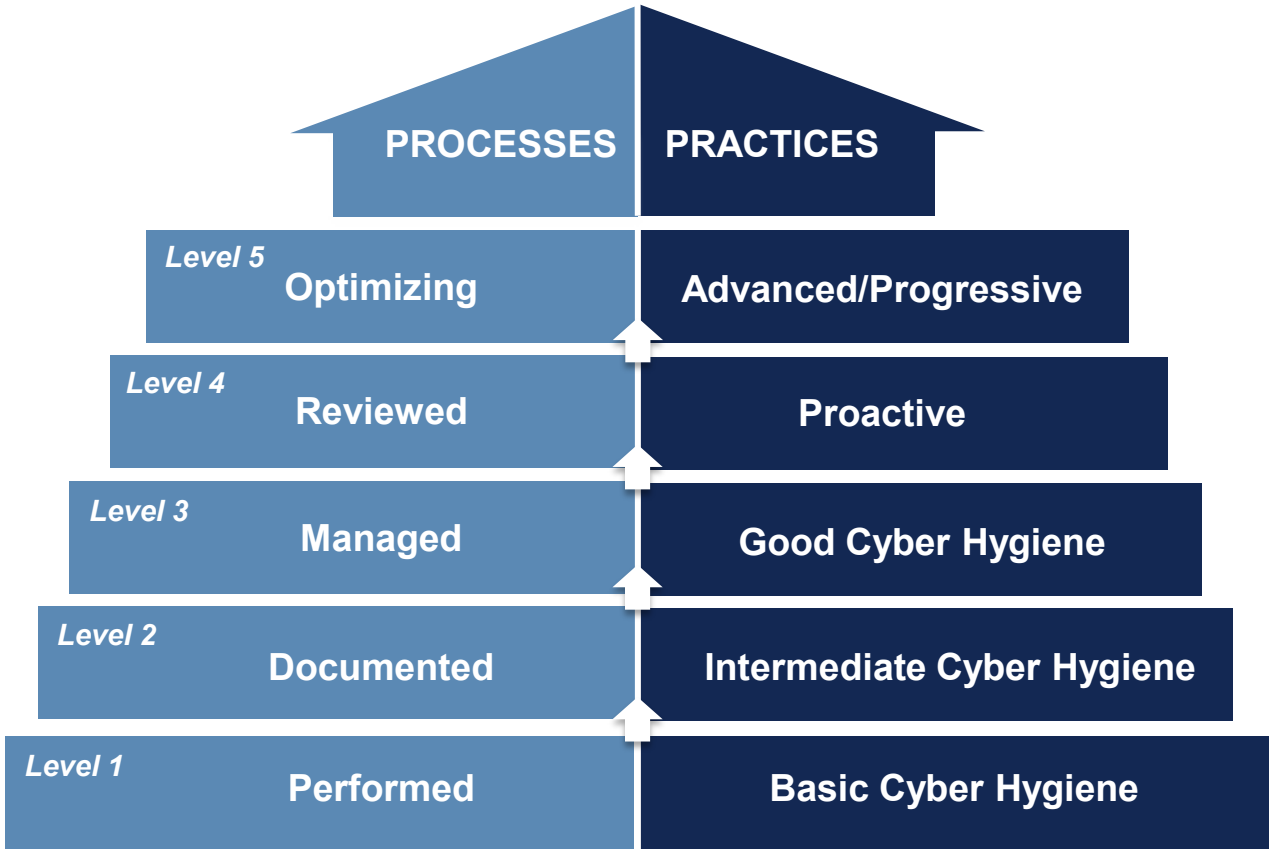

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# CIS Top 20 for SMEs



# CMMC Maturity Model




Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

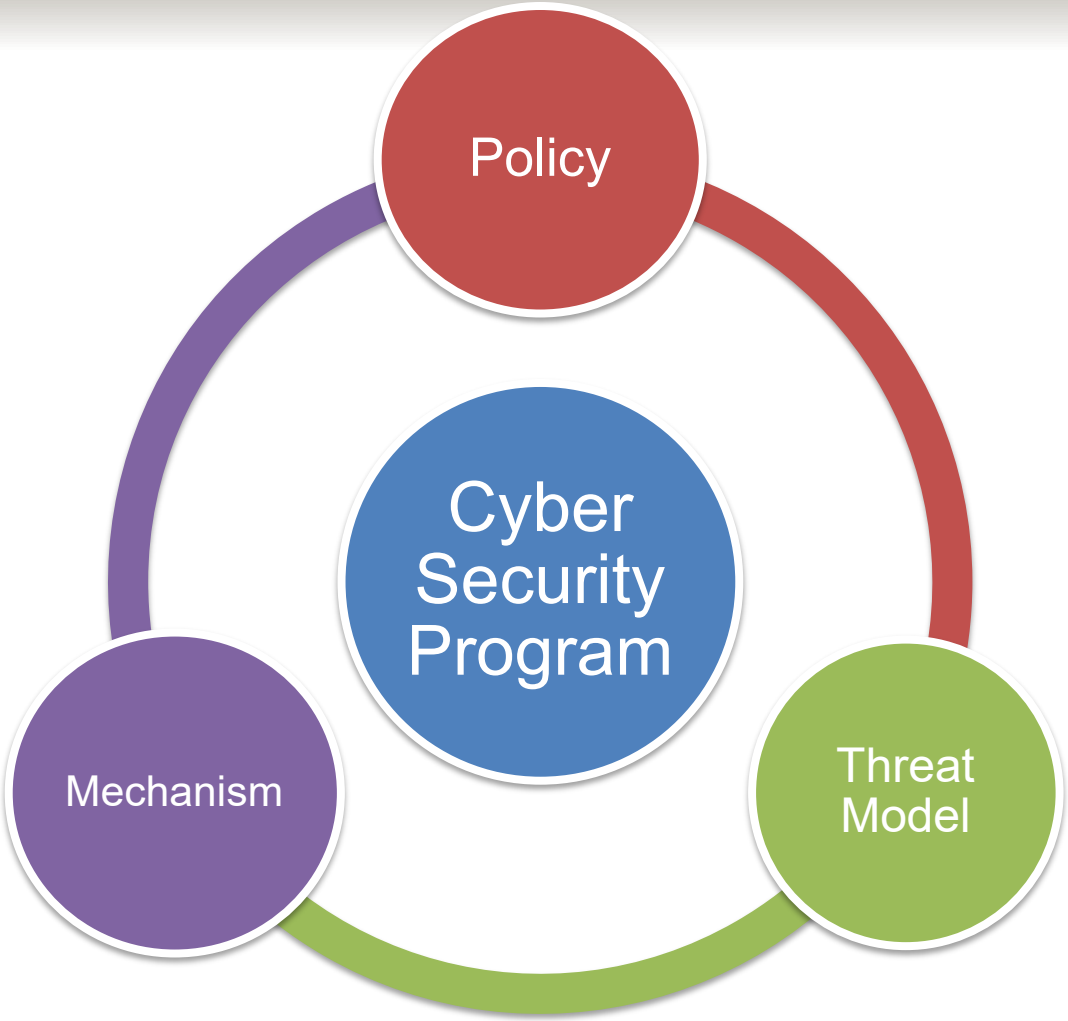
# CMMC Capability Domains

| | | |
|---|---|---|
| Access Control (AC) | Incident Response (IR) | Risk Management (RM) |
| Asset Management (AM) | Maintenance (MA) | Security Assessment (CA) |
| Awareness & Training (AT) | Media Protection (MP) | Situational Awareness (SA) |
| Audit and Accountability (AU) | Personnel Security (PS) | System & Communications Protection (SC) |
| Configuration Management (CM) | Physical Protection (PE) | System & Information Integrity (SI) |
| Identification & Authentication (IA) | Recovery (RE) | |

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

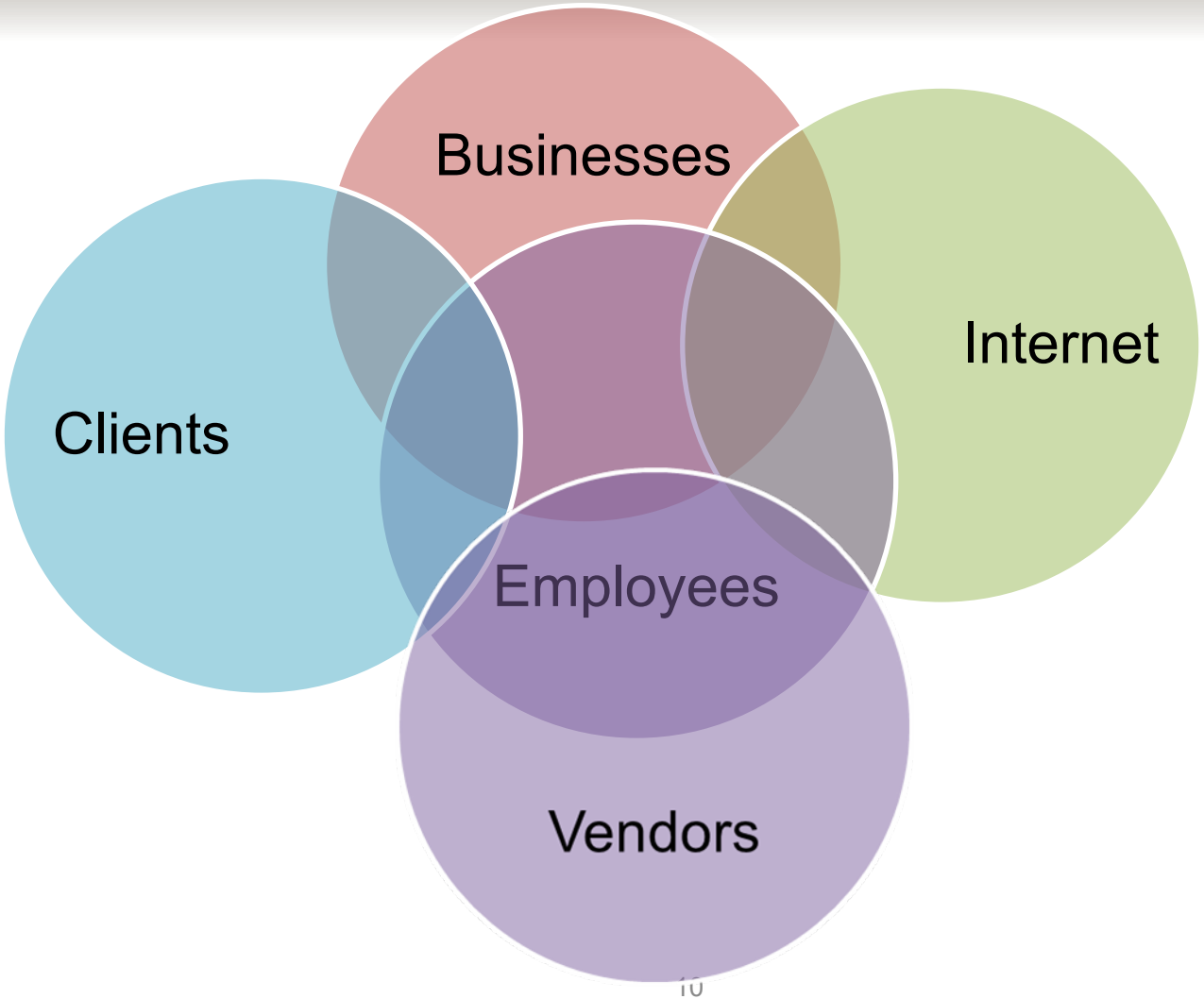
# Cyber Security Program Triad




Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# Know Your Web of Trust






Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS


# KNOW YOUR RISK PROFILE

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# Do We Have a Cyber & Privacy Program?

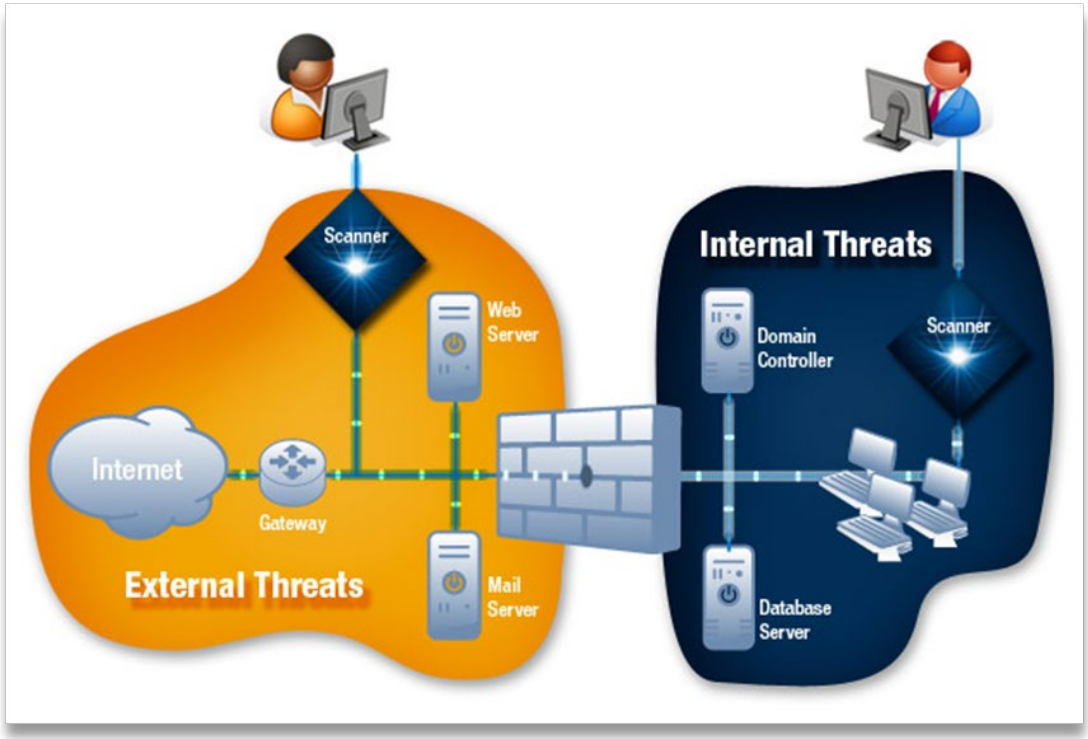
- Is it an active program?
  - Committee in place?
- Is it well planned/budgeted?
- Is it based on a methodology?
  - NIST/CMMC/CIS
  - ISO
  - GDPR/HIPAA


Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# Do We Know Our IT Vulnerabilities?

- Do we periodically conduct a vulnerability scan?
  - New vulnerabilities are discovered daily
  - Internal vulnerability scans occur from within the network
  - External vulnerability scans simulate the effect of Internet users attempting to access a network




Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# Are We Monitoring Threats?

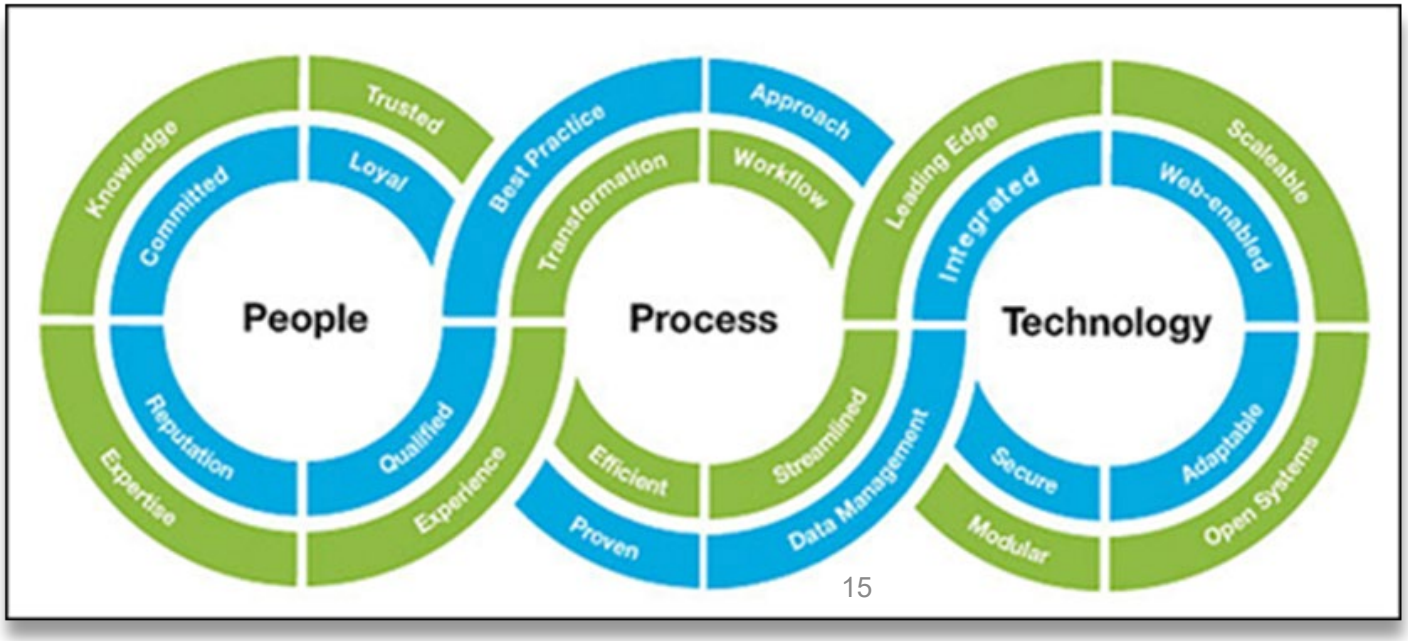
- Detecting potential intrusions?
- Review of user/insider activities?
- Staying on top of latest threats out there?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# Do We Have Updated Policies?

- Employee on boarding, acceptable use, termination?
- Data classification, access and protection?
- Data handling and privacy considerations?
- Vendor/contractor proper data handling and confidentiality?
  - IT department/provider(s) considerations?






Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

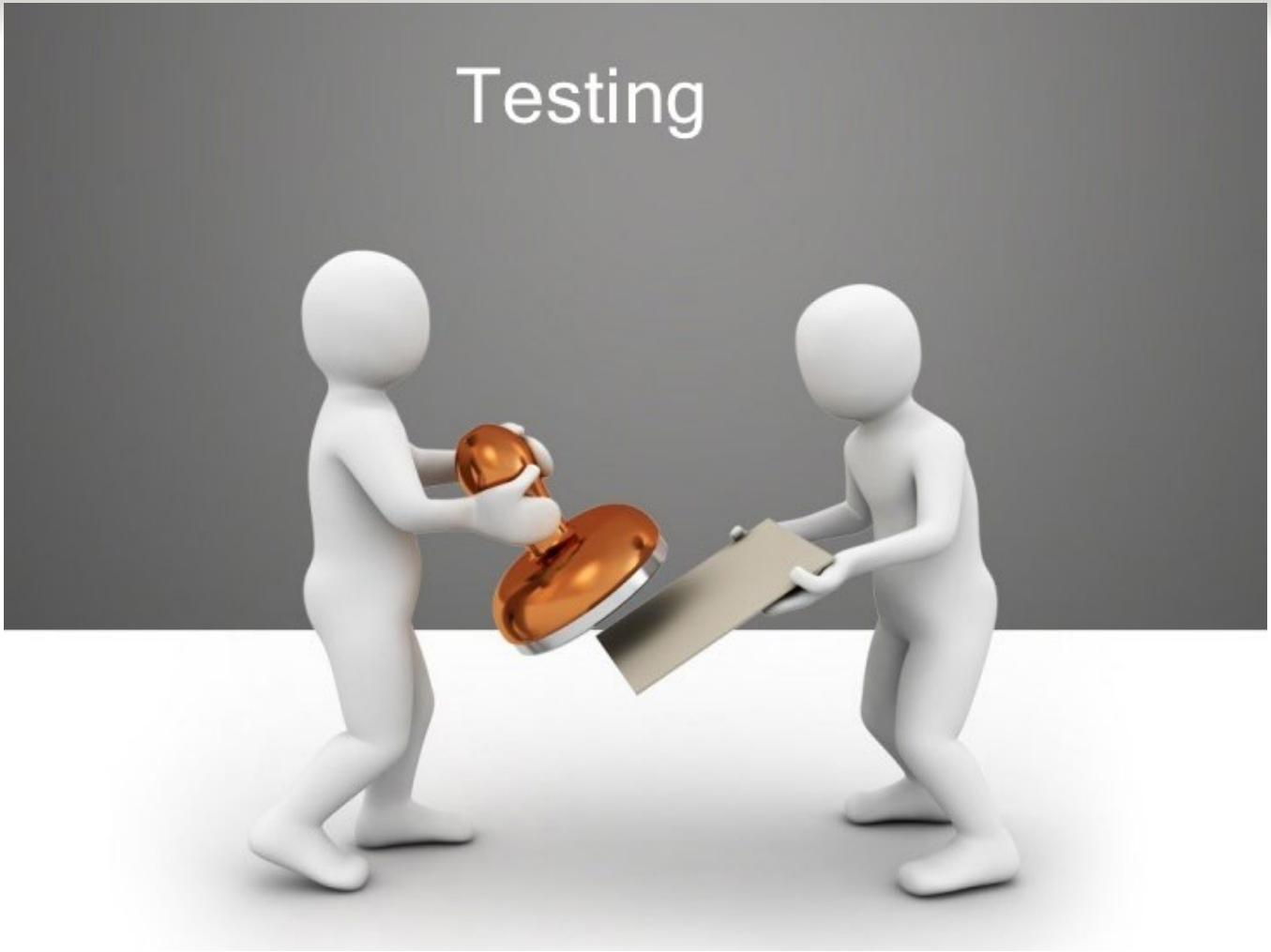
# Do We Have a Cyber Training Program?




Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# Are We Validating User Knowledge?




Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

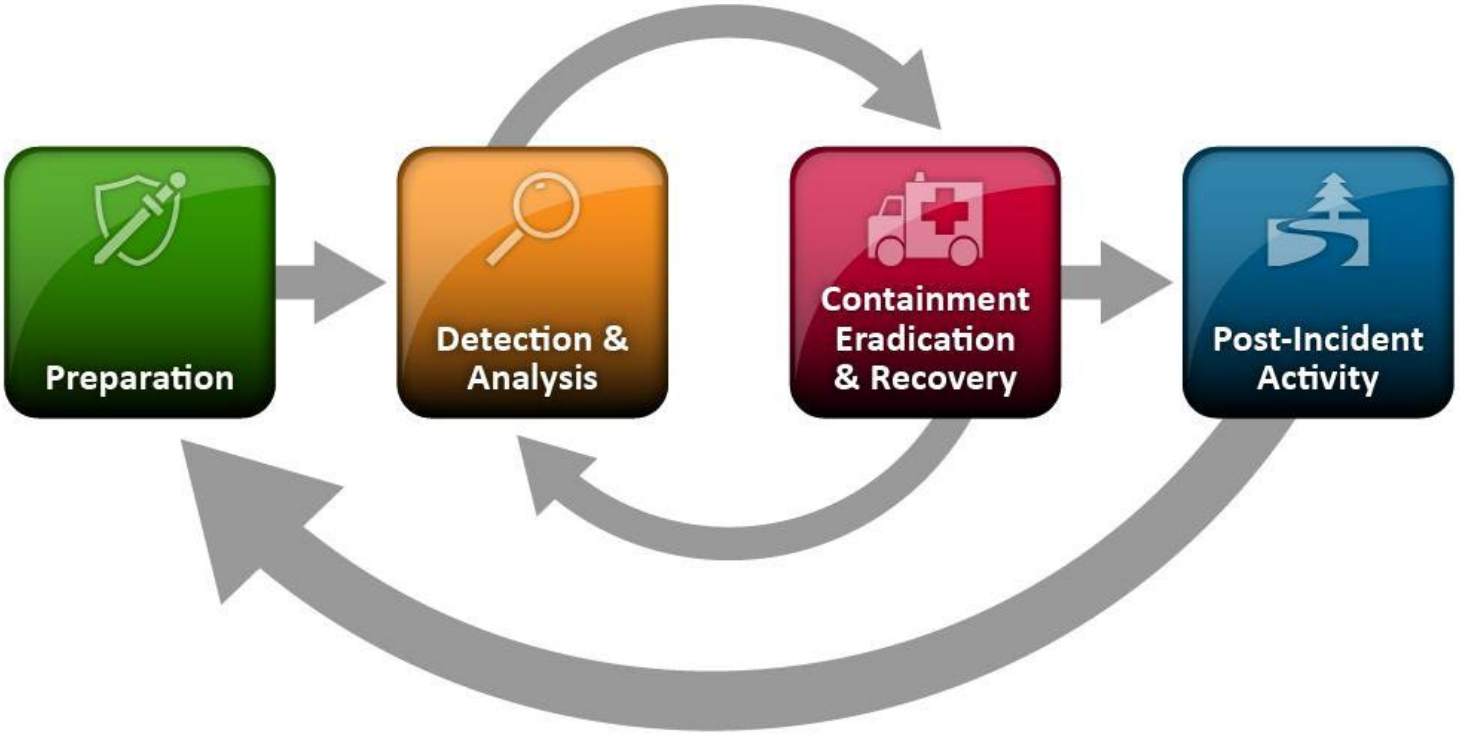
# Users Only Access What They Need?

- Principle of least privilege
  - a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose
- Review access levels and have proper change control procedures in place
- Apply this principle to all employees and third parties


Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# Do we Have an Incident Response Plan?




***Cyber Insurance Considerations***

Kreischer Miller

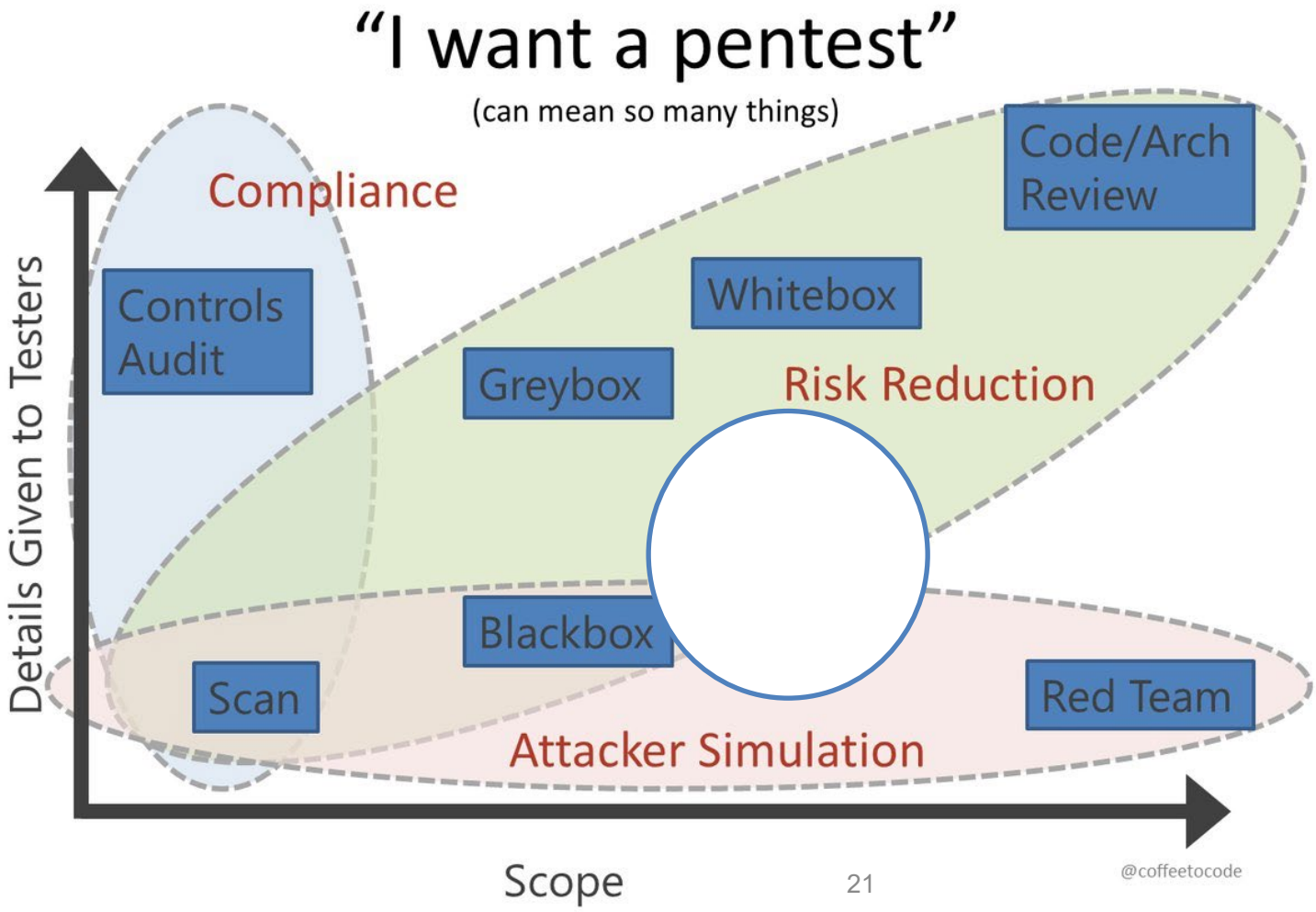
PEOPLE | IDEAS | SOLUTIONS

# Do We Have a Recovery Plan?


Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# Have We Paid Someone to Break In?






Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# What is Your Risk Profile?

- **Assign a 10 to all YES responses**
- **Assign a 5 to all SOMEWHAT responses**
- **Assign a 0 to all NO responses**
- **Add up all your points from the 10 questions**
  - Scored below 50, organization at a **CRITICAL RISK LEVEL**
  - Scored between 50-70, at a **HIGH RISK LEVEL**
  - Scored between 70-90, at a **MODERATE RISK LEVEL**
  - Scored above 90, at a **MANAGED RISK LEVEL**

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# Concluding Comments

- Executives are ultimately responsible for their organizations cyber security and information security readiness.
- Executives and Board members need to stay highly engaged in the cyber and information security readiness efforts to lead their organization's culture towards a security aware and empowered one.
- ***Increasing cyber hygiene and information privacy is not a costly endeavor. It could be accomplished if addressed in a systematic program fashion to best protect ongoing digital transformation efforts and assets.***

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

# Thank You for Attending!

**Sassan S. Hejazi**
**Director, Technology Solutions Group**
**shejazi@kmco.com**
**215.734.0803**

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS