CYBER & INFORMATION SECURITY

WHAT EXECUTIVES NEED TO KNOW AND ASK

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Donald G. Cook, CISSP
Sassan S. Hejazi, Ph.D.

JUNE 2020

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
- IoT implications
- Operational continuity issues
- Legal and branding concerns

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

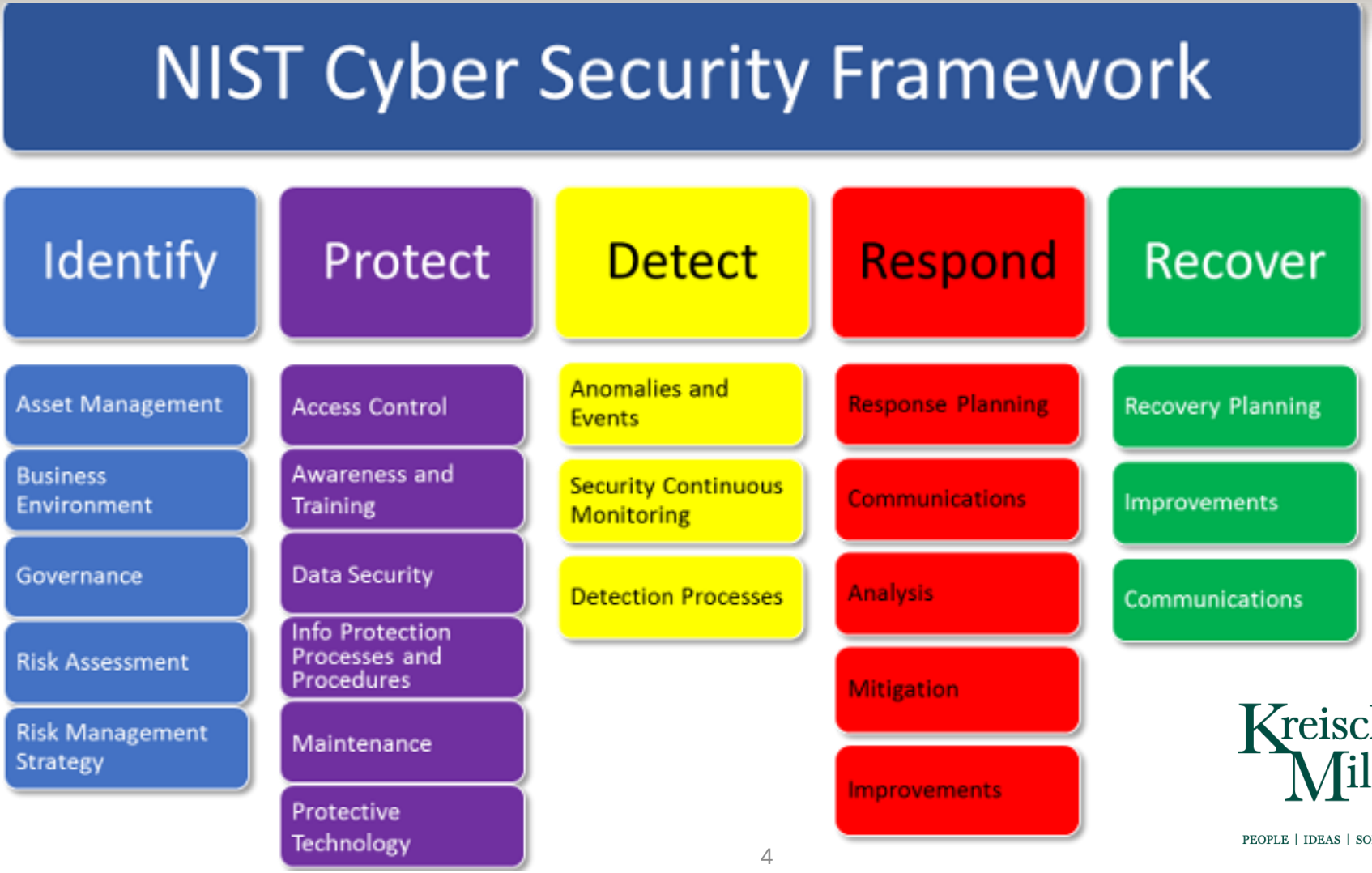
Middle Market & Information Security

- Increased frequency of attacks
- Limited internal resources
- Increased regulatory pressures
- Confusion among management regarding roles, responsibilities and priorities
  - Assuming IT is addressing it all!
- Lots of noise/offering in the IT vendor community
- Need for a unified methodology and approach

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

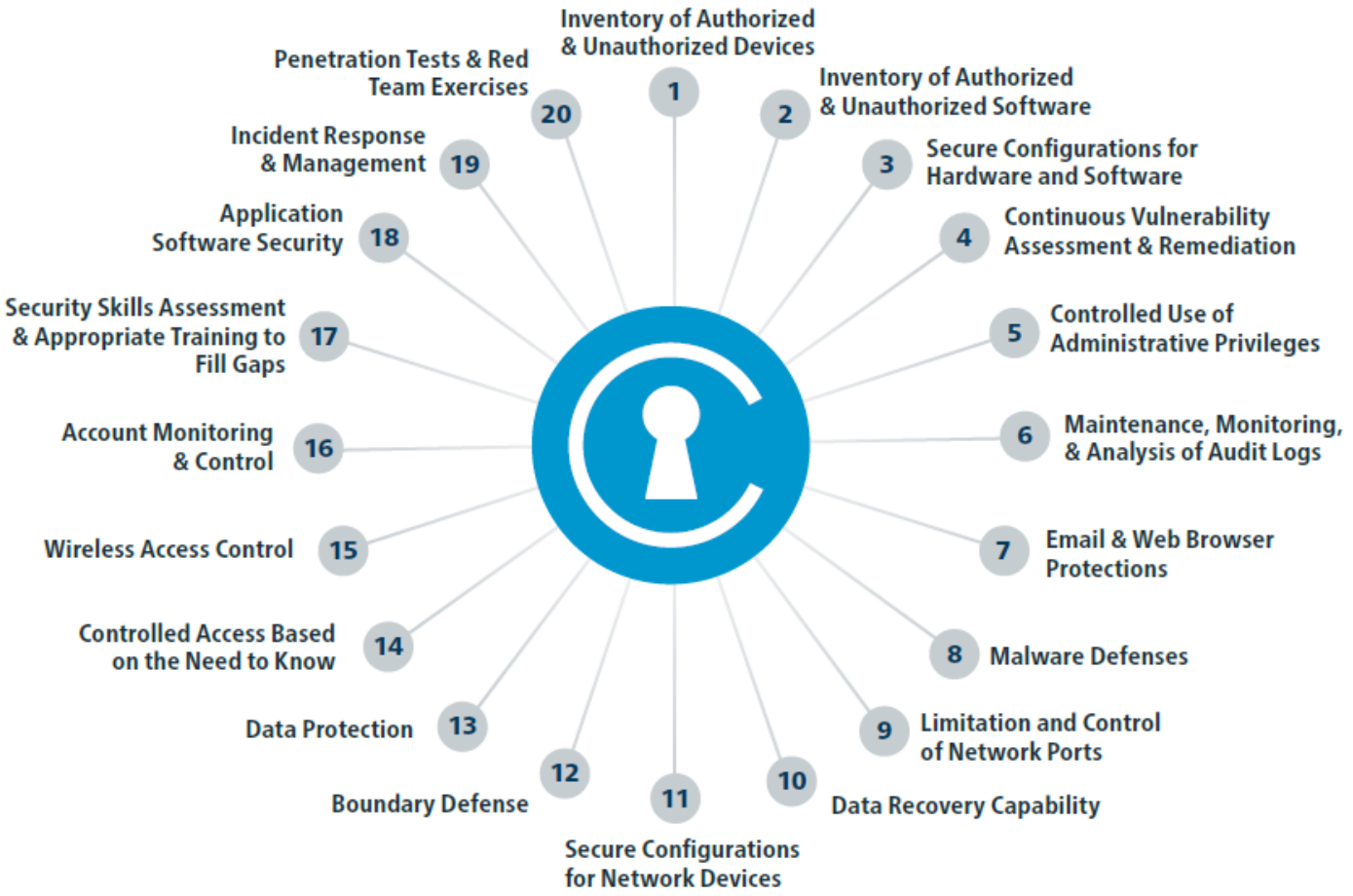
Leveraging Frameworks



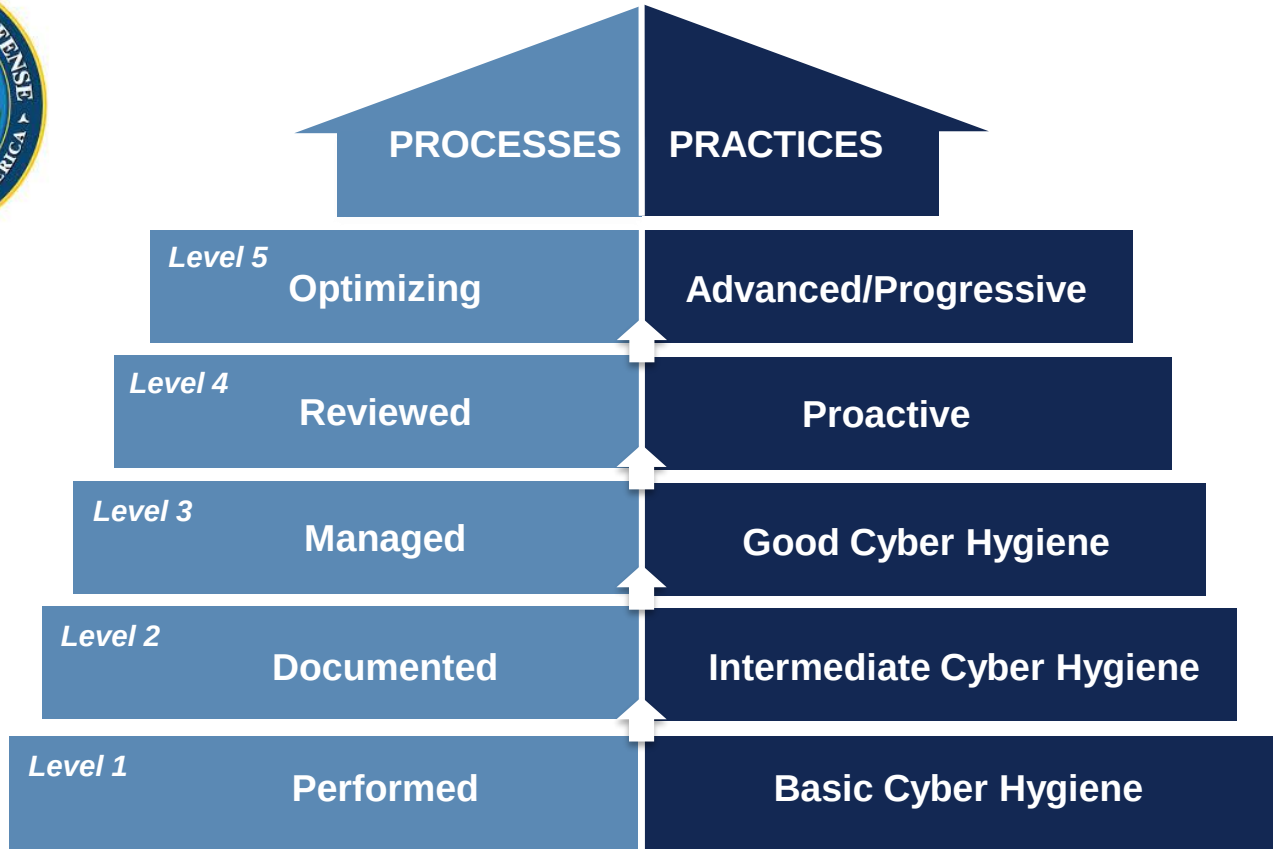
Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

CIS Top 20 for SMEs



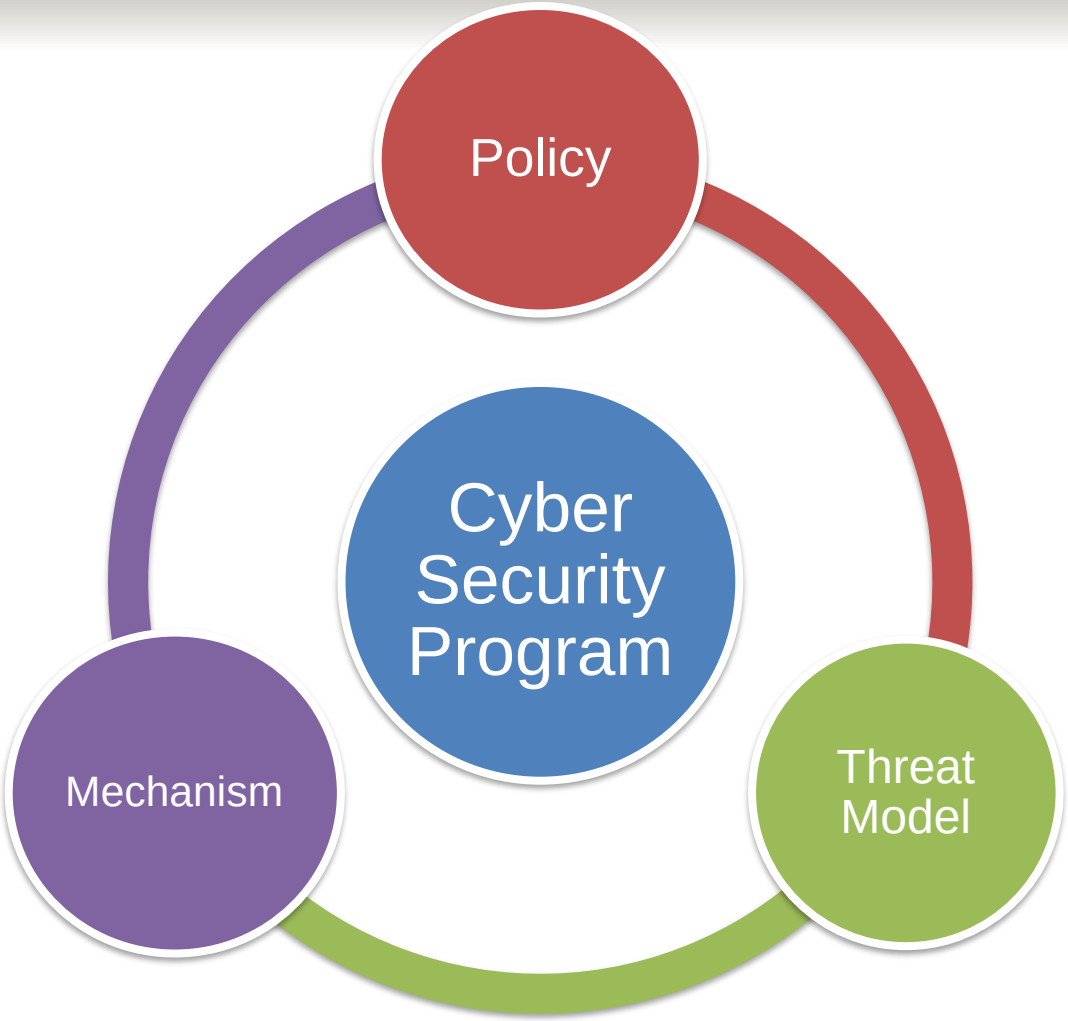
Governmental Contracting DFARS/CMMC



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

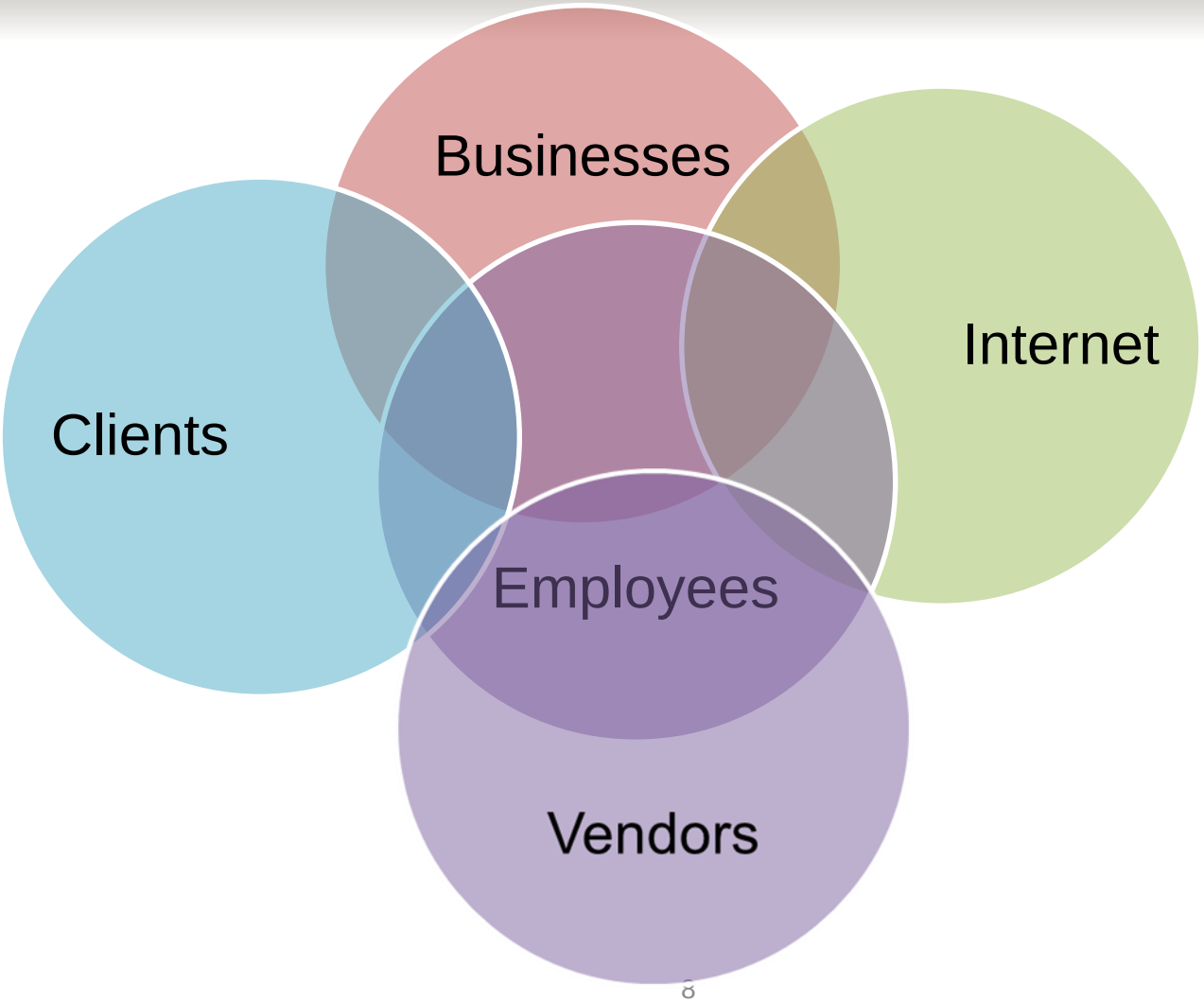
Cyber Security Program Triad



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Know Your Web of Trust



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

10 QUESTIONS TO ASK

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Do we have a cyber program?

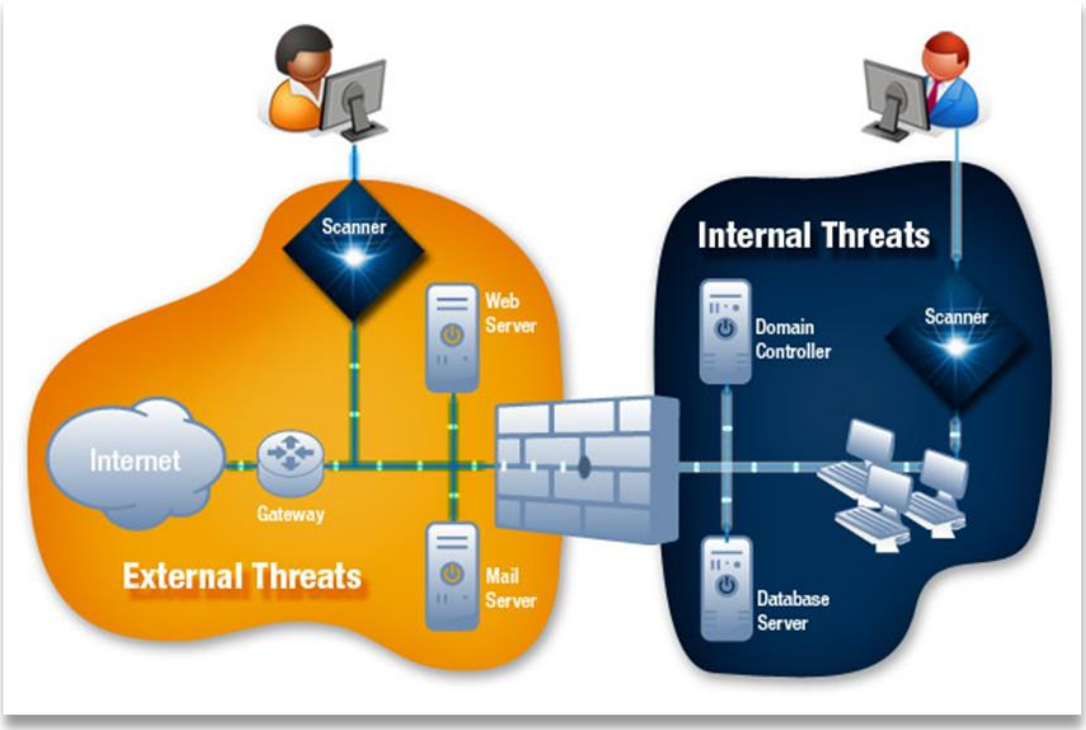
- Is it an active program?
  - Cyber versus Privacy
- Is it well planned/budgeted?
- Is it based on a methodology?
  - NIST
  - CIS
  - DFARS/CMMC
  - ISO
  - GDPR/HIPAA

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Do we know our vulnerabilities?

- How often do we 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?

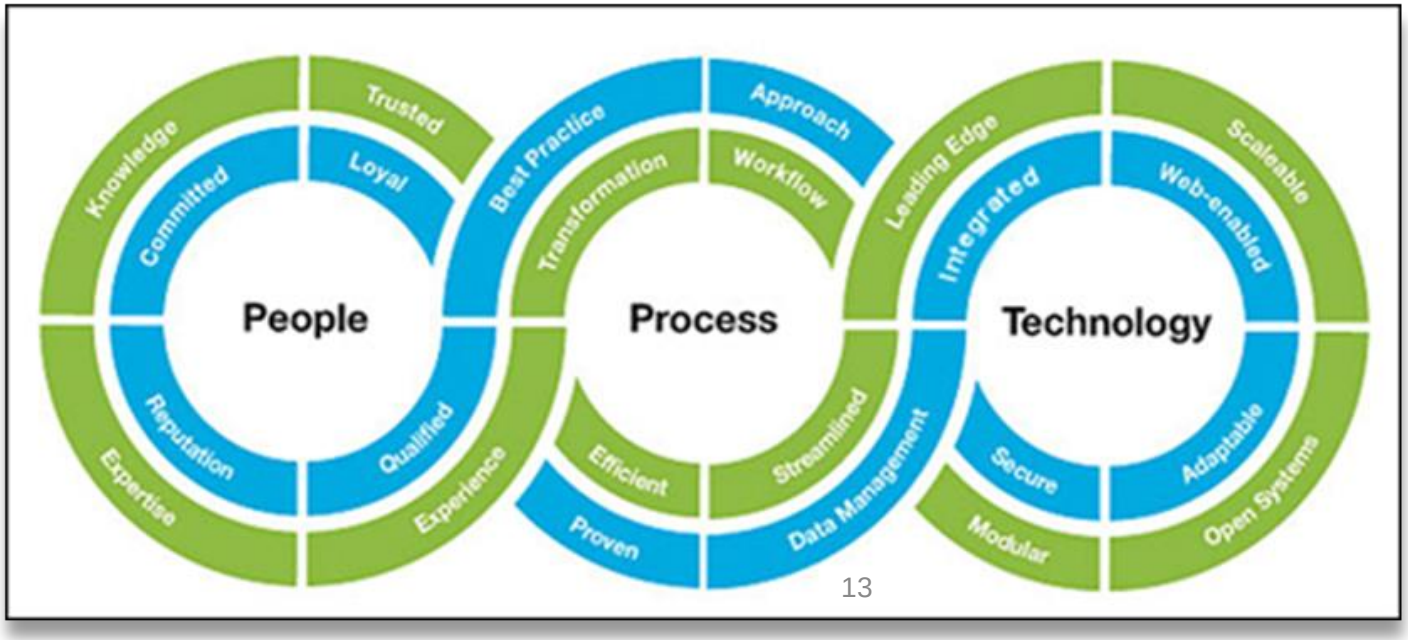
- Detecting potential intrusions?
- Review of user activities?
- Staying on top of latest threats out there?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Do we have updated policies?

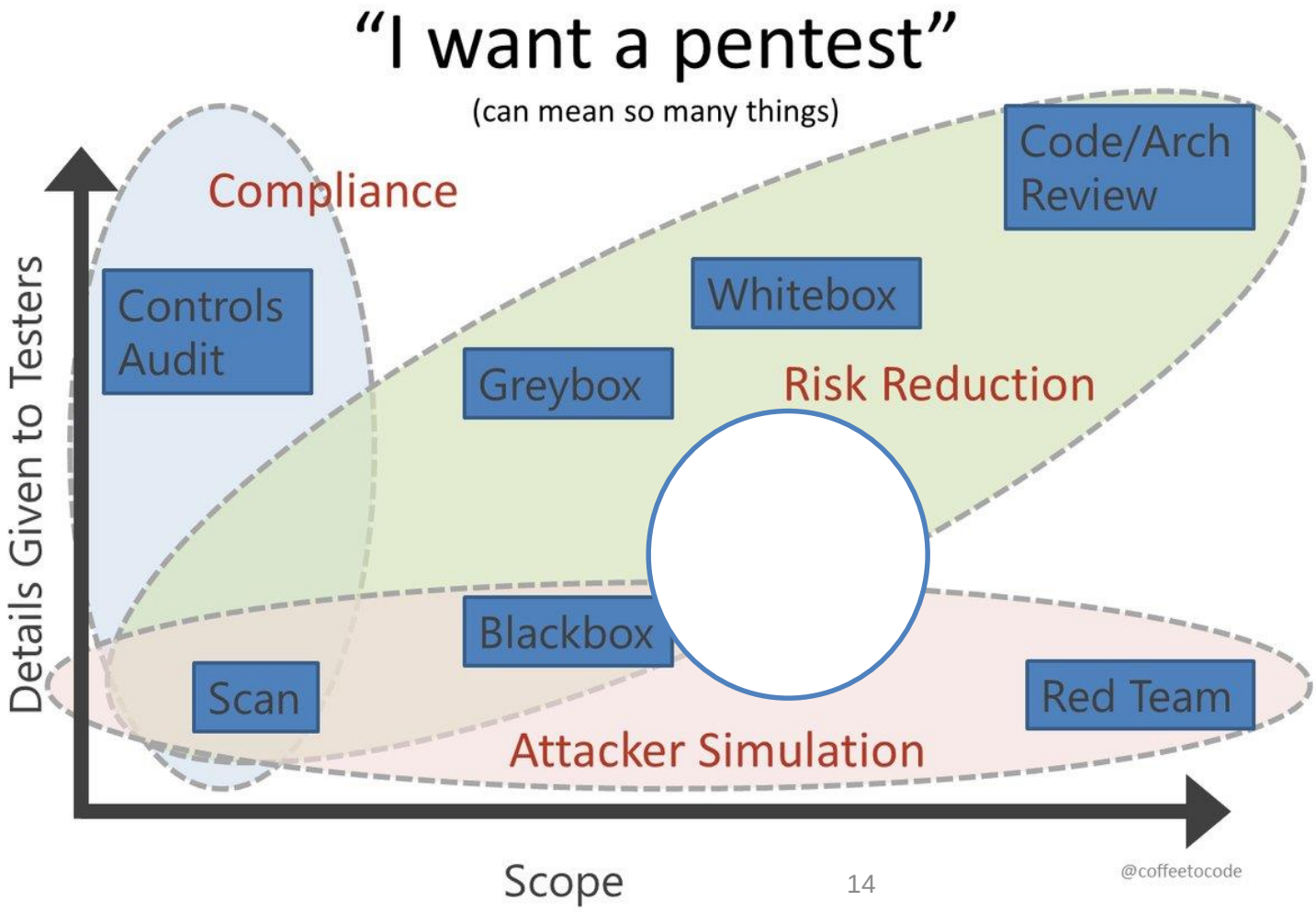
- Employee on boarding, acceptable use, termination?
- Customer data handling and privacy?
- IP and internal data confidentiality, access and protection?
- Vendor/contractor proper data handling and confidentiality?
- IT department/provider cyber policies & procedures?



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Have we paid someone to break in?



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

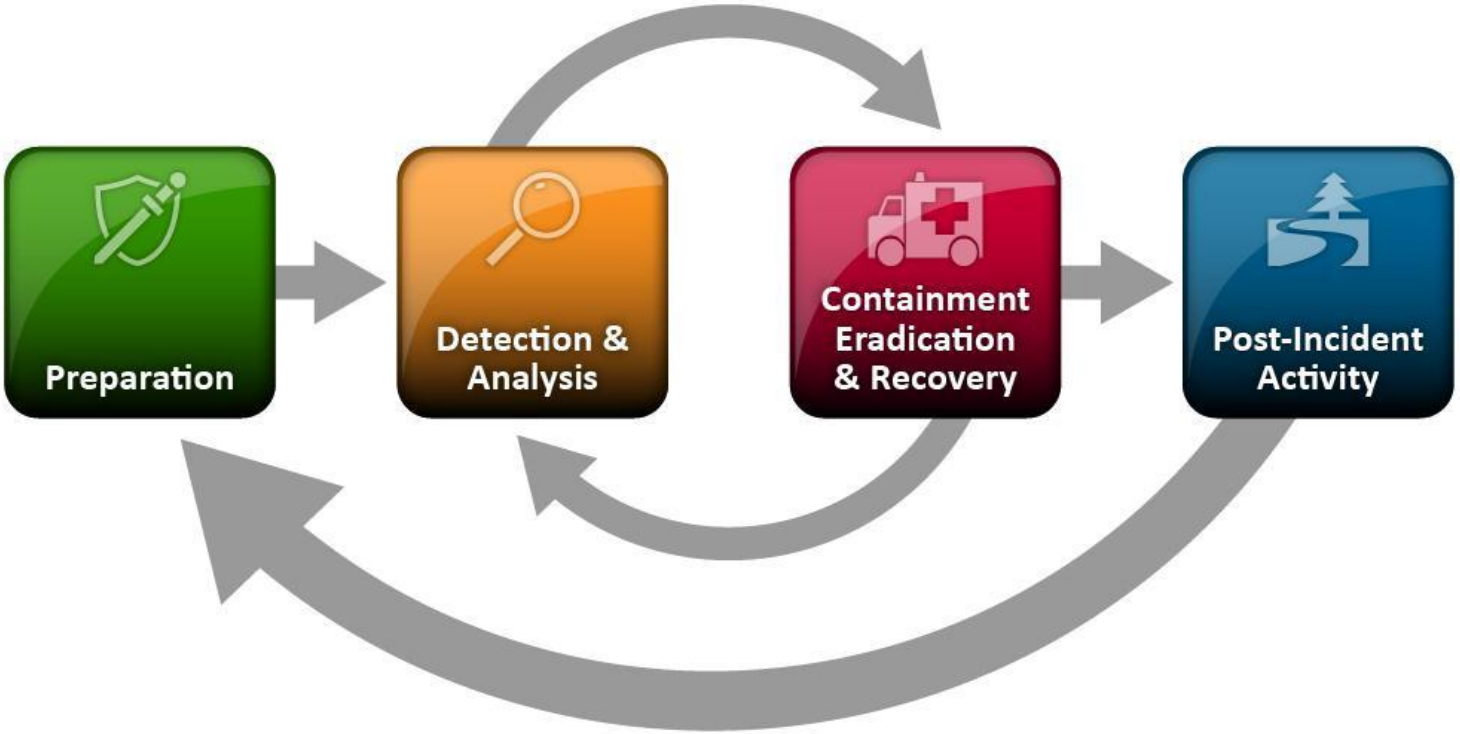
Users only access what they need?

- 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?



Kreischer Miller

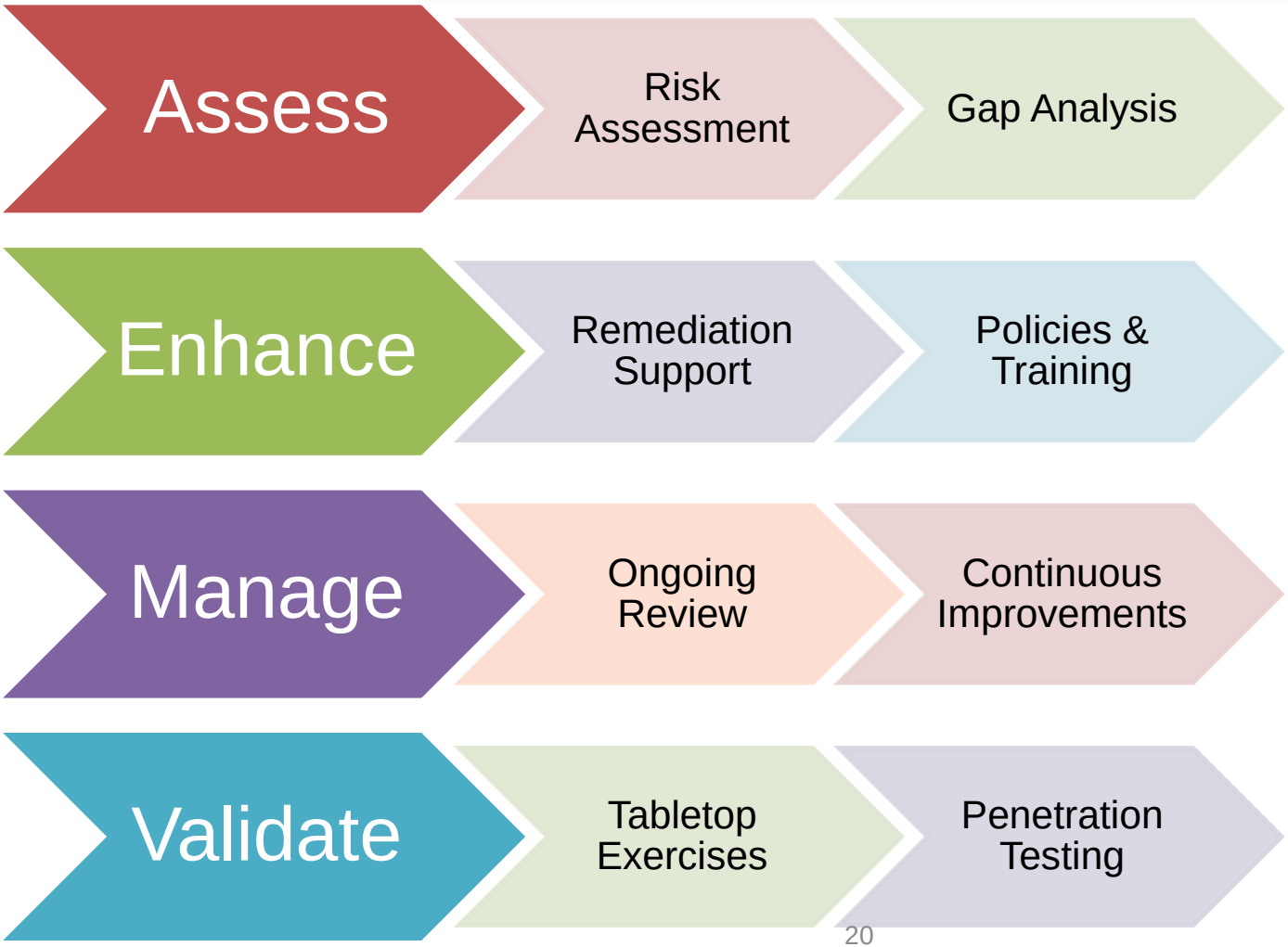
PEOPLE | IDEAS | SOLUTIONS

Do we have a recovery plan?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

KM 4 Phases of Information Security



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!

Donald G. Cook, CISSP
dcook@kmco.com

Sassan S. Hejazi, Ph.D.
shejazi@kmco.com

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS