CYBER & INFORMATION SECURITY EXECUTIVE FORUM

REDUCING EXPOSURE & MANAGING RISK

Sassan S. Hejazi, Ph.D.
Robert Rittich, CISSP

OCTOBER 2021

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

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

- **Based on Cisco's 2021 Report, cryptomining, phishing, ransomware, and trojans averaged 10x the internet activity:**
  - 86% of organizations had at least one user try to connect to a phishing site
  - 70% of organizations had users that were served malicious browser ads
  - 69% of organizations experienced some level of unsolicited cryptomining
  - 50% of organizations encountered ransomware-related activity

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.

Cyber Readiness Approaches

Minimal

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

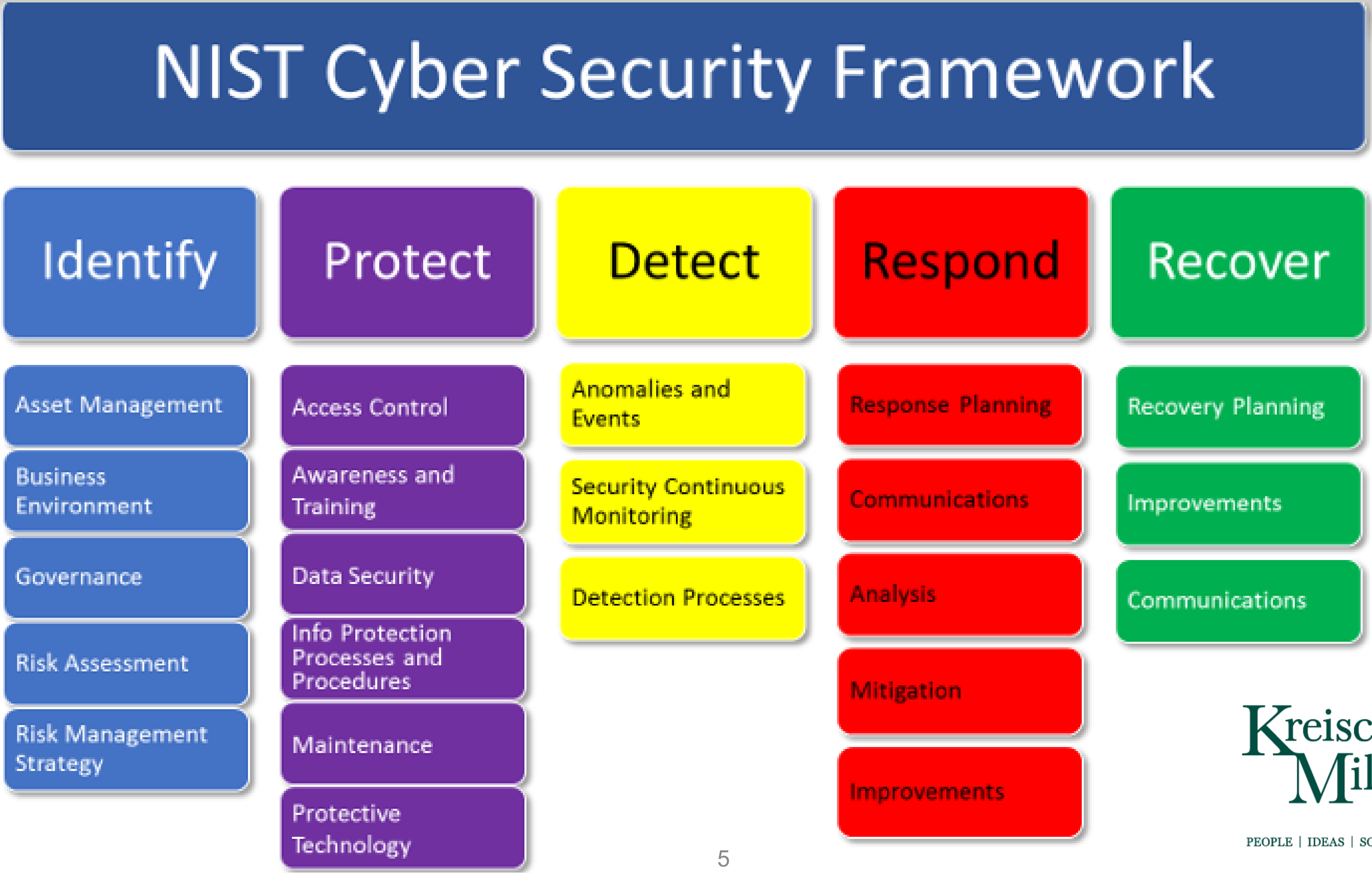
Traditional

- 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

Leveraging Frameworks



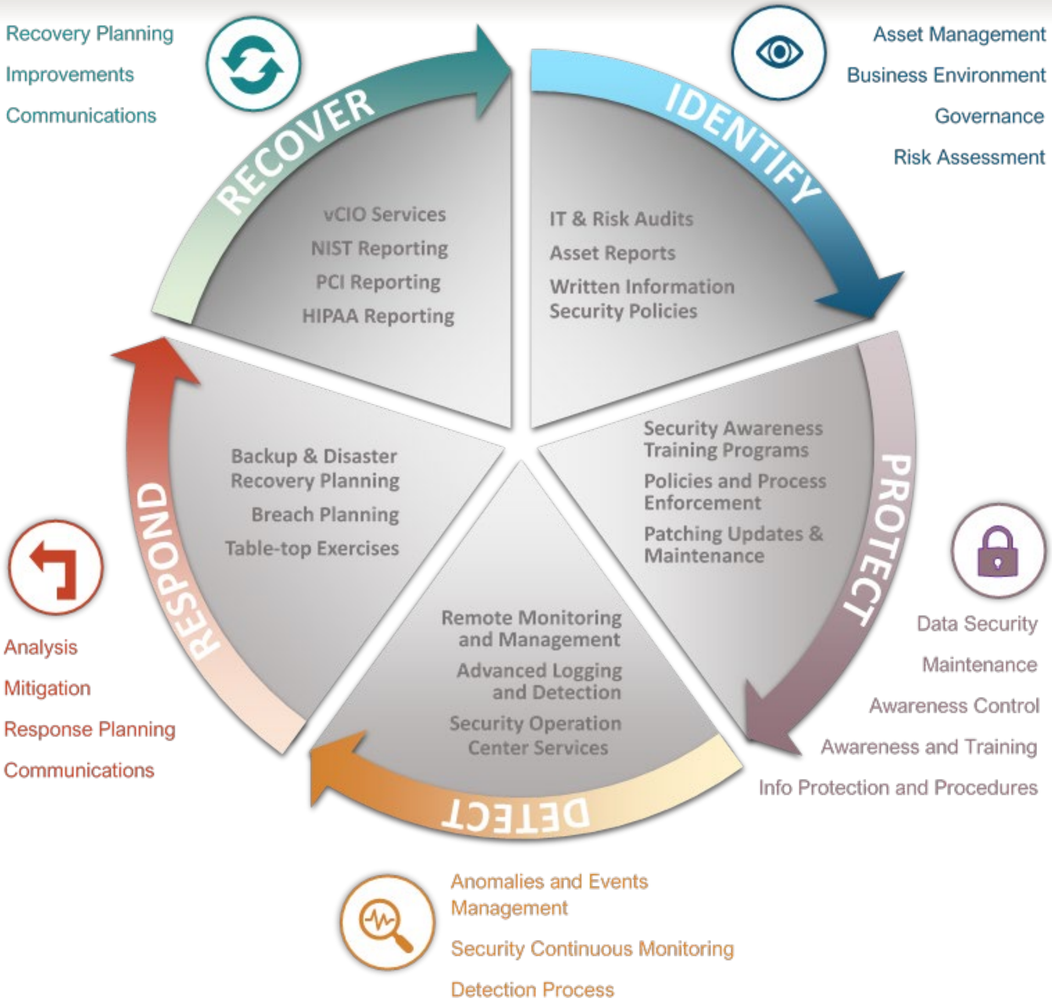
NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

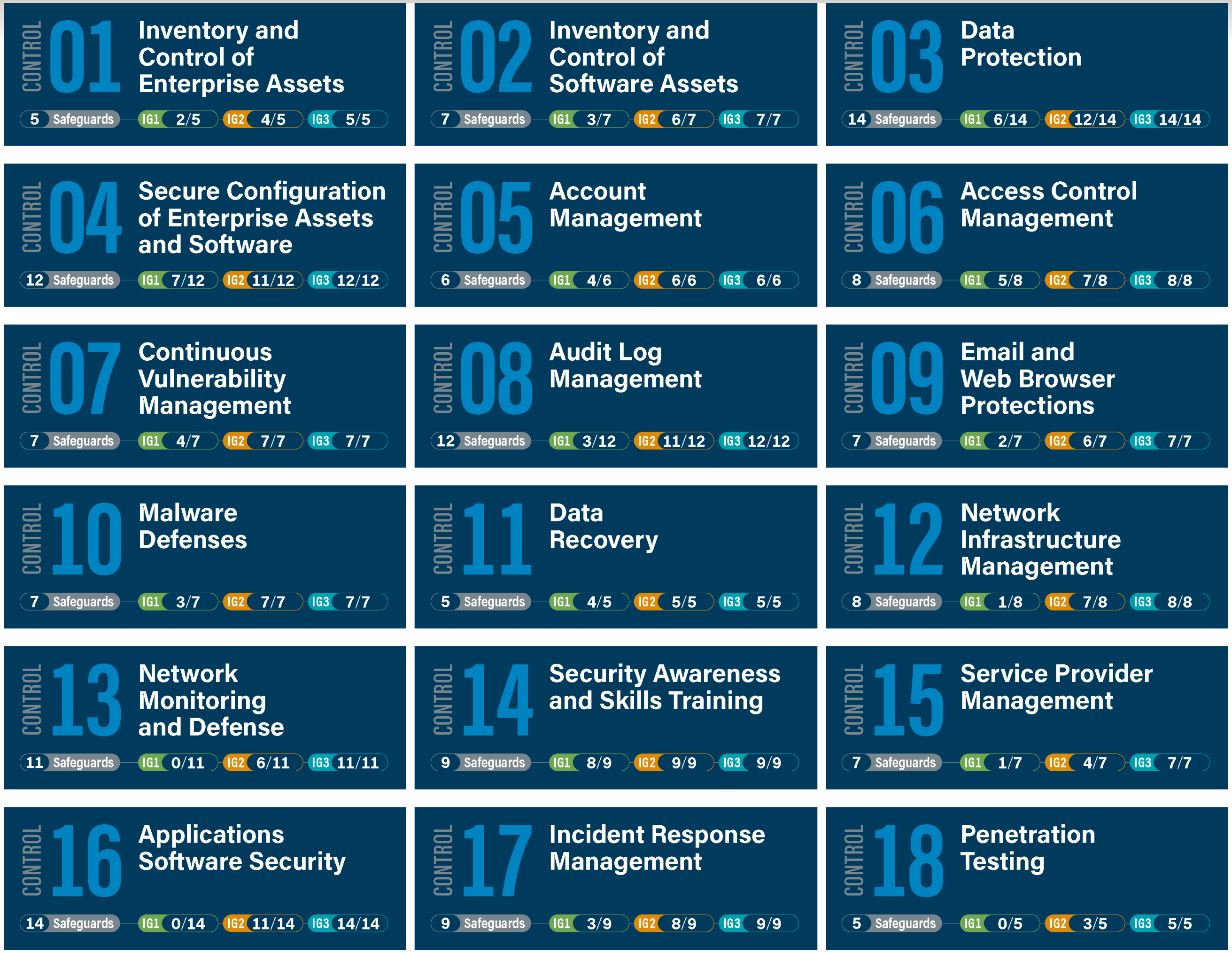
Leveraging Frameworks



Kreischer Miller

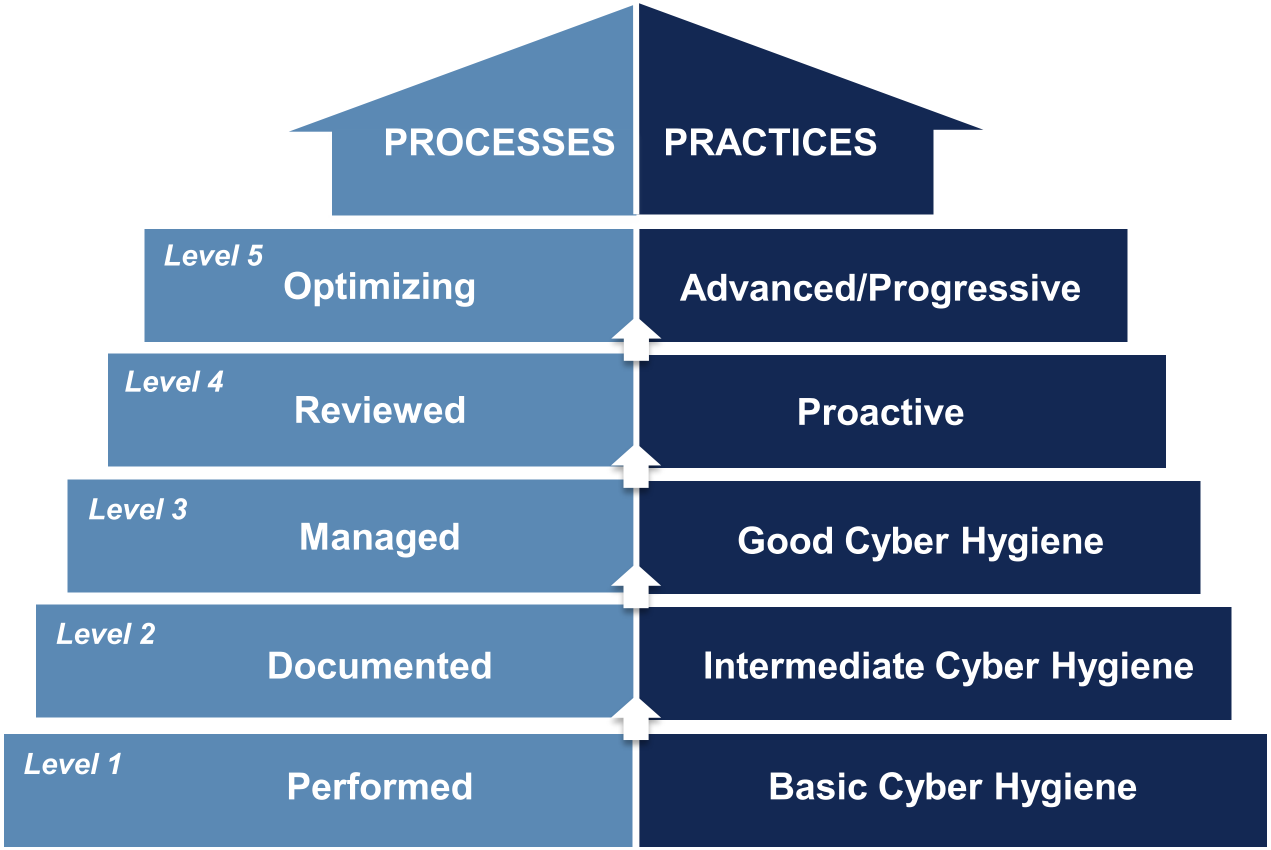
PEOPLE | IDEAS | SOLUTIONS

CIS Controls Overview



CONTROL 01	Inventory and Control of Enterprise Assets	5 Safeguards	IG1 2/5	IG2 4/5	IG3 5/5
CONTROL 02	Inventory and Control of Software Assets	7 Safeguards	IG1 3/7	IG2 6/7	IG3 7/7
CONTROL 03	Data Protection	14 Safeguards	IG1 6/14	IG2 12/14	IG3 14/14
CONTROL 04	Secure Configuration of Enterprise Assets and Software	12 Safeguards	IG1 7/12	IG2 11/12	IG3 12/12
CONTROL 05	Account Management	6 Safeguards	IG1 4/6	IG2 6/6	IG3 6/6
CONTROL 06	Access Control Management	8 Safeguards	IG1 5/8	IG2 7/8	IG3 8/8
CONTROL 07	Continuous Vulnerability Management	7 Safeguards	IG1 4/7	IG2 7/7	IG3 7/7
CONTROL 08	Audit Log Management	12 Safeguards	IG1 3/12	IG2 11/12	IG3 12/12
CONTROL 09	Email and Web Browser Protections	7 Safeguards	IG1 2/7	IG2 6/7	IG3 7/7
CONTROL 10	Malware Defenses	7 Safeguards	IG1 3/7	IG2 7/7	IG3 7/7
CONTROL 11	Data Recovery	5 Safeguards	IG1 4/5	IG2 5/5	IG3 5/5
CONTROL 12	Network Infrastructure Management	8 Safeguards	IG1 1/8	IG2 7/8	IG3 8/8
CONTROL 13	Network Monitoring and Defense	11 Safeguards	IG1 0/11	IG2 6/11	IG3 11/11
CONTROL 14	Security Awareness and Skills Training	9 Safeguards	IG1 8/9	IG2 9/9	IG3 9/9
CONTROL 15	Service Provider Management	7 Safeguards	IG1 1/7	IG2 4/7	IG3 7/7
CONTROL 16	Applications Software Security	14 Safeguards	IG1 0/14	IG2 11/14	IG3 14/14
CONTROL 17	Incident Response Management	9 Safeguards	IG1 3/9	IG2 8/9	IG3 9/9
CONTROL 18	Penetration Testing	5 Safeguards	IG1 0/5	IG2 3/5	IG3 5/5

CMMC Maturity Model



PROCESSES

PRACTICES

Level 5 Optimizing — Advanced/Progressive

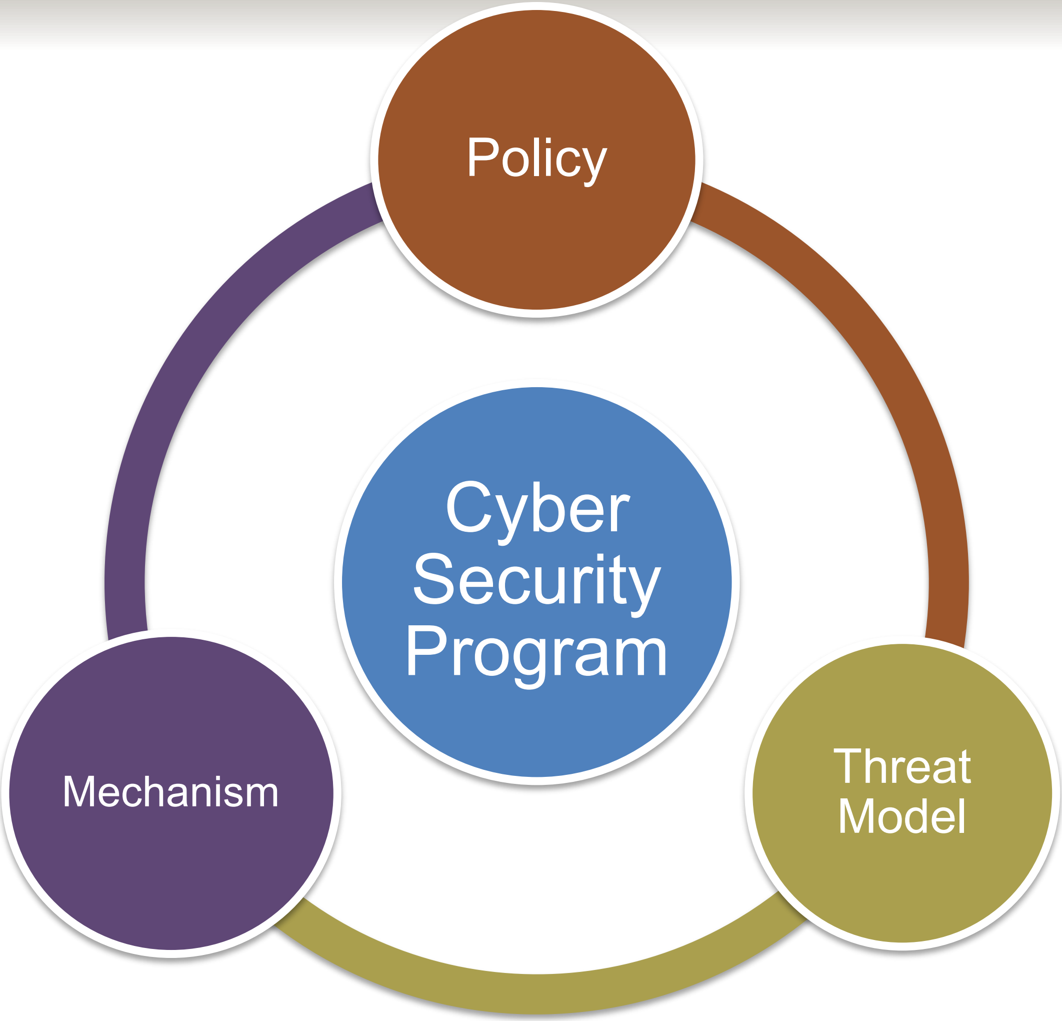
Level 4 Reviewed — Proactive

Level 3 Managed — Good Cyber Hygiene

Level 2 Documented — Intermediate Cyber Hygiene

Level 1 Performed — Basic Cyber Hygiene

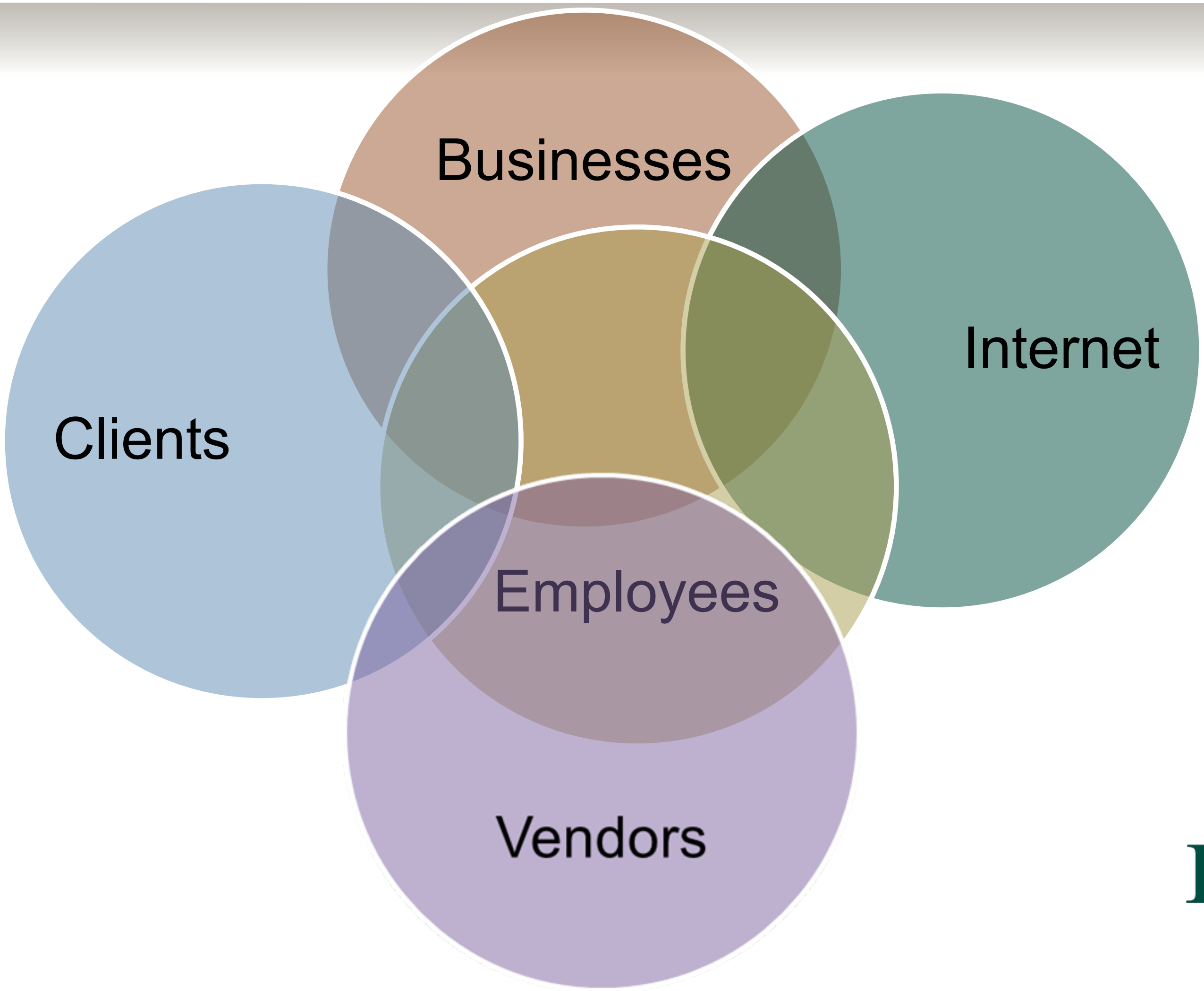
Cyber Security Program Triad



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Know Your Web of Trust



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

WHAT IS YOUR RISK PROFILE?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Do We Have a Cyber & Privacy Program?

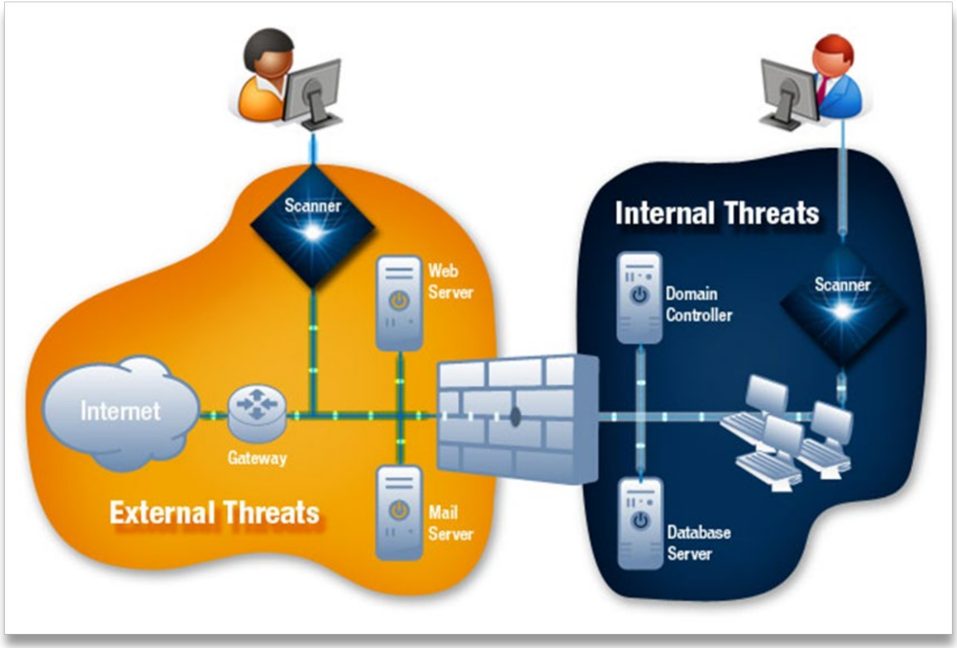
- Is it an active program?
  - Committee in place?
- Is it well planned/budgeted?
- Is it based on a methodology?
  - NIST/CMMC/CIS
  - ISO
  - GDPR/HIPAA

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

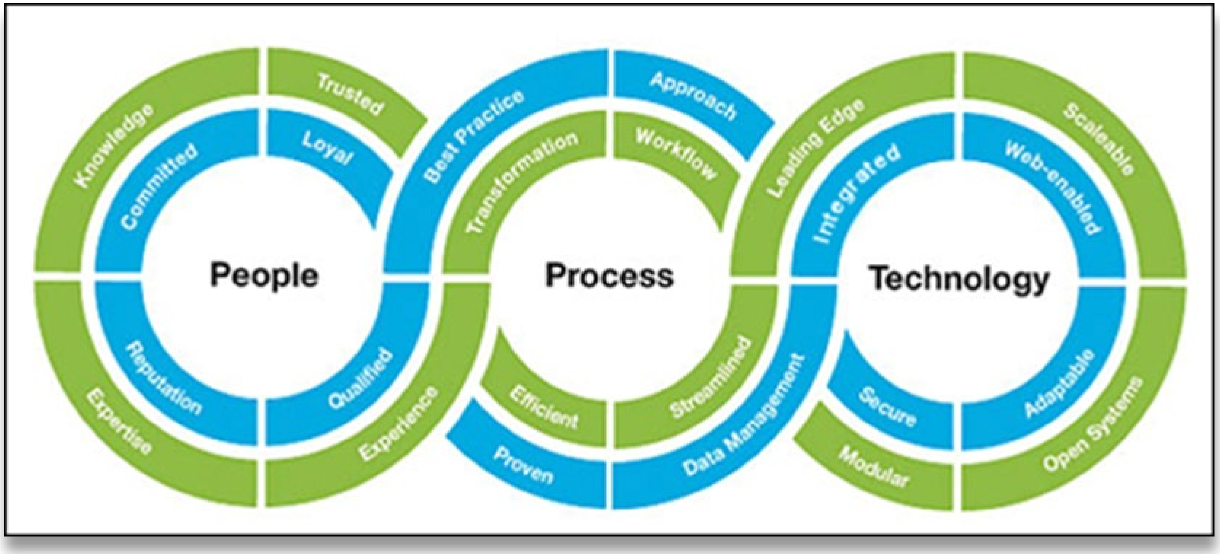
Are We Monitoring Threats?

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

shutterstock.com • 1073337962

Do We Have Updated Policies?

- ► Employee onboarding, 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?



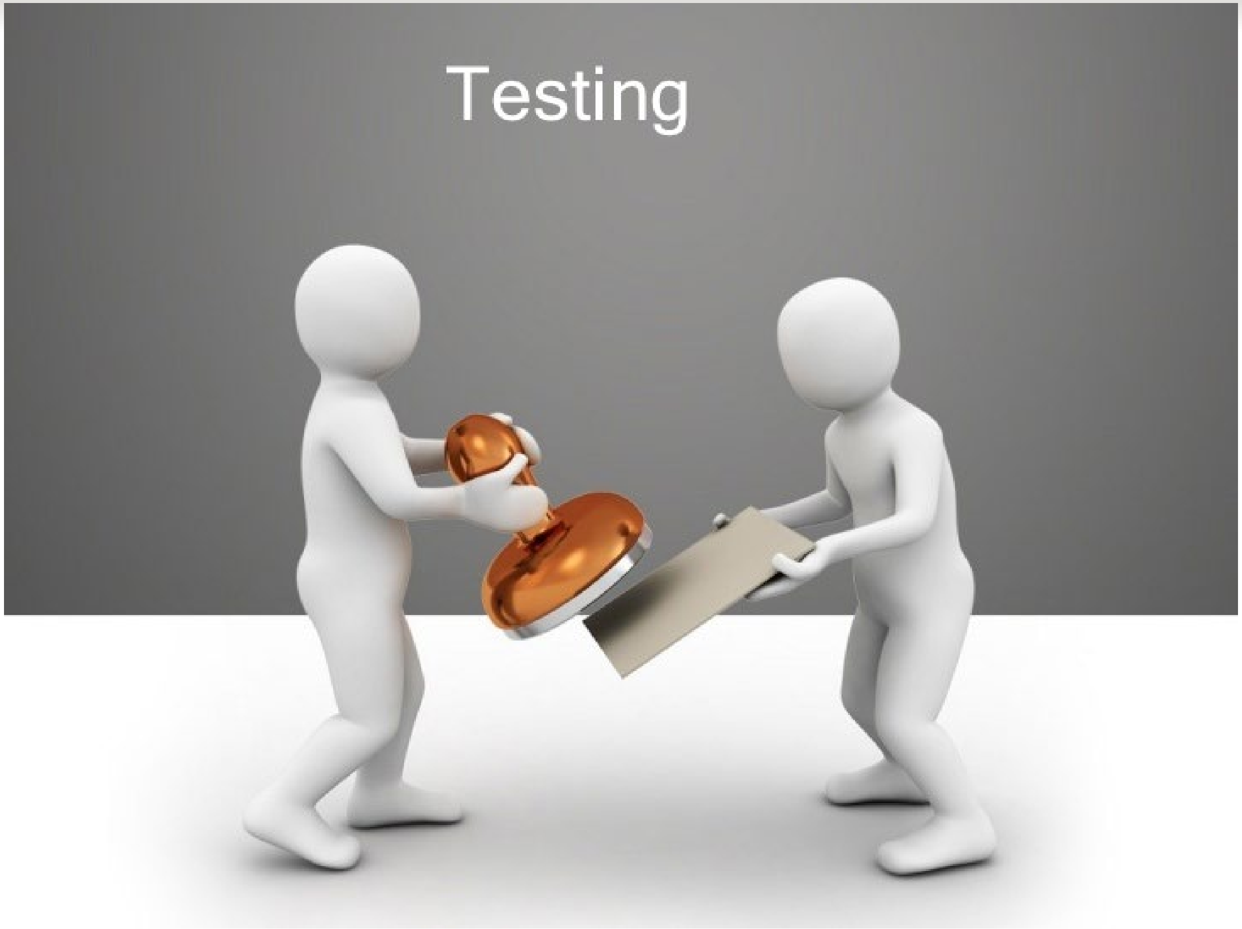
Kreischer Miller
PEOPLE | IDEAS | SOLUTIONS

Do We Have a Cyber Training Program?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Are We Validating User Knowledge?



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

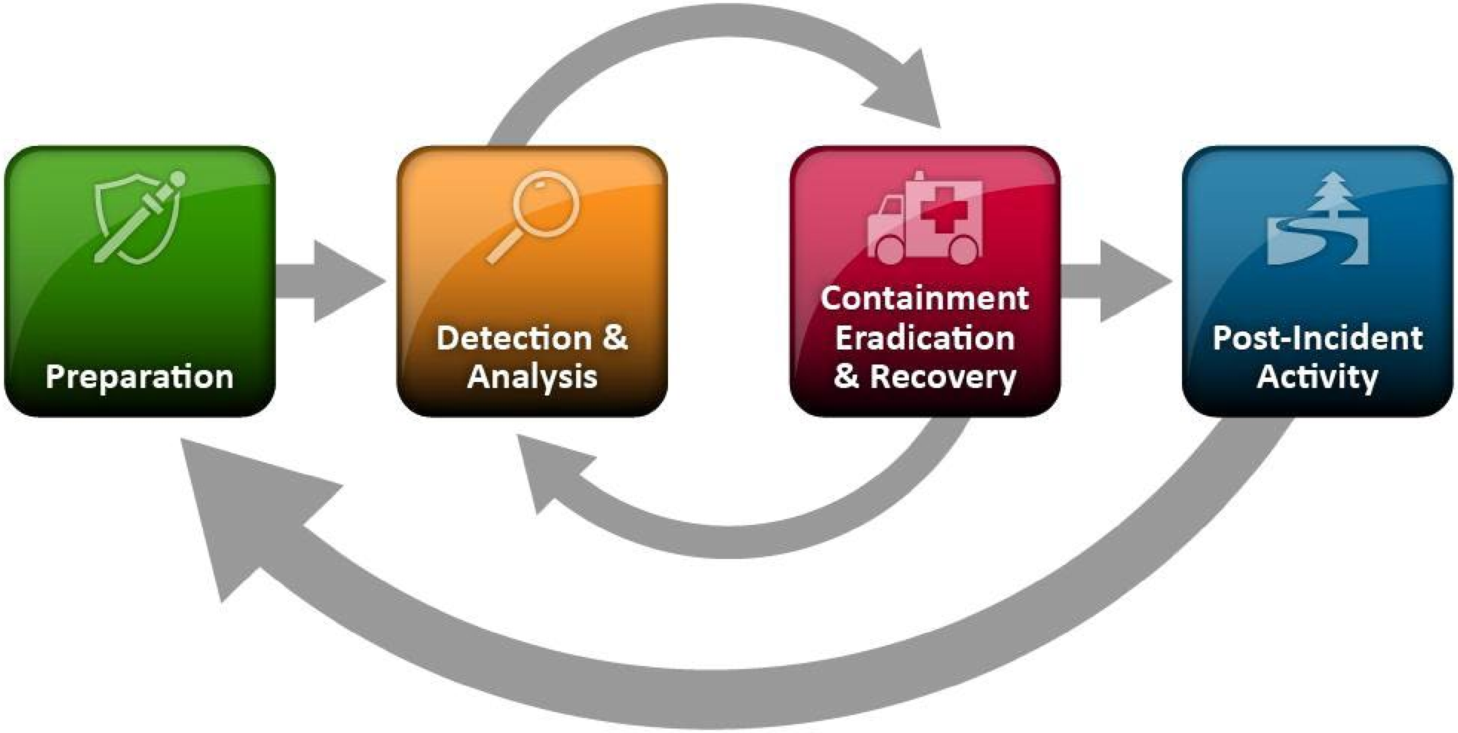
Users Only Access What They Need?

- 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

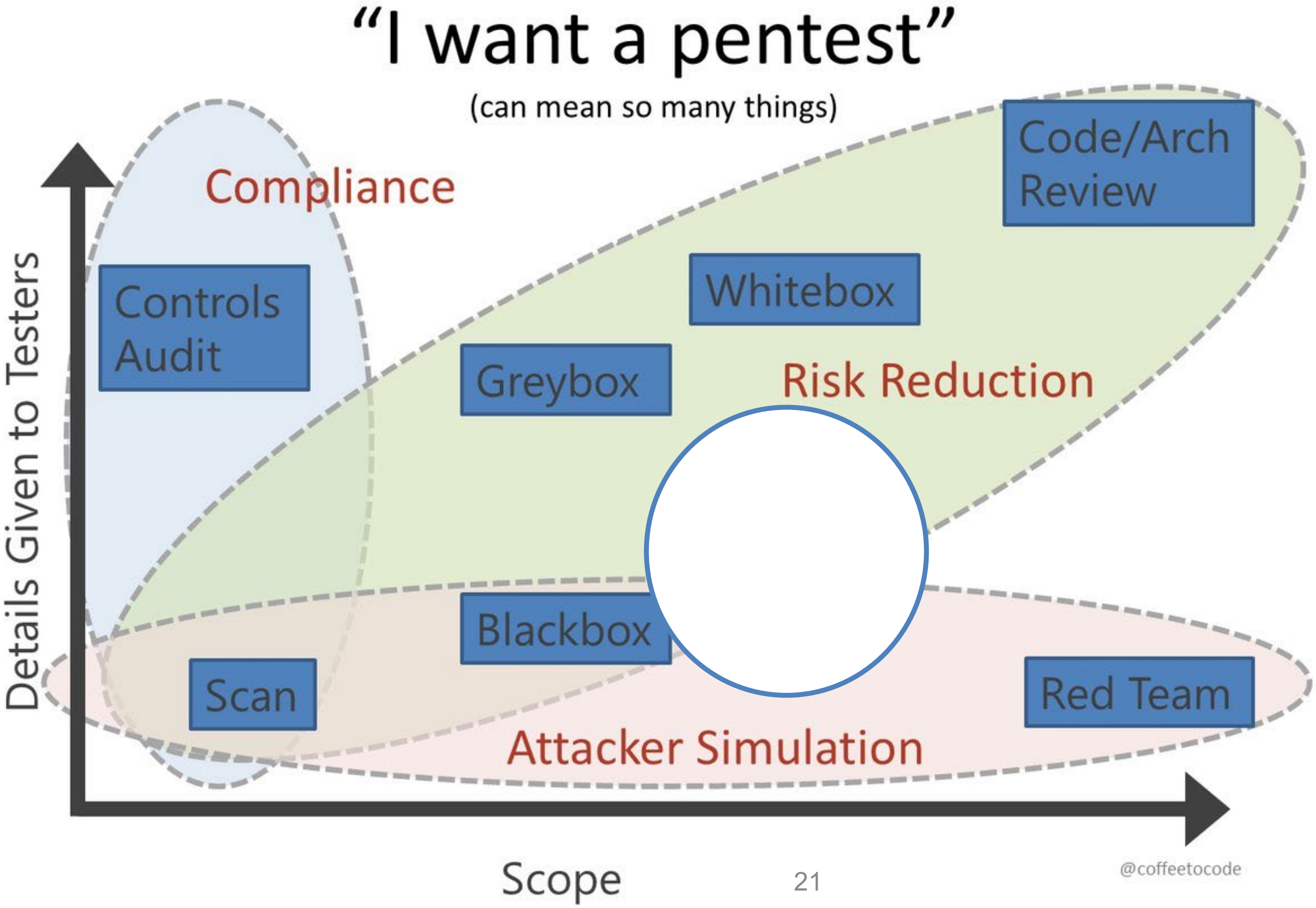
Do we Have an Incident Response Plan?



Cyber Insurance Considerations

Do We Have a Recovery Plan?

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**

What To Do if Breached?

- Do not panic and take care to not overreact
  - When faced with a breach, do not give in to knee-jerk reactions, impulse or pressure. Take a step back to assess the situation.
- Preserve the evidence and document
  - Assume you are sued over this, what evidence would help your case?
- Establish the scope of the breach
  - Attack vectors, time frames, compromised areas, etc.
- Get advice from a trusted advisor
  - Cyber insurance, independent party consults
- Take control of the narrative
  - External reporting considerations

What NOT To Do if Breached?

- Never trust the criminals
  - Don't assume they will give you the correct unlock key if you pay a ransom.
- Never ‘hack back’
  - You don't know who you are dealing with.
- Never assume you regained control
  - The amount of ancillary information adversaries may have gathered could be making the next breach.
- Never assume it cannot get worse
  - Breaches have a ‘long tail’, with many unforeseen consequences.
- Never become complacent
  - Don’t stop being vigilant and staying flexible to adjust.

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Concluding Comments

- Executives are ultimately responsible for their organization’s 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.***

OPEN FORUM SESSION

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Sassan S. Hejazi, Ph.D.
Robert Rittich, CISSP