Cyber & Information Security Readiness

A HOLISTIC APPROACH

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

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

September 24, 2020

Middle Market Cyber & Information Security

- Increased frequency of attacks and breaches
- Limited internal resources and confusion among management on what is getting addressed
- Increased expectations by all stakeholders in regards to safeguarding privacy
- Increased operational, financial, legal and reputational risks
- Need for a unified methodology and an easy way to measure and manage

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

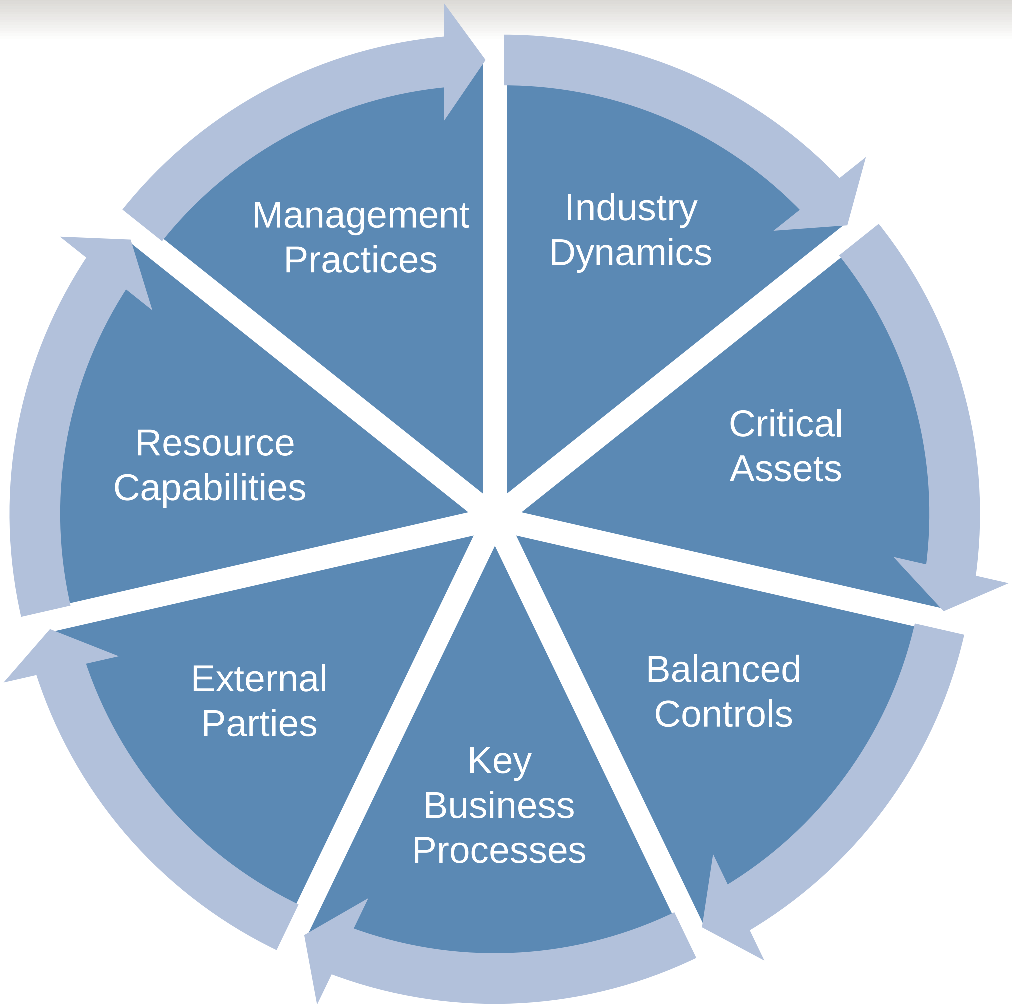
Traditional

- 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

A Holistic Approach



Management Practices

Industry Dynamics

Critical Assets

Balanced Controls

Key Business Processes

External Parties

Resource Capabilities

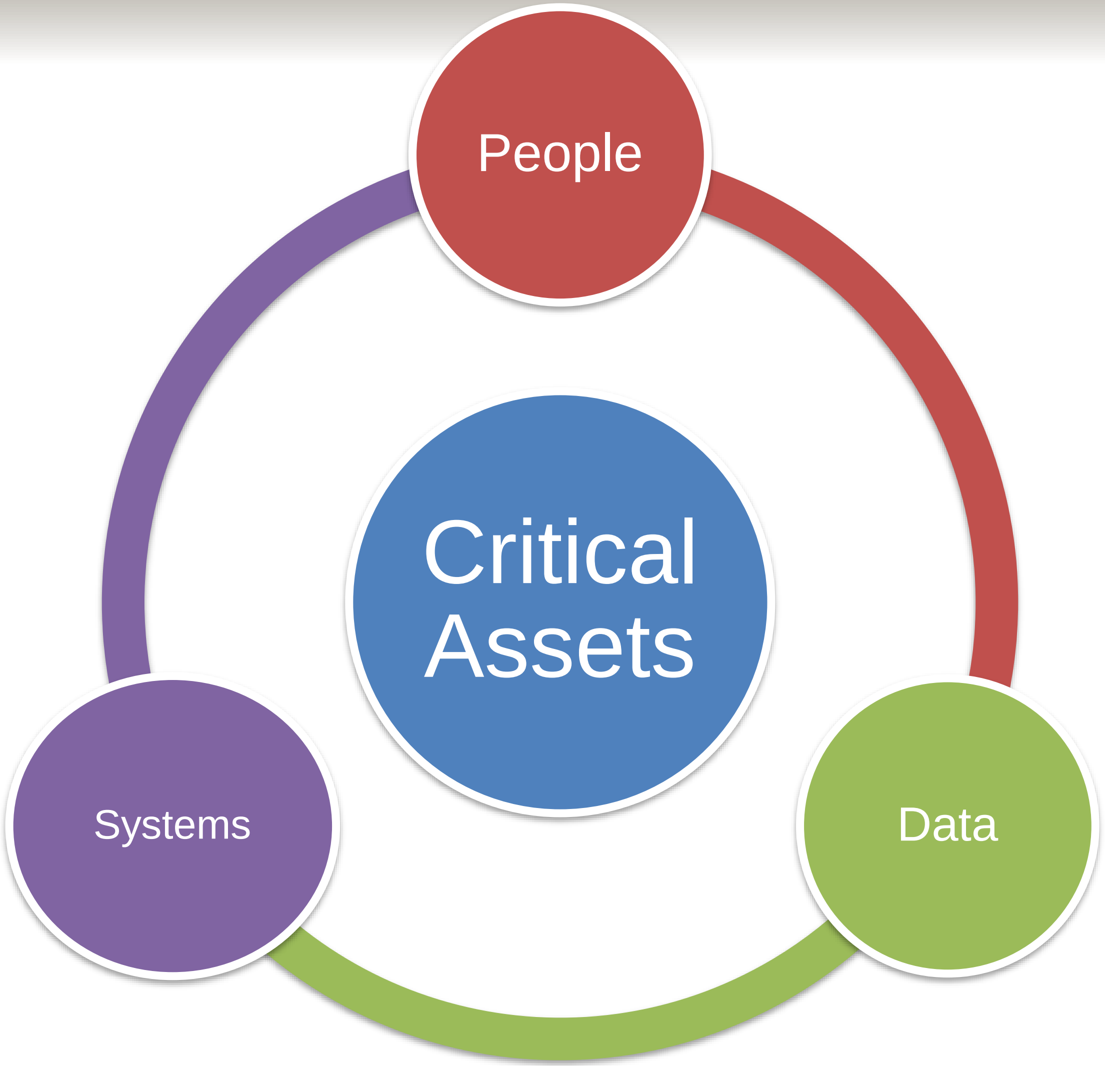
Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Industry Dynamics

- Competitive Landscape – Each industry is subject to its own unique competitive realties that can impact each firms appropriate security postures.
- Business Vision – Each firm within a certain industry segment has their own plans and priorities, creating their unique strategy and as such, will influence their overall security posture.
- Client Requirements – Customers are demanding more flexibilities and options when dealing with their providers that will create new potential challenges for many companies.
- Regulatory Realities – Compliance requirements add another layer to be dealt with for many businesses.

Securing Critical Assets



Critical Assets

People

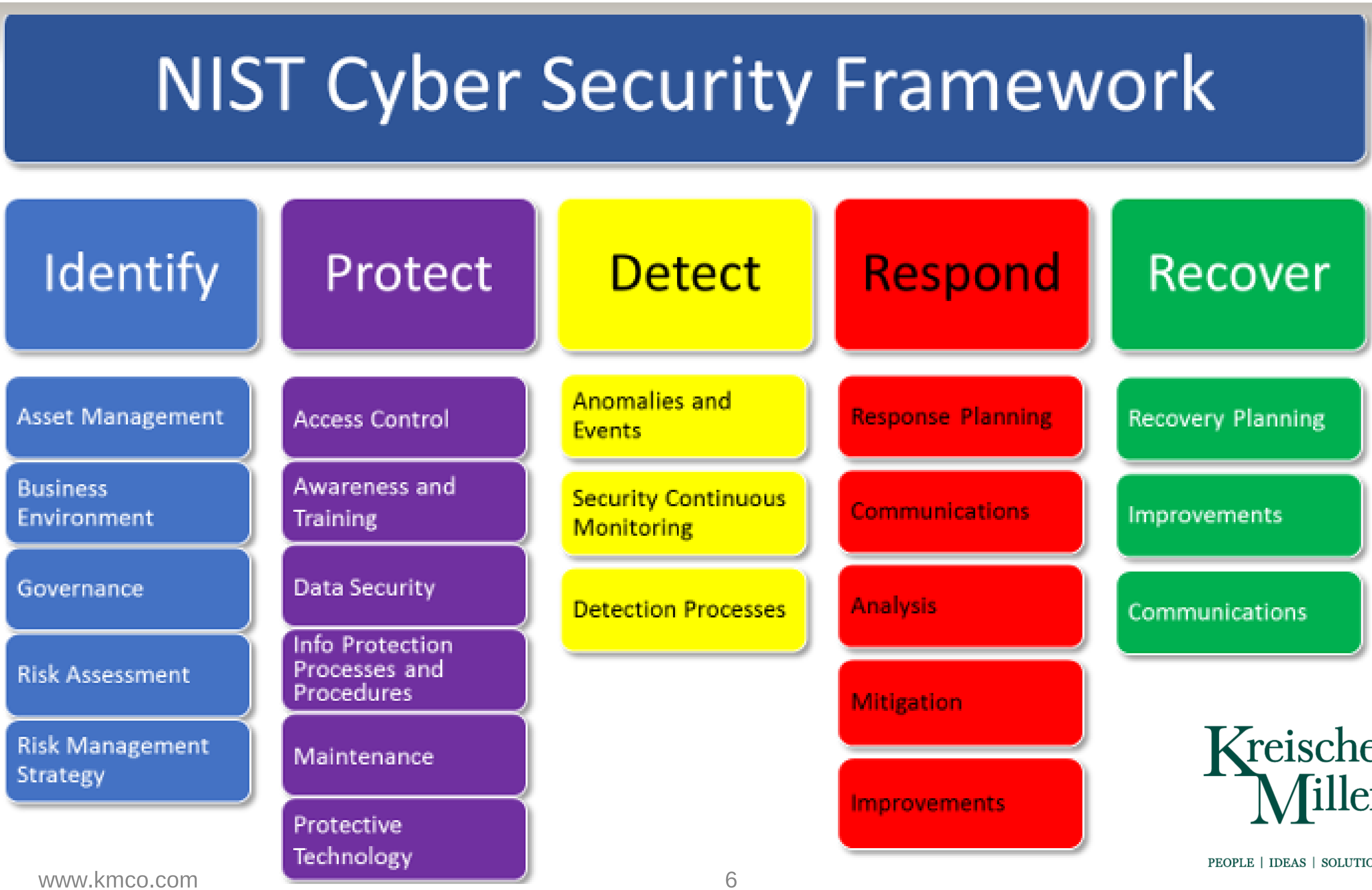
Data

Systems

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

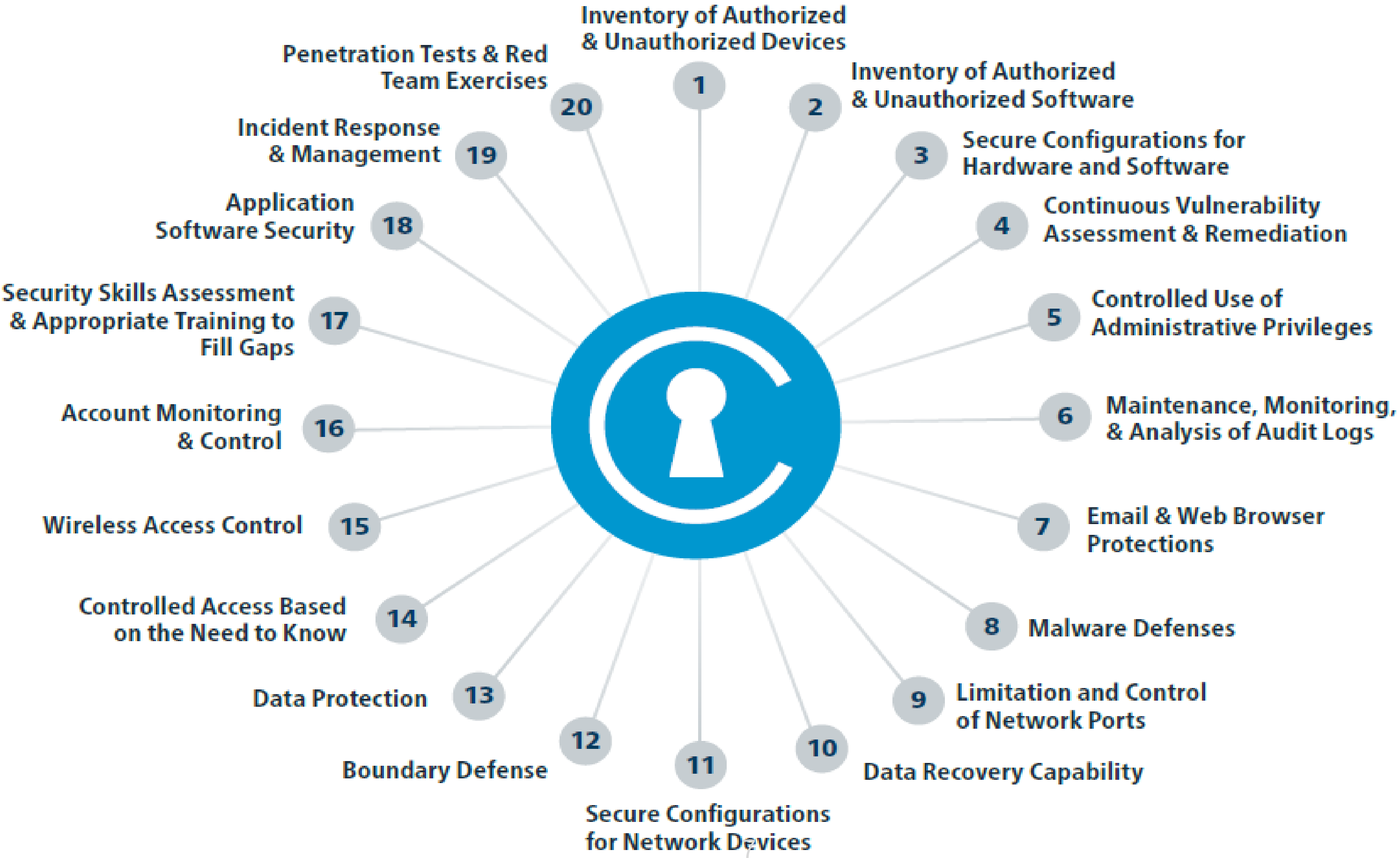
Leveraging Frameworks



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			

CIS Top 20 Controls Approach



1 Inventory of Authorized & Unauthorized Devices

2 Inventory of Authorized & Unauthorized Software

3 Secure Configurations for Hardware and Software

4 Continuous Vulnerability Assessment & Remediation

5 Controlled Use of Administrative Privileges

6 Maintenance, Monitoring, & Analysis of Audit Logs

7 Email & Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports

10 Data Recovery Capability

11 Secure Configurations for Network Devices

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring & Control

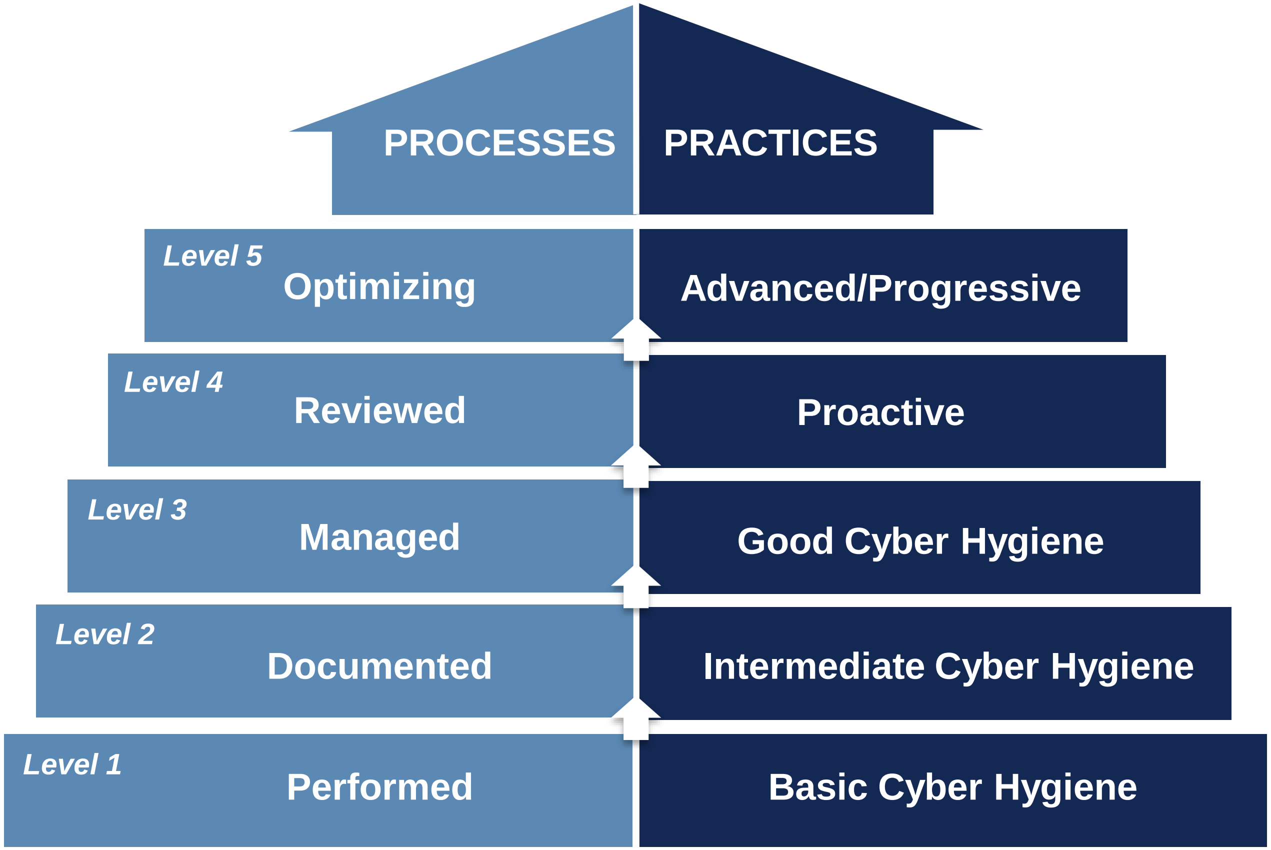
17 Security Skills Assessment & Appropriate Training to Fill Gaps

18 Application Software Security

19 Incident Response & Management

20 Penetration Tests & Red Team Exercises

CMMC/DoD Controls Approach

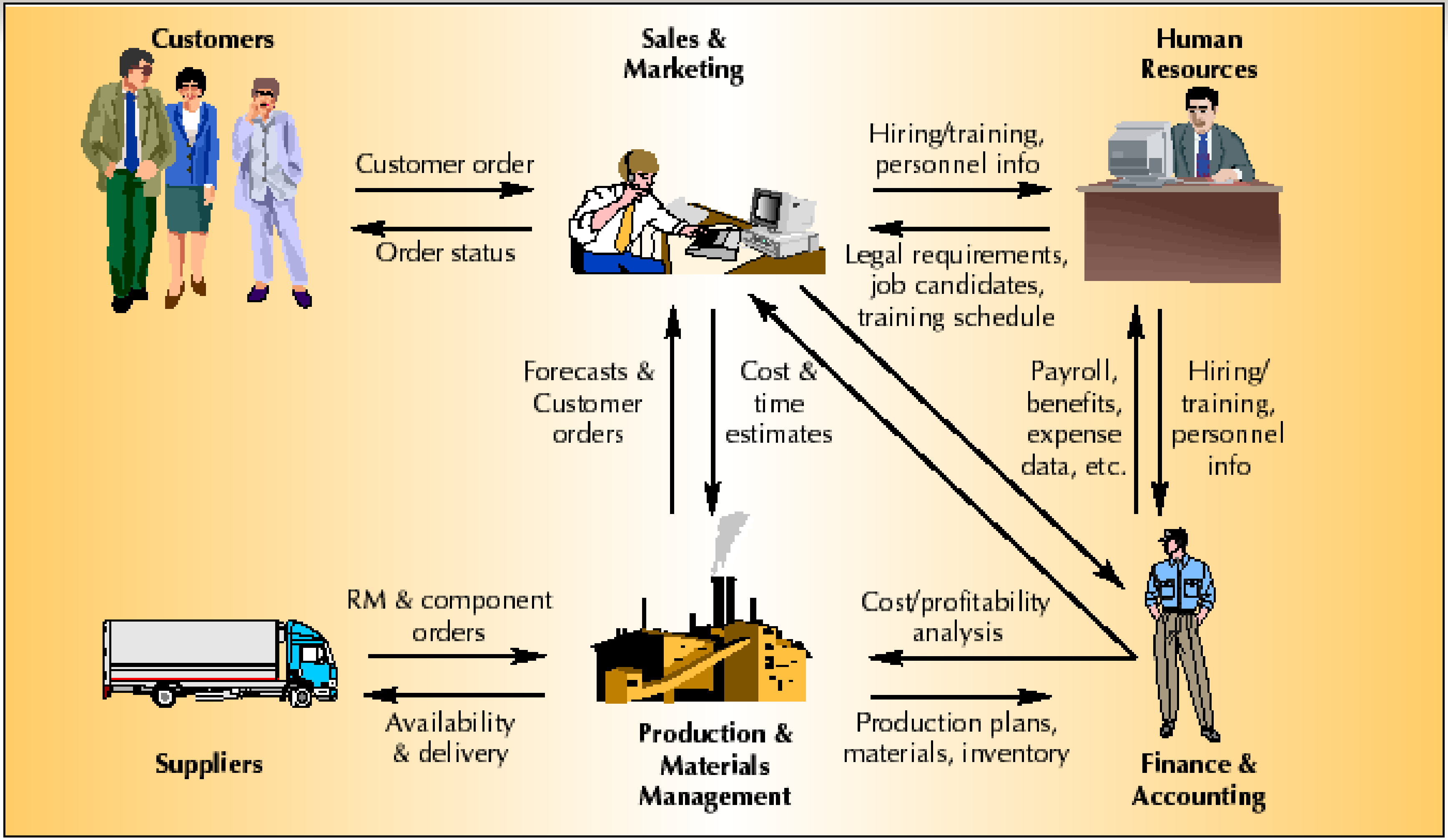


	PROCESSES	PRACTICES
Level 5	Optimizing	Advanced/Progressive
Level 4	Reviewed	Proactive
Level 3	Managed	Good Cyber Hygiene
Level 2	Documented	Intermediate Cyber Hygiene
Level 1	Performed	Basic Cyber Hygiene

Kreischer Miller

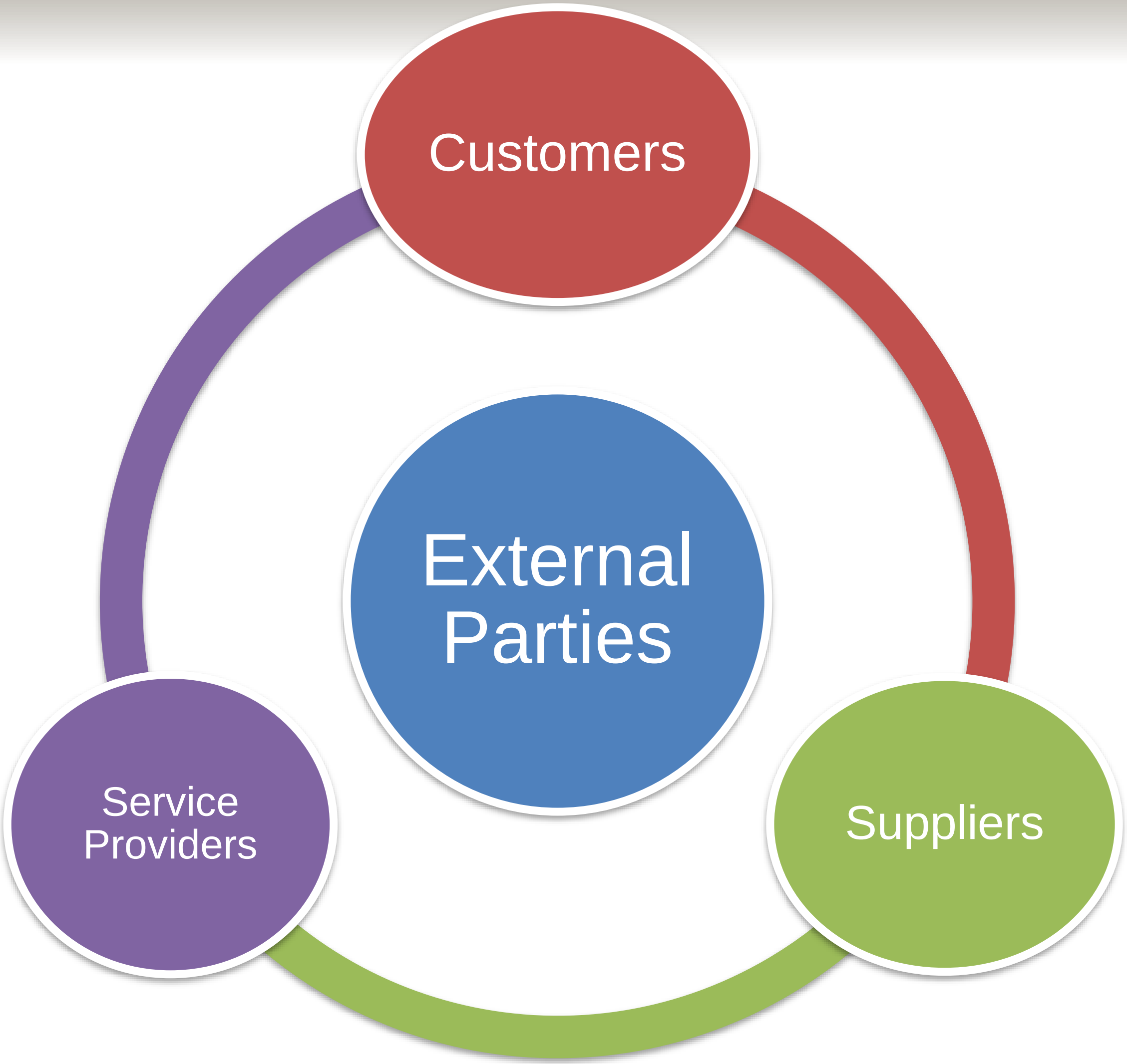
PEOPLE | IDEAS | SOLUTIONS

Key Business Processes



Customers
Sales & Marketing
Human Resources
Customer order
Order status
Hiring/training, personnel info
Legal requirements, job candidates, training schedule
Forecasts & Customer orders
Cost & time estimates
Payroll, benefits, expense data, etc.
Hiring/ training, personnel info
RM & component orders
Availability & delivery
Cost/profitability analysis
Production plans, materials, inventory
Suppliers
Production & Materials Management
Finance & Accounting

External Parties



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Resource Considerations

- Middle market companies are the ones feeling the impact of IT security resources the most:
  - Larger firms have dedicated security teams
  - Small businesses rely on affordable cloud based tools
- There is no shortage of cyber and information security solutions on the market.
- Most often middle market companies go on an investment binge after experiencing a cyber incident, resulting in a “fog of more” solution impact.
- Selecting proper tools and partners could significantly impact middle market organizations cyber readiness levels.

Management Practices

- Management is ultimately responsible for safeguarding company assets and ensuring effective operations during disruptive periods.
- IT is responsible for educating management on effective technology enabled solutions while management is responsible for defining organizations risk management approach and priorities using such tools.
- Managements responsibility extends to Board members and external advisors in relation to effective cyber and information privacy considerations.
- IT management by itself can not achieve a holistic approach towards increased cyber effectiveness.

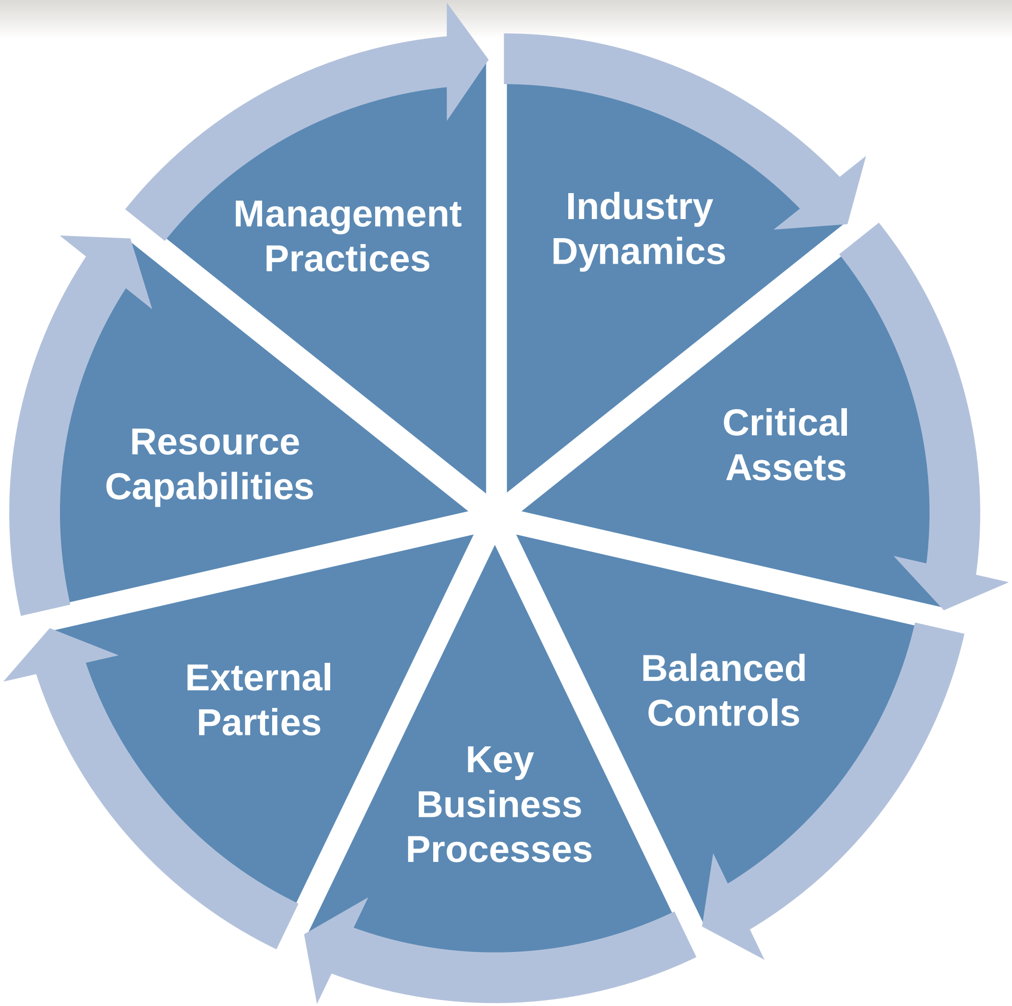
How do we get there?

- Conduct a detailed review of existing IT system vulnerabilities including scanning your computing environment.
- Review applicable control methodologies ranging from CIS to DFARS/CMMC, SOC, HIPAA or PCI to evaluate your controls.
- Interview executives and key business process owners, conduct walkthroughs to identify potential cyber and information privacy risks in your critical business processes.
- Establish baseline competency evaluation of users cyber and information security knowledge.
- Review all existing policies and procedures related to internal and external use of data and systems.
- Analyze data, develop scores, to identify risk factors and establish remediation priorities.

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

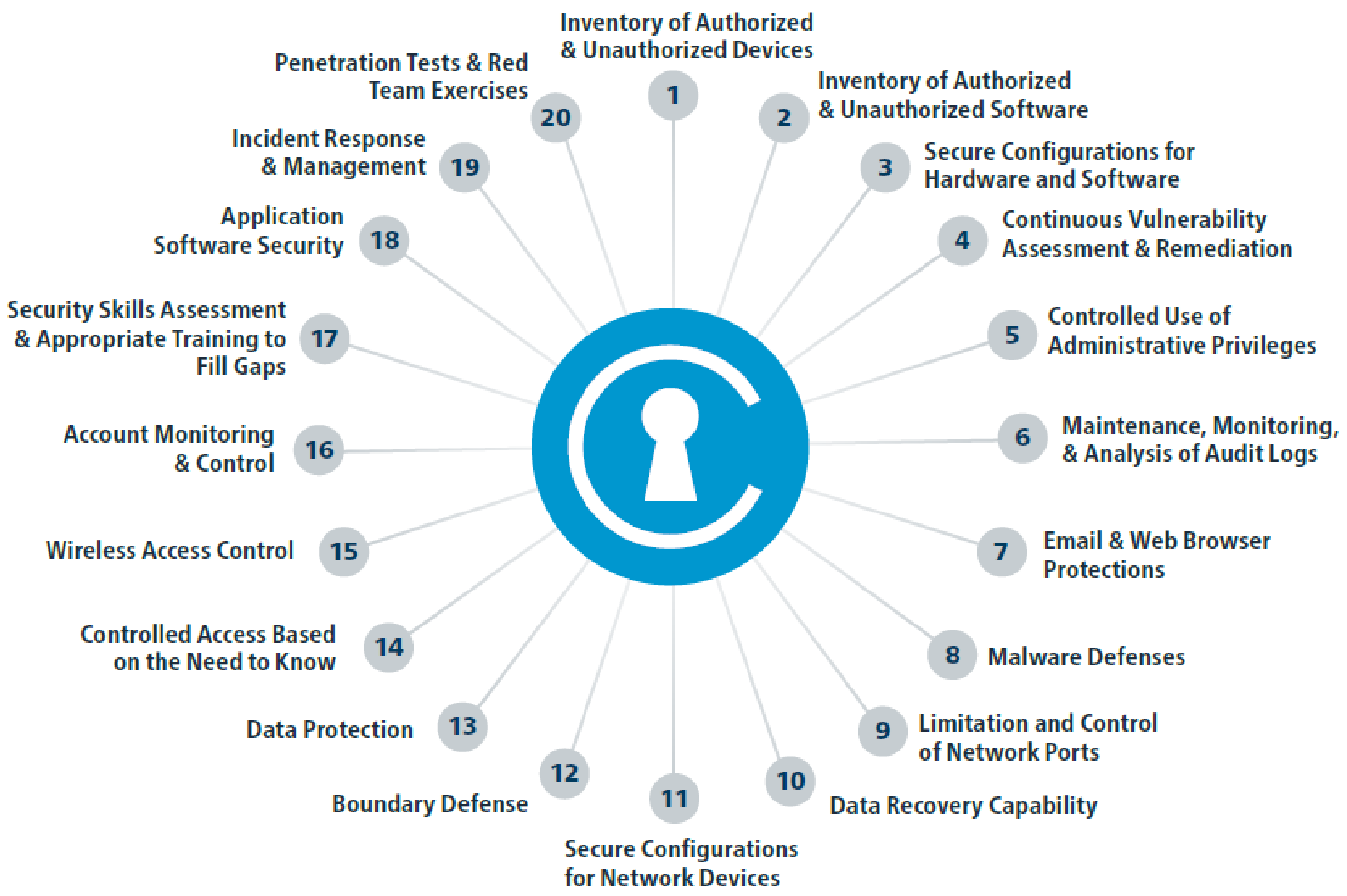
A Holistic Approach – NIST+



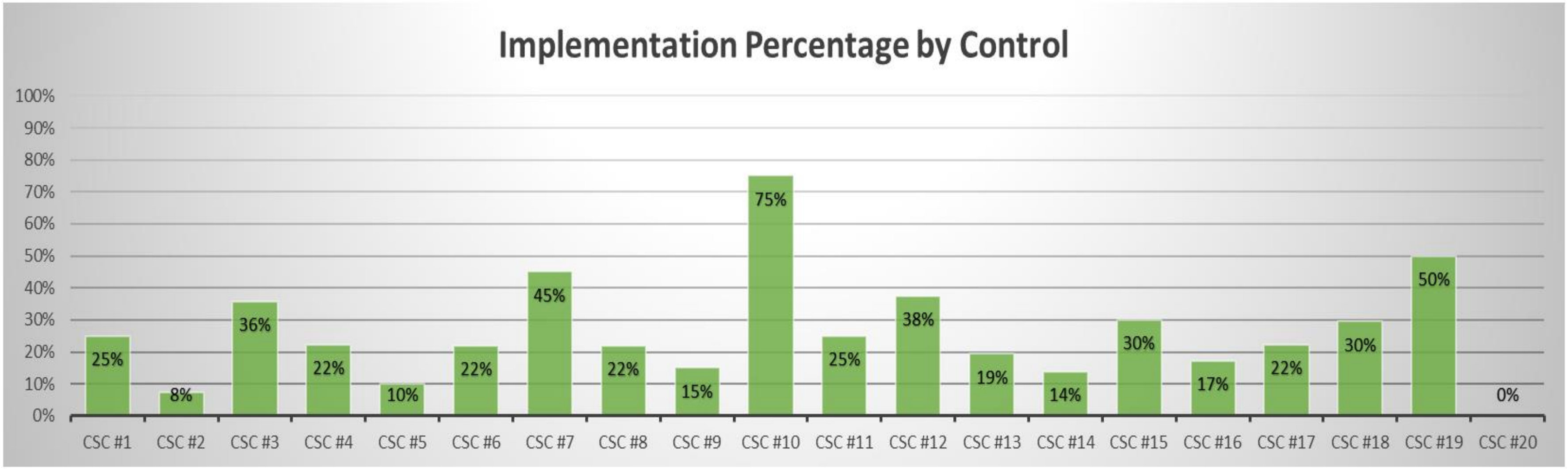
Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

CIS Top 20 Controls Approach


1 Inventory of Authorized & Unauthorized Devices
2 Inventory of Authorized & Unauthorized Software
3 Secure Configurations for Hardware and Software
4 Continuous Vulnerability Assessment & Remediation
5 Controlled Use of Administrative Privileges
6 Maintenance, Monitoring, & Analysis of Audit Logs
7 Email & Web Browser Protections
8 Malware Defenses
9 Limitation and Control of Network Ports
10 Data Recovery Capability
11 Secure Configurations for Network Devices
12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring & Control
17 Security Skills Assessment & Appropriate Training to Fill Gaps
18 Application Software Security
19 Incident Response & Management
20 Penetration Tests & Red Team Exercises

CIS Top 20 Dashboard



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

CIS Top 20 Controls Risk Summary

CONTROL GROUP	Grade	Sampling of Key Findings
BASIC	B+	- Effective hardware & software management practices - Need to address Admin account privileges
INTERMEDIATE	B	- Effective data recovery capabilities - Need to improve device security configurations
ADVANCE	B	- Effective application software controls in place - Need to develop incident response plan

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Key Business Process Cyber Risks

PROCESS	GRADE	Sampling of Key Findings
Sales	C+	- Improved control of CRM access credentials - Handling of client confidential information - Implement MDM solution for sales team
Operations	B	- Improve warehouse wireless security
H/R	B	- Update current employee onboarding cyber related policies and procedures
Finance	B+	- Implement multi factor authentication for bank account access

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

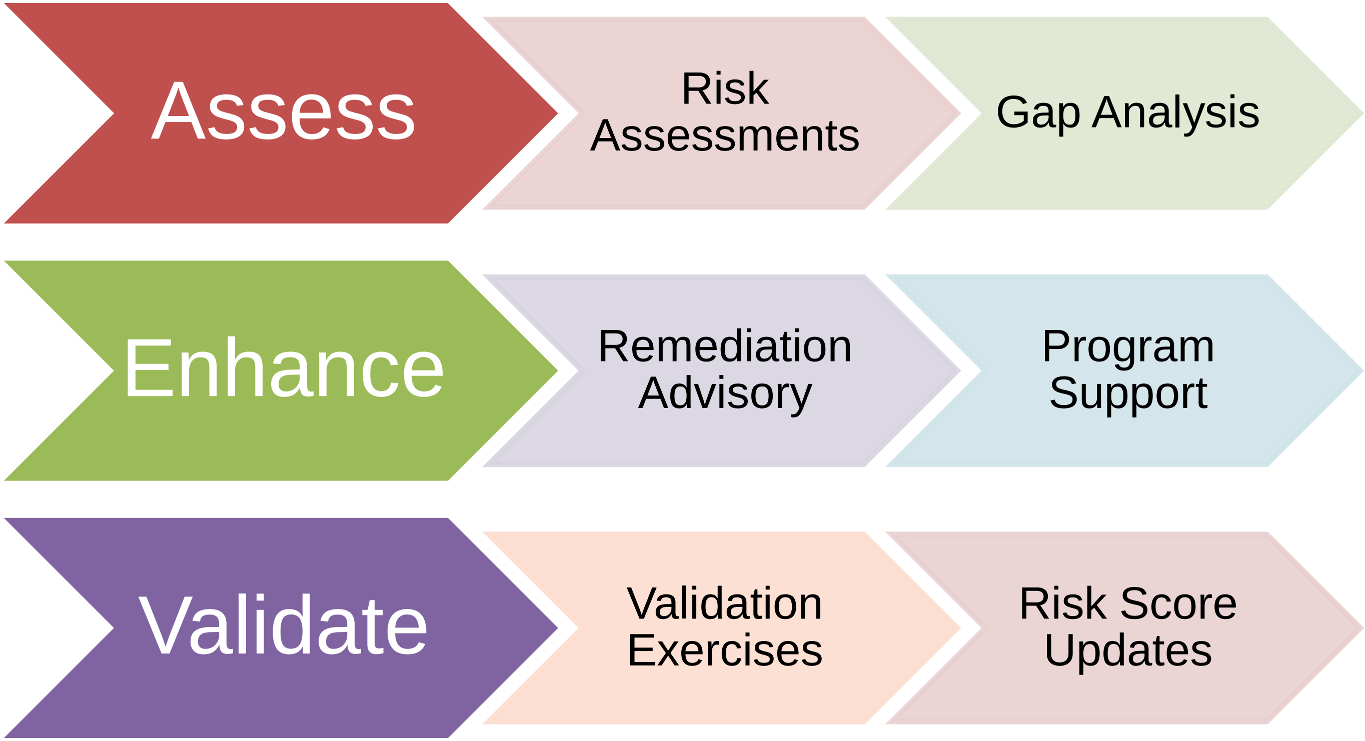
External Party Risk Summary

CONTROL GROUP	GRADE	Sampling of Key Findings
Customers	B	- Safeguard client credit card information
Suppliers	B	- Establish proper vendor system access policies and procedures
Service Providers	C	- Validate IT provider security credentials

Benefits of a Holistic Cyber Approach

- Conducting a periodic “grading” of cyber and information privacy readiness to ensure we have a better understanding of potential risks as technologies, key processes and threat vectors are changing at all times.
- Ability to plan IT related initiatives and remediation efforts that would have maximum Risk Mitigation ROI as seen best fit by executive management.
- Establishing a collaborative mindset between IT and non-IT to ensure most effective planning and execution, resulting in increased competitive capabilities for the firm.
- Reducing risks of a future cyber and information security event and being better prepared if one occurs.

KM 3 Phases of Cyber & Information Security Program Support



Assess

Risk Assessments

Gap Analysis

Enhance

Remediation Advisory

Program Support

Validate

Validation Exercises

Risk Score Updates

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Thank you for attending!

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

For more information,
visit **www.kmco.com**.

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS