ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

CREATe Compliance
An ETHISPHERE® Business

Introducing CREATe Compliance: Aligning Your Cybersecurity Approach to Leading Practices and International Guidance

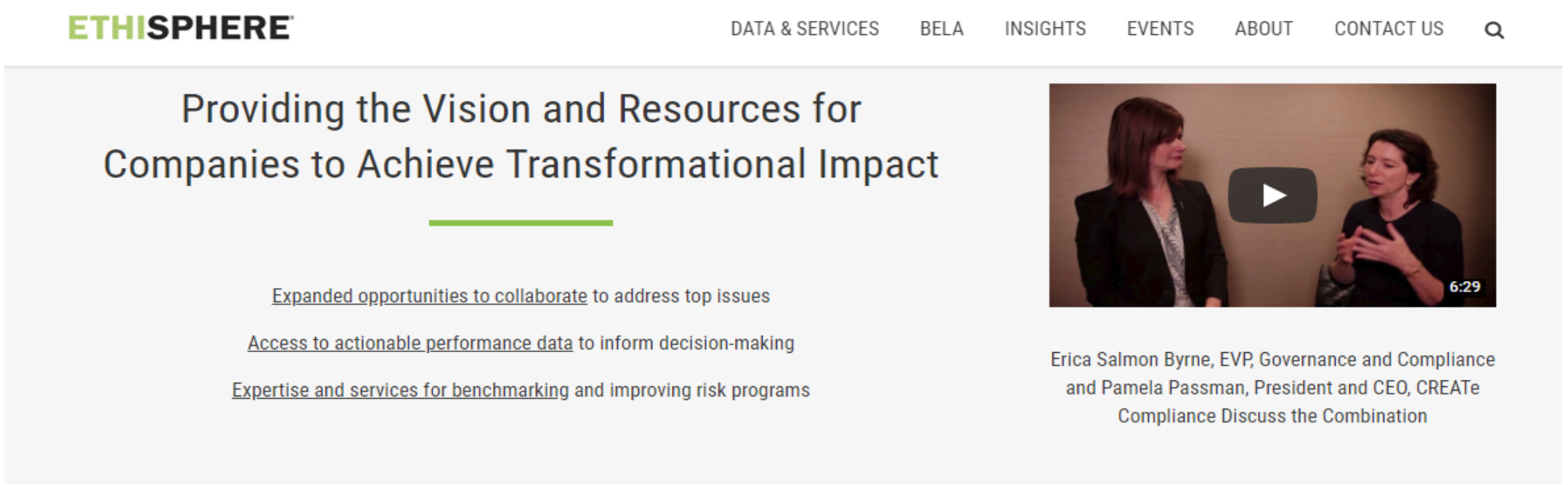
Erica Salmon Byrne, Executive Vice President, Governance and Compliance, Ethisphere Institute

Pamela Passman, Vice Chair, Ethisphere Institute and Chief Executive Officer, CREATe Compliance

Today we will discuss…

- Ethisphere and CREATe Compliance
- The evolving cybersecurity landscape
- Engaging a cross-functional team
- Leading guidance – how global companies manage risks
- A new benefit for BELA members

CREATe Compliance Joins Ethisphere



"Ethisphere combining with CREATe Compliance brings together two complementary approaches to helping companies foster a stronger values-based leadership and the robust and effective programs to back it up."

-- Brad Smith, President and Chief Legal Officer, Microsoft

ETHISPHERE
GOOD. SMART. BUSINESS. PROFIT.
CREATe Compliance
An ETHISPHERE Business

CREATe Compliance works with enterprises to better manage internal and third party global risk for key issues.

CREATe Compliance's services – *CREATe Leading Practices* – provide a practical and scalable way to measure, improve, benchmark and monitor compliance and risk programs:

- **CREATe Leading Practices for Cybersecurity** – *Aligned to the NIST Cybersecurity Framework*
- **CREATe Leading Practices for Intellectual Property Protection**
- **CREATe Leading Practices for Trade Secret Protection**
- **CREATe Leading Practices for Anti-Corruption** – *Aligned to leading international guidance and the ISO 37001 Anti-Bribery Management Systems Standard*

The evolving cybersecurity landscape – top trends and topics to watch

CREATE Compliance
An ETHISPHERE Business

ETHISPHERE
GOOD. SMART. BUSINESS. PROFIT.

Headlines Focus on Personal Data …

USA TODAY

Cyber breach at Equifax could affect 143M U.S. consumers

Kevin McCoy, USA TODAY Published 5:17 p.m. ET Sept. 7, 2017 | Updated 3:12 p.m. ET Sept. 8, 2017

WIRED

LILY HAY NEWMAN SECURITY 02.24.17 12:53 PM

MASSIVE BUG MAY HAVE LEAKED USER DATA FROM MILLIONS OF SITES. SO … CHANGE YOUR PASSWORDS

LILY HAY NEWMAN SECURITY 06.19.17 07:37 PM

THE SCARILY COMMON SCREW-UP THAT EXPOSED 198 MILLION VOTER RECORDS

… Yet Cyber Risks Go to the Core of Business

#CYBER RISK MAY 12, 2017 / 6:25 AM / 5 MONTHS AGO

REUTERS

Telefonica, other Spanish firms hit in "ransomware" attack

---

theguardian

Monday 25 September 2017 08.00 EDT

Deloitte hit by cyber-attack revealing clients' secret emails

---

SC MEDIA

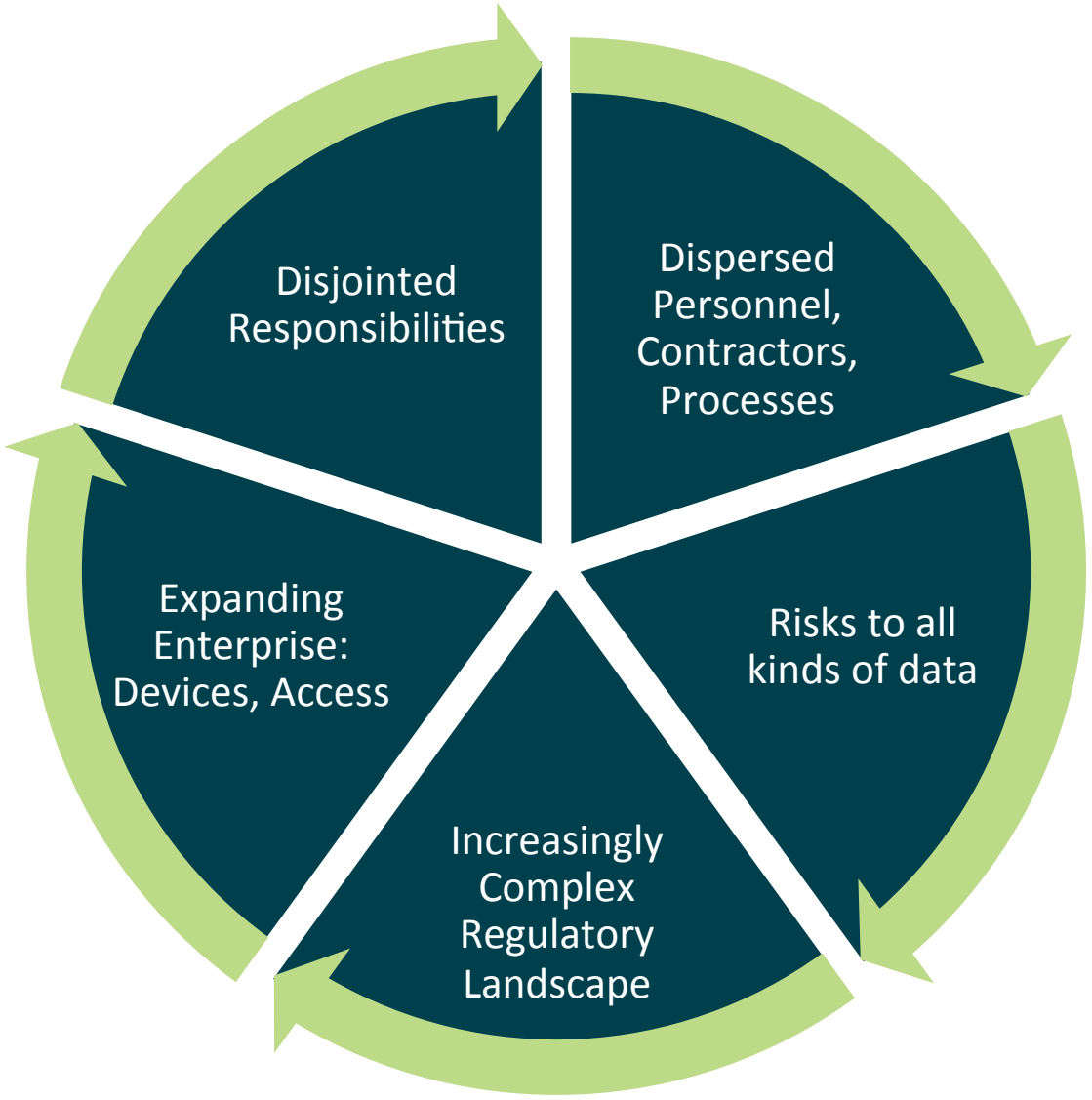
March 16, 2017

IT pros fear cyberespionage may be top 2017 threat

December 10, 2016

Stealing steel's secrets: Industrial conglomerate ThyssenKrupp breached by pro hackers

The Situation for Businesses



Cyber Risk Threat Landscape

Threat Actor	Objectives	Methods	Vulnerabilities
Malicious Insiders	Competitive advantage, financial gain, national goals	Blunt force hacking Social Engineering Trojan Horse Spear phishing Watering Hole Exploits Malware Co-opted Credentials Physical/Non-technical	People Processes Technology
Nation States	Military technology, help national companies		
Competitors	Competitive advantage		
Transnati'l Organized Crime	Financial gain		
Hacktivists	Political/social goals		

Source: CREATe.org – PwC Report: Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential thefts, February 2014

Threats and Challenges Ahead

The Cloud
- Expands networks
- Attack Target

Internet of Things (IoT)
- Access points
- Security vulnerabilities

"You can't protect everything equally…we have to find a way to control only what matters," **said Earl Perkins, research vice president, Gartner**

Compliance and Data Protection Convergence
- EU General Data Protection Regulation (GDPR)

Highly targeted data collection:
- Intellectual property
- Competitive intelligence

Increase in attacks and sophistication
- Cybercrimes go mainstream
- Mobile device attacks
- Harder to 'detect, investigate, remediate'

Engaging a cross-functional team – working together to secure confidential information

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

CREATE Compliance
An ETHISPHERE® Business

Cybersecurity Integrated into Business

Board Oversight

Executive Level Decision-Making

Cross-Functional and Incident Response Team

Legal
Chief Compliance Officer (CCO)
Risk
Chief Information Officer (CIO)
Chief Information Security Officer (CISO)

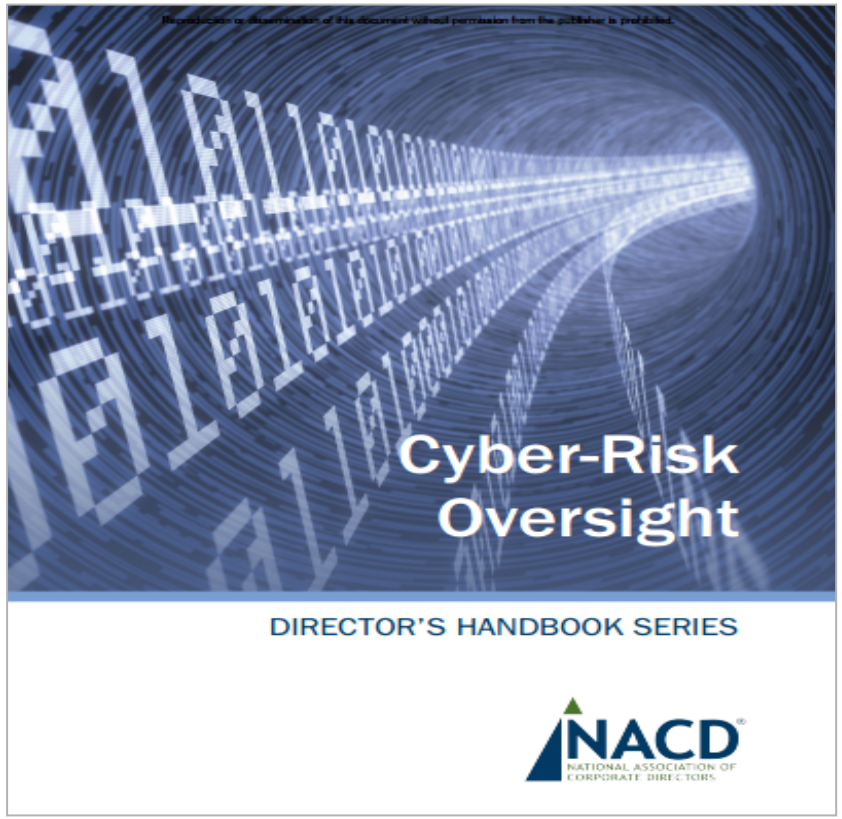
Finance
Communications/PR
Physical Security
Supply Chain
Customer Support
Human Resources

Stakeholders

Employees
Customers
Vendors/Suppliers
Partners
Lenders

Shareholders
Regulatory agencies
Law enforcement
Media (formal and informal)

Questions from the Board



Download the report at: https://www.nacdonline.org/cyber

How would you answer these questions?

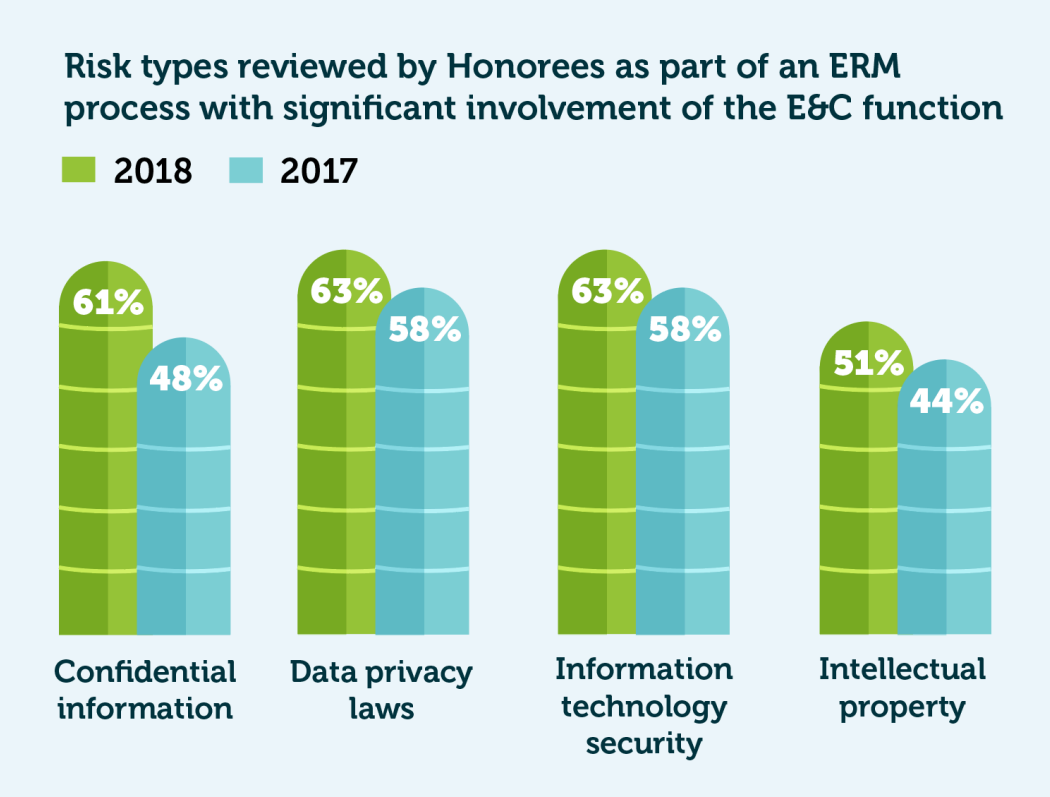
- Do we have appropriately differentiated strategies for general cybersecurity and for protecting our mission-critical assets?
- What are the company's cybersecurity risks?
- How is the company managing these risks?
- Who are our likely adversaries?
- How will we know if we have been breached? How will we find out?
- Do we have a systematic framework, such as the NIST Cybersecurity Framework, in place to address cybersecurity and assure adequate cybersecurity hygiene?

Leading guidance – how global companies are managing risk

ETHISPHERE
GOOD. SMART. BUSINESS. PROFIT.

CREATE Compliance
An ETHISPHERE Business

Cybersecurity:
World's Most Ethical Companies



An ERM Approach to Protecting Confidential Data

Trends:

- Breaking information security out of the IT silo
- Viewing sensitive, valuable and confidential information as a risk if compromised

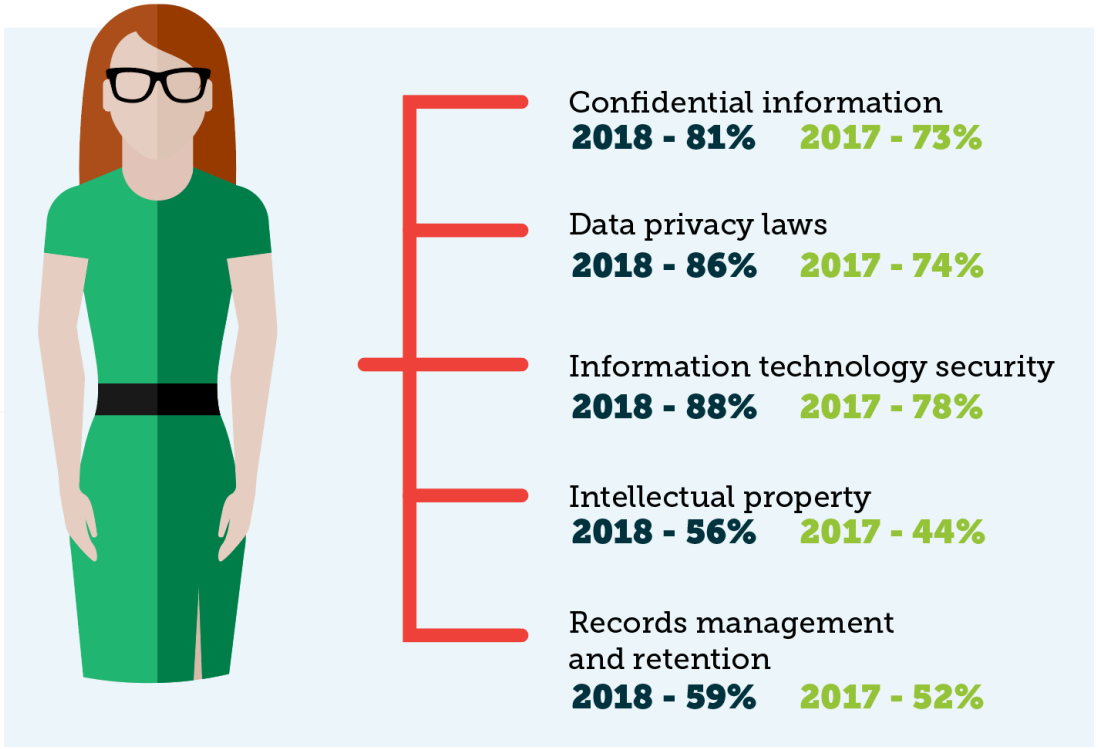
Cybersecurity:
The World's Most Ethical Companies

Engaging with Boards

- **68%** provide cybersecurity education to Board Directors
- **53%** provide education on privacy regulations
- **93%** report on information security program updates
- **86%** conduct privacy risk assessment and results

WME Data: Insiders and Third Parties

Training Employees



Addressing Third Party Risk

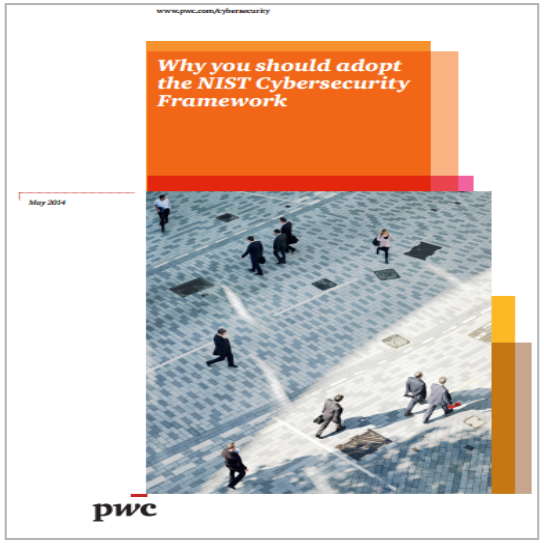
- **84%** consider data security as part of the Ethics and Compliance due diligence
- **76%** conduct data security audits of third parties that access and store sensitive company information

The NIST Cybersecurity Framework

National Institute of Standards and Technology
U.S. Department of Commerce

"By 2020, more than 50% of organizations will use the NIST Cybersecurity Framework, up from 30% in 2015."

Gartner: Best Practices in Implementing the NIST Cybersecurity Framework
January, 21, 2016

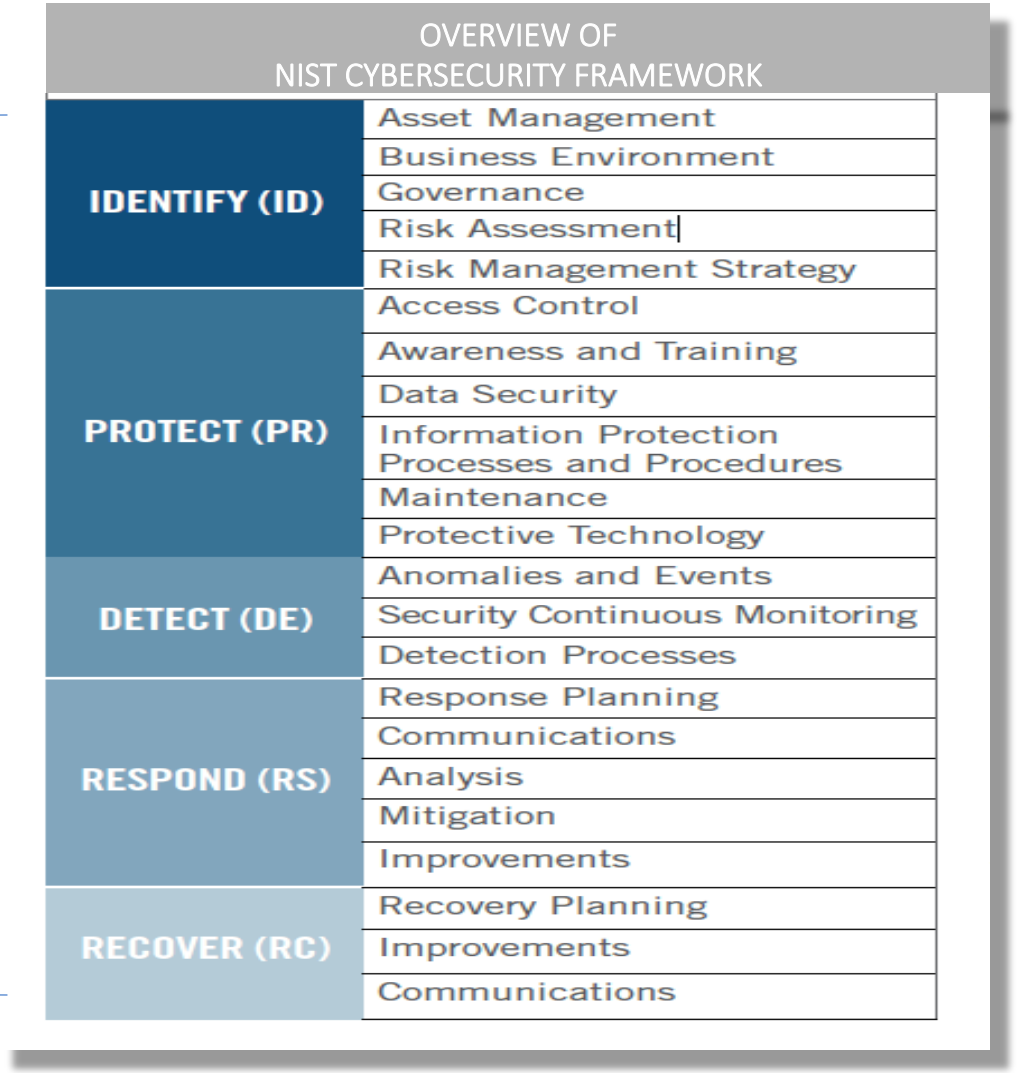


"The Framework creates a common language for the discussion of cybersecurity issues that can facilitate internal and external collaboration."

"Organizations that adopt the Framework at the highest possible risk-tolerance level may be better positioned to comply with future cybersecurity and privacy regulations."

Elements of the NIST Framework

Five main Functions



22 Categories & 98 Subcategories of Controls

Providing an analysis of technical and management capabilities

Measuring maturity of cybersecurity programs – promoting consistency and reporting to the C-suite and Board

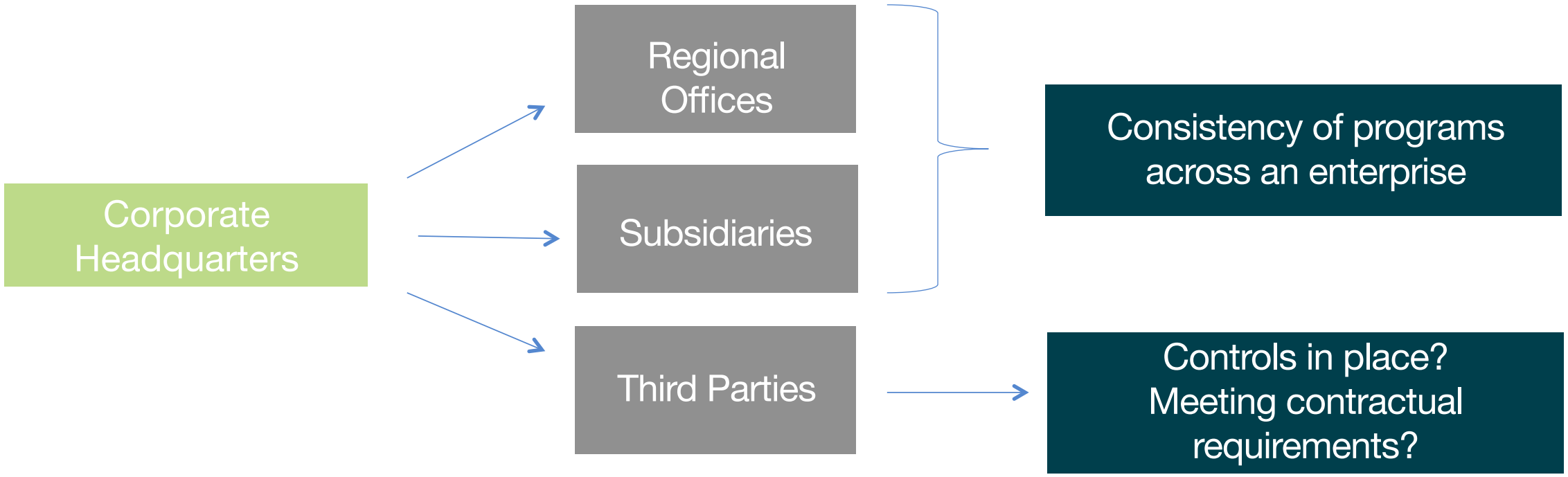
ETHISPHERE
GOOD. SMART. BUSINESS. PROFIT.

CREATE Compliance
An ETHISPHERE Business

Top Four Challenges in Evaluating Cybersecurity Risk

- Scope
- Calibration
- Verification
- Linkage to Improvement

Opportunities to Better Manage Risk



A new benefit for BELA members

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

CREATE Compliance
An ETHISPHERE® Business

Why we offer this benefit to BELA members

- Cybersecurity is critical to companies, boards, investors and customers
- Ethisphere is committed to bringing best practice approaches to BELA members
- A valuable resource for helping BELA members work to advance business integrity
- Aligns with our efforts to help build measurement and improvement into programs

CREATe Leading Practices for Cybersecurity

Aligns with the NIST Cybersecurity Framework

1 Robust Assessment

Online Q&A:

Measures maturity of systems against the NIST Framework's 98 sub-categories of controls

Rates maturity on a scale from 1 to 5

2 Independent Verification

CREATe expert evaluation:

Review program

Check documents

Generate a verified score

3 Improvement Plan

Based on rating:

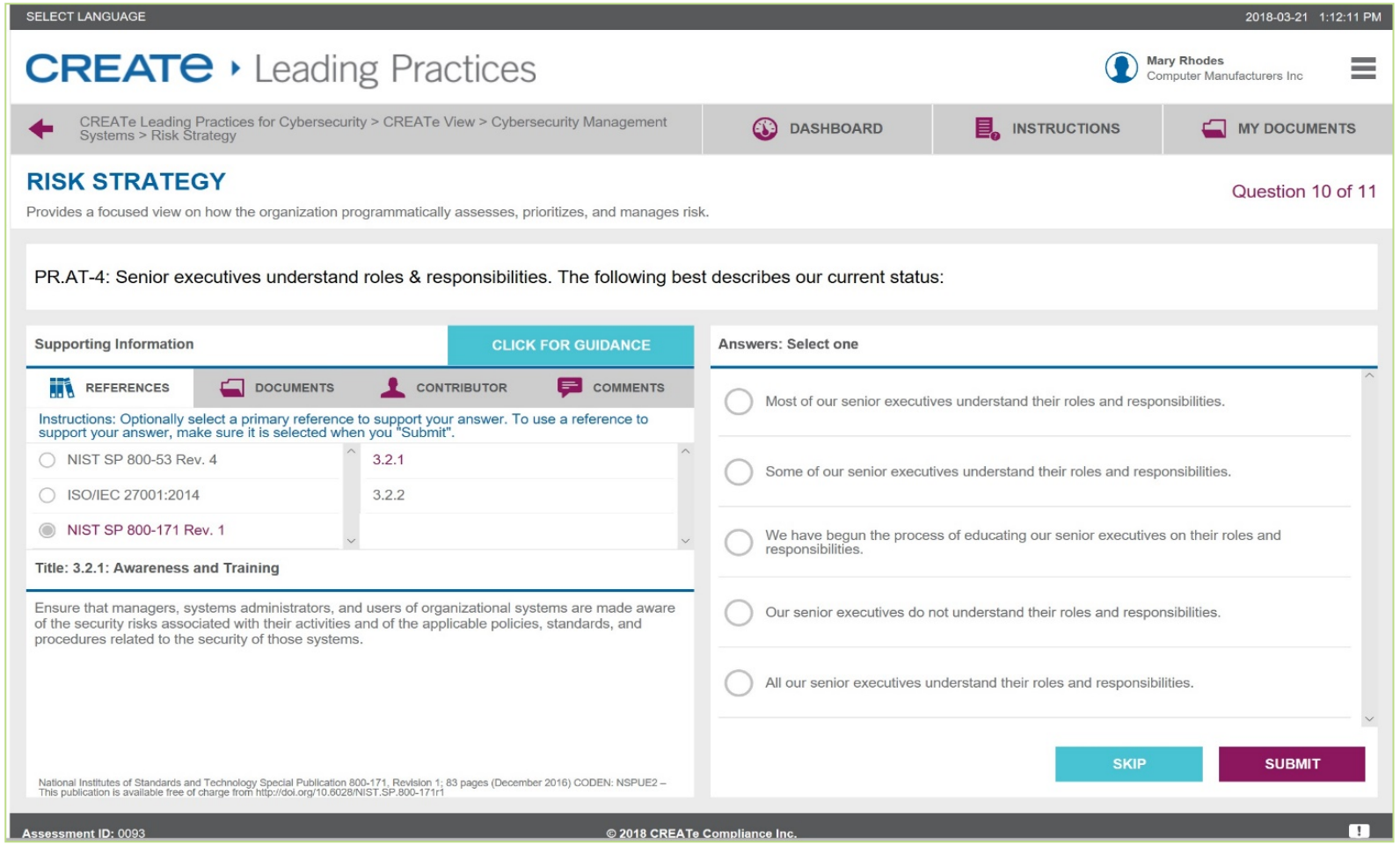
Improvement steps to move to next level

Benchmarking report

CREATe Platform

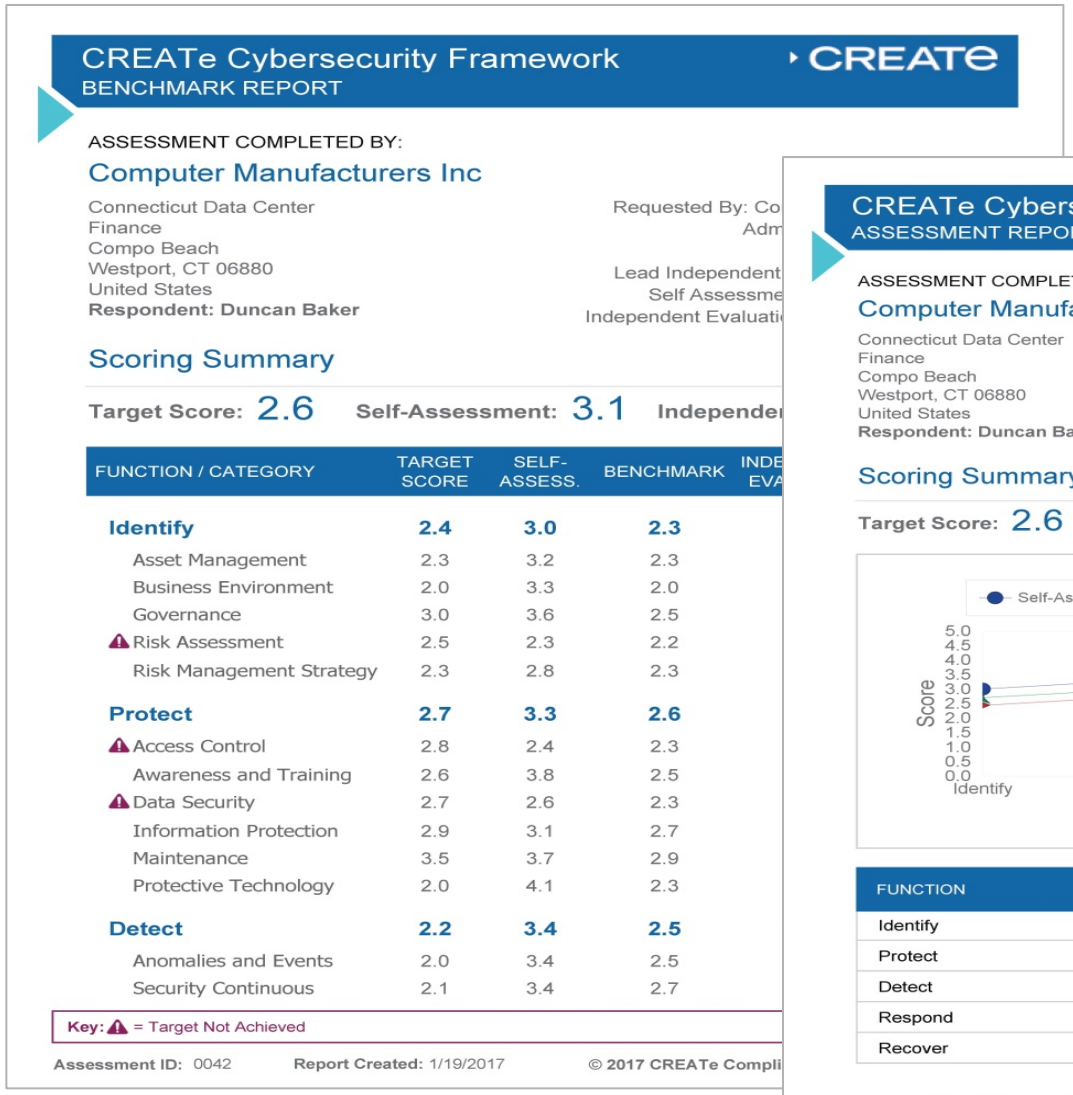
Unique Assessment

- **Based on 98 outcomes/ controls** of the NIST Cybersecurity Framework
- **Five-level maturity matrix** enables calibration and identification of gaps
- **Answer sets and guidance** ensures consistent context for benchmarking



Report Options for Different Audiences

- **Ability to pull data and develop reports** to share maturity of programs to diverse audiences
- **Different views of data** based on requirements



CREATe Cybersecurity Framework
BENCHMARK REPORT

ASSESSMENT COMPLETED BY:
Computer Manufacturers Inc

Connecticut Data Center
Finance
Compo Beach
Westport, CT 06880
United States
Respondent: Duncan Baker

Requested By: Co
Adm
Lead Independent
Self Assessme
Independent Evaluati

Scoring Summary

Target Score: 2.6 **Self-Assessment:** 3.1 **Independe**

FUNCTION / CATEGORY	TARGET SCORE	SELF-ASSESS.	BENCHMARK	INDE EVA
Identify	**2.4**	**3.0**	**2.3**	
Asset Management	2.3	3.2	2.3	
Business Environment	2.0	3.3	2.0	
Governance	3.0	3.6	2.5	
⚠ Risk Assessment	2.5	2.3	2.2	
Risk Management Strategy	2.3	2.8	2.3	
Protect	**2.7**	**3.3**	**2.6**	
⚠ Access Control	2.8	2.4	2.3	
Awareness and Training	2.6	3.8	2.5	
⚠ Data Security	2.7	2.6	2.3	
Information Protection	2.9	3.1	2.7	
Maintenance	3.5	3.7	2.9	
Protective Technology	2.0	4.1	2.3	
Detect	**2.2**	**3.4**	**2.5**	
Anomalies and Events	2.0	3.4	2.5	
Security Continuous	2.1	3.4	2.7	

Key: ⚠ = Target Not Achieved

Assessment ID: 0042 **Report Created:** 1/19/2017 © 2017 CREATe Compli

CREATe Cybersecurity Framework
ASSESSMENT REPORT

ASSESSMENT COMPLETED BY:
Computer Manufacturers Inc

Connecticut Data Center
Finance
Compo Beach
Westport, CT 06880
United States
Respondent: Duncan Baker

Requested By: Computer Manufacturers Inc
Administrator: Andrew Garber
Internal Code: CM
Lead Independent Evaluator: Duncan Baker
Self Assessment Completion: 1/19/2017
Independent Evaluation Completion: 1/19/2017

Scoring Summary

Target Score: 2.6 **Self-Assessment:** 3.1 **Independent Evaluation:** 2.7

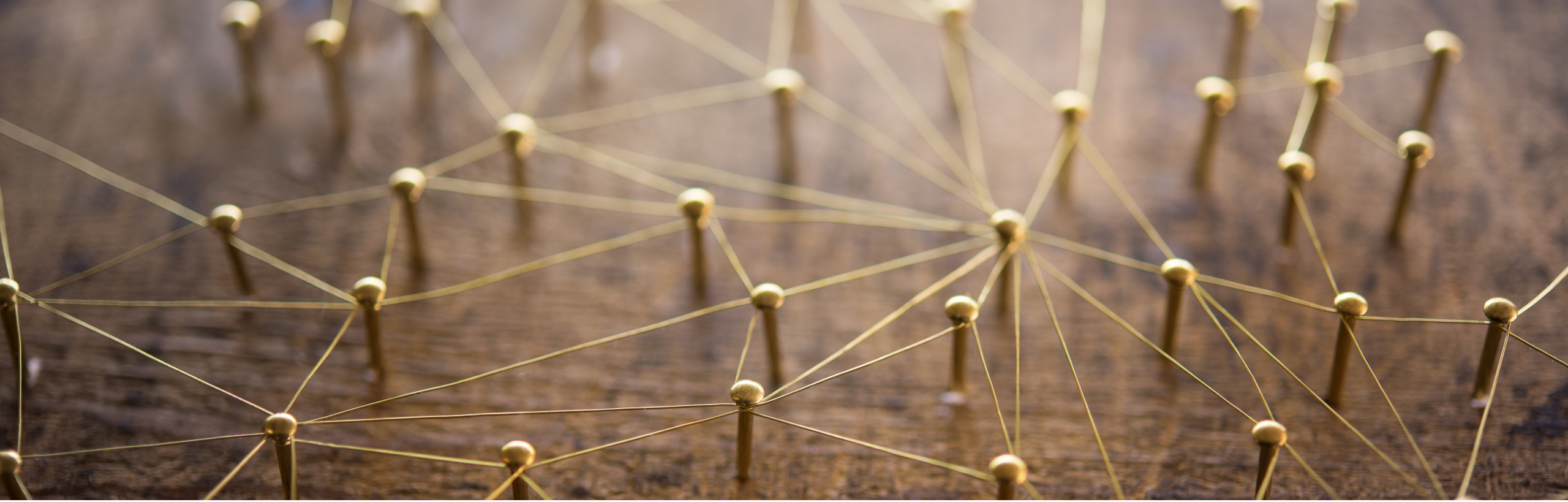
FUNCTION	SELF-ASSESSMENT	INDEPENDENT EVALUATION	TARGET SCORE
Identify	3.0	2.7	2.4
Protect	3.3	3.0	2.7
Detect	3.4	2.9	2.2
Respond	2.9	2.3	3.0
Recover	2.9	2.6	2.8

Assessment ID: 0042 **Report Created:** 1/19/2017 © 2017 CREATe Compliance Inc. All rights reserved.

Questions and Discussion

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

CREATE Compliance
An ETHISPHERE® Business



Thank You

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

Contact Us

Erica Salmon Byrne
erica.salmonbyrne@ethisphere.com

Pamela Passman
pamela.passman@ethisphere.com