

The presentation will begin shortly.

Thank you for  
joining us!



CPAs & ADVISORS



# Presenters

*Meet the instructors*



**Ricardo Trujillo**



**Mac Lillard**



**Darren Hulem**



**Melissa Musser**



**Ronald McLean**



**Derek Symer**



**Jodi Daniels**



**Orion Reynolds**



# Housekeeping

*Additional Information*

<b>Learning Objective</b> To provide attendees with strategies to improve cyber and operational IT functions.	<b>Instructional Delivery Methods</b> Group Internet-based
<b>Recommended CPE</b> 3 CPE Credits	<b>Recommended Fields of Study</b> Specialized Knowledge
<b>Prerequisites</b> None required	<b>Advance Preparation</b> None
<b>Program Level</b> Basic	<b>Course Registration Requirements</b> None
<b>Complaint Resolution Policy</b> GRF CPAs & Advisors is committed to our participants' 100% satisfaction and will make every reasonable effort to resolve complaints as quickly as possible. Please contact <a href="mailto:nmcelveen@grfcpa.com">nmcelveen@grfcpa.com</a> with any concerns.	
<b>Disclaimer</b> This webinar is not intended as, and should not be taken as, financial, tax, accounting, legal, consulting or any other type of advice. Readers and users of this webinar information are advised not to act upon this information without seeking the service of a professional accountant.	



# GRF CPAs & Advisors



Personal  
Service With  
Powerful  
Solutions

**Audit & Advisory Firm Headquartered in Washington, DC Metro Region,  
servicing clients across the Globe.**





# GRF Solutions

---



**AUDIT & ASSURANCE**



**OUTSOURCED  
ACCOUNTING**



**RISK & ADVISORY**



**TAX**



# Topics for Today

---

- Welcome
- Data Privacy: A Scalable Approach to Integrating Strategy and Compliance
- Navigating the Modern Risk Landscape: Best Practices in Cybersecurity, IT General Controls, and Third-Party Risk Management
- Integrating NIST CSF 2.0 into Enterprise Risk Management: A Unified Approach to Cybersecurity and Risk Management
- Fireside Chat – The Role of Internal and External Audits in Enhancing Cyber and Operational IT Risk Resilience
- Closing Remarks



# Data Privacy: A Scalable Approach to Integrating Strategy and Compliance



Jodi Daniels





A glowing green padlock is centered on a dark blue background with a complex circuit board pattern. The padlock has a bright green, pixelated or particle-like texture. The circuit board lines are thin and light blue, with some points of light. The overall image has a high-tech, digital feel.

# Navigating the Modern Risk Landscape: Best Practices in Cybersecurity, IT General Controls, and Third-Party Risk Management



**Derek Symer**  
*Partner, The Baldwin Group*

**Ricardo Trujillo**  
*CPA, CISA, CITP*  
*Partner, Audit*

**Darren Hulem**  
*CISA, CEH, Security +*  
*Manager*

# Presenters

*Meet the Instructors*



**Derek Symer**

*Partner, The Baldwin Group*



**Darren Hulem**

**CEH, CISA, Security +**

*Manager, RAS*



**Ricardo Trujillo**

**CPA, CITP, CISA**

*Partner, Audit*





# Agenda

Current Landscape

Insurance Considerations

IT General Controls

Navigating Third Party Risk Management

Key Takeaways

Q&A



# Current Landscape

11



# Current Landscape



Each year more goes from physical to digital



Enhanced Reputation Risk



Losing sight of the basics

## Cybersecurity, Information Security and Data Privacy

- How is your organization protecting the network/systems/data?

## Business Continuity and Disaster Recovery Planning

- Minimize the negative effects of unforeseen risk events (i.e. cyber breach, fire, pandemic)
- Disaster recovery planning is a component of business continuity planning that focuses on the restoration of systems to minimize downtime

## Third-Party Risk Management

- What liability is posed to your organization through third parties?
- Is your process for vetting, monitoring, and evaluation vendors adequate based on the level of risk associated with the relationship?



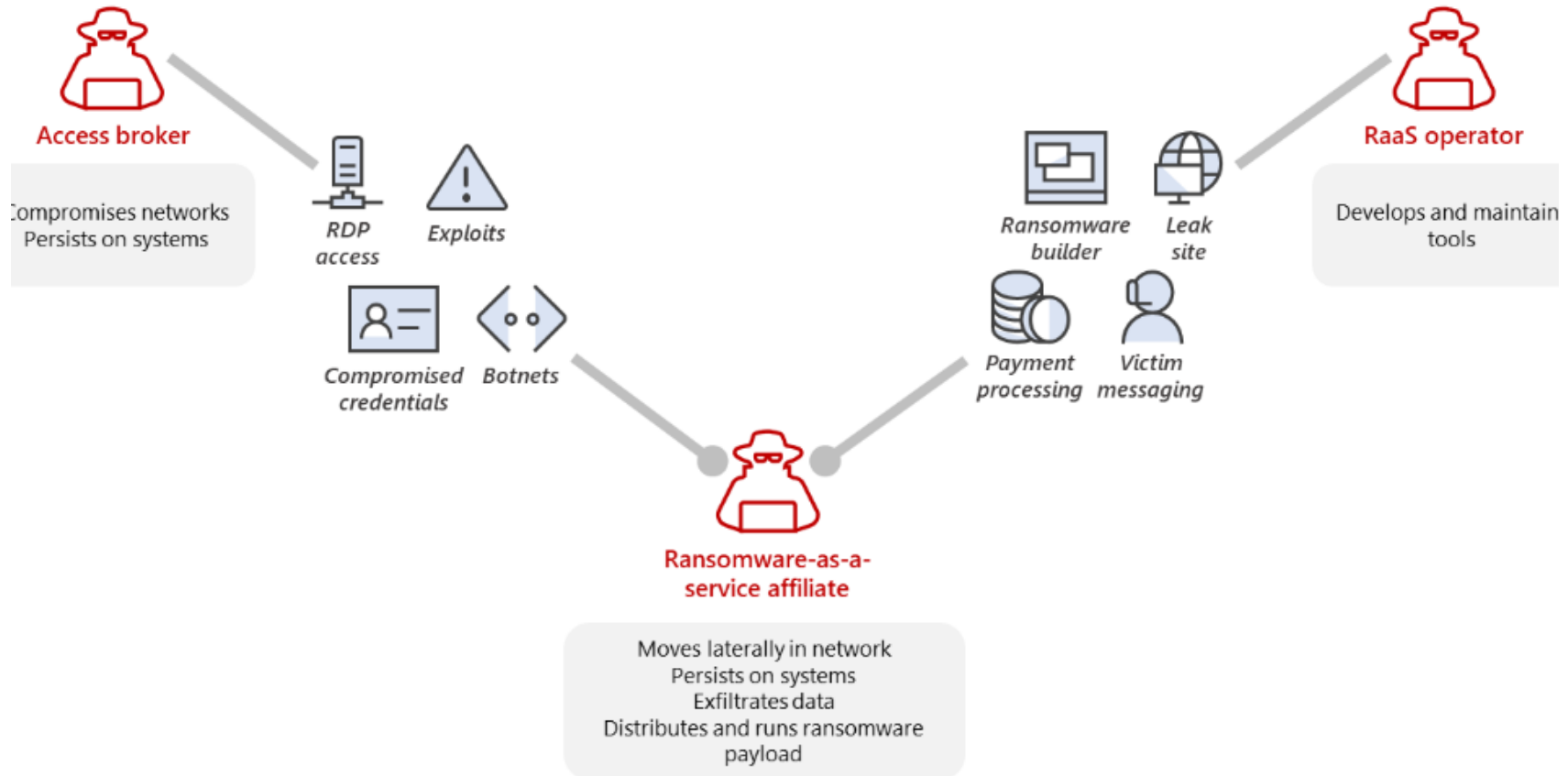
# Common Threats and Attacks

- Malware- code created to do harm to a computer, network, or server. (Rootkit, Keylogger, etc)
- Ransomware- malware designed to deny access until a ransom is paid
- Phishing- uses email, voice, social engineering, etc to gain sensitive information
  - Vishing, smishing, whaling, spear phishing
- Password Attack- attempt to gain unauthorized access to a system by trying various passwords
  - Dictionary- common words and phrases
  - Brute force- high number of combinations in short amount of time
  - Credential stuffing- attempts old password from prior data leaks hoping they have not been changed
  - Password Spraying – Attempting common passwords against multiple accounts



# Increase in Cyber Events

## Ransomware-as-a-Service



Source: Microsoft





# Polling Question

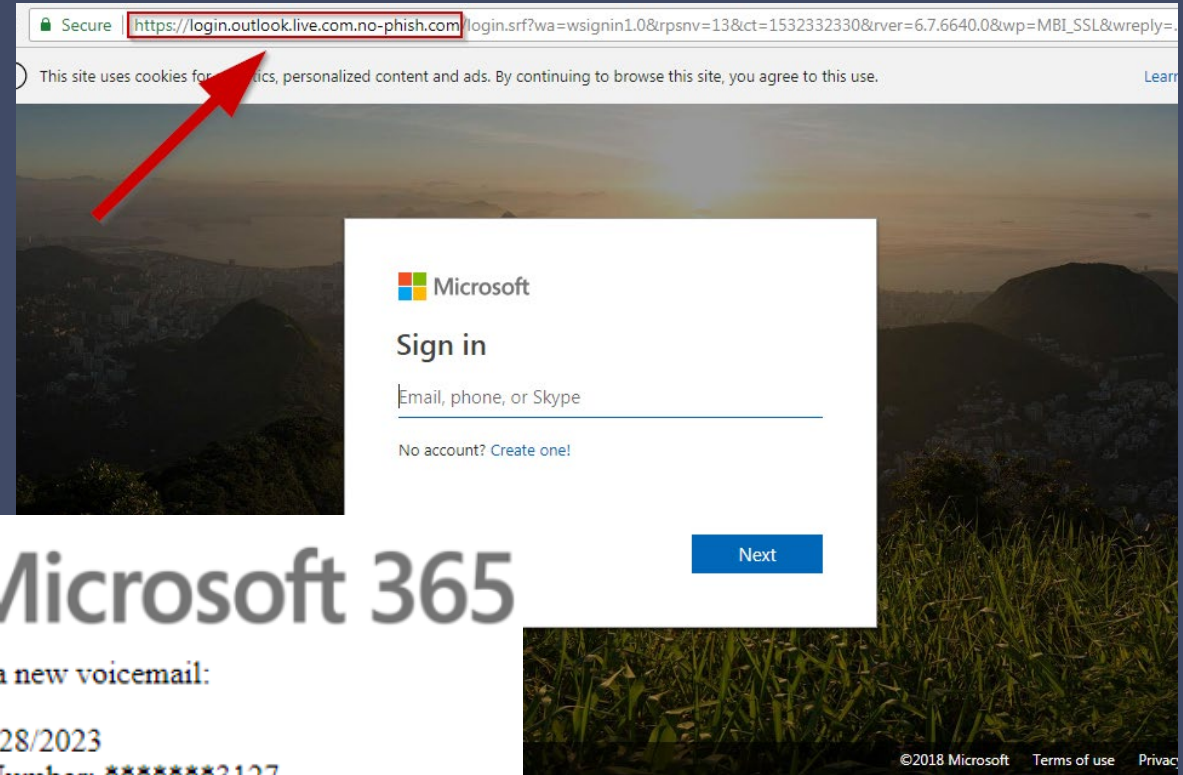
I feel my online accounts are sufficiently protected with just traditional MFA, such as Microsoft/Google Authenticator, Duo, RSA, etc...

*A. Yes*

*B. No*



# Example of Social Engineering



Evilginx  
no nginx - pure evil  
by Kuba Gretzky (@mrgretzky) version 2.3.1

```
[19:12:08] [inf] loading phishlets from: /usr/share/evilginx/phishlets/
[19:12:08] [inf] redirect parameter set to: hb
[19:12:08] [inf] verification parameter set to: zw
[19:12:08] [inf] verification token set to: 20cd
[19:12:08] [inf] unauthorized request redirection URL set to: https://www.youtube.com/watch?v=dQw4w9W
[19:12:09] [war] server domain not set! type: config domain <domain>
[19:12:09] [war] server ip not set! type: config ip <ip_address>
```

phishlet	author	active	status	hostname
github	@audibleblink	disabled	available	
instagram	@prrrrinnee	disabled	available	
linkedin	@mrgretzky	disabled	available	
okta	@mikesiegel	disabled	available	
outlook	@mrgretzky	disabled	available	
reddit	@customsync	disabled	available	
twitter	@white_fi	disabled	available	
amazon	@customsync	disabled	available	
citrix	@424f424f	disabled	available	
facebook	@mrgretzky	disabled	available	
o365	@jamescullum	disabled	available	
protonmail	@jamescullum	disabled	available	
twitter-mobile	@white_fi	disabled	available	

You received a new voicemail:

- Date: 8/28/2023
- Caller Number: \*\*\*\*\*3127
- Voicemail Length: 00:43 Secs

Click [here to login](#) and access your message.

Thank you,  
Microsoft 365  
Download expires in 24 hours.

# What Could Happen



```
[14:55:58] [imp] [0] [o365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.114 Safari/537.36 Edg/103.0.1264.49 (86.82.180.135)
[14:55:58] [inf] [0] [o365] landing URL: https://login.microsoftonline.com/tHk0kMjT
[14:56:19] [+++] [0] Password: [-3mLhA-qzcPcUwwq62KAXMDXPyEf28q2vFe.ogRm]
[14:56:19] [+++] [0] Username: [irvins@m365x341716.onmicrosoft.com]
[14:56:19] [+++] [0] Username: [irvins@m365x341716.onmicrosoft.com]
[14:56:24] [+++] [0] Username: [irvins@m365x341716.onmicrosoft.com]
[14:56:27] [+++] [0] all authorization tokens intercepted!
[14:56:27] [imp] [0] redirecting to URL: https://portal.office.com (1)
: sessions
```

id	phishlet	username	password	tokens	remote ip	time
7	o365	irvins@m365.....	-3mLhA-qzcP.....	captured	86.82.180.135	2022-07-21 14:56

: sessions 7


```
id : 7
phishlet : o365
username : irvins@m365x341716.onmicrosoft.com
password : -3mLhA-qzcPcUwwq62KAXMDXPyEf28q2vFe.ogRm
tokens : captured
landing url : https://login.microsoftonline.com/tHk0kMjT
user-agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.114 Safari/537.36 Edg/103.0.1264.49
remote ip : 86.82.180.135
create time : 2022-07-21 14:55
update time : 2022-07-21 14:56
```

```
[{"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1689951394, "value": "0.AU4A22TlBx0IWUike5T6K2izp1tEZUfGMrBjg-Ydk3ZSdspOAC0.AgABAAQAAAD--DLA3V07QrddgJg7WevrAgDs_wQA9P9TJwR0XAQu8gRimpXm5TJiTe0NERUKdTNZE1S0j4UuyOrNg0BhKHRZz_xqjCe7KnkC_XyPm8Q5_nJjTK3sXkEbmZf7-67qvgHxwH2F9IKrtKfXLP6-bQ8HNELRLXZat_jf8DeMI6ch8hcsFVEPVtZ9h9lskq0IjZ614mHjmqvQ1r8Galu0C7yLqHSOKL7MQURqzwoVdM1WU90EcYm02IKM7A-f3cu6nUwv0AMKwZxNDZ-ErdaTo2gyr6iNit_VQX65zhe210JKDfTrvs5s0QG094EUHbFJBfHuxKooeYcWesT9Pt0zY6_Qk2V-gogUCIdGybnDQY5GmGcF6jh113w1pQsz2qMYN5k1vxRRh3vH3j4Q1BwZwn51_J6gzjB-Y4Dby33D30zfd1BRipVHS7uB6ZnYDbAp3d8AmS1PGW0pCg25r9fQ5kEbVHSfjV0hdlerS58VFTDB5_2Mxw48vFRIFjP02FEDLVWCUzDk2v5_TQeRgQXqP9YfZxNg2JcX84E3Hxc_PNXtMwz4PTp9Y211Mq95tvHE8S28Ltk5UKXJHeWwdtbD4k-bnqtgen_A901payq4D4wkSL-P", "name": "ESTSAUTHPERSISTENT", "httpOnly": true}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1689951394, "value": "CAgABAAIAAAD--DLA3V07QrddgJg7WevrAgDs_wQA9P_EnByi4yHMK_C5y2kcACCNEVWanHld-FUAWfDNYyN5zuVn8pdQ8qkIcjcncK9vPQhacD0bnpLczszGhnk4o6V3DSgP8v3PDxbLnJwTkuQ16lg0v0A-GzEBD-iHRY8V7rL_GaFbP6ChPmg5T4RPi1njsqD7N3tNULNGkhtXdd5NDc6V5J76z0810jgNq_nMGZF0xooFD8H31D_qwK5GgLXxoTfToNrjMS0rSlneJXs1_FeTrn1CASSV97nDx-GB5eU-54Q", "name": "SignInStateCookie", "httpOnly": true}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1689951394, "value": "0.AU4A22TlBx0IWUike5T6K2izp1tEZUfGMrBjg-Ydk3ZSdspOAC0.AgABAAQAAAD--DLA3V07QrddgJg7WevrAgDs_wQA9P8NHat0zr8eoH4wc7StgB3hQA2lcD_ab6BIfatFR9FKL0442zIzQV3YmK1G4A_wen0a48bch4YhKq", "name": "ESTSAUTH", "httpOnly": true}]
```

# Account Accessed



id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect\_uri=https%3A%2F%2Fwww.office.com%2Flandingv2&response\_type=



## Sign in

Email, phone, or Skype

No account? [Create one!](#)

Can't access your account?

Next

Sign-in options

### Cookie-Editor - Import

Supported format: JSON, Header string, Netscape.

```
JSON:
[{"name": "Cookie", "value": "text", [...]}]

Header String:
Cookie=text;Editor=yes

Netscape:
# Netscape HTTP Cookie File
# [...]
cookie-editor.com[...] Cookie text
```



# Cyber Risk and Insurance Considerations

19





---

# Cyber Risk and Insurance Considerations in 2024

- 2024 Cyber Overview
- Cyber Coverages – The Basics
- Defining Cyber Coverage & Limits
- Quantifying Cyber Risk
- Best Practices



# 2024 Cyber Overview

- Cyber claims increased year-over-year
- Businesses with revenues between \$25 million and \$100 million saw largest spike in claim activity
- Cybercrime including Ransomware / Cyber Extortion Actions
- Ransomware is a \$1 billion global business
- Many claims associated with Business email compromise
- Phishing / Social Engineering (Financial and/or Data) Attempts and Successes
- Actual, attempted, and/or suspected intrusion and/or breach of organization's network
- 3<sup>rd</sup> Party Risks including contracted services/managed networks
- Boundary devices put organizations at greatest risk
- Lost/Stolen laptop or mobile device
- Paper record breaches where privileged information is denoted



# Polling Question

Does your organization have cyber insurance?

- A. *Yes*
- B. *No*
- C. *Unsure*



# Cyber Coverages – The Basics

## Third-Party Coverages

- Network Security & Privacy Liability e.g. lawsuits, arbitration/mediation actions, etc.
- Regulatory Defense Expenses & Fines including PCI-DSS Fines & Penalties

## First-Party Coverages

- Computer Forensics & Security Breach Remediation
- Privacy Breach Response Costs e.g. notification, legal, credit monitoring, etc.
- Crisis Management Event Expenses including Public Relations Expenses
- Cyber Extortion / Ransomware
- Cyber Crime (Social Engineering & Telecommunications Fraud)
- Business Interruption & Contingent or Dependent Business Interruption (Revenue Loss Coverage from a Cyber Claim)
- Data Restoration



# Sample Client's Cyber Coverage & Limits

**Policy Limit: \$5,000,000 Aggregate**

Cyber Coverage	Limit	Retention
Privacy & Network Security Liability	\$5,000,000	\$250,000
Payment Card Industry – Data Security Standards (PCI-DSS) Fines	\$1,000,000	\$250,000
Regulatory Proceeding	\$1,000,000	\$250,000
Cyber Incident Response Fund	\$5,000,000	\$250,000
Non-panel Incident Response	\$2,500,000	\$250,000
Public Relations Expense	Included	\$250,000
Forensic and Legal Expense Services	Included	\$250,000
Extortion Loss	\$5,000,000	\$250,000
Ransomware Loss	\$5,000,000	\$250,000
Digital Data Recovery	\$5,000,000	\$250,000
Business Interruption – System Disruption	\$5,000,000	24 Hour Waiting Period





# How Do We Quantify Cyber Risk?

---

- # Records Stored (PII, PHI)
- Cost Per Record
- Contractual Risk Transfer
- Outsourcing Risk via Third Party Providers
- Risk Left Over After Insurance and Self-Retention
- Measuring and Example of Residual Risk



# Cyber Event – Best Practices

1

## **Report under the Cyber policy & Trigger Internal Crisis Management Team Procedures**

Reporting should occur regardless of whether you think it will fall under the policy deductible.

2

## **Crisis Management Group Activation**

Control knowledge access of the event and trigger protocols based on internal Crisis Management team and advice from Cyber Breach Response Team

3

## **Attorney/Client Privilege**

Reporting to carrier will trigger legal representation first and allow counsel to consult in a legally privileged manner in conjunction with the outsourced breach investigator

4

## **Consider Current Environment and Backups to be “At Risk” and Exposed**

Work to verify overall scope of compromise and which systems/areas remain “safe”.



# Cyber Event – Best Practices

5

## Internal Communication – Determine Safest Method Given Scope of Compromise

Based on scope of the breach, should non-corporate phone and email correspondence be considered? Is phone VOIP safe?

6

## Don't Negotiate or Engage before Specialists are Engaged for Ransomware

Triggering the policy will allow for the utilization of advice and guidance from team of cyber breach experts to delineate best response & approach to extortionists.

7

## Reporting to Authorities

Work with insurer's Cyber Breach Team on required reporting to appropriate authorities e.g. FBI, regulatory bodies, etc.

8

## After Action Review

What are the lessons learned and what steps can be taken to prevent similar events in the future?



# IT General Controls

28



# IT General Controls (ITGCs)

IT General Controls ensure the integrity, reliability, and security of IT systems and data, serving as the foundation for effective IT governance and compliance. **They provide the basis for establishing robust IT policies and procedures within your organization.**

## Key Point:

**Your IT policies and procedures cannot be fully outsourced to a Third-Party Managed Service Provider. For example, your organization must define an internal information security policy to govern access to critical systems, such as accounting or payroll platforms.**





# IT General Controls (ITGCs)



## Access Controls

Manage user access to systems and data (e.g., authentication, authorization, role-based access).



## Change Management

Ensure proper authorization, testing, and documentation for system changes (e.g., software updates, patches).



## IT Operations

Monitor and maintain IT infrastructure for performance, availability, and backups.



## Data Integrity

Safeguard against data corruption through secure storage and regular validation.



## Disaster Recovery and Incident Response

Data backup, recovery controls and procedures help organizations minimize disruption operations.



# Polling Question

Does your organization have a formal information security / IT policy and procedures?

- A. *Yes*
- B. *No*
- C. *Unsure*



# Potential Management Letter Comments

- **Information Security Policies**
  - Lack of policies and procedures documenting Information Technology General Controls (ITGCs)
- **Segregation of Duties**
  - One individual has System Administrator access to multiple platforms and/or is the sole System Administrator for a platform
- **Review of System Administrator Activity**
  - No procedures in place to monitor activity of System Administrators
- **Access Management**
  - Inappropriate assignment and/or monitoring of user access rights
- **Third-Party Risk Management**
  - No process for assessing risk related to third parties, specifically those with access to system, data, PII, financials, etc.
- **Change Management**
  - Lack of policies/procedures around approval and logging of changes to system design, controls, access rights, etc. Particularly important for organization's considering technology projects.
- **Enterprise/Cybersecurity Risk Management**
  - No process for identifying, assessing, managing and monitoring risks on a continuous basis and reporting to the Board. This can be accomplished through formal risk assessments, vulnerability scanning, benchmarks, maturity assessments, etc.



# Scoping IT & Cybersecurity Audits

*Depending on your risk assessment, consider rotating a variety of audit checks. When asking for an audit make sure you understand your risk and the scope you would like to include. Examples as follows:*

User Access and  
Identity  
Management  
Audit

Data Backup and  
Recovery Audit

Change  
Management  
Audit

Incident Response  
Audit

Endpoint and  
Network Security  
Audit

Vendor and Third-  
Party Risk Audit

System and Data  
Integrity Audit

Vulnerability and  
Patch  
Management  
Audit

Penetration  
Testing and  
Vulnerability  
Assessment

IT and  
Cybersecurity  
Governance Audit

Logging and  
Monitoring Audit

Cloud Security  
Audit

SOC 2 Audit



# Navigating Third Party Risk Management

34





# Negative Media Attention

## *Pentagon Staff Hit by Major Data Breach*

### **30,000 civilian and military personnel PII Compromised**

“The department is continuing to gather additional information about the incident, which involves the potential compromise of personally identifiable information (PII) of DoD personnel maintained by a single commercial vendor that provided travel management services to the department,” the statement noted. “This vendor was performing a small percentage of the overall travel management services of DoD.”

<https://www.infosecurity-magazine.com/news/pentagon-staff-hit-by-major-data/>



# Third Party Risk Management (TPRM)

Third-party risk management is now a critical component of any enterprise risk management framework as **Third Parties** are more involved in all aspects of business.



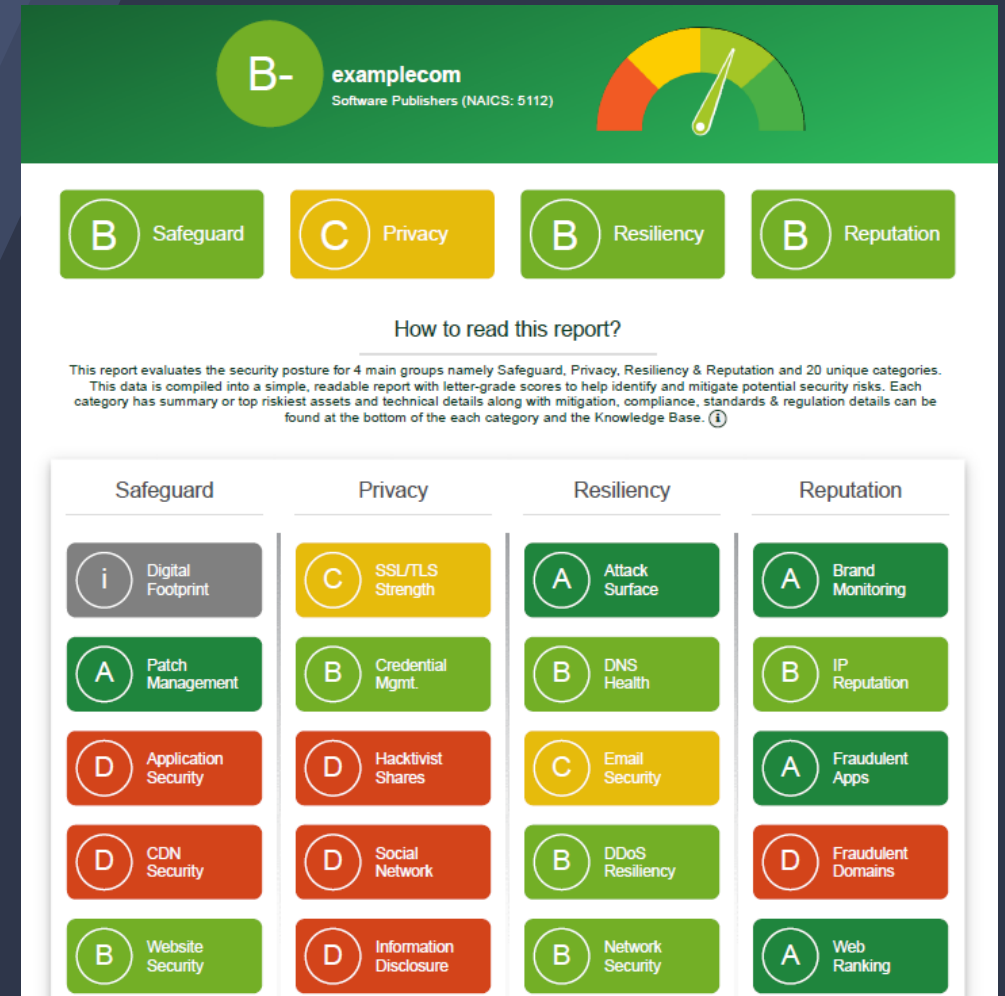
# Polling Question

Does your organization consider third parties when conducting your IT risk Assessments?

- A. *Yes*
- B. *No*
- C. *Unsure*

# Track Your Third Party Risk

Use open source threat intelligence to monitor your own organization and third parties.



# Example Category:

# Patch Management

Service(s)	Total CVSS Score	# of Vuln(s)
php/7.4.1 nginx/1.19.2	81.2	12
windows server 2012 r2	53.6	8
windows server 2016	16.5	3

## Service Version:

windows server 2012 r2  
cpe:2.3:o:microsoft:windows\_server:2012:r2:\*:\*:\*:\*

CVE-2022-26904

7.0

## Description:

Windows User Profile Service Elevation of Privilege Vulnerability. [More about CVE-2022-26904](#)

## References:

<https://nvd.nist.gov/vuln/detail/CVE-2022-26904>  
<https://capec.mitre.org/data/definitions/26.html>  
<https://capec.mitre.org/data/definitions/29.html>



Verified  Has App

Show 15

Date	D	A	V	Title
2022-04-26	↓		×	GitLab 14.9 - Stored Cross-Site Scripting (XSS)
2022-04-26	↓		×	Gitlab 14.9 - Authentication Bypass
2022-04-19	↓		×	EaseUS Data Recovery - 'ensserver.exe' Unquoted Service Path
2022-04-19	↓		×	PTPublisher v2.3.4 - Unquoted Service Path




















Ecosystem List Company List

Search:

Filter Columns Actions

Company	Ecosystem(s)	Industry	Country	Last Update Date	Grade	Cyber Rating	Financial Impact (FAIR - Annualized)	Compliance Rating	DBI	RSI	
 Example Corp <i>example.com</i> Belarus - IT Asset Identified Russia - IT Asset Identified Ukraine - IT Asset Identified	- My Companies - Eco 3	Other Services (except Public Administration) (NAICS: 81)		One off scan	75 0 percent 100	C	\$811.4K	81%	0.148	0.048	
	- My Companies - Eco 1	Data Processing, Hosting, and Related Services (NAICS: 518)		5 days ago	89 0 percent 100	B+	\$313K	89%	0.53	0.117	
	- My Companies - Eco 1	Data Processing, Hosting, and Related Services (NAICS: 518)		5 days ago	65 0 percent 100	D	\$4.2M	93%	0.949	0.163	
	- My Companies - Eco 2	Software Publishers (NAICS: 5112)		5 days ago	71 0 percent 100	C-	\$2.5M	95%	0.671	0.105	
 Example Corp. <i>examplesite.com</i>	- My Companies - Eco 2	Other Services (except Public Administration) (NAICS: 81)		5 days ago	86 0 percent 100	B	\$25K	87%	0.609	0.155	

Show 10 entries

Previous 1 Next

# Develop Your Third Party Ecosystem

- Identify all third parties within your risk universe.
- View their overall risk to your organization
- Track and manage your third parties.



# Design

## *Third Party Due Diligence*

---



Risk Assessment



Financial projections  
& review



Insurance Review



Legal Review



Vendor Audits and/or  
SOC reports



Background check



# Questions to Ask Third Parties

Are they solvent?

Do they follow any information security standards or frameworks? Are they certified?

Do they outsource any of their services?

Have they experienced an cybersecurity incident?

Are formal information security policies and procedures implemented?

Are employees required to complete security awareness training?

Do they have data recovery capabilities such as offsite backups?

Are there DLP solutions in place to prevent exfiltration of sensitive data?

Are there ongoing vulnerability tests internally and externally facing?

Is there a formal patching policy in place?



# Key Takeaways

43



# Polling Question

Has your organization conducted an IT / Cybersecurity Audit in the past year?

- A. *Yes*
- B. *No*
- C. *Unsure*



# Cybersecurity Best Practices

Employee Awareness and Training

Implement Multi-Factor Authentication (MFA)

Regularly Update and Patch Systems

Adopt Zero Trust Architecture (least privilege)

Encrypt Sensitive Data

Conduct Regular Security Audits

Backup Data Regularly

Monitor and Respond to Threats

Control Access to Resources

Secure Endpoints and Networks

Implement Strong Password Policies

Prepare for Ransomware

Comply with Regulations and Standards

Secure Third-Party Access





# Annual Process



**ASSESS RISK**



**UPDATE  
POLICIES**



**TRAIN  
EMPLOYEES**



**MONITOR**





# Explore GRF Resources



[Cybersecurity and Privacy Risk Services](#)



[GRF Cybersecurity Scorecard & Risk Assessment Demonstration](#)



[Cybersecurity Blog Series](#)



[Subscribe to GRF Newsletters](#)



[Read Our Whitepaper – Elements of Successful Cybersecurity](#)







# Integrating NIST CSF 2.0 into ERM

*A Unified Approach to  
Cybersecurity and Risk  
Management*



CPAs & ADVISORS



# Presenters



Melissa Musser,  
*CPA, CIA, CISA, CITP*

Partner and Director  
Risk & Advisory Services



Darren Hulem,  
*CEH, CISA, Security +*

Manager  
Risk & Advisory Services



**CPAs & ADVISORS**



# Agenda



OVERSIGHT BEST  
PRACTICES AND TOP RISKS



WHY SO MUCH FOCUS ON  
CYBER?



ABOUT NIST  
CYBERSECURITY  
FRAMEWORK (CSF)



Q&A



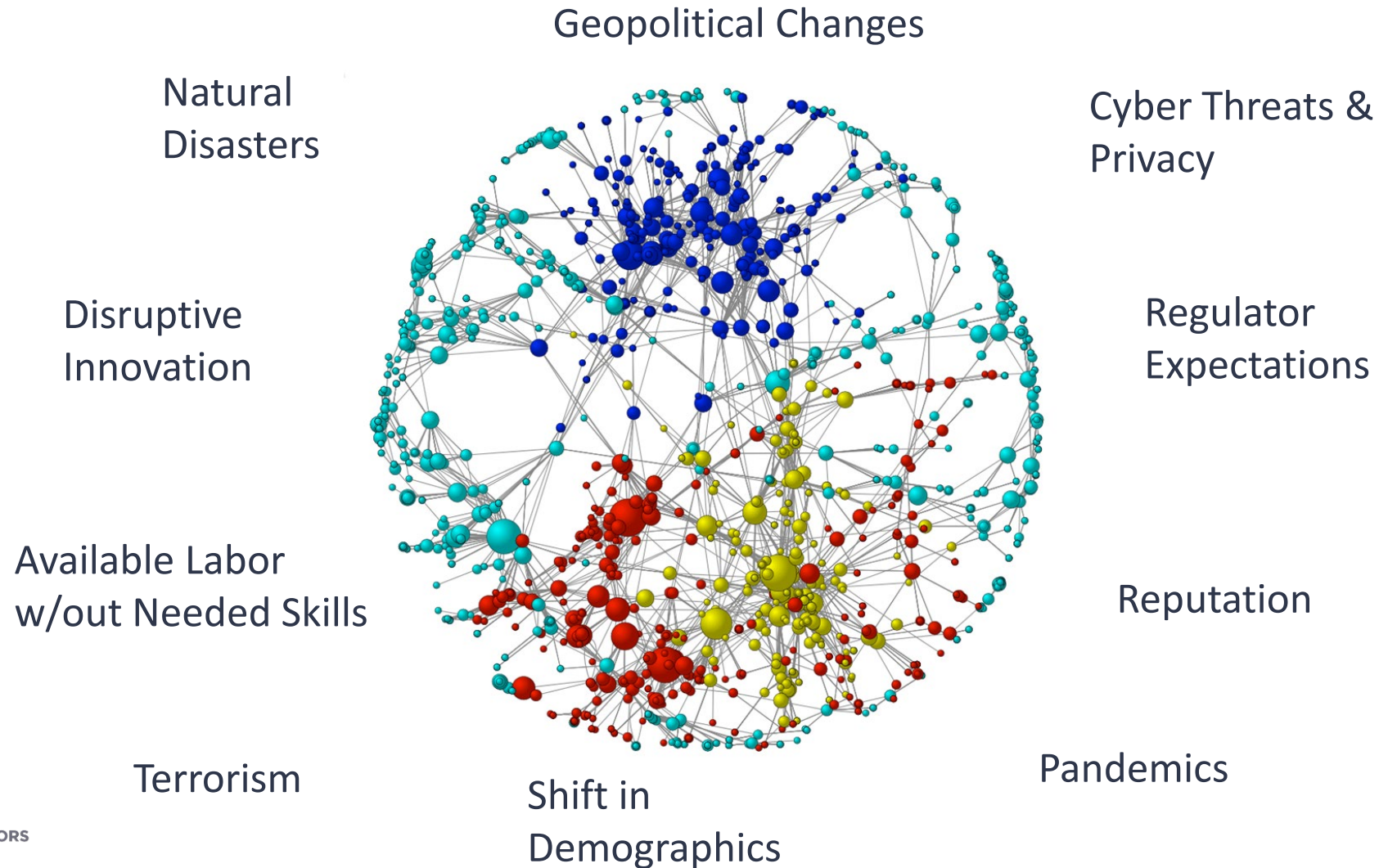
# Oversight Best Practices and Top Risks





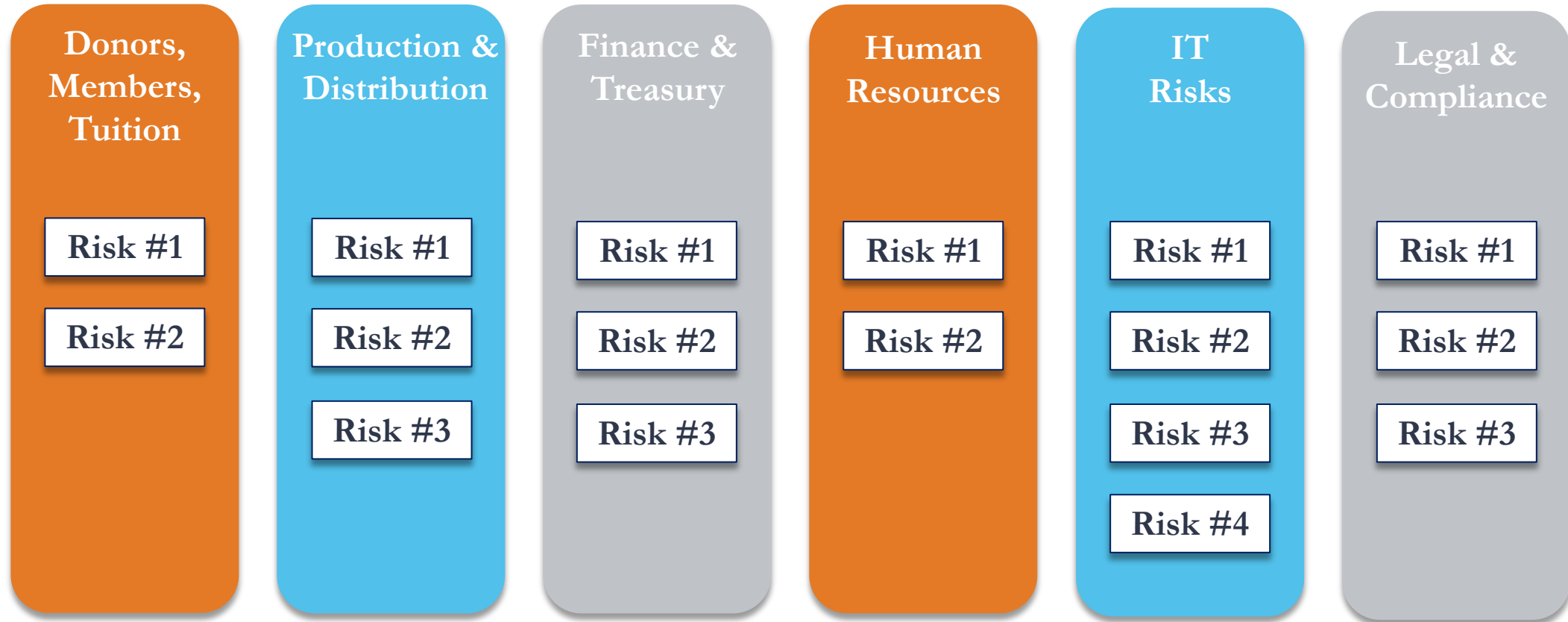
# Understanding the Need for Better Risk Oversight

## *Growing Uncertainty*



# Understanding the Need for Better Risk Oversight

## *Traditional Approach to Risk Management*



## “Silo” or “Stove-Pipe” Risk Management

Source: NC State ERM Initiative



# Differences Between Traditional Risk Management and Enterprise Risk Management (ERM)

## Traditional Risk Management

- **Focus:** Manages risks in silos (e.g., specific departments like IT, finance, or operations).
- **Scope:** Typically addresses operational risks only.
- **Approach:** Reactive, focusing on mitigating risks after they arise.
- **Accountability:** Risk ownership often resides at the departmental level.
- **Alignment:** Rarely integrated into strategic planning or organizational objectives.

## Enterprise Risk Management (ERM)

- **Focus:** Holistic, organization-wide approach to identifying, assessing, and managing risks.
- **Scope:** Covers strategic, operational, financial, compliance, and reputational risks.
- **Approach:** Proactive, emphasizes risk identification and planning to minimize impact.
- **Accountability:** Involves senior leadership, with shared responsibility across all levels.
- **Alignment:** Fully integrated into strategic decision-making and organizational goals.

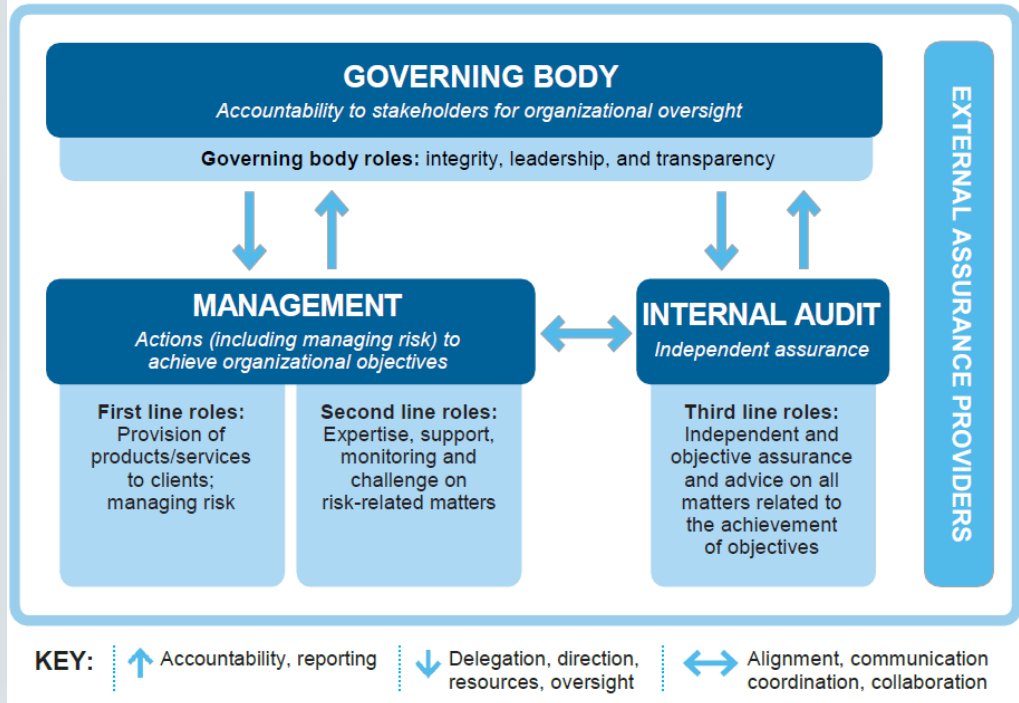


# Understanding the Need for Better Risk Oversight

## Frameworks & Models



### The IIA's Three Lines Model





<https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/risk-in-focus/2025/global-summary-risk-in-focus-2025-hot-topics.pdf>





# Polling Question #1

What do you believe is the most significant risk organizations will face in 2025?

- A. Cybersecurity*
- B. Business Continuity*
- C. Human Capital*
- D. Digital Disruption (Including AI)*
- E. Regulatory Change*
- F. Other*





# GLOBAL – RISK TRENDS

Cybersecurity, business continuity, and human capital continue to hold the top three spots in risk rankings. In the next three years, digital disruption is expected to increase 20 percentage points to rank second. At the same time, climate change is expected to increase 16 percentage points to be ranked fifth. None of the other 14 risk areas are expected to see such dramatic changes in ranking or percentages.

## Global – Top 5 Risk Levels – Trend

**Survey questions:** What are the top 5 risks your organization currently faces?  
What do you think the top 5 risks will be 3 years in the future?

Last Year's Risk		Current Year's Risk		Risk Expectations in 3 Years	
1. Cybersecurity	73%	1. Cybersecurity	73%	1. Cybersecurity	
2. Human capital	51%	2. Business continuity	51%	2. <b>Digital disruption (including AI)</b>	
3. Business continuity	47%	3. Human capital	49%	3. Business continuity	
4. Regulatory change	39%	4. <b>Digital disruption (including AI)</b>	39%	4. Human capital	
5. <b>Digital disruption (including AI)</b>	34%	5. Regulatory change	38%	5. <b>Climate change/environment</b>	
6. Financial liquidity	32%	6. Market changes/competition	32%	6. Regulatory change	
7. Market changes/competition	32%	7. Financial liquidity	31%	7. Geopolitical uncertainty	
8. Geopolitical uncertainty	30%	8. Geopolitical uncertainty	30%	8. Market changes/competition	
9. Governance/corporate reporting	27%	9. Governance/corporate reporting	25%	9. Financial liquidity	
10. Supply chain (including third parties)	26%	10. Organizational culture	24%	10. Supply chain (including third parties)	
11. Organizational culture	26%	11. Fraud	24%	11. Governance/corporate reporting	
12. Fraud	24%	12. Supply chain (including third parties)	23%	12. Fraud	
13. Communications/reputation	21%	13. <b>Climate change/environment</b>	23%	13. Organizational culture	



# Global – Top 5 Risk Levels per Region

Survey question: What are the top 5 risks your organization currently faces?

Risk area	Global Average	Africa	Asia Pacific	Europe	Latin America	Middle East	North America
Cybersecurity	73%	64%	64%	83%	74%	66%	88%
Business continuity	51%	57%	62%	32%	49%	63%	41%
Human capital	49%	44%	57%	52%	47%	43%	54%
Digital disruption (including AI)	39%	34%	36%	40%	37%	38%	48%
Regulatory change	38%	32%	32%	46%	45%	27%	47%
Market changes/competition	32%	15%	49%	32%	26%	29%	41%
Financial liquidity	31%	42%	19%	27%	33%	38%	28%
Geopolitical uncertainty	30%	23%	30%	39%	37%	27%	26%
Governance/corporate reporting	25%	31%	22%	20%	18%	41%	16%
Organizational culture	24%	34%	23%	21%	28%	21%	21%
Fraud	24%	42%	22%	14%	32%	27%	9%
Supply chain (including third parties)	23%	16%	24%	29%	17%	26%	29%
Climate change/environment	23%	25%	26%	33%	29%	12%	12%
Communications/reputation	20%	26%	21%	14%	17%	21%	20%
Health/safety	11%	10%	11%	12%	9%	12%	13%
Mergers/acquisitions	6%	4%	4%	8%	4%	8%	8%



# THE STATE OF RISK OVERSIGHT

AN OVERVIEW OF ENTERPRISE RISK MANAGEMENT PRACTICES  
15TH EDITION | 2024

<https://www.aicpa-cima.com/resources/download/2024-state-of-risk-oversight-report-15th-edition>

**MARK S. BEASLEY**  
Alan T. Dickson Distinguished Professor of Accounting  
Director, ERM Initiative

**BRUCE C. BRANSON**  
Alumni Distinguished Professor of Accounting  
Associate Director, ERM Initiative



## Percentage of Respondents

If Board delegates formal responsibility of risk oversight to a subcommittee, which committee is responsible?	Full Sample	Large Organizations	Public Companies	Financial Services	Not-for-Profit Organizations
Audit Committee	48%	56%	47%	38%	64%
Risk Committee	27%	19%	34%	44%	12%
Executive Committee	10%	11%	9%	7%	5%



## Percentage of Respondents

NUMBER OF TOP RISKS REPORTED TO BOARD	Full Sample	Large Organizations	Public Companies	Financial Services	Not-for-Profit Organizations
Less than 5 risks	42%	13%	11%	37%	32%
Between 5 and 9 risks	26%	26%	27%	32%	31%
Between 10 and 19 risks	24%	49%	51%	20%	26%
20 or more risks	12%	12%	11%	11%	11%





# What is a significant Risk to your Organization?

Viewpoints Differ Re: “Significant Risk”

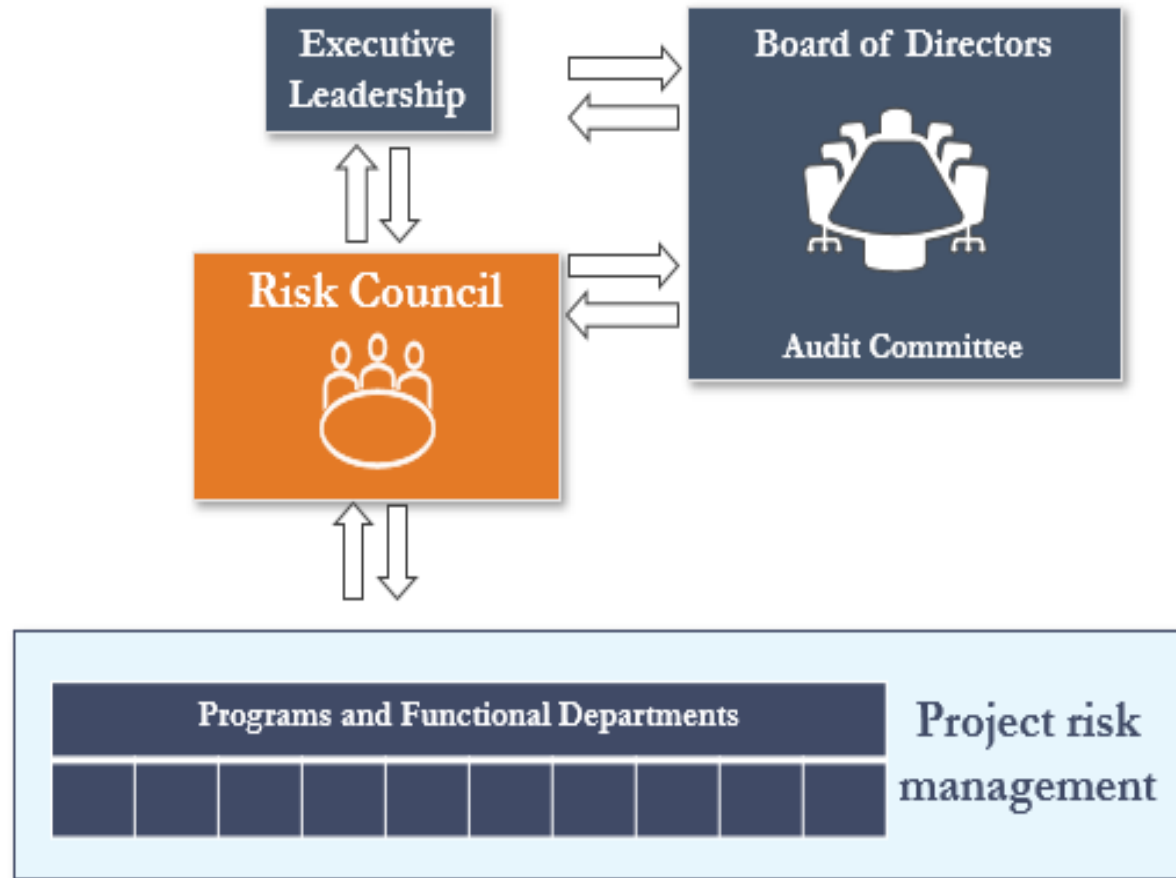
Board member	0
CEOs	13
CFOs	1
CTOs/CIOs	17

WHO IS CORRECT?





# Example Governance Structure



- Alignment with Organizational Objectives
- Board and Senior Management Involvement
- Risk Ownership and Accountability



## Polling Question #2

Does your organization have a formal ERM program?

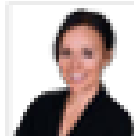
*A. Yes*

*B. No*



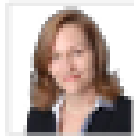


## Enterprise Risk Management (ERM) The Handbook for Association Board Members



*Melissa Musser*

Melissa Musser, CPA, CITP, CISA, Partner



*Susan E. Colladay*

Susan Colladay, CPA, Partner



*Joe Pugh*

Joseph M. Pugh\*, CCEP, CFE, RIMS-CRMP, CRMA, CDPSE, Senior Director, ERM, AARP

<https://www.grfcpa.com/resource/erm-handbook-for-association-board-members/?highlight=ERM>





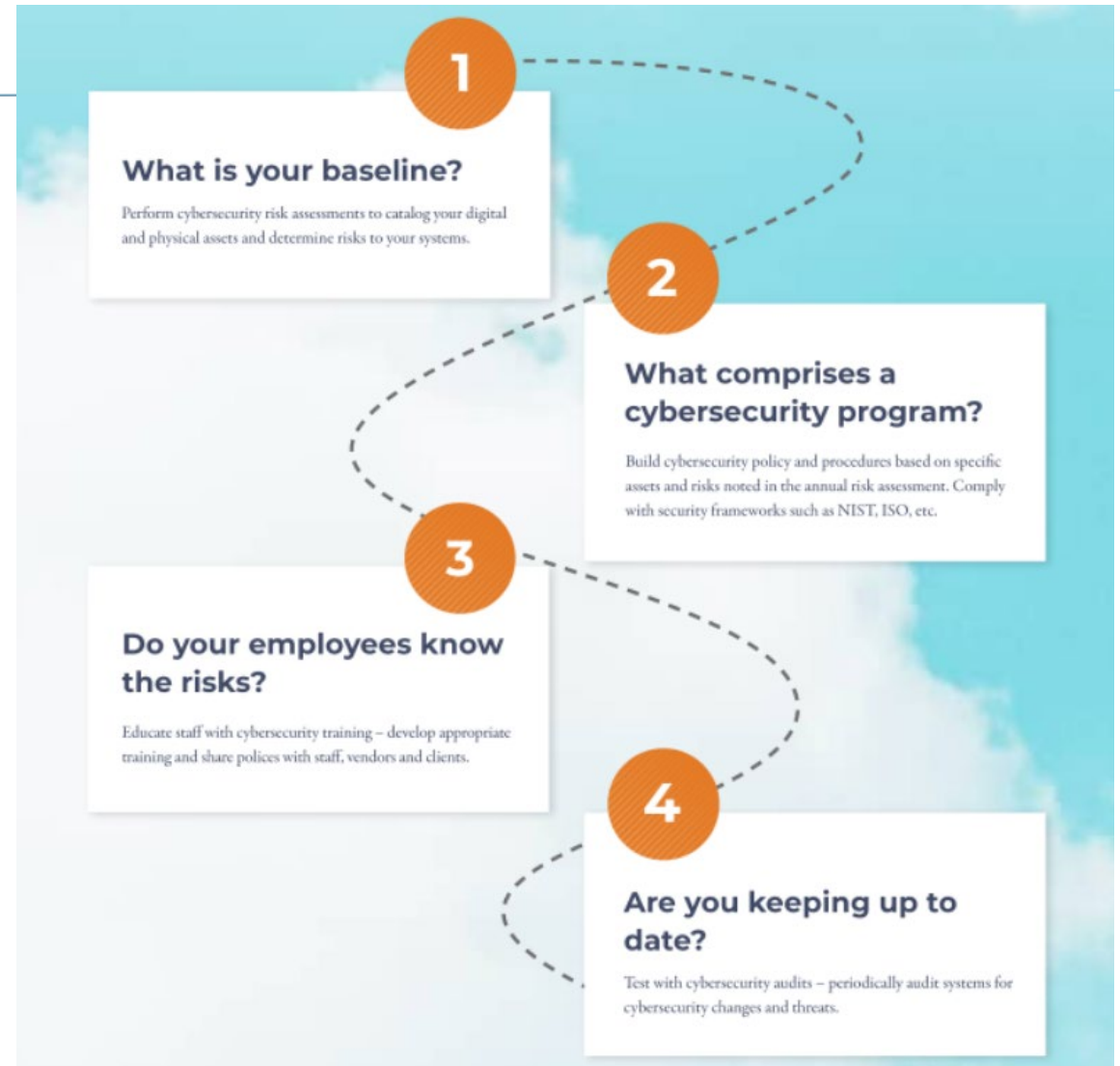
# Why so much focus on Cyber?

---



# Cybersecurity Pathway

- Determine IT Assets: Determine systems, applications, and data that are in your universe
- Identify the threats: Identify potential threats to the IT assets, such as natural disasters, cyber attacks, human error, insider threats.
- Assess the vulnerabilities: Determine the vulnerabilities of the IT assets, such as outdated software, weak passwords, and lack of encryption.
- Determine the likelihood: Assess the likelihood of each threat occurring and the potential impact on the IT assets.
- Evaluate the risks: Evaluate the risks based on the likelihood and impact of each threat and vulnerability.
- Develop risk mitigation strategies: Develop strategies to mitigate or reduce the identified risks, such as implementing security measures, creating data backups, and updating software.





# Uniform Guidance Cybersecurity Changes

## Uniform Guidance Cybersecurity changes

[200.206\(b\)\(2\) Federal awarding agency review of risk posed by applicants](#): Pre-award requirements will include an agencies assessment of cyber security risks for recipients.

[200.303\(e\) Internal Controls](#): Now includes internal controls over cybersecurity

[200.413\(b\) Direct Costs](#): Cybersecurity, if specific to the award, may be a direct cost

Take ***reasonable cybersecurity*** and other measures to safeguard information including protected personally identifiable information (PII) and other types of information. This also includes information the Federal agency or pass-through entity designates as sensitive or other information the recipient or subrecipient considers sensitive and is consistent with applicable Federal, State, local, and tribal laws regarding privacy and responsibility over confidentiality.

GRF Blog Post on UG Cybersecurity Changes:

[Understanding Reasonable Cybersecurity Measures under New Federal Guidelines for Uniform Guidance](#)



# Cybersecurity Maturity Model Certification (CMMC)

- Effective December 16th 2024
- Focuses on CUI and FCI
- CMMC Only applies to DoD Contractors and Subcontractors ( DIB – Defense Industrial Base)
- **Federal contract information** means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.
- **Controlled Unclassified Information** is unclassified information the United States Government creates or possesses that requires safeguarding or dissemination controls limiting its distribution to those with a lawful government purpose. CUI may not be released to the public absent further review.



## Polling Question #3

Can CUI (Controlled Unclassified Information) apply to contracts outside the DoD?

*A. Yes*

*B. No*



# Contract Language

## E. CONTROLLED UNCLASSIFIED INFORMATION (CUI). EXECUTIVE ORDER 13556

**defines** CUI as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The Contractor (and/or any subcontractor) must comply

with *Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR, part 2002)* when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "*handling*" refers to "...any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 81 Fed. Reg. 63323. The requirements below apply only to nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, must be:

- i. **Marked appropriately;**
- ii. Disclosed to authorized personnel on a Need-To-Know basis;
- iii. **Protected in accordance with NIST SP 800-53**, *Security and Privacy Controls for Information Systems and Organizations* applicable baseline if handled by a Contractor system operated on behalf of the agency, **or NIST SP 800-171**, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* if handled by internal Contractor system; and



# CCPA Drafted Regulations

Requiring **annual independent, detailed cybersecurity audits** for businesses whose use and processing of consumer data meets a threshold for presenting a "significant risk" to consumer security.

The auditor is specifically required to report issues regarding the cybersecurity audit **directly to the business's board of directors or governing body, as opposed to reporting issues to business management** with direct responsibility for the business's cybersecurity program





## Polling Question #4

What Cybersecurity Framework does your organization follow?

- A. NIST Cybersecurity Framework (CSF)*
- B. CMMC or NIST 800-171*
- C. ISO 27001*
- D. CIS Critical Security Controls*
- E. Other*
- F. None*



# About NIST Cybersecurity Framework (CSF)

---



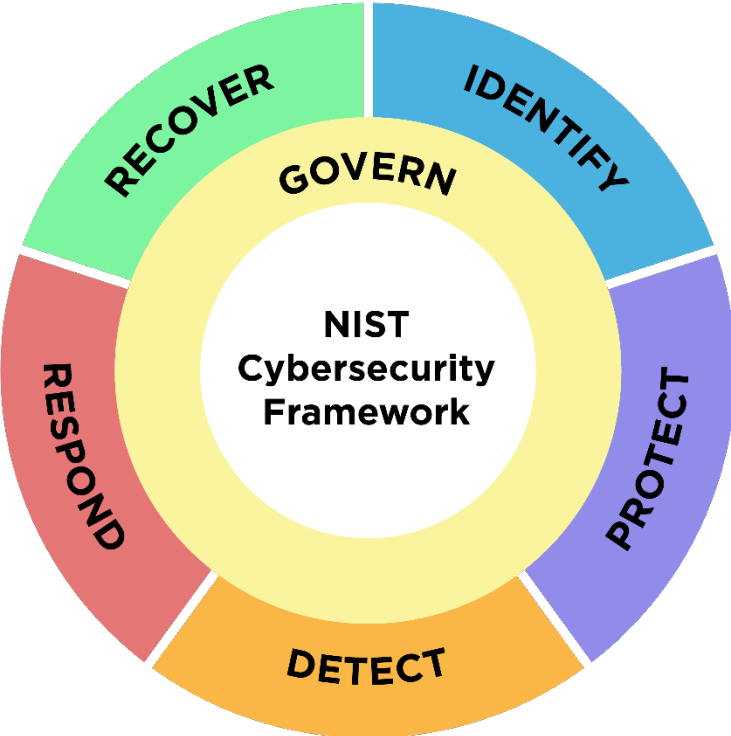


# Cybersecurity Framework (CSF) History

- February 2013 - Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*
- December 2014 - *Cybersecurity Enhancement Act of 2014 (P.L. 113-274)*
- May 2017 - Executive Order 13800: *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- *NIST CSF 2.0 Released February 2024*
- *Originally developed for critical infrastructure organizations*



# What's new in 2.0?



# The Framework's Core Functions 1.1 vs 2.0

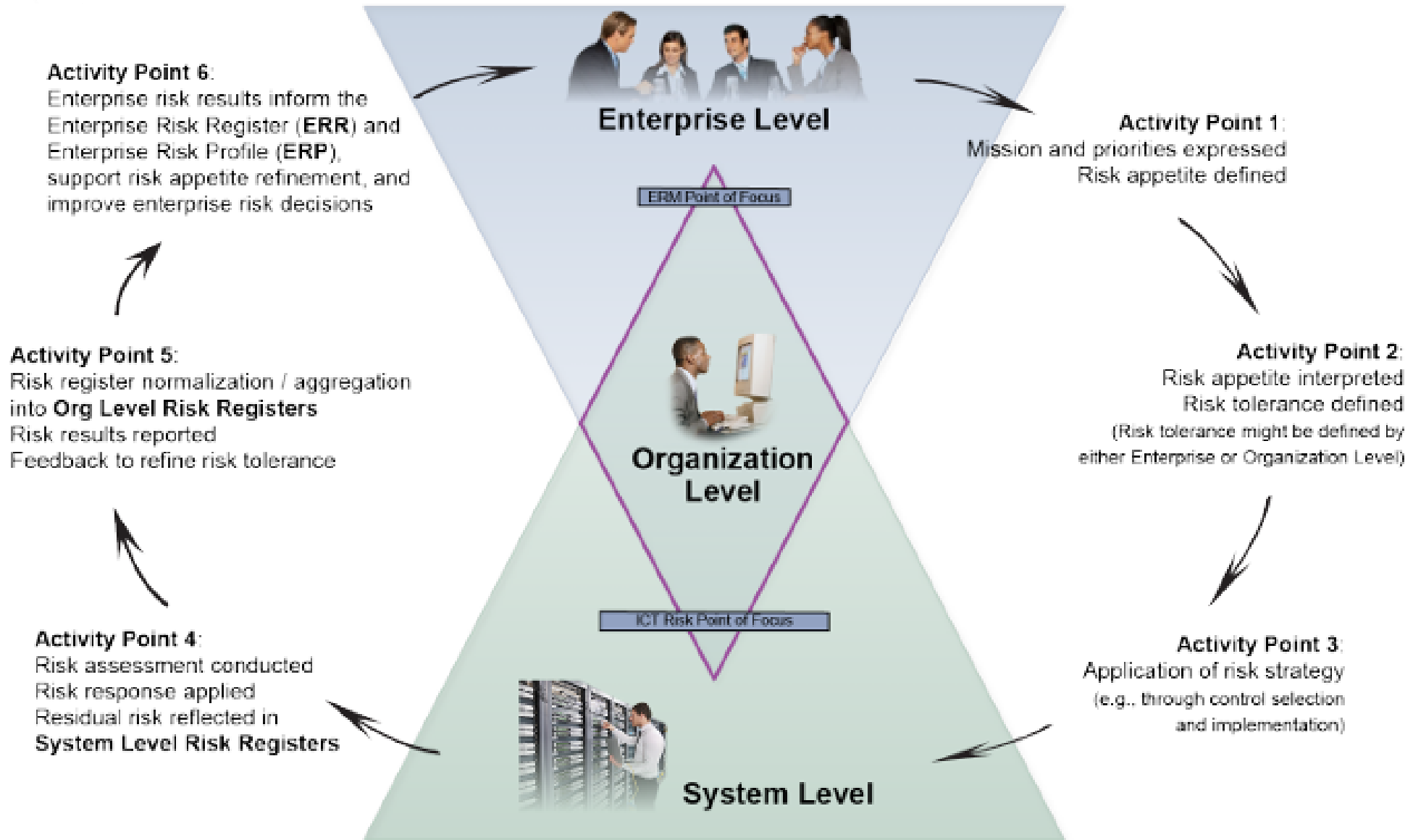
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Function	Category	Category Identifier	
<u>Govern (GV)</u>	Organizational Context	GV.OC	
	Risk Management Strategy	GV.RM	
	Roles, Responsibilities, and Authorities	GV.RR	
	Policy	GV.PO	
	Oversight	GV.OV	
		Cybersecurity Supply Chain Risk Management	GV.SC
<u>Identify (ID)</u>	Asset Management	ID.AM	
	Risk Assessment	ID.RA	
	Improvement	ID.IM	
<u>Protect (PR)</u>	Identity Management, Authentication, and Access Control	PR.AA	
	Awareness and Training	PR.AT	
	Data Security	PR.DS	
	Platform Security	PR.PS	
	Technology Infrastructure Resilience	PR.IR	
<u>Detect (DE)</u>	Continuous Monitoring	DE.CM	
	Adverse Event Analysis	DE.AE	
<u>Respond (RS)</u>	Incident Management	RS.MA	
	Incident Analysis	RS.AN	
	Incident Response Reporting and Communication	RS.CO	
	Incident Mitigation	RS.MI	
<u>Recover (RC)</u>	Incident Recovery Plan Execution	RC.RP	
	Incident Recovery Communication	RC.CO	





# CSF as part of ERM



# NIST CSF Resources

## CSF 2.0 Organizational Profiles

- Guidance for organizations, with considerations for creating and using spreadsheets called *Profiles*, to implement the CSF 2.0.

## Small Business

- Resources specifically tailored to small businesses with modest or no cybersecurity plans currently in place.

## Cybersecurity Supply Chain Risk Management

- Helps organizations become smarter acquirers and suppliers of technology products and services.

## Tiers

- Organizations can use these to apply the CSF 2.0 Tiers to Profiles to characterize the rigor of their cybersecurity risk governance and management outcomes.

## Enterprise Risk Management

- How ERM practitioners can utilize the outcomes provided in the CSF 2.0 to improve organizational cybersecurity risk management.





# Fireside Chat – The Role of Internal and External Audits in Enhancing Cyber and Operational IT Risk Resilience



Mac Lillard



Ronald McLean



Orion Reynolds





# Questions?



## CPAs & ADVISORS



Serving clients across the globe  
301-951-9090 | [www.grfcpa.com](http://www.grfcpa.com)



**Ricardo Trujillo**



**Mac Lillard**



**Darren Hulem**



**Melissa Musser**



**Ronald McLean**



**Derek Symer**



**Jodi Daniels**



**Orion Reynolds**

