Rob Clark, Jr., CIA, CCEP, CBM, CVP
Chief Audit & Compliance Officer
Howard University
robert.clark@howard.edu
https://www.linkedin.com/in/robclarkjr/
www.RobClarkJr.com
770.815.7922

Audits

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

SACUBO
SOUTHERN ASSOCIATION OF COLLEGE AND UNIVERSITY BUSINESS OFFICERS

UK Auxiliary Services

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Objectives of the Session

- Understand what auditors do
- Tips on how to effectively go through an audit
- Provide insights on what YOU can do to mitigate risks in your area
- Emerging issues of risk in higher education
- Using risk assessment tools in your area
- Case studies (in breakout groups)

What's the first thing you think of when you hear the word, "auditors"?

[SLIDO INSERT]
What is your view of auditors?

1) Necessary evil
2) Spawn of Satan
3) A profession mostly for suited for individuals with poor social skills and deep emotional scars
4) A profession in which you actually have an opportunity to make a positive difference and help protect the organization

So, what do you do for a living?

Why is Internal Auditing the Best Job at the University?

- ✓**Broad view of the entire institution**
- ✓**Diverse work**
- ✓**Exposure to all parts of organization**
- ✓**Exposure to new technologies and practices and emerging issues**

Why It's the Best Job…

- **Because we have an opportunity to help the organization and to make a difference**
- **What are your trophies?**

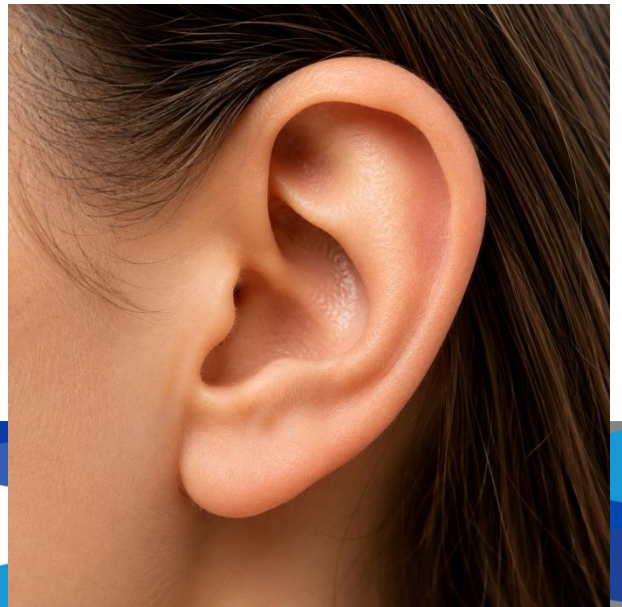
Internal Auditing – Institute of Internal Auditing Definition

- **"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."**

IIA *Standards for the Professional Practice of Internal Auditing*

What auditors tell their friends…

- "As an internal auditor, I do for the officers and management of the university what they would do themselves, if they had the time. I act as senior management's 'eyes' and 'ears' making sure that the university's assets are protected and that we are being good stewards of the resources that have been entrusted to the university."



Reporting Structure

“New Terrain”
Scott Leibs, February 01, 2004
article from CFO Magazine

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

- "Internal audit has always walked a fine line," says Barger. "But it's their job to look for weaknesses and fix them, and we absolutely want them to do that." Adds Paul Schmidt, controller at General Motors Corp., "We have 200 people in internal audit, and it's now a more exciting place to work. Our audit committee values them, and even when we downsize, they keep a close eye on the size of internal audit to make sure we have the resources there that we need."
- Pitney Bowes Inc. CFO Bruce Nolop goes a bit further. "**[Internal] auditors are rock stars now**," he says. "This is their day in the sun."

Emerging Issues: Rapid increase in regulatory issues over data

- Gramm-Leach-Bliley Act
- FERPA
- HIPAA
- Higher Education Opportunity Act
- GDPR
- Sarbanes-Oxley
  (not yet “directly” applicable
  to higher ed, but indirectly)
- California SB 1386
- … in addition to other State laws

Yates Memo

- Sept. 9, 2015, Deputy U.S. Attorney General Sally Quillian Yates memo to AGs
- “Individual Accountability for Corporate Wrongdoing”
- Imposes criminal liability on individuals to enhance the deterrent value of corporate criminal liability
- Prevention remains best defense

“Are you the guy who requested a printout of the latest Higher Education regulations?”

Whose responsibility is it to mitigate legal risks at your institution?

- General Counsel
- President/Chancellor
- Chief Compliance Officer
- Each employee of the institution

COSO Framework: Enterprise Risk Management

"Enterprise Risk Management -- Integrating with Strategy and Performance"

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Define the organizational structure, board policies, management risk appetite

Define objectives for strategy, operations, reporting, & compliance

What could go wrong?

What is the impact and likelihood of risks?

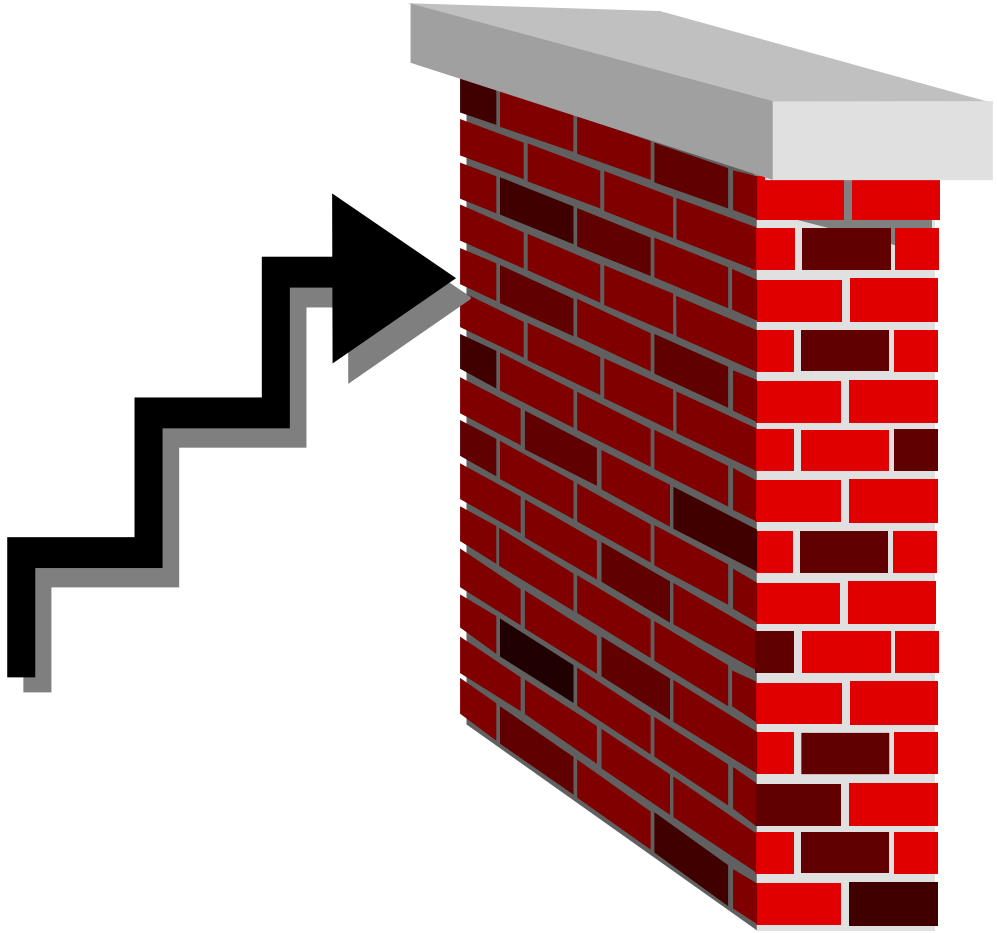
How to manage risk: Share it, avoid it, reduce it, or accept it

Procedures to ensure effective risk mitigation

Education & awareness of effective policies and practices

Management reviews & audit assesses

What is RISK?



Strategic Plan

Anything that could prevent the organization from meeting its goals

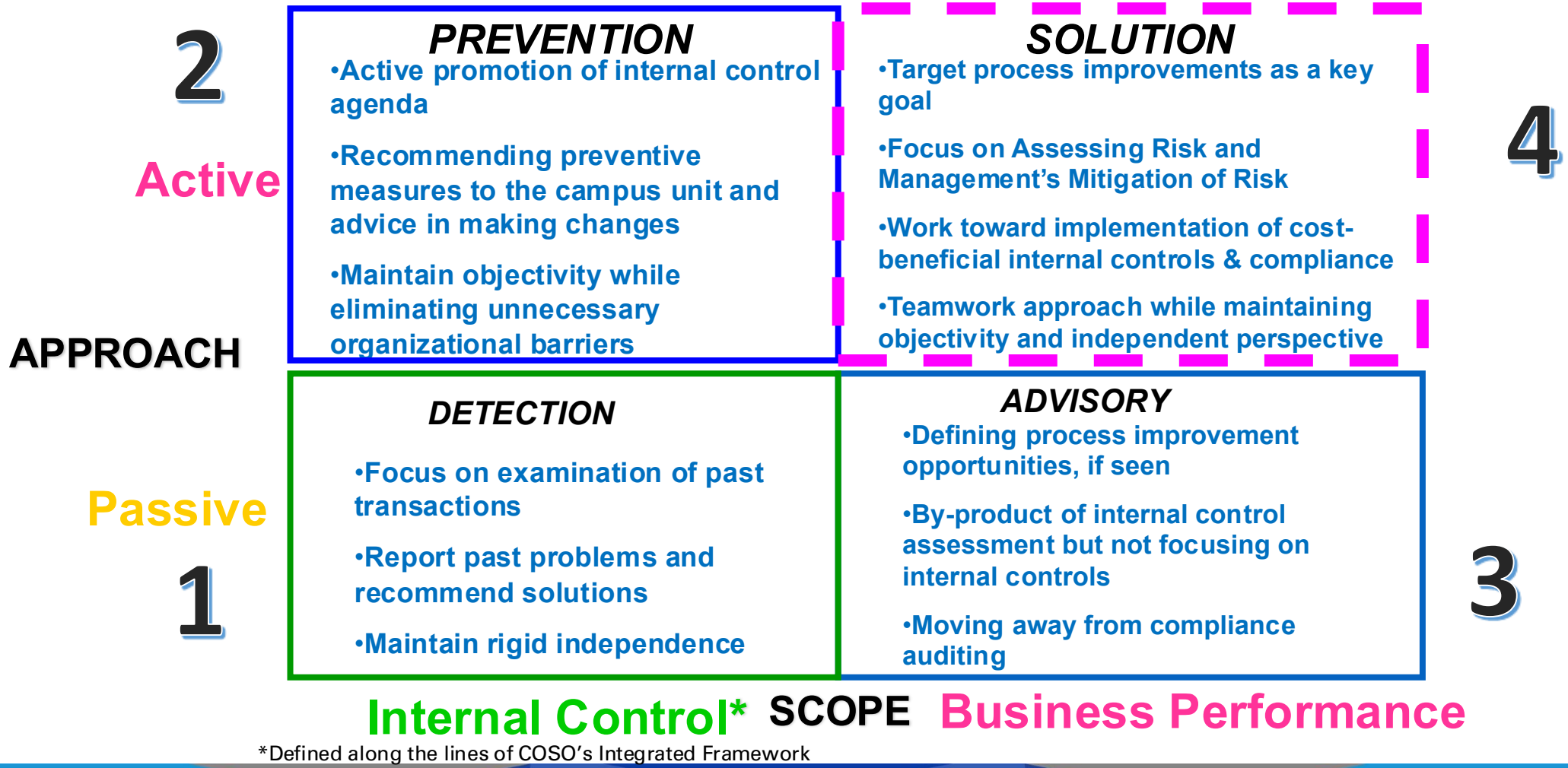

ACTION NEWS 2
WSB-TV·DT ATLANTA
COVERAGE
YOU CAN COUNT ON
[HIGH DEFINITION TELEVISION]

Have you read your institution's strategic plan?

- See what senior management views as most important
- Map your job responsibilities to the accomplishment of the Plan
- Better communicate the value of the services you and your department provide

Internal Audit Primary Mission

Four Potential Orientations

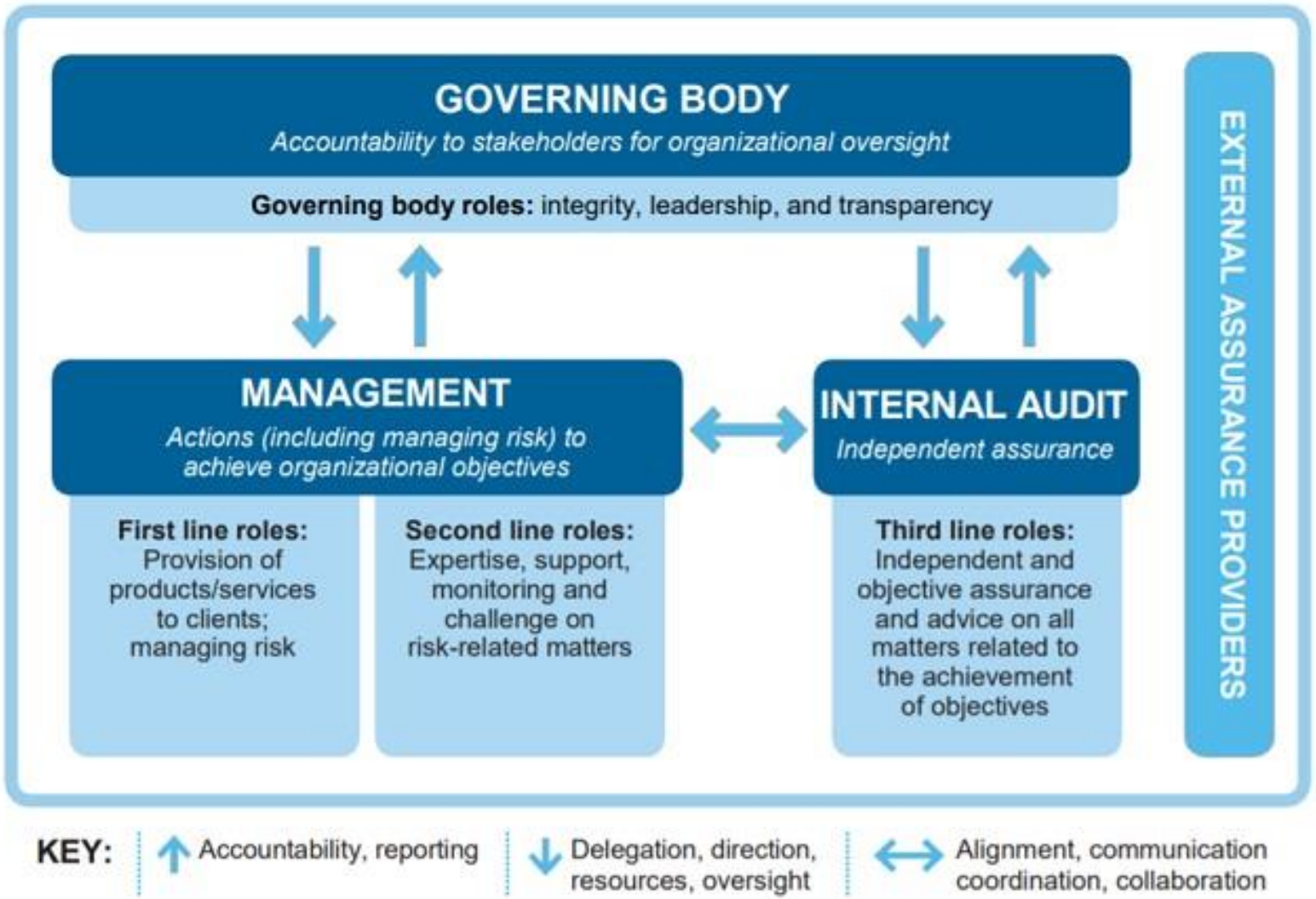


*Defined along the lines of COSO's Integrated Framework

Please fill in the survey

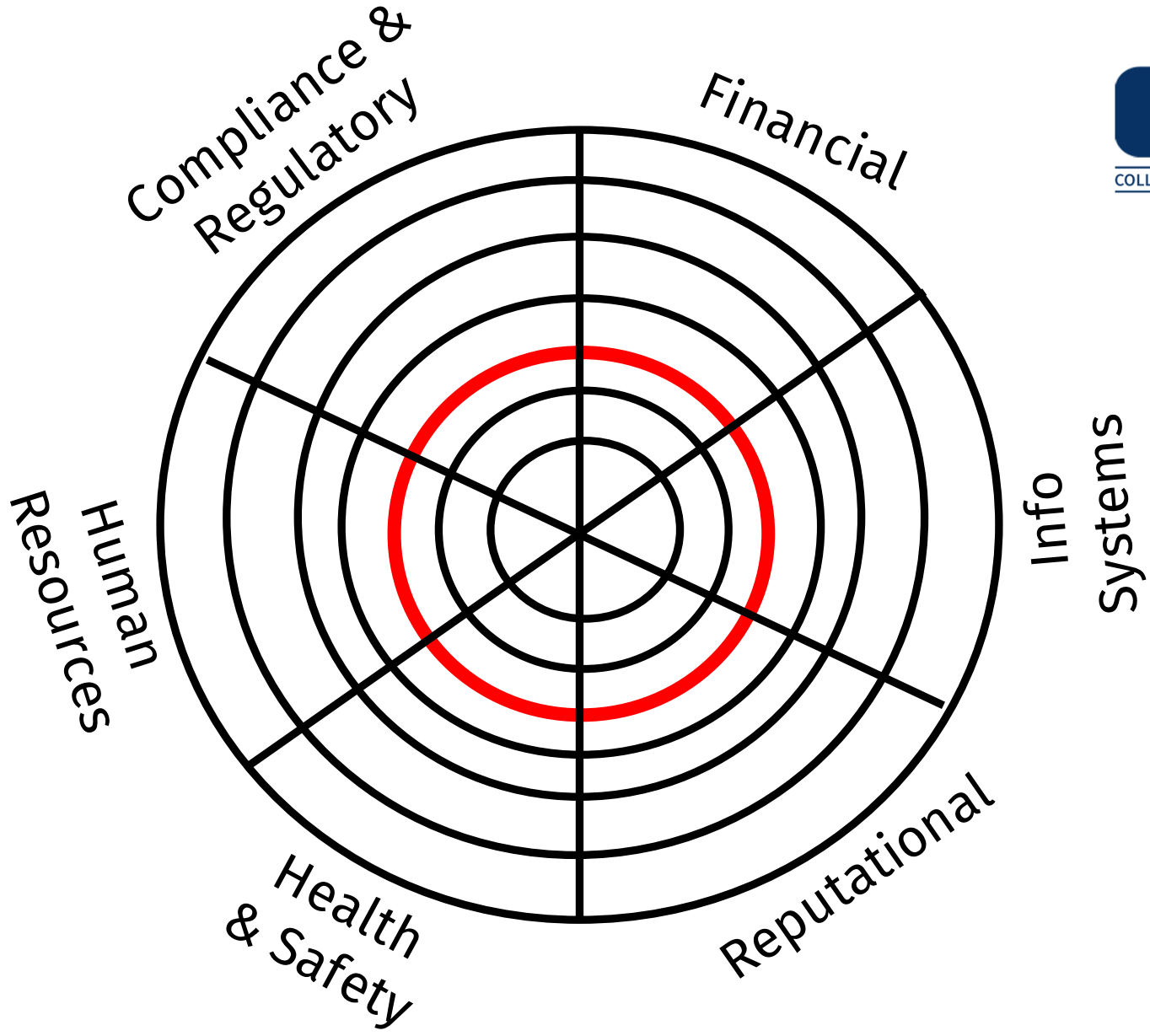
cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

The IIA's Three Lines Model

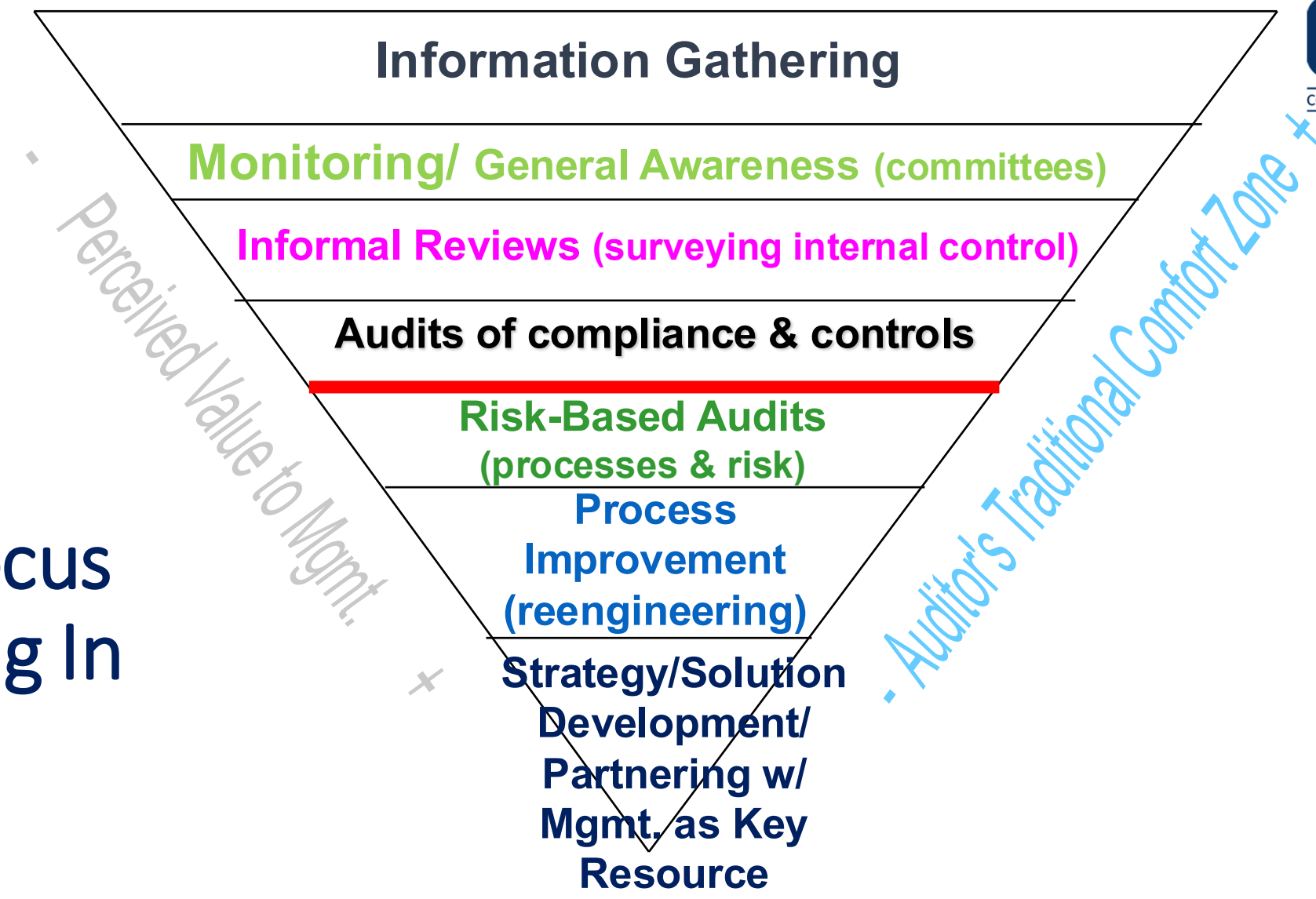


Source: Institute of Internal Auditors

Audit Risk Universe

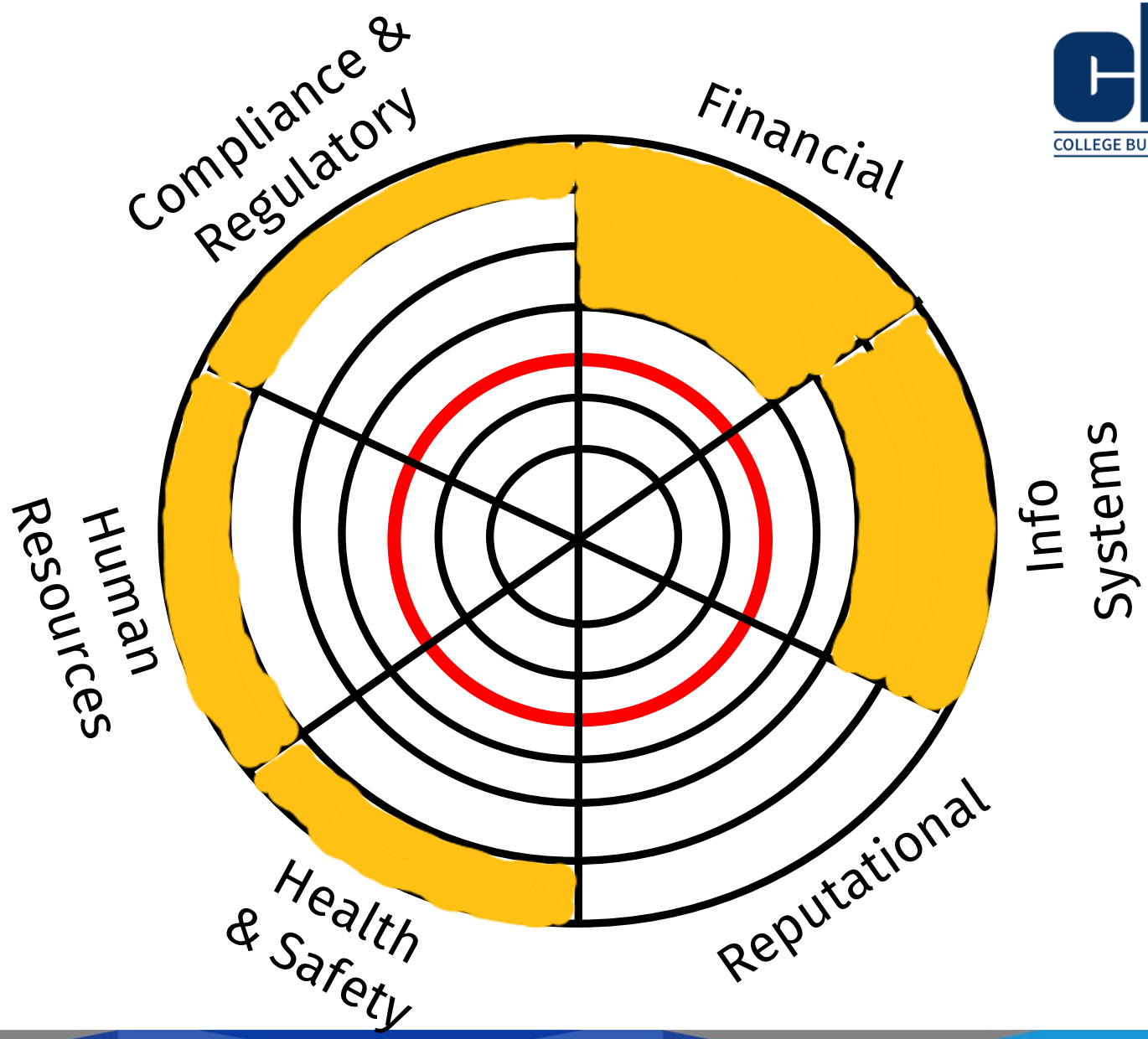


Audit Focus -- Zeroing In

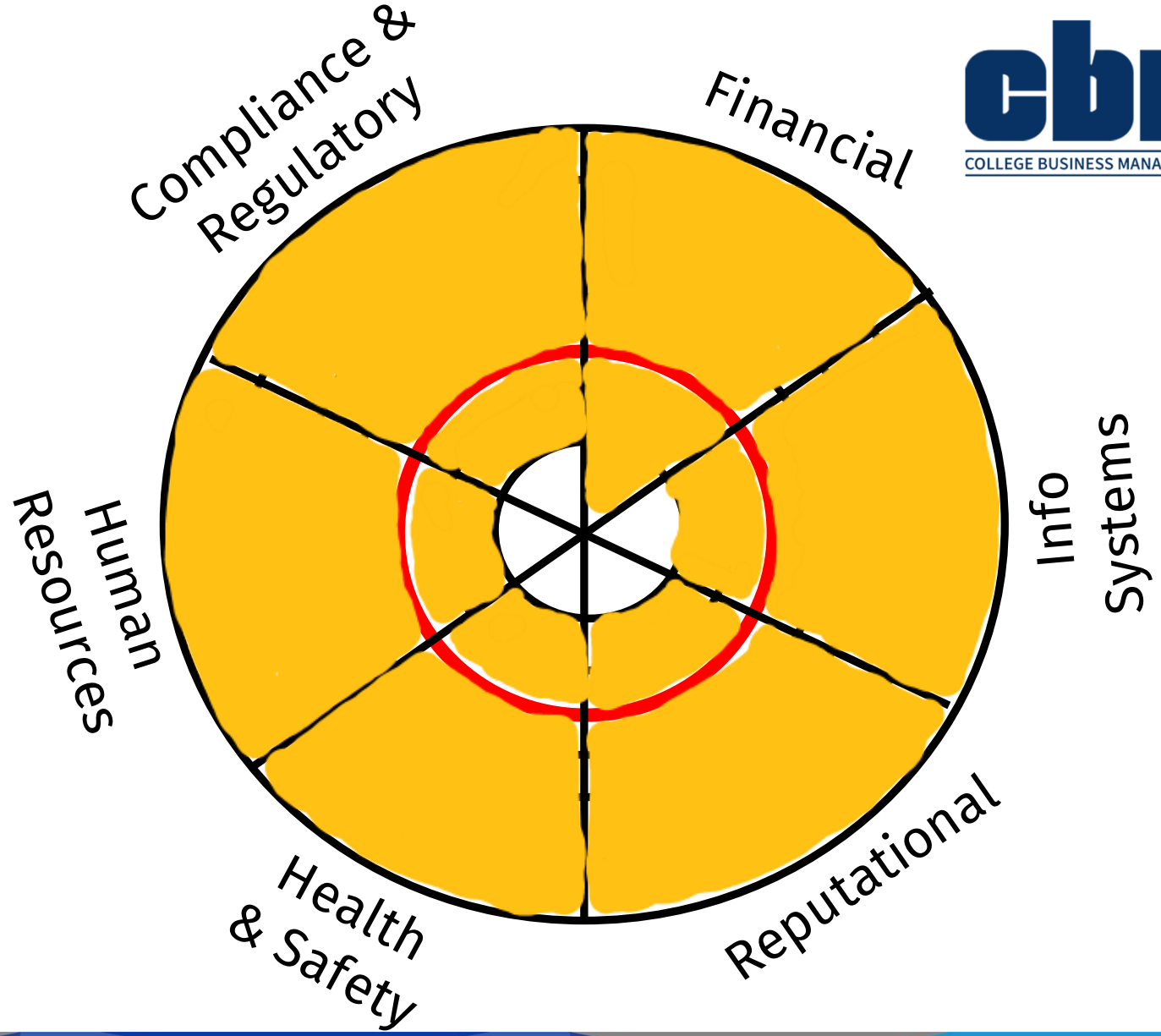


cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Audit Risk Universe - Past Focus



Audit Risk Universe - Focus Goal



The Approach – Setting the Scope

- Talk with all members of Senior Management (one-on-one discussions)
- Talk with line-level and managers as well
- Ask key questions, such as:
- **“Where are potential exposures?”**
- **“What keeps you up at night?”**
- **“Where do you see risks for your unit and the institution?”**
- Complete worksheet to inventory the risks

Risk Assessment Discussion Tool

Category of Risk	Risk Description (Explanation of Threat)	Potential Impact [1 (low) to 5 (high)]	Likelihood [1 (low) to 5 (high)]	Risk Rating	Primary Point of Contact to Mitigate Risk	Current Strategies for mitigating the risk	What Monitoring is in place
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			

Count the F's

Feature films are the result
of years
of scientific study combined with the
experience of years

What is YOUR Strategy for Risk Assessment?

Translation: If I ignore it and do nothing, then maybe the problem will go away… it won't

The Questions:

- “What are some of the potential adverse situations that could occur within…?”
- Note: We are NOT asking, “What would you like Internal Auditing to do for you?”
- Neither are we asking “What internal controls should be in place?”

Risks: Financial

- Accuracy of records
- Sponsored programs
- Foundation funds
- Travel
- Procurement/ P-Cards
- Telecommunications
- Capital Assets
- Cash and Receivables
- Payroll
- Risk Management

Risks: Information Systems

- Logical Security
- Environmental and Physical Controls
- Data Security and Stewardship
- Management of IS Resources
- Equipment Maintenance
- Back-up and Recovery
- Training and Documentation
- Operations/ Administration
- Web Site Operation/ Development
- Software Licensing

Why?

- Cybersecurity threats continue to evolve
- Cybercriminals have changed
- Higher Ed is a growing target
- Increasing number of exploits target individual users
- Greater need for awareness of risks and sound practices

THE COST OF CYBER CRIME IN 2026

Cyber crime continues to rise—driving unprecedented costs for businesses and people worldwide.

GLOBAL COST OF CYBER CRIME IN 2026

$10.5 TRILLION

UP 15% FROM 2025

Cyber crime costs are projected to surge past $10 trillion annually by 2026.

KEY COST DRIVERS

Rising sophistication of attacks
Attackers are using AI, automation, and advanced techniques.

Expanding attack surface
Cloud, remote work, IoT, and third-party risks increase exposure.

High impact on operations
Downtime, data loss, and regulatory penalties drive greater costs.

COST BREAKDOWN BY TYPE OF CYBER CRIME (2026)

RANSOMWARE	PHISHING & SOCIAL ENGINEERING	CLOUD COMPROMISE	PAYMENT FRAUD & FINANCIAL CRIME	IDENTITY THEFT
$2.73T	$1.76T	$1.47T	$1.26T	$1.12T
Business disruption, ransom payments, and recovery	Fraud, credential theft, and account takeover	Data breaches, service disruption, and misconfiguration	Unauthorized transactions and online payment fraud	Account takeover, new account fraud, and identity misuse

MALWARE & VIRUSES	BUSINESS EMAIL COMPROMISE	INSIDER THREATS	IOT/OT & SUPPLY CHAIN ATTACKS	WEB ATTACKS
$0.91T	$0.74T	$0.56T	$0.44T	$0.27T
Damage, data loss, and system recovery	Fraudulent wire transfers and scams	Data theft, sabotage, and policy violations	Operational disruption and third-party risk	DDoS, defacement, and web exploits

BY THE NUMBERS (2026)

$4.88M	277 DAYS	66%	$1.9M
Average cost of a data breach	Average time to identify and contain a breach	Of organizations expect higher losses in 2026	Average ransom demand

TOP 5 INDUSTRIES BY TOTAL COST (2026)

Financial Services	Healthcare	Manufacturing	Retail	Technology
$2.27T	$1.56T	$1.22T	$1.11T	$0.97T

THE OUTLOOK

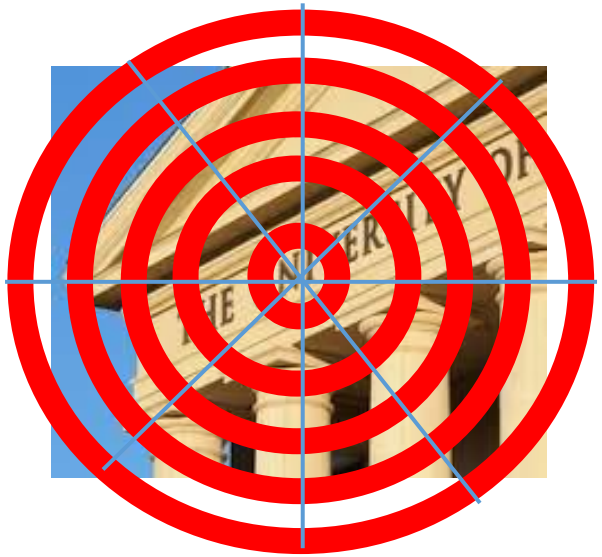
Cyber crime is a trillion-dollar challenge—but proactive security and resilience can reduce the risk.

Invest in prevention. Strengthen defenses. Build resilience.

Source: Cybersecurity Ventures – 2026 Cybercrime Report

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Higher Education Growing Target

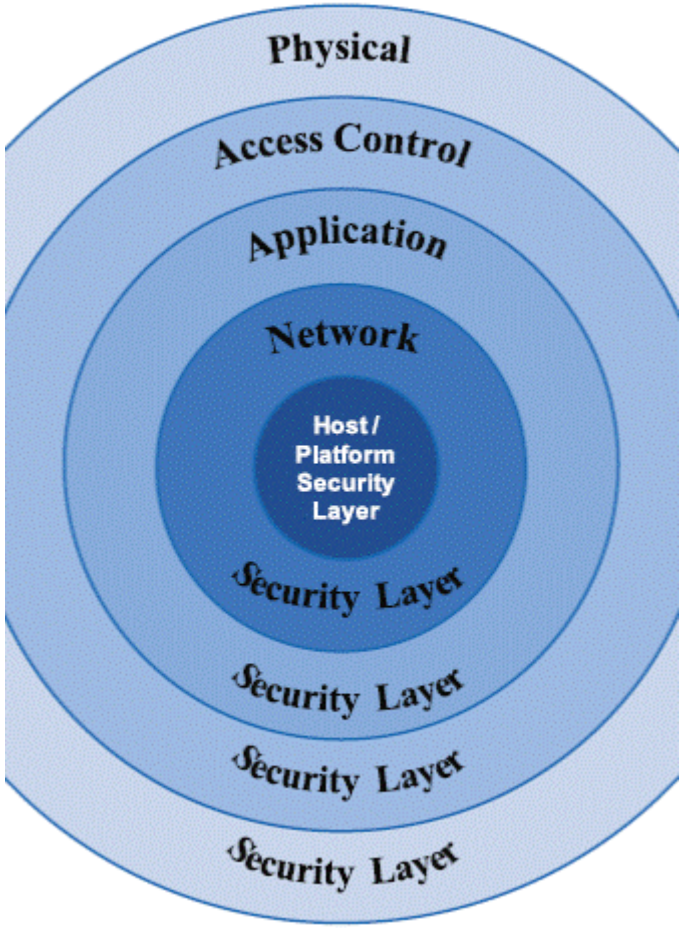


LOTS of valuable info:

- SS#, financial aid (tax returns), financial info, banking info, medical records
- Known for its “open” environment (“academic freedom”) and lax security
- Decentralized security profile
- Typically under-funded for information security

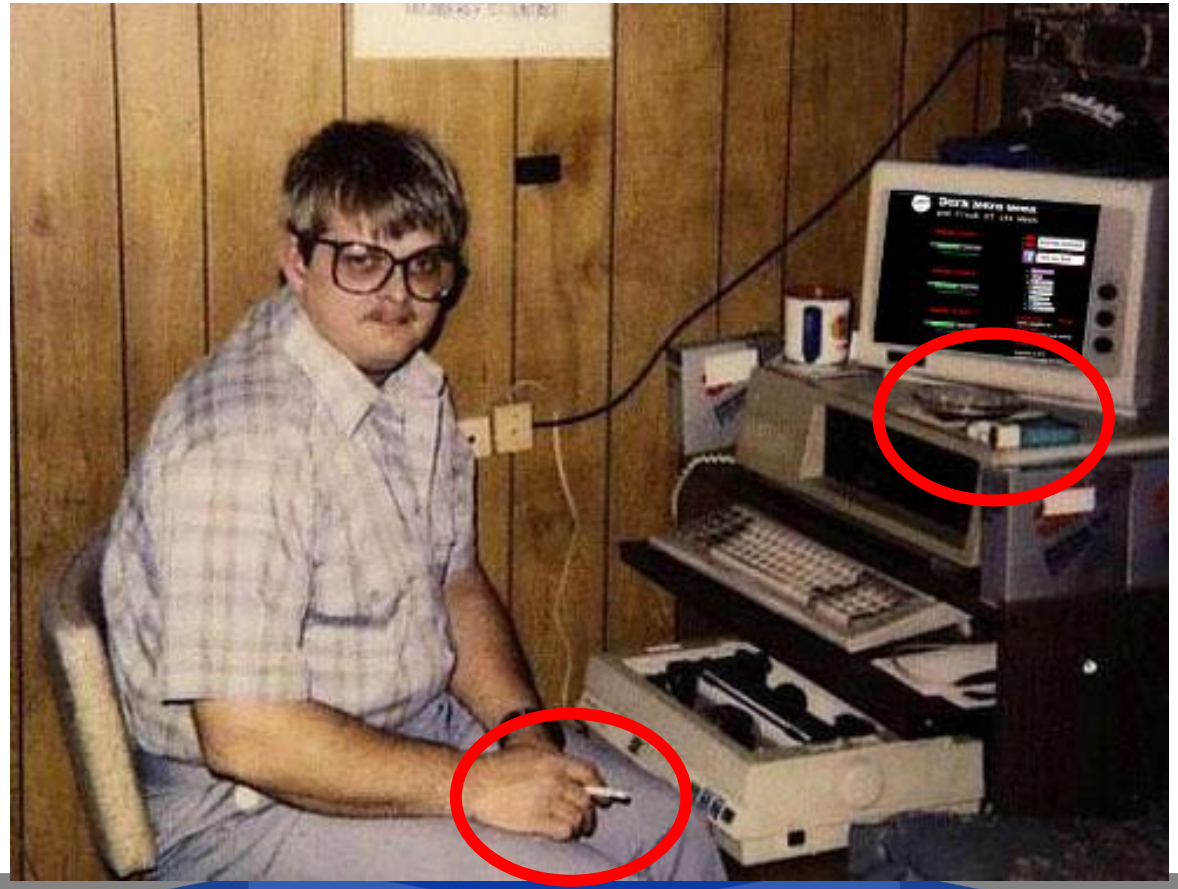
Layers to Computer Security

- Access-controlled server rooms
- Firewalls & Intrusion Prevention Systems (IPS)
- Intrusion Detection Systems (IDS)
- Multi-factor authentication
- Antivirus scanning
- File and data encryption
- Secure coding of applications
- Enterprise rights management
- User controls



Why Does This Matter To Me?

Because IT security is not just for “techie nerds”

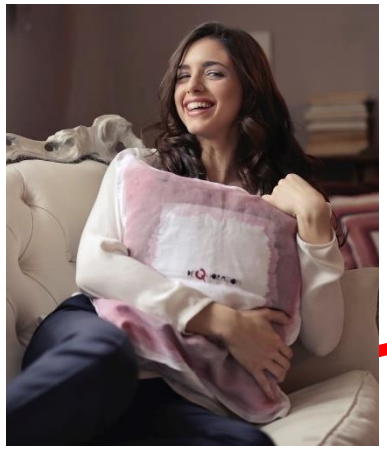


Information Security – Weakest Link:

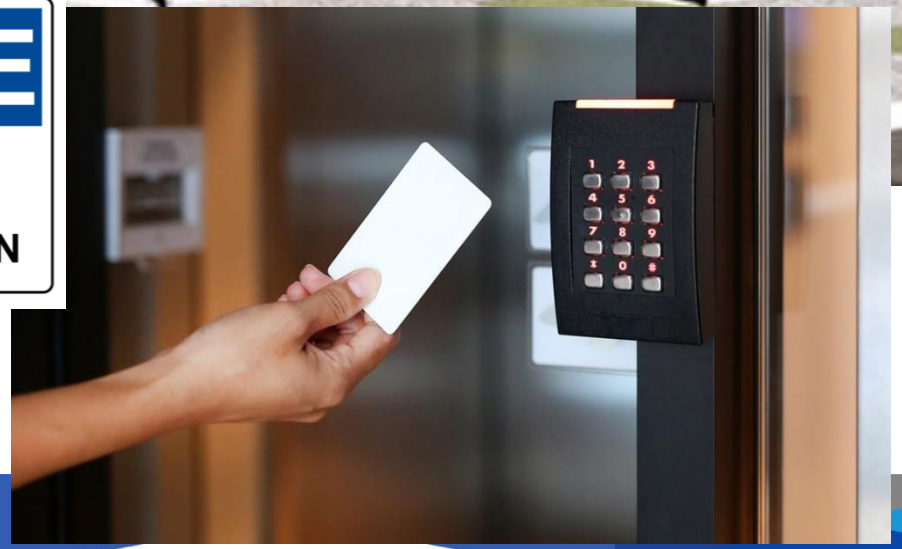
cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

PEBCAK

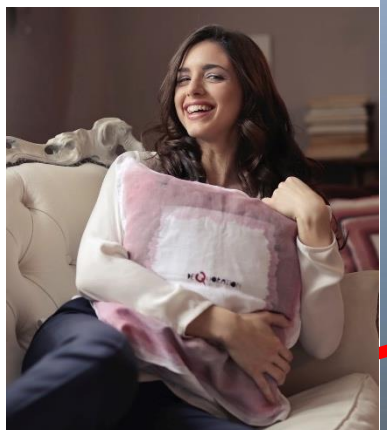
95% of cyber-attacks start with an employee being tricked



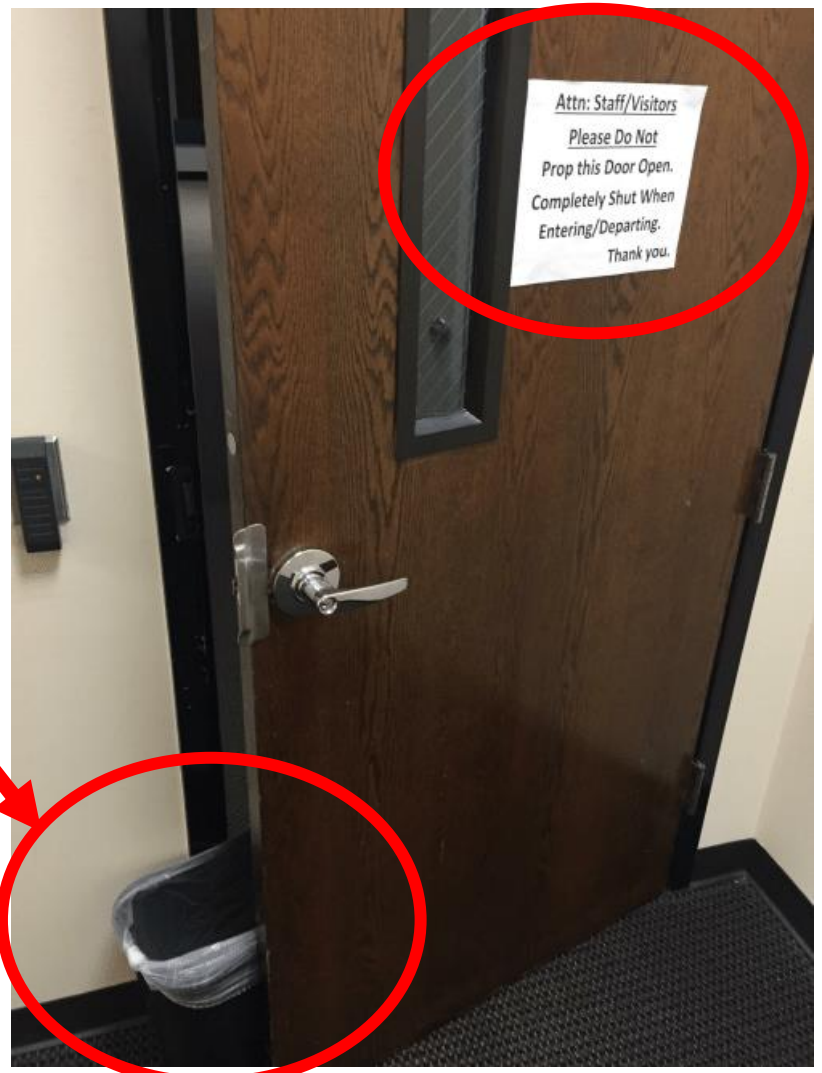
cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE



cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE



Do not prop open door and allow coyotes into sandwich shop



Now *everyone* in the building is at risk

What are Cyber Criminals Seeking?

- Personal Identifying Information (PII)
  - Social Security Numbers
  - Credit card numbers, security codes, exp. dates
  - Birth Dates
  - Home addresses
  - Mothers' maiden names
  - Banking info
  - Intellectual Property
  - Medical records
- **Login credentials & trusted access**

What YOUR data is worth on the Dark Web

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Spotify Account	Hulu Account	Netflix Account	PayPal Credentials	Social Security Number
$2.75	**$2.75**	**$1.00 - $3.00**	**$1.50**	**$1.00**

Driver's License	Credit Card	Email Address & Password	Medical Record from Large Scale Attack	Complete Medical Record
$20.00	**$8.00 - $22.00**	**$0.70 - $2.30**	**$1.50 - $10.00**	**Up to $1000.00**

Source: Dark web market listings Markets monitored were Dream, Point and Wall Street Market. Prices collected in USD as displayed on listings. Per Top10VPN

How Do Cyber Criminals Get Your Information?

Attacker

Phishing Email

User (Target)

Exploit Document

Backdoor Trojan

Once Backdoor Access is Gained…

- Attacker can install rootkits, bootkits, **keystroke-loggers**, anti-antivirus malware, etc.
- Most users will be unaware that their system has been compromised

How to Protect Yourself

- Regularly update your ***strong, unique*** password
- Never use same password for multiple platforms
- Treat your passwords like underwear…

➢**Change** them often,

➢keep them **private** (don't leave them laying around), and

➢**never share** them with anyone

How long does it take to use AI to crack a password?

GDPR
ISO 27001
ISO 27002

PCI DSS
NIST 800.53

DOD/CMMC

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Source: Hive Systems

Note:
It takes AI 6 days to crack an 18-character numbers-only password. Add an uppercase and lowercase letter, and it'll take AI 26 trillion years! Once you get above 16 characters, it is much harder for AI to run through all the password combos, so the longer the password, the better.

How long should your password be?

We laugh – but she was trying…
During a recent password audit by a company, it was found that an employee was using the following password:
“MickeyMinniePlutoHueyLouieDeweyDonaldGoofy1Sacramento”

When asked why she had such a long password, she rolled her eyes and said, “Hello! I was told it had to be at least 8 characters and include at least one number and a capital.”

Ways to Spot Phishing Schemes

1) Double check the ***origin*** of an email before opening or acting or responding.

- Email addresses can be spoofed. ***Look for unusual domains*** (e.g., example.com.hk)
- ***Sense of urgency***? Criminals are looking to have you respond quickly.
- Body of message and signature: ***generic or personalized?*** Customary to what you would expect from sender?

Extremely Urgent: Final attempt to contact you...this is time sensitive

Heather <patricia@mshmoss.com> Sep 14, 2015, 3:15 PM

to: "[redacted]@gmail.com" <[redacted]@gmail.com>

What would you say if I told you the government owed you up to $5,775 cash to go to school? Well, they DO and all you have to do is pick a school, pick a subject and claim it!

- THIS IS NOT A LOAN, you will never have to pay this back
- Online classes are available

Take this SERIOUSLY, Soon This Program Will Close Until Next Year. Click below to take the two-minute questionnaire and start the approval process...

Click Here To Let Us Know If You'd Prefer Check Or Direct Deposit

PO box 105603
Atlanta, GA 30348-5603

You are receiving this message us and we respect your privacy. We hope you find these communications valuable; however, if you would prefer to no longer receive emails from us, please click here.

Example #4:
The content of the message makes promises, often about large sums of money that seem "too good to be true." This example also attempts to collect personal banking information and uses a spoofed email address.

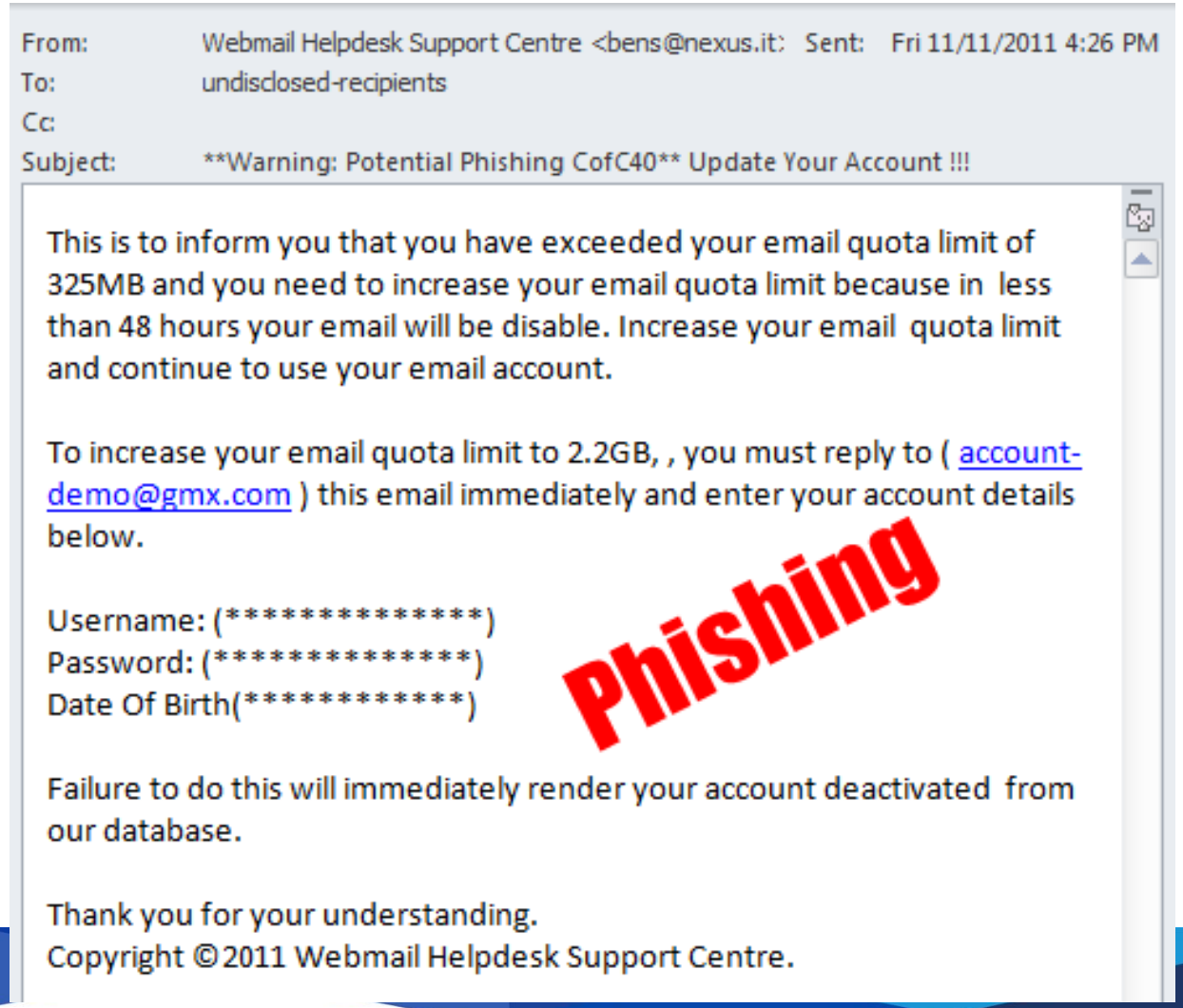
cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

What to look for in email (cont.)

- Content – asking you to ***open a file*** or go to a ***website link***?
- ***Hover*** mouse over link (**DO NOT CLICK**… just ***hover***). It should show the actual link.

2) Never share personal identifiable information via email

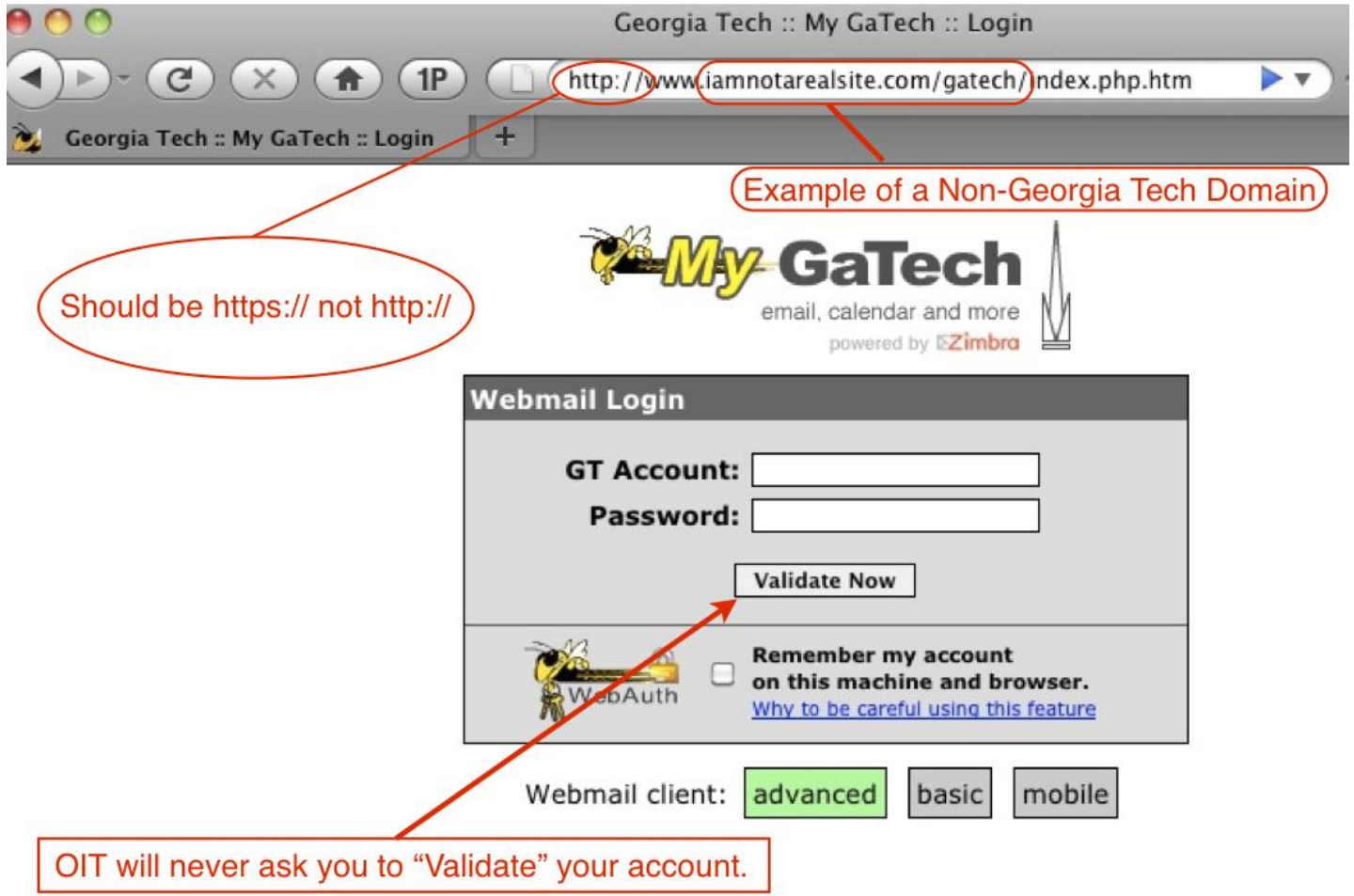
- Legitimate emails will never ask you to share sensitive PII. Most phishing emails are bait to see if you will.



3) Never use login forms embedded in emails

- Instead, access the organization's webpage directly from your browser.
- If you receive a call ("Vishing"), ask for a call-back number and verify that against known numbers

Double and triple check URL before filling out ANY form



4) Check legitimacy of email

Legitimate companies are less likely to use public email providers like Yahoo, Gmail, Hotmail, Outlook, etc.

What to do when you receive a spurious email?

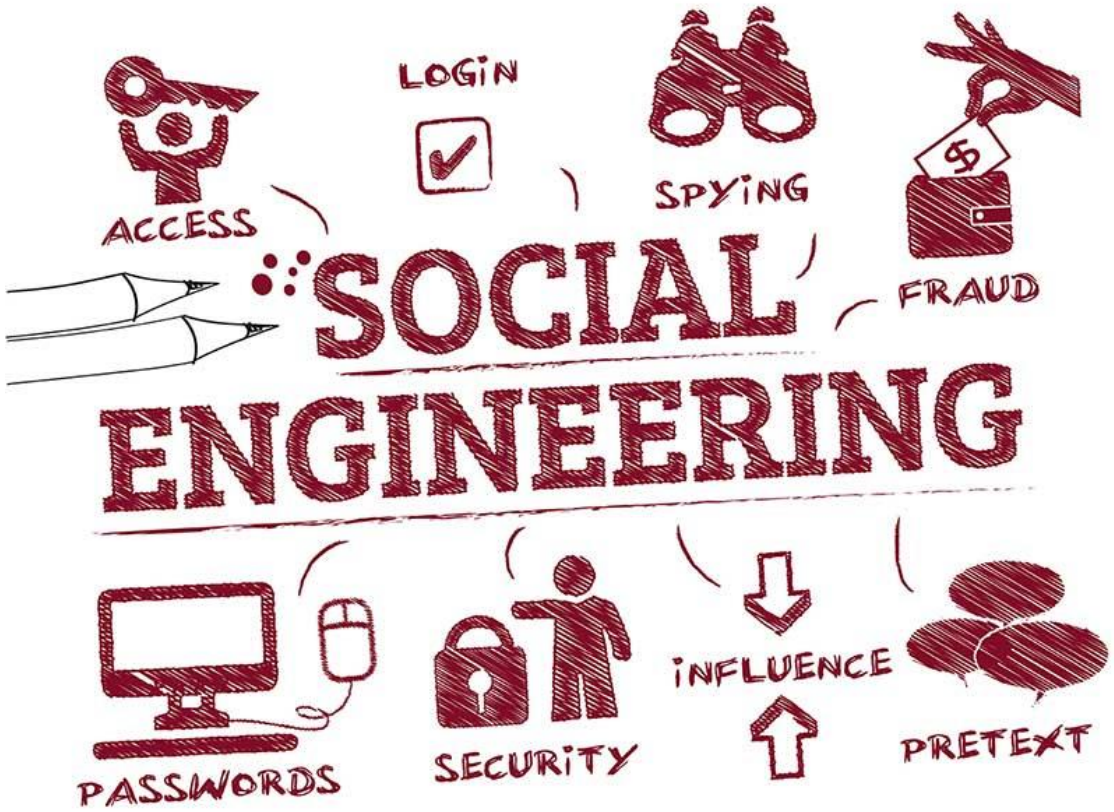
- **DO NOT CLICK ON ANY LINK or download any attachment!**
- **Alert IT Department**
- ***SHIFT-DELETE*** (permanently delete email)

Other IT Security Effective Practices

- Develop clear computer use policies for employees and 3rd party vendors
- Restrict users from having administrator access
- Review user access in each dept. to ensure “need-to-know” for each user
- Regularly update system software and antivirus software (don’t forget other devices, e.g., printers, routers, etc.)
- Ensure against software piracy in dept.
- Back up data and store securely

Other IT Security Effective Practices (cont.)

- Use end-to-end encryption to access or send any sensitive data (e.g., VPN)
- Beware of social engineering (be prudent about what information you share on social media)
- Develop incident-response plan



Incident Response Model

1 Event or Incident Requiring Collaboration

Critical incidents that require collaboration are incidents that extend beyond the borders of the local hardware or software system and pose a threat of an adverse impact on the University's reputation, financial position, information systems security posture, or health and safety of faculty, staff and students. Examples of incidents requiring collaboration:

Unauthorized access to sensitive information, (e.g., SS#, credit card #'s, etc.)

Suspected misuse of IS resources resulting in widespread compromise of information security

Large scale intrusions

2 Ad-Hoc Group Convenes

-via phone, Teams or live conference

- Chief Compliance Officer
- Chief Information Officer
- Chief Information Security Officer
- Chief Operating Officer
- General Counsel
- Director of Public Safety
- AVP, Controller & Chief Accounting Officer

2a Other Resources to be considered on a situational basis:

- Assistant VP External Affairs, Chief of Staff
- Chief Human Resources Officer
- Vice President, Communications
- Unit head(s) of affected area(s)

3 Ad-Hoc Group determines the resources necessary to reach a resolution on the incident. The Group will make the following assessments:

3a Is this incident likely to result in criminal or civil legal action?

If yes, the path below should be followed. If no, 3b should be followed.

Scope:

A decision needs to made to determine the point at which HU will stop its internal investigation and hand it over to law enforcement and then to which law enforcement agency (e.g., FBI, Secret Service, and/or local law enforcement).

Review Method:

The standards of evidence for an investigation which is likely to result in criminal prosecution are far higher than those for which administrative action only is expected. For example, prior to any internal investigation of the machine(s) involved, it would likely be appropriate to have law enforcement image or mirror the drives of the machines then turn the mirrored drives back to HU for its internal investigation.

Investigation:

After coordinating with law enforcement and preserving the integrity of the data on the machines, HU will proceed with an investigation of the mirrored drives.

3b Is this incident likely to not result in legal action and result in an administrative action that is localized within the university?

If yes, the path below should be followed.

Scope:

A decision needs to made at what level the investigation will take place and the standard of evidence that will be maintained. A decision will also need to be made regarding the point at which enough evidence has been obtained to satisfy the requirement to take appropriate administrative action.

Review Method:

The standards of evidence for an administrative investigation are less stringent than those which may result in legal actions but are important to maintain nonetheless. This ad-hoc group must decide at what level evidence of the investigation should be documented.

Investigation:

As the internal investigation proceeds, the ad-hoc group must be cognizant of the situations encountered which may change the examination from administrative to a potential legal investigation and take appropriate steps.

4 Assigning Investigation Oversight:

The ad-hoc group will determine which internal office will take the lead for coordinating the investigation and communicating the results. This designated lead group will:

- Coordinate all efforts related to the investigation
- Determine the custodians of data
- Have responsibility for reporting results and ensuring continuing lines of communication

5 Conducting the Investigation:

The department or group with oversight of the investigation has the responsibility to communicate the results of the investigation and ensure as soon as data on this incident relevant to the position of the University is uncovered, it reaches the executive decision makers.

6 Follow-up and Reporting:

The department or group with oversight of the investigation reconvenes the ad-hoc group at the end of the investigation and reports on:

- The outcome of the investigation
- Lessons learned (how the process worked)
- Cost of incident (in hard costs and personnel time devoted to the incident response)
- Discuss methods to prevent future incidents

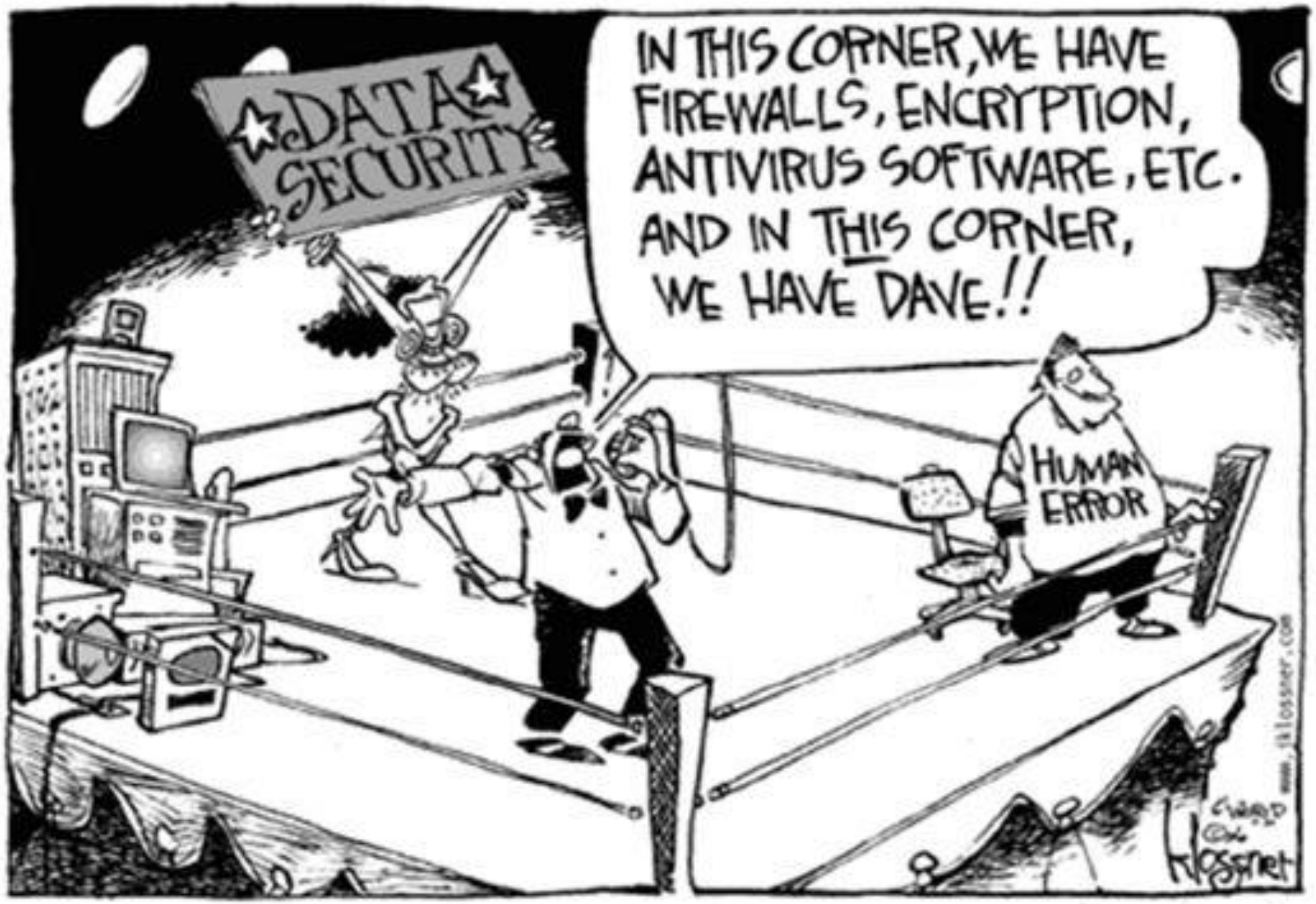
cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Other IT Security Effective Practices (cont.)

- Develop business continuity plan for each unit
- TEST each unit's ability to implement business continuity

Other IT Security Effective Practices (cont.)

- Educate and train ALL employees and ***HOLD ACCOUNTABLE***
- ***MONITOR*** to ensure compliance



cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Don’t become the weakest link…

… to avoid the IT department assigning you an error code:

“ID – 10 –T”

IDIOT

IT Security…

… is **EVERYBODY'S** responsibility

Risks: Human Resources

- Appropriate hiring (EEOC)
- Leave Reporting
- Sexual Harassment Awareness
- Employment Eligibility Verification
- Consultant or Employee?
- Annual Performance Evaluations
- Off campus assignments
- Non-standard work assignments

Risks: Health & Safety

- Safety of Workplace
- Hazardous Materials
- Biological Safety
- Chemical Safety
- Hazardous Equipment
- Emergency Plans
- Training

Risks: Legal & Regulatory

- Who is authorized to contract on behalf of the university?
- Policy on receipt of Gifts
- Awareness of Open Records Act requirements

The Audit Plan

- Focus on reviewing how each organization is moving toward effectively and efficiently ***managing*** **each of the risks**
- Independent verifications & attestations to determine strength of processes
- Conclusions are forward-looking - **how well positioned are they to deal with risk ?**

HOWARD UNIVERSITY Office of Audit & Compliance

Summary of Observations and Opportunities for Improvement – Howard University School of ABC (HUABC)

This departmental review covers controls and procedures related to various operational areas within HUABC. The Office of Audit & Compliance (OAC) testing scope covered from **August 1, 2021,** to **September 30, 2023**. Our assessment work occurred from September 2023 until January 2026 and identified 22 opportunities for improvement that impact the management of risks related to HUABC controls and procedures.

The individual observations contributing to each overall observation noted to the right along with management recommendations are detailed in slides 2 – 5. Each individual observation is given one of the ratings noted below.

Rating	OAC Rating Description
	Green: Low Risk. Strong controls in place with limited to no further opportunity for improvement.
	Light Green: Medium-low Risk. Reasonable controls in place. There may be minor opportunities for business process enhancement and control improvement.
	Yellow: Medium Risk. Opportunity for improvement. A vulnerability in internal controls or business processes that requires attention.
	Orange: Medium-high Risk. Opportunity for moderate improvement. Ineffective design and/or inconsistent application of the framework of governance and controls. Senior management attention is recommended, and operating management action is required.
	Red: High Risk. Opportunity for significant improvement. Weaknesses in the process that present risk exposure to unit/University. Senior management attention is required.

TABLE OF CONTENTS AND SUMMARY

Results of Audit Approach

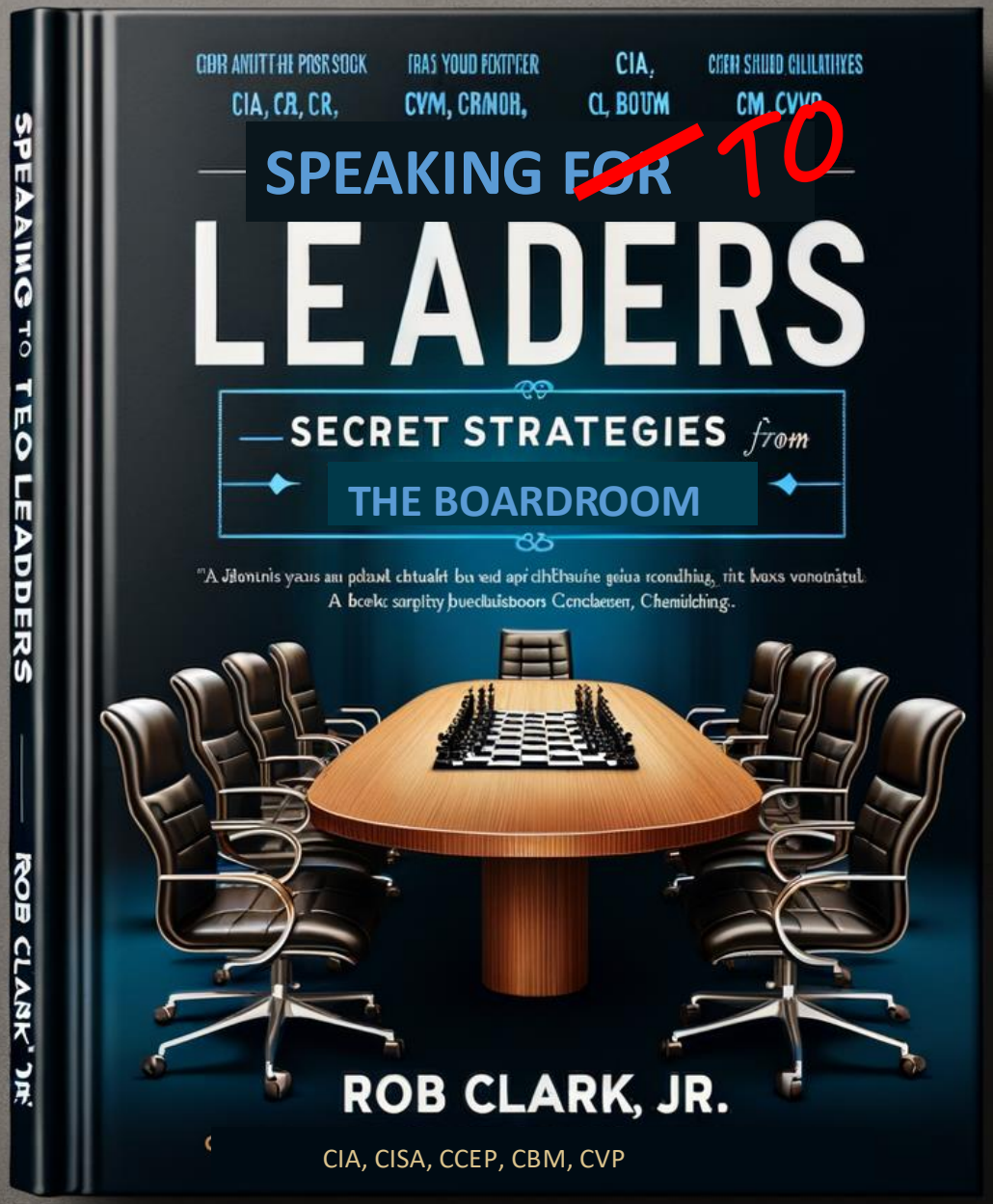
- Senior Management had a direct hand in identifying key areas of risk and setting the scope of reviews... **= "BUY-IN"**
- Audit Plan & Program seen as "**valuable**," "**useful**," "**on-target**," "**focusing on what matters**"
- **Action Plan** becomes a "**Management Tool**" not just an audit report
- Guiding the organization in developing a plan to manage its risks
- Lead to centralized policy improvements

Category of Risk	Risk Description (Explanation of Threat)	Potential Impact [1 (low) to 5 (high)]	Likelihood [1 (low) to 5 (high)]	Risk Rating	Primary Point of Contact to Mitigate Risk	Current Strategies for mitigating the risk	What Monitoring is in place
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			

If you suspect fraud, waste, abuse…

- Contact Internal Auditing
- Contact Hotline
- Report it

What NOT to do…



Next Steps

- Read & align with your strategic plan
- Assess the risks & “audit” your own unit

  With your team!
  - What adverse situations could occur?
  - What would the impact be?
  - What’s the likelihood that could occur?
- Ensure there are mitigation strategies in place
- Monitor, monitor, monitor

Be a Risk Champion

CPE Credit Code

RobClarkSpeaking@gmail.com
770.815.7922
linkedin.com/in/robclarkjr/
www.RobClarkJr.com