

CUAV 2025

Leading Practices in Internal Audit

Rob Clark, Jr., CIA, CCEP, CBM, CVP

Chief Audit & Compliance Officer

Howard University

robert.clark@howard.edu

RobClarkSpeaking@gmail.com

<https://www.linkedin.com/in/robclarkjr/>

www.RobClarkJr.com

770.815.7922



Objectives of the Session

- Emerging issues of risk in higher education
- What Audit Committees are looking for
- Corrective Action Plans for audit findings
- Promoting User Awareness in Cybersecurity
- Case study (in breakout groups)




How do people view you?

- 1) Necessary evil
- 2) Spawn of Satan
- 3) A profession mostly for suited for individuals with poor social skills and deep emotional scars who take great delight in writing people up for the slightest policy violation
- 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?





*"We have the sacred
responsibility of helping to
educate other peoples' children
and develop future leaders."*

Rob Clark, Jr.



158

2,839

Why It's the Best Job...

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



Emerging Issues: Rapid increase in regulatory issues over data

- Gramm-Leach-Bliley Act
- FERPA
- HIPAA
- Higher Education Opportunity Act
- GDPR
- CMMC
- Title IX
- California SB 1386 ... in addition to other State laws



Other risks on our radar...

- Third-Party risks
- Cloud computing
- A.I.
- NCAA compliance
- Financial Aid
- Laboratory safety
- Hazardous waste
- Clery Act
- Research compliance
- Impact of Executive Orders
- Enrollment
- Increased student financial need
- Mental health needs
- Financial & Reputational risks

Assoc. of College and University Auditors (ACUA)

- Risk Dictionary

	A	B	C	D	E	F	G
1	Category	Area	Area Code	Risk Code	Risk	Control Code	Control
2	Human Resource Development	Human Resources	HR-A046	R0997	Confidential personnel information is exposed (confidentiality).	C2040	Staff must sign confidentiality agreements.
3	Human Resource Development	Human Resources	HR-A046	R0997	Confidential personnel information is exposed (confidentiality).	C2041	Training and Awareness Program.
4	Human Resource Development	Human Resources	HR-A046	R1000	The classification system for employees is not an accurate and complete reflection of the duties and responsibilities needed.	C2042	Conduct a periodic review of HR classification system.
5	Human Resource Development	Human Resources	HR-A046	R1000	The classification system for employees is not an accurate and complete reflection of the duties and responsibilities needed.	C2043	Develop an appropriate set of minimum qualifications for each position.
6	Human Resource Development	Human Resources	HR-A046	R1001	Inability to attract qualified candidates.	C2045	Develop an appropriate career ladder for employees.
7	Human Resource Development	Human Resources	HR-A046	R1001	Inability to attract qualified candidates.	C2044	Benchmark compensation packages with peer institutions.
3543	Human Resource Development	Human Resources	HR-A046	R0977	Benefits do not meet employee needs.	C2019	review.
3544	Human Resource Development	Human Resources	HR-A046	R0978	Discrimination in workplace.	C2017	Supervisors and others responsible for hiring and management of employees attend EEO training on a periodic basis.
3545	Human Resource Development	Human Resources	HR-A046	R0978	Discrimination in workplace.	C2018	HR reviews any disciplinary action for classified employee demotions, suspensions without pay, or dismissals.

3545 Human Resource D

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

- 1) General Counsel
- 2) President/Chancellor
- 3) Chief Compliance Officer
- 4) Chief Audit Executive
- 5) Board of Trustees
- 6) Each employee of the institution

COSO Framework: Enterprise Risk Management

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

Define the organizational structure, board policies, management risk appetite

Define objectives for strategy, operations, reporting, & compliance

What could go wrong?

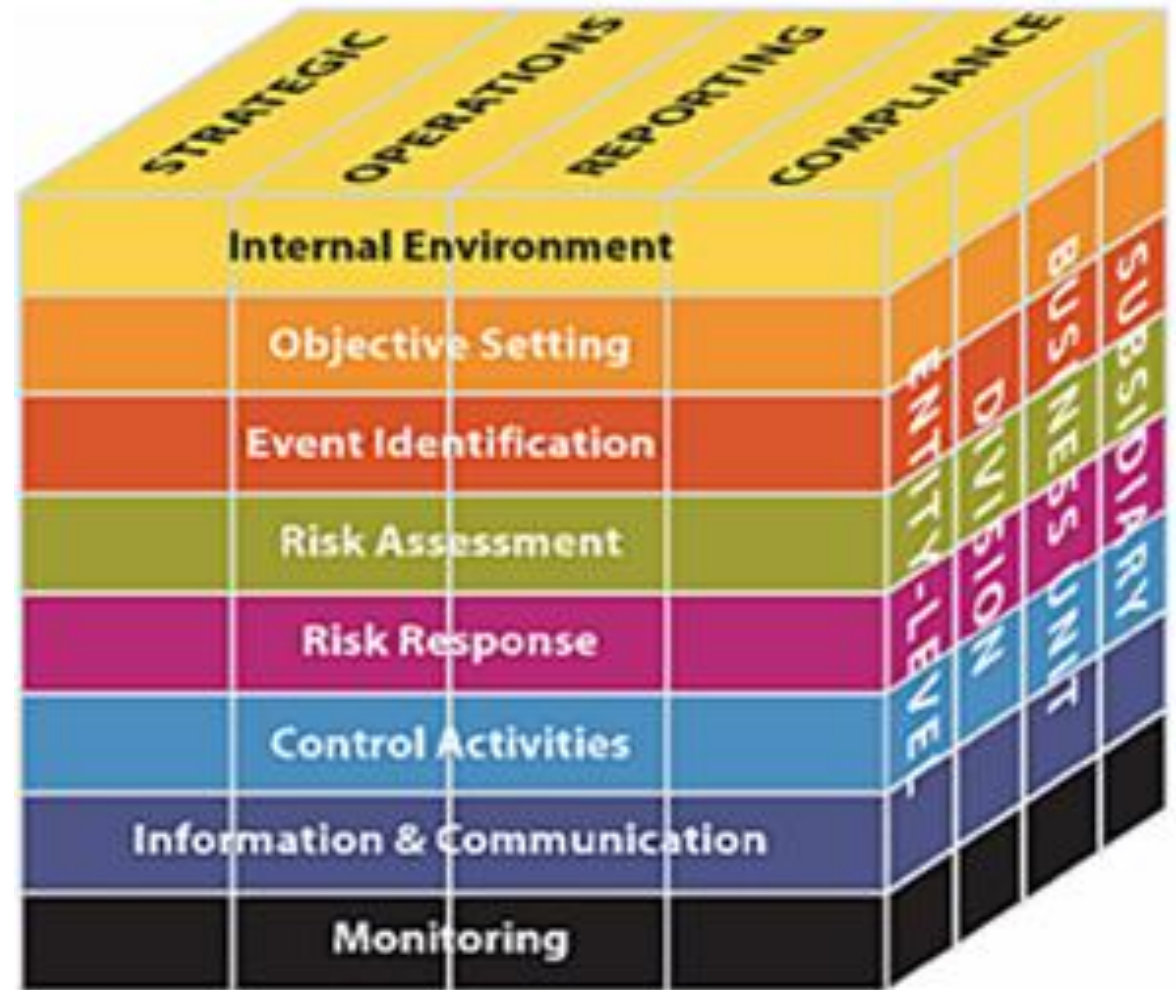
What is the impact and likelihood of risks?

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

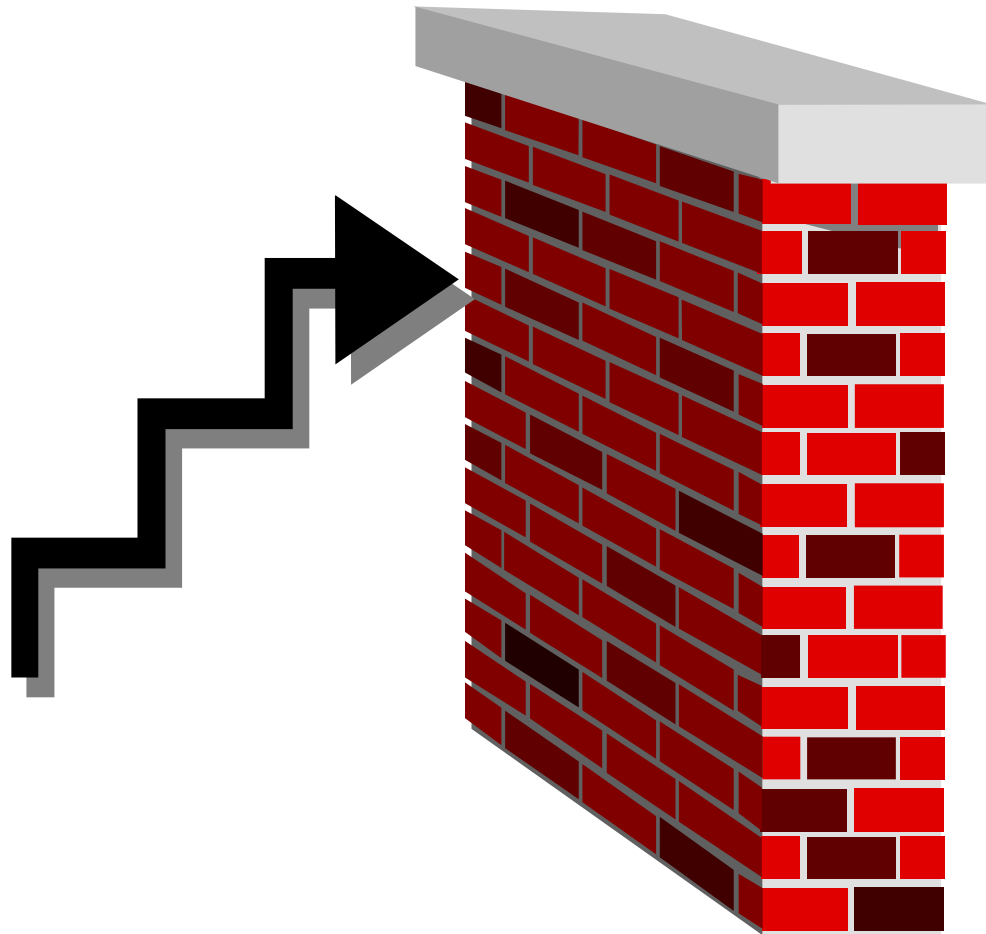
Procedures to ensure effective risk mitigation

Education & awareness of effective policies and practices

Management reviews & audit assesses



What is RISK?



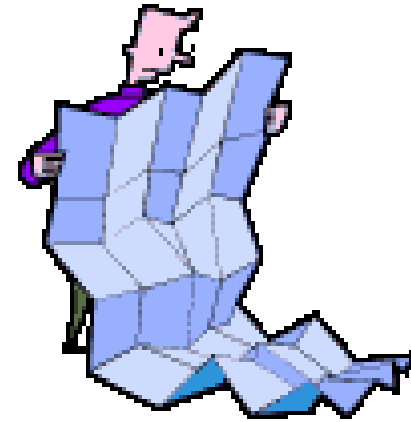
Strategic Plan



Anything that could prevent the organization from meeting its goals

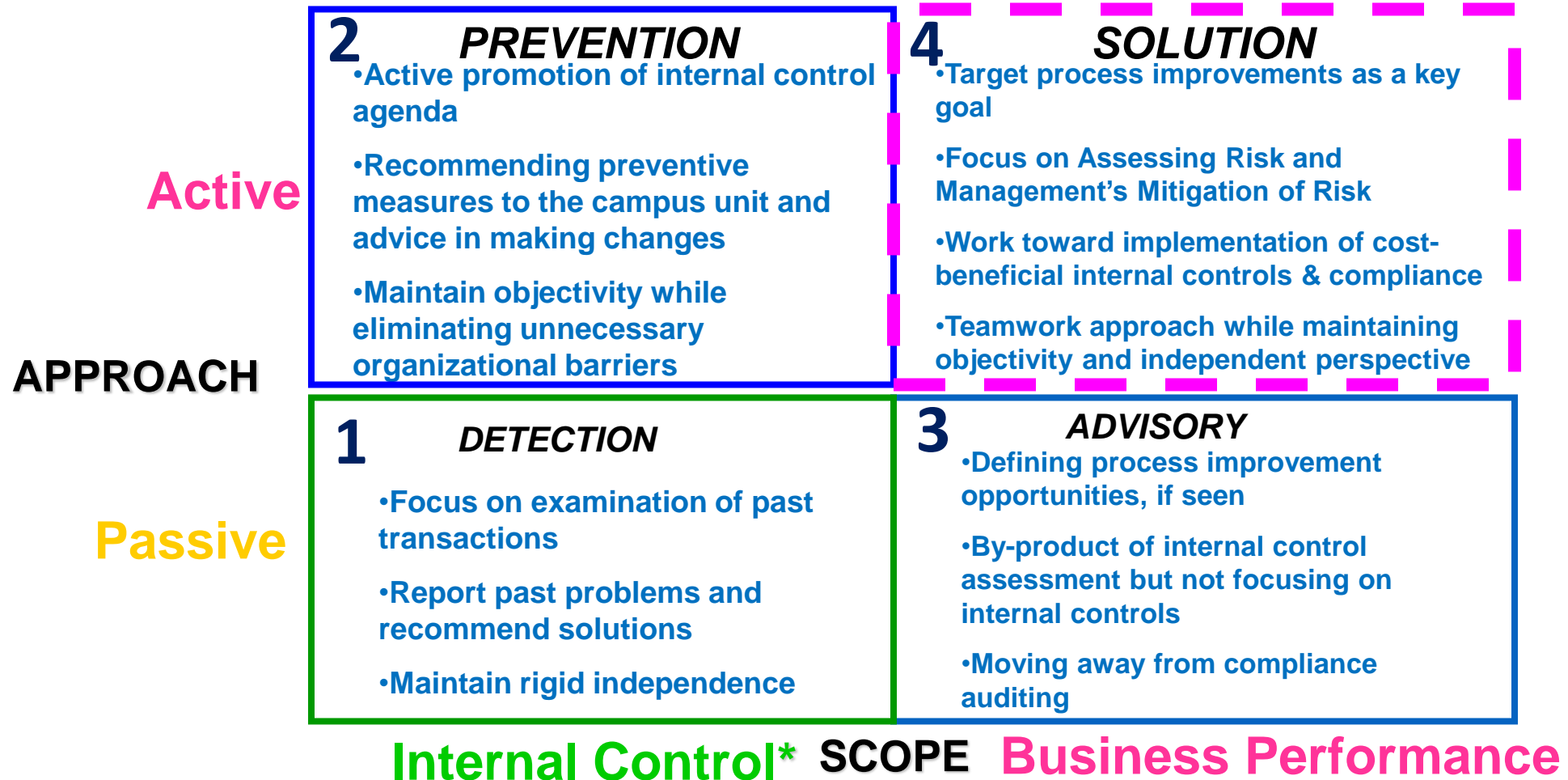
Have you read your institution's strategic plan?

- 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



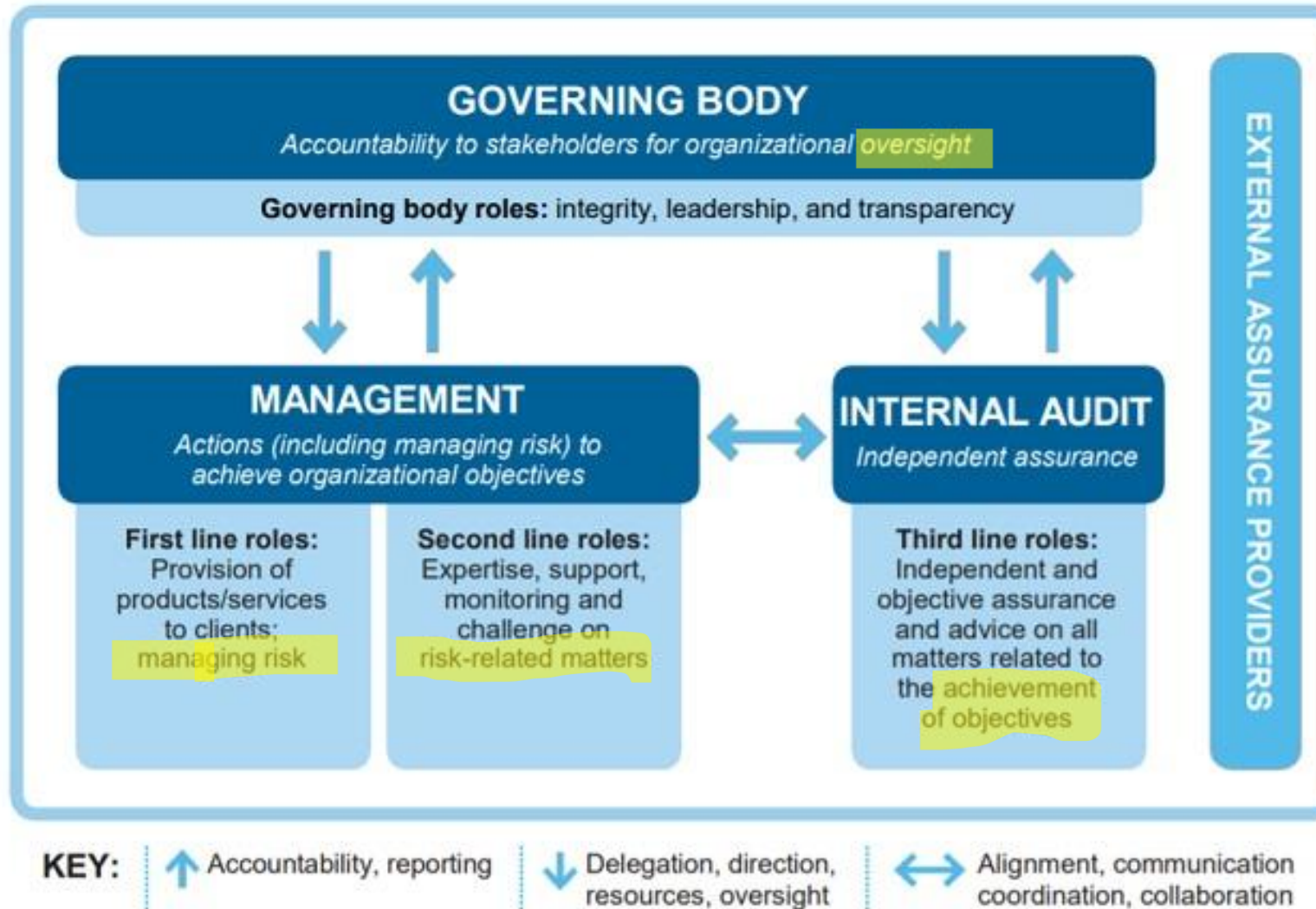
Internal Audit Primary Mission

Four Potential Orientations



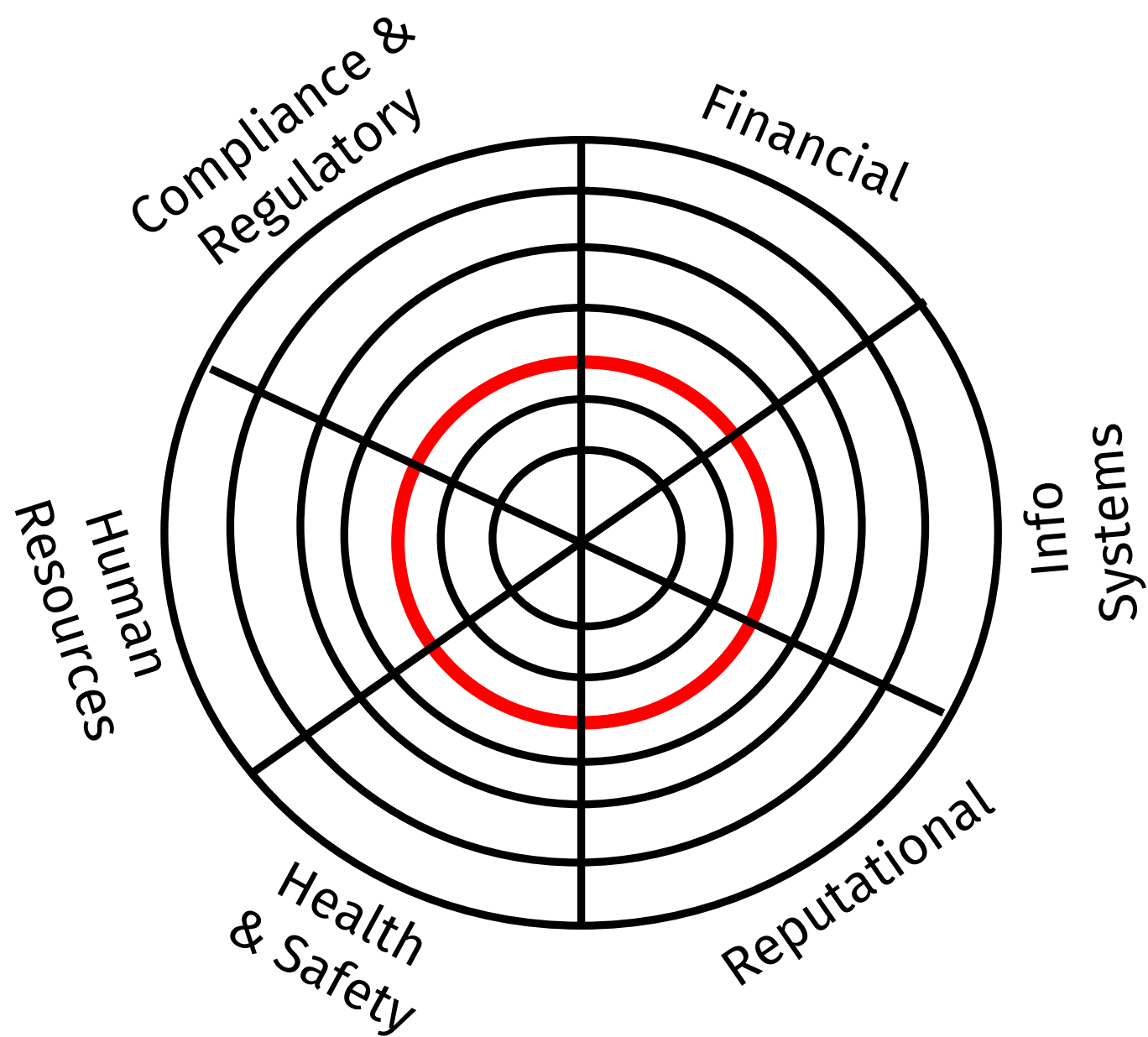
*Defined along the lines of COSO's Integrated Framework

The IIA's Three Lines Model

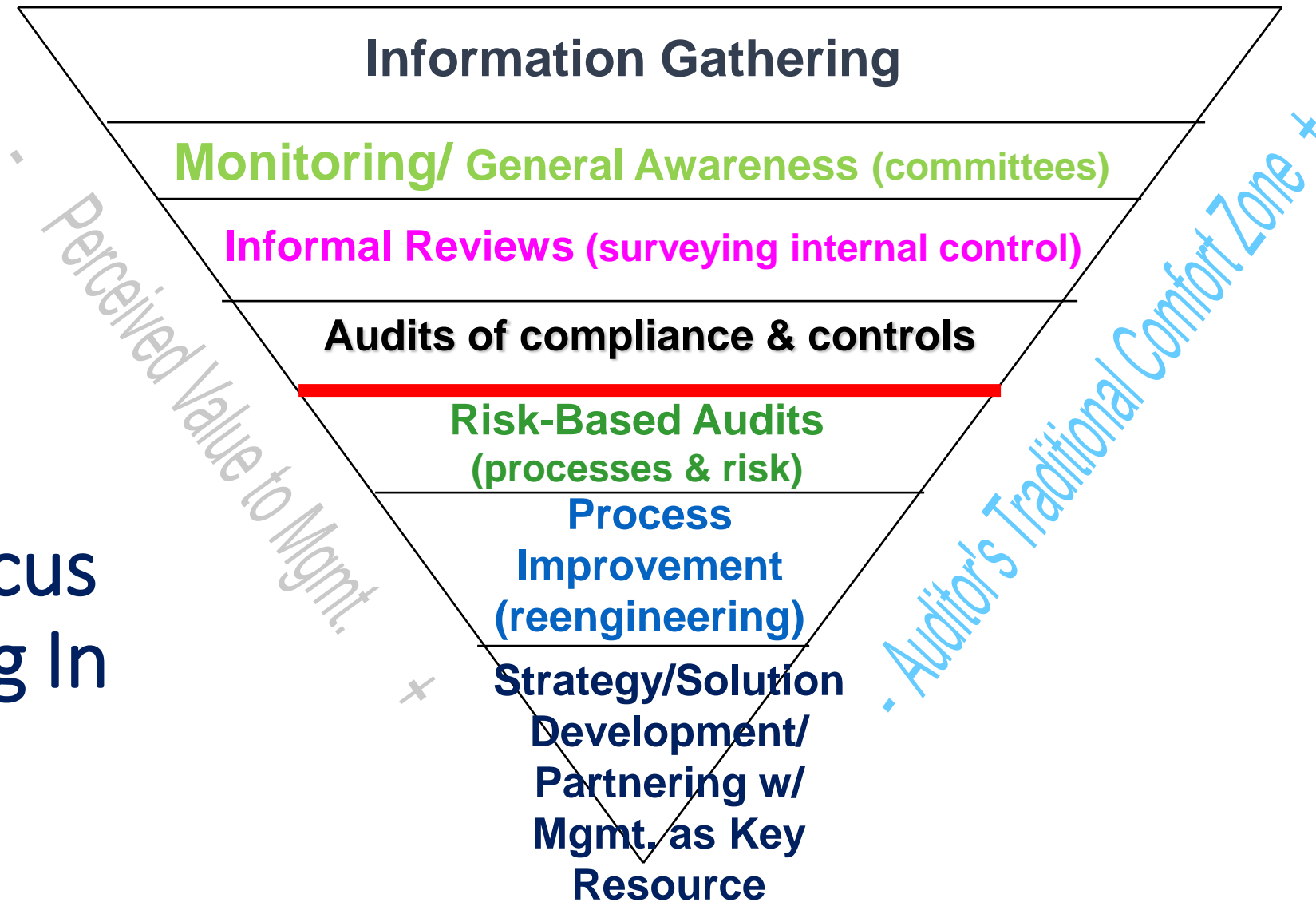


Source: Institute of Internal Auditors

Audit Risk Universe



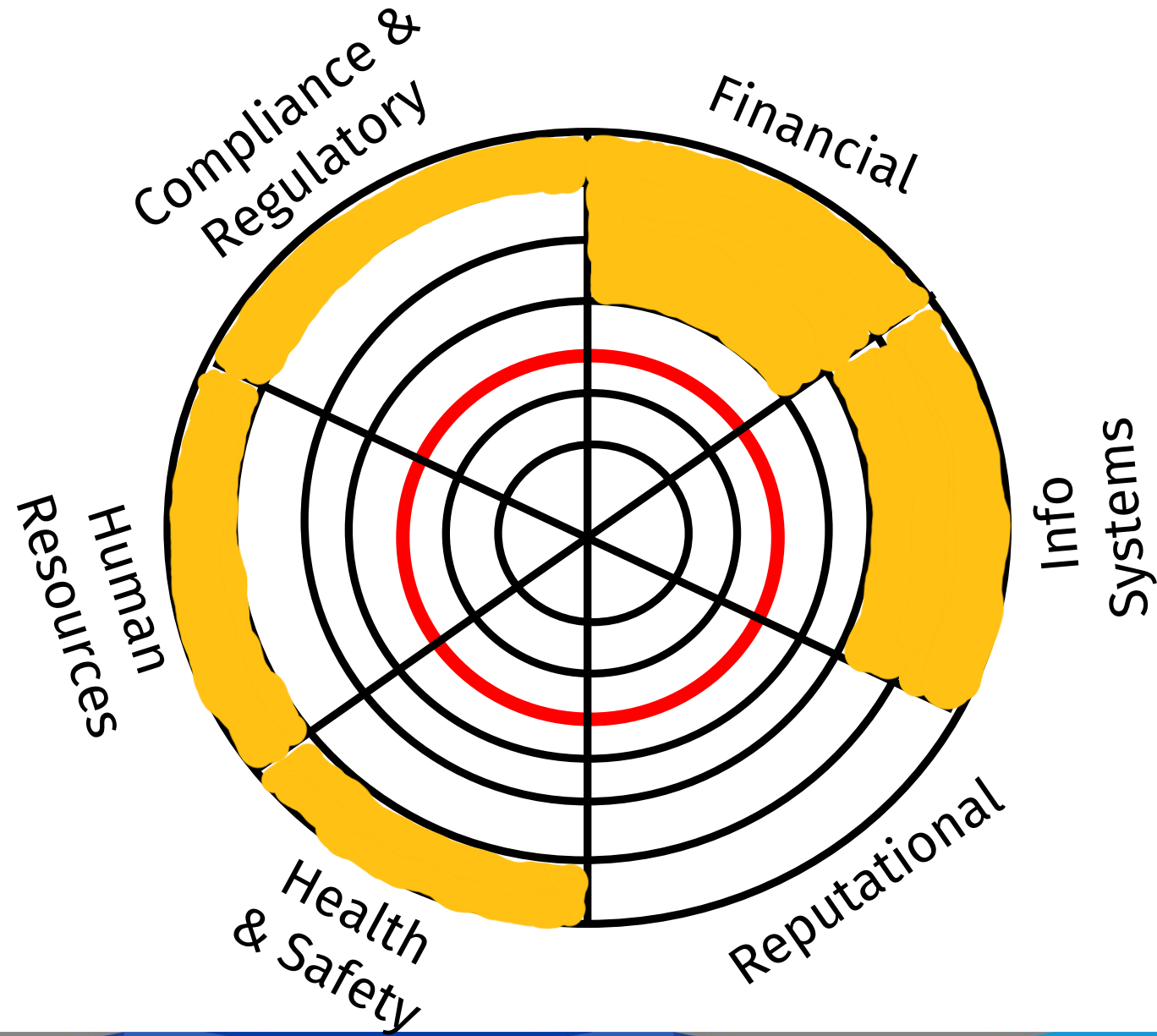
Audit Focus -- Zeroing In



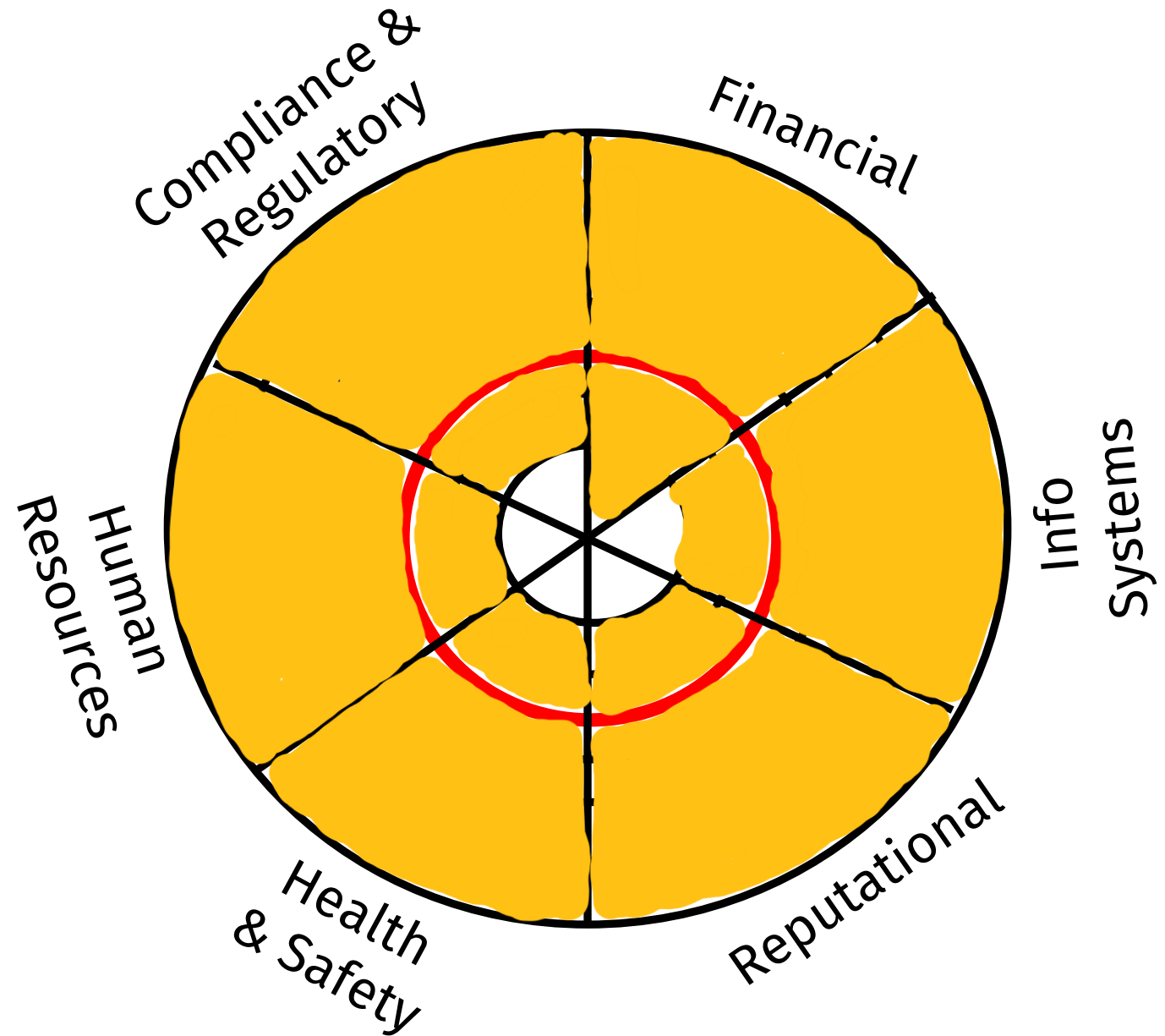
© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com



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			
				0			

What is YOUR Strategy for Risk Assessment?

It'll sort itself out



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: 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



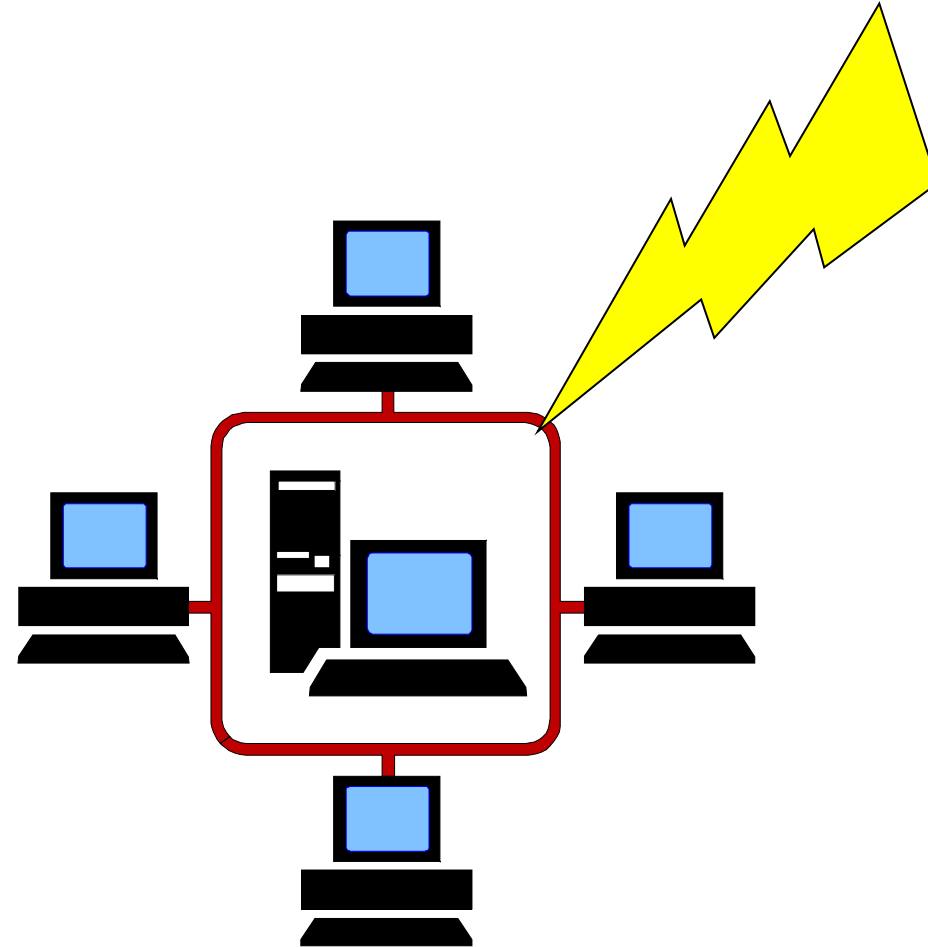
Risks: Students

- Employing students
- Protection of information
- Accommodations for disabilities
- Exam accommodations
- Exam administration
- Grievances
- Grade changes
- Withdrawals



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



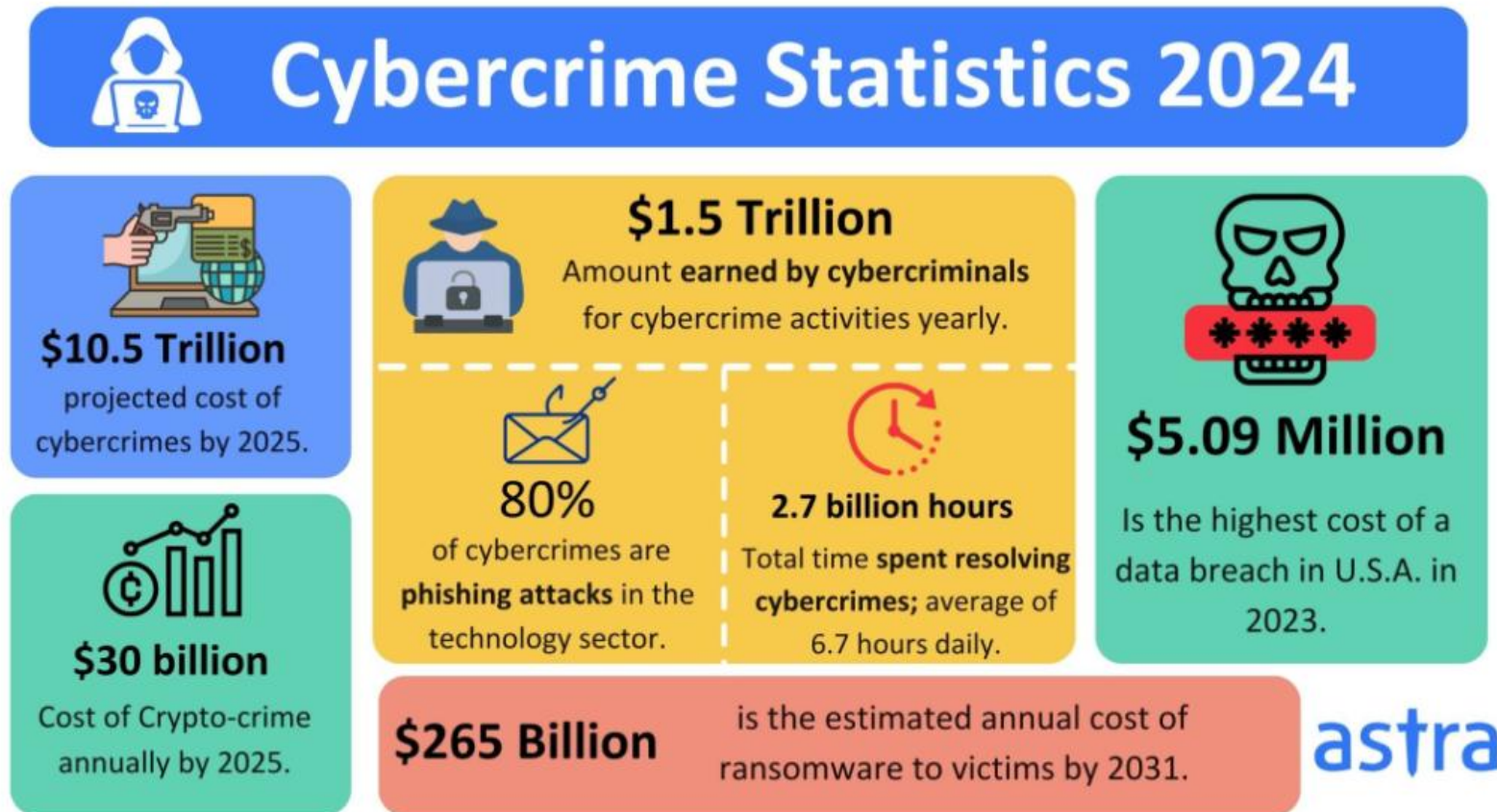
Why?

- 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



Cost of Cyber Crime

Top Cyber Crime Statistics 2024



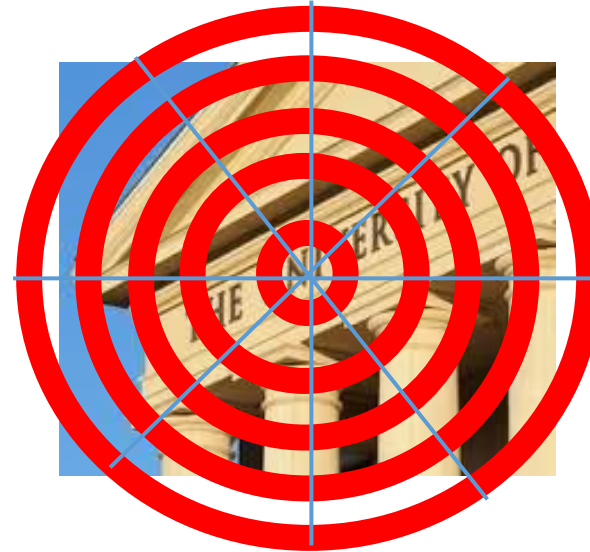
1. The next five years will see a 15% increase in cybercrime costs reaching 10.5 trillion by 2025. – [Cybercrime Magazine](#)

Source: Astra

Higher Education Growing Target

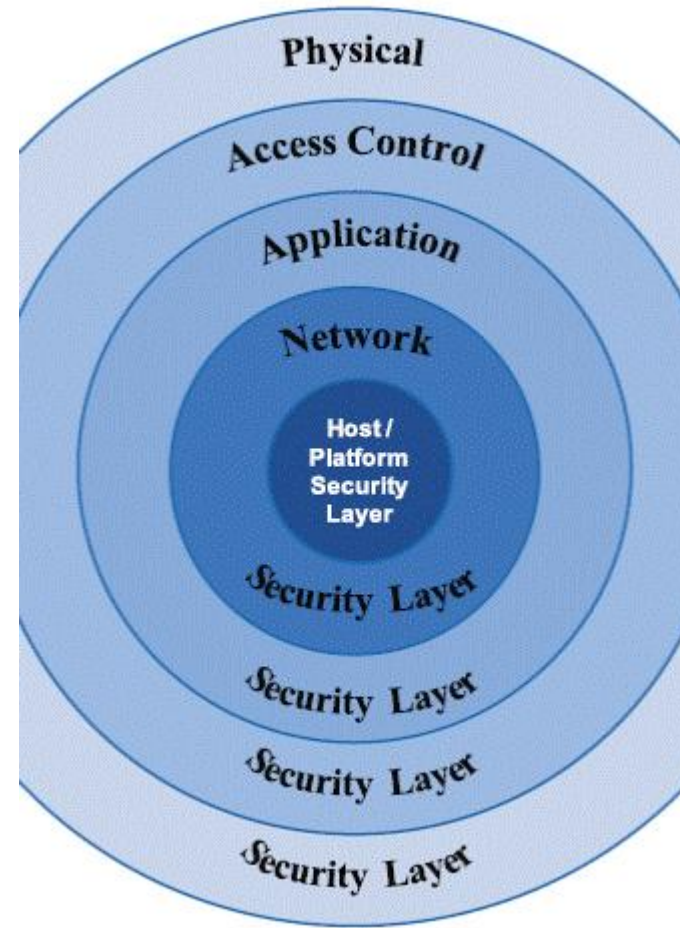
LOTS of valuable info:

- 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:

PEBCAK



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







NOTICE
DO NOT PROP
DOOR OPEN
FOR ANY REASON



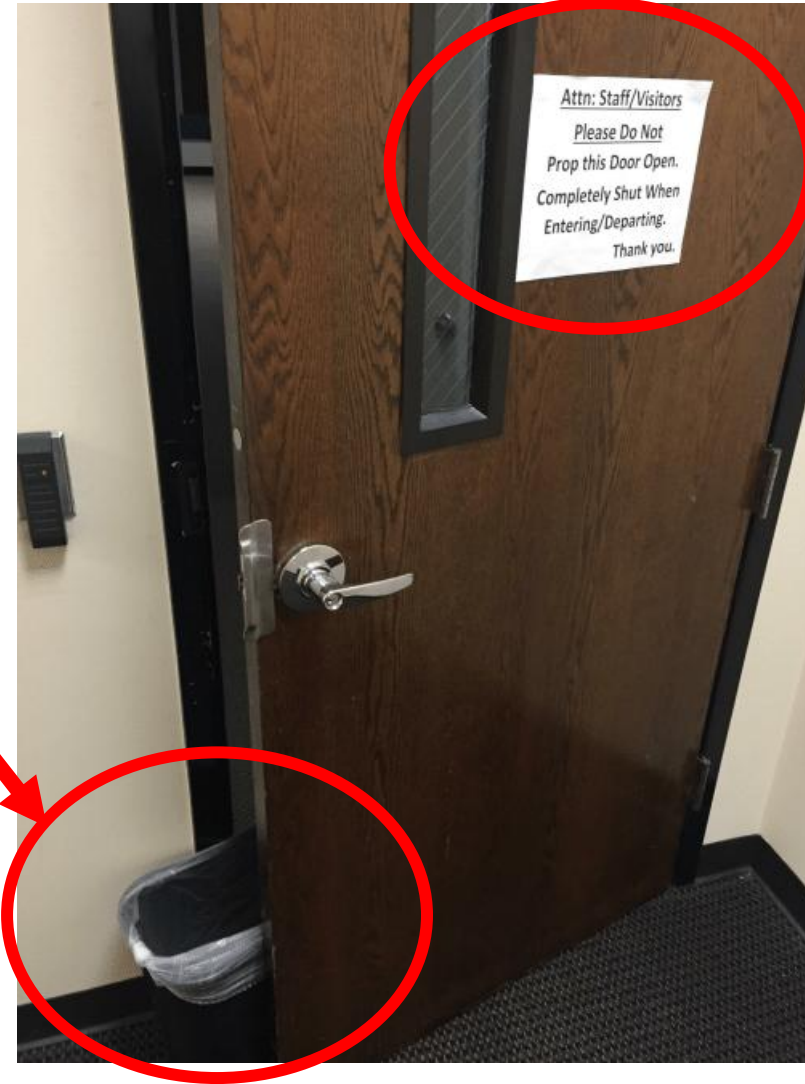


**Do not prop open
door and allow
coyotes into
sandwich shop**





**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



Spotify Account

\$2.75



Hulu Account

\$2.75



Netflix Account

\$1.00 - \$3.00



PayPal Credentials

\$1.50



Social Security Number

\$1.00



Driver's License

\$20.00



Credit Card

\$8.00 - \$22.00



Email Address & Password

\$0.70 - \$2.30



Medical Record from
Large Scale Attack

\$1.50 - \$10.00

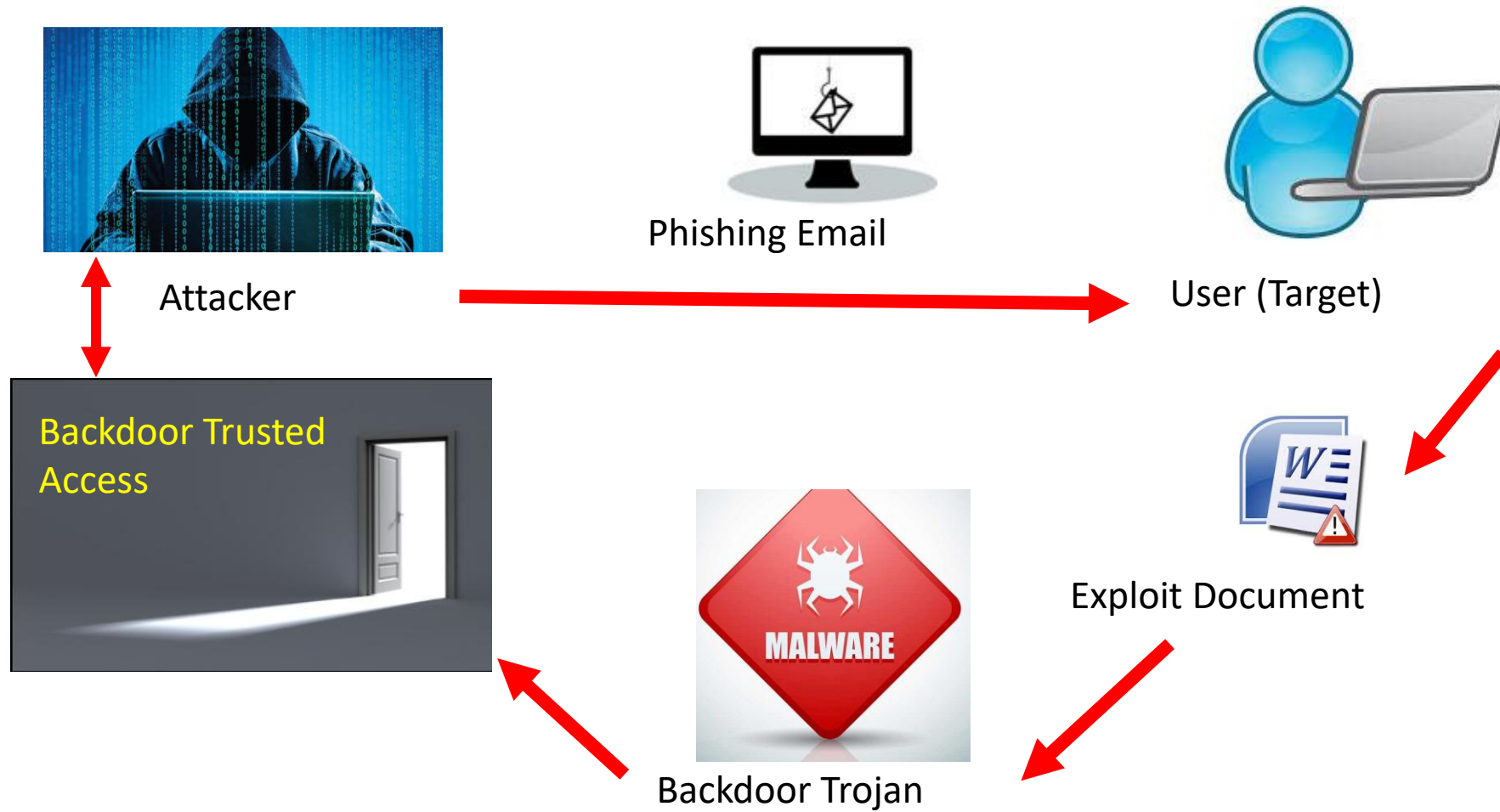


Complete Medical Record

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?



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

See my
password
on the back
side

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



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.

Source: Hive Systems

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”

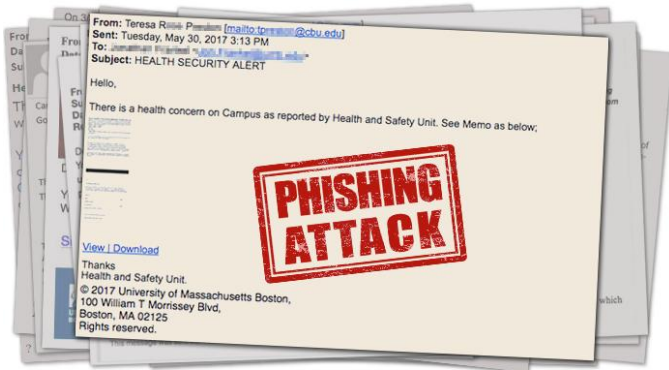
When asked why she had such a long password, she rolled her eyes and said, “Hello! I was told it had to be at least 8 characters and include at least one number and a capital.”

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@mshmoos.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](#)

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.

PO box 105603
Atlanta, GA 30348-5603

You are receiving this message as 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](#).

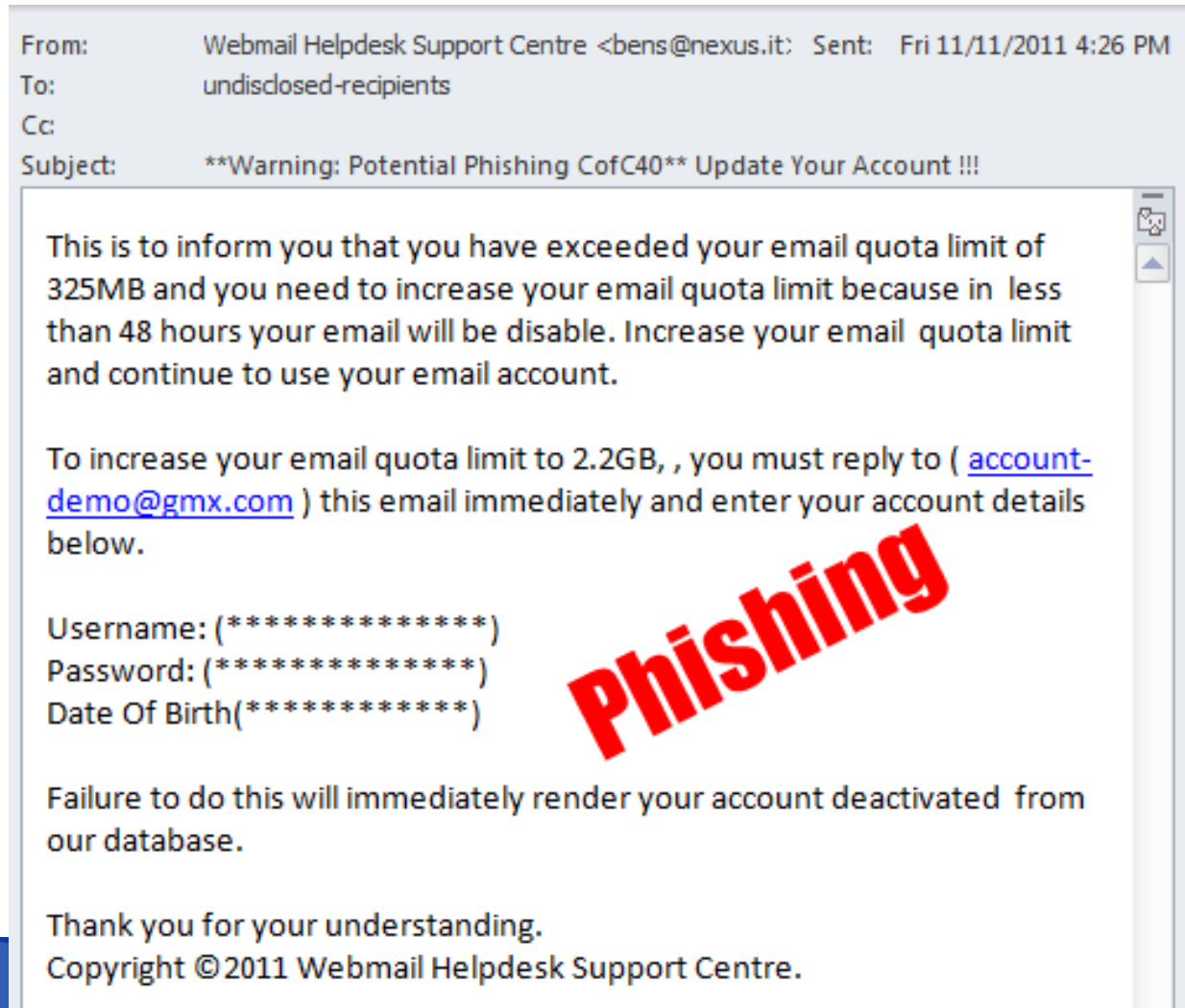
What to look for in email (cont.)

- 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.

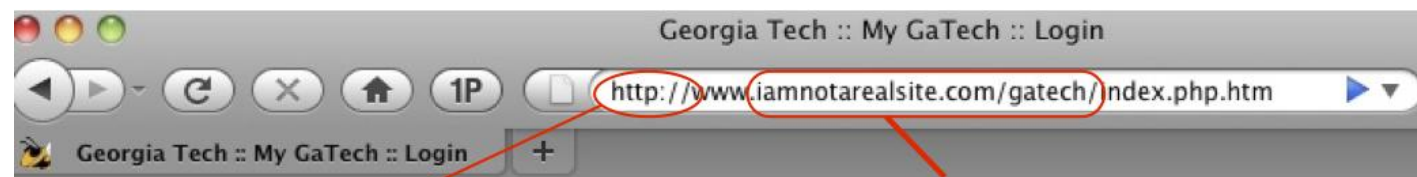


3) Never use login forms embedded in emails

- 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



Example of a Non-Georgia Tech Domain

Should be https:// not http://



Webmail Login

GT Account:

Password:

☐ Remember my account on this machine and browser.
[Why to be careful using this feature](#)

Webmail client:

OIT will never ask you to "Validate" your account.

4) Check legitimacy of email

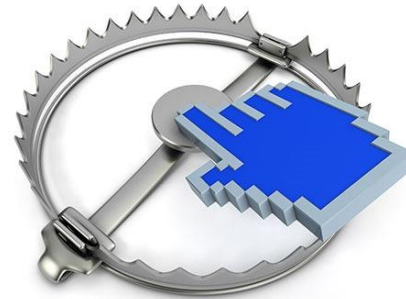
Legitimate companies are less likely to use public email providers like Yahoo, Gmail, Hotmail, Outlook, etc.

The logo for Yahoo!, featuring the word "YAHOO!" in a purple, serif font.The logo for Gmail, featuring the word "Gmail" in a colorful, sans-serif font. The "G" is blue, the "M" is red, the "a" is yellow, and the "i" is green.The logo for Hotmail, featuring an orange envelope icon with a yellow ribbon and the word "Hotmail" in a black, sans-serif font.The logo for Outlook, featuring a blue square icon with a white envelope and the word "Outlook" in a blue, sans-serif font.

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)

Stop! Don't click that link!



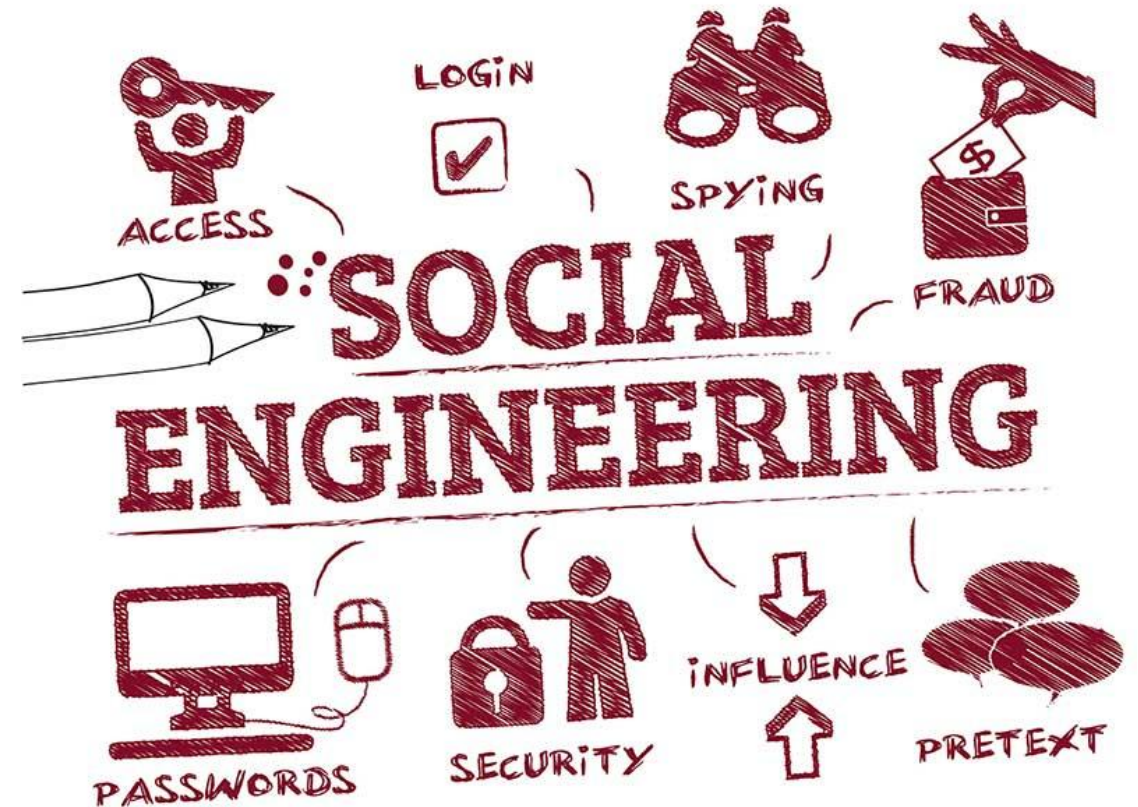
Other IT Security Effective Practices

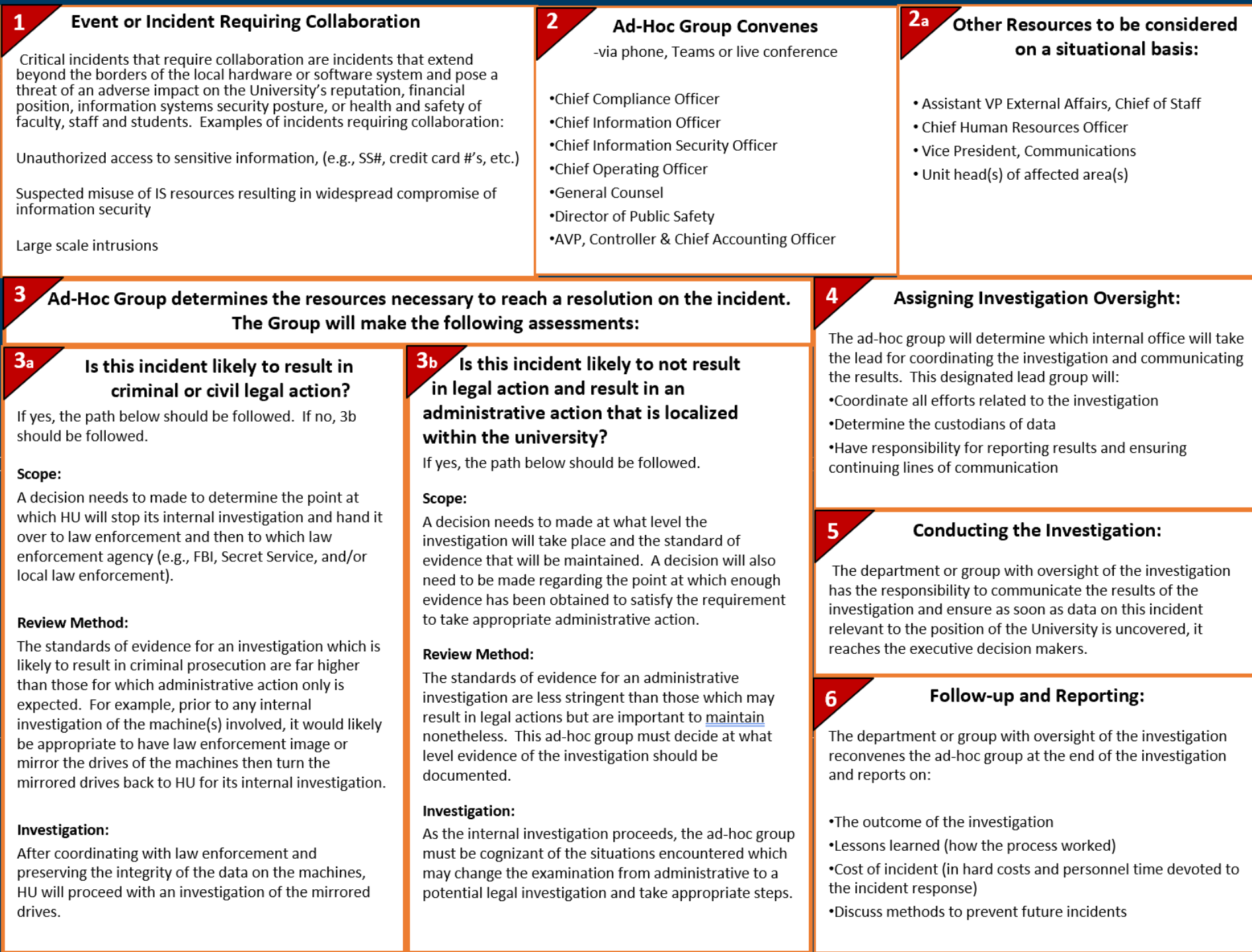
- Develop clear computer use policies for employees and 3rd party vendors
- Restrict users from having administrator access
- Review user access in each dept. to ensure “need-to-know” for each user
- Regularly update system software and antivirus software (don’t forget other devices, e.g., printers,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

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



Don't become the weakest link...

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

“ID – 10 –T”

IDIOT



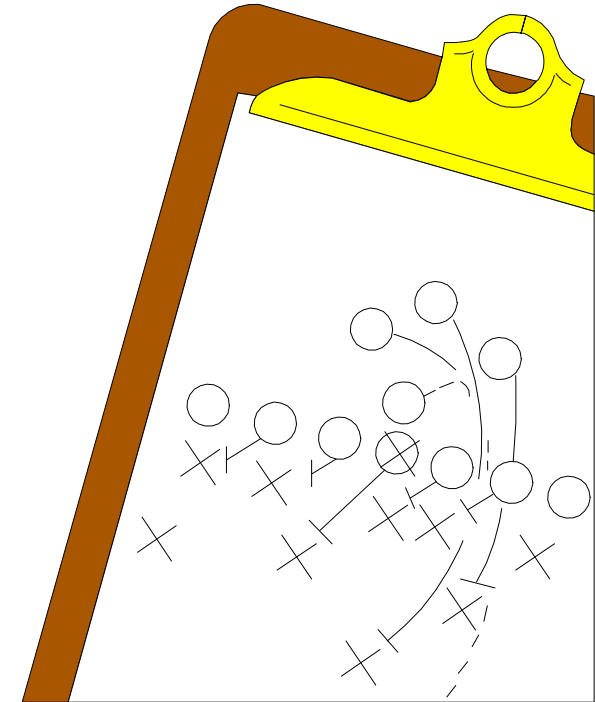
IT Security...

... is **EVERYBODY'S** responsibility



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 ?**



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 2025 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

AREA OF RISK MITIGATION	Low Risk	Medium-low Risk	Medium Risk	Medium High	High Risk	Page
EXECUTIVE SUMMARY						
FISCAL – Policies, Procedures, Training						2
Accuracy of Financial Records						3
Payroll Processing						4
Procurement						5
Procurement Card						6
Travel						7
Sponsored Programs						8
Tuition Remission						9
HR– Policies, Procedures, Training						10
Hiring/Onboarding process						11
Consultants vs. Employees						12
Compliance with EEOA & Title IX						13
Performance Evaluations						14
Conflict of Interest						15
Bison One Card						16
Student Time Reporting						17
IT – Policies, Procedures, Training						18
Business Continuity of Info Systems						19
Physical and Environmental Controls						20
Website Operation						21
STUDENTS- Policies, Procedures, Training						22
Accommodations for Disabilities						23
Exam Accommodations						24
Final Exam Schedule & Administrative						25
Exam Administration						26
Grievances						27
Grade Changes						28
Withdrawals						29
Structural Analysis						30
Protection of Information						31

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



Rob Clark, Jr. © 2025

Management Response vs Corrective Action Plan

- Management responses are initial high-level views of actions that management commits to take.
- Corrective Action Plans provide a greater level of detail to address these actions.

Corrective Action Plan / Risk Assessment Evaluation

Finding/Area of Risk:

Primary Point Person:

•

A. Audit Finding/Area of Risk and Current Condition:

B. Risk: Adverse Situation that Could Occur (or has occurred):

C. Impact this risk would have: (1, low, to 5, high)

D. Explanation of Impact Rating:

E. Vulnerability: (1, low, to 5, high)

F. Risk Rating: (Impact X Vulnerability)

G. Explanation of Vulnerability Rating:

H. Cause for Condition:

I. Management Response from Audit Report:

Detailed Action Plan to Mitigate Risk:

J. Specific Steps/Tasks that Must be Taken to Mitigate the Risk	K. Responsible Office & Individual	L. Timeframe to Complete	M. Status

N. Other organizational units involved:	Action Steps Other Units Must Take:

O. Potential Obstacles/Challenges to Mitigating the Risk:			

P. Status of Implementation Actions for Sustainability:

Q. Who Initiates Action:

When:

R. How Is This Action Documented:

When:

S. Who Monitors that Action (in Q) was Taken and Completed:	When:

T. Comments:

U. This document completed by:_____ Date:_____

V. Reviewed and approved by:_____ Date:_____

W. Reviewed and vetted by Internal Audit and Compliance Office by:_____ Date:_____

Corrective Action Plan (CAP) Dashboard

2022-005	Disbursements to or on Behalf of Students - Credit Balances	Initial Risk Ranking	Risk Ranking to Date	Office of the Bursar									
		8	4	Risk Mitigating Steps									
	Number of Risk Mitigating Steps	6		1	2	3	4	5	6				
	Comments:	% of Completion											
	Full engagement and implementation of a business continuity plan would be most effective after Workday has been implemented. Familiarity with Workday will be required for the effectiveness of the business continuity plan.			100%	80%	100%	100%	100%	100%				
		Target Completion Date		12/31/21	12/31/23	08/31/23	01/30/24	09/30/23	12/31/23				
2022-006	Procurement and Suspension and Debarment	Initial Risk Ranking	Risk Ranking to Date	Office of Procurement and Contracting									
		20	20	Risk Mitigating Steps									
	Number of Risk Mitigating Steps	8		1	2	3	4	5	6	7	8	9	10
	Comments:	% of Completion											
	OPC currently reviews all POs over \$25,000.			100%	100%	50%	75%	100%	75%	50%	75%	50%	50%
		Target Completion Date		September 2022	November 2022	October 2023	June 2025	September 2022	June 2025	June 2025	12/31/2024	7/30/2025	7/30/2025

Risk Key Percentage of Completion

High Risk: 0-25% or information not supplied

Medium Risk: 26-75% or due date not yet passed

Low Risk: 76-100%

Risk Key Percentage of Completion

	High Risk: 0-25% or information not supplied
	Medium Risk: 26-75% or due date not yet passed
	Low Risk: 76-100%

Reporting to Senior Leadership and Board

- The most critical part of the Audit
- Incorporate different presentation techniques
- Formatting of reports
- Use of visualization
- De-mystify technical subjects into laymen's terms
- Competent oral presentation



Join at menti.com | use code 1536 9564

Mentimeter

Info Audit Committees Want More of from Audit



- 1st | Audit plan and changes to it
- 2nd | Implementation of new IIA Standards
- 3rd | Status of Corrective Action Plans
- 4th | Systemic governance issues
- 5th | Highest-impact emerging risks
- 6th | Trends in root causes
- 7th | Cost-reducing process improvements
- 8th | Risk Management culture of org.



Menti

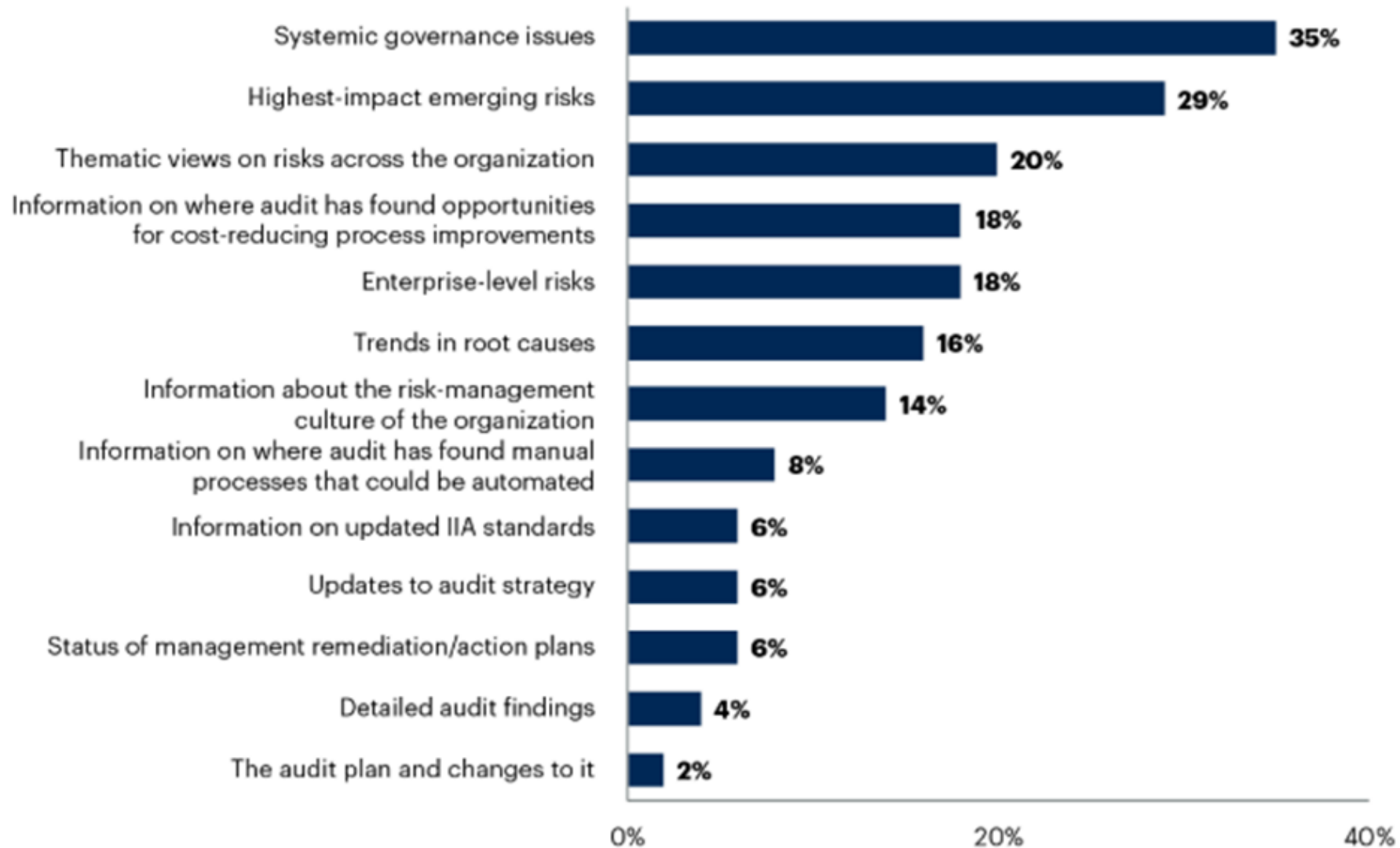
What ACs want more of ...

Choose a slide to present



Information That ACs Want More of From Audit

Percentage of respondents selecting more or significantly more



n = 49

Q: Of the following types of information provided to you by internal audit, please indicate which you would like to receive more or less of?

Source: 2024 Gartner Audit Committee Priorities and Preference Survey

823808_C

Source: Gartner

Audit Committee Presentation – Dos & Don'ts

Keep it simple and concise

- Think “Executive Summary”
- Put details in appendix and verbally refer to it if relevant to discussion
- If you had only 5 minutes, what are the main points on which you would focus?



Audit Committee Presentation – Dos & Don'ts

Focus on trends rather than point-in-time assessments

- How is the risk profile and audit's work evolving over time?
- What are the largest and highest-important matters, concerns that are thematic or systemic?
- What are the reasons behind an increase or decrease?



Audit Committee Presentation – Dos & Don'ts

Focus on content, not delivery platform

- Make sure the emphasis is on the subject matter, not the fancy graphics



Audit Committee Presentation – Dos & Don'ts

Provide the full context

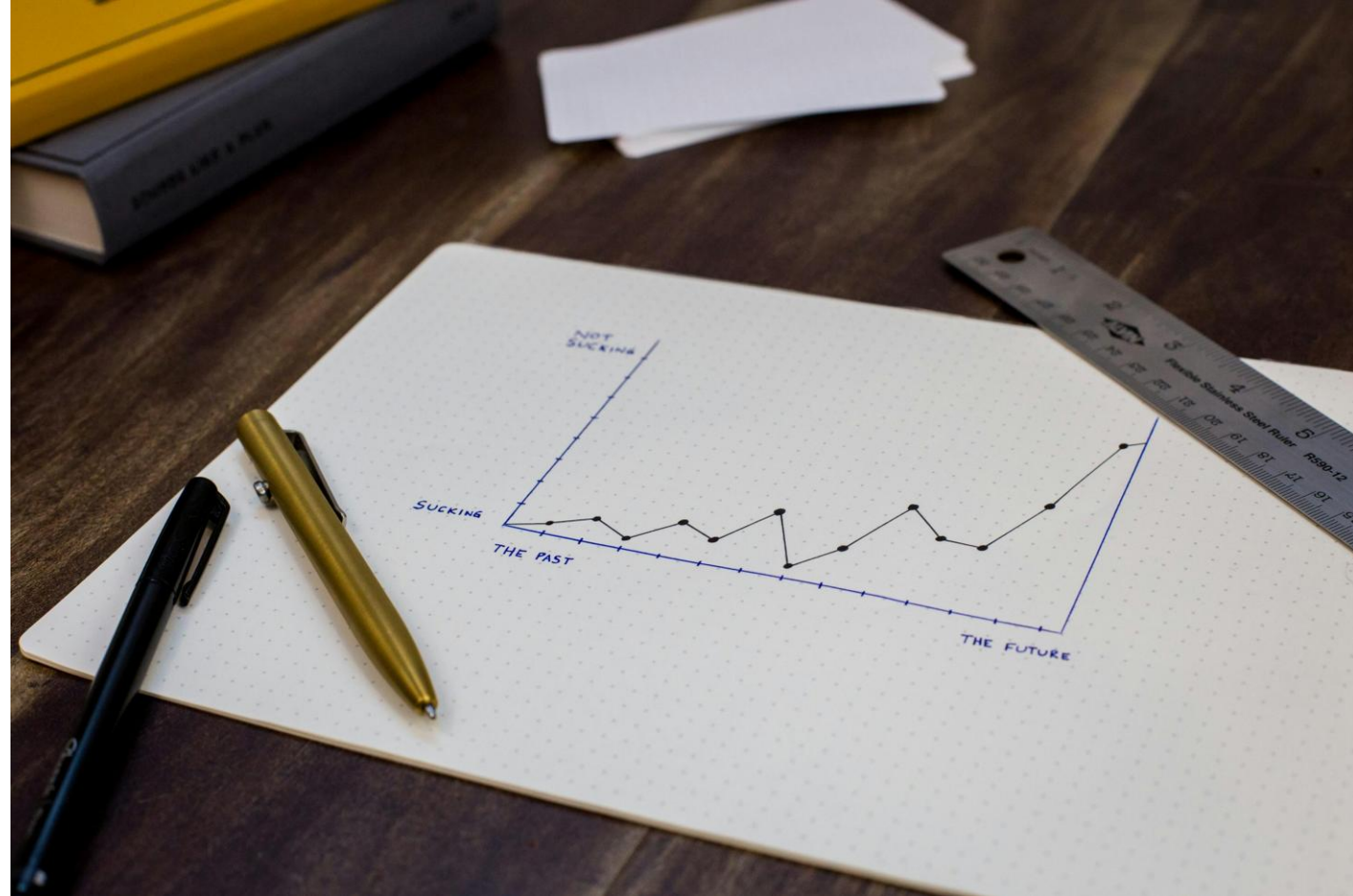
- Include data from other assurance functions
- Provide board with full understanding of organization's risk management posture



Audit Committee Presentation – Dos & Don'ts

Use visuals when appropriate

- Can the data be better expressed in a visual form
- Simplify the visual to make the main point clear
- More is not better



Take-aways

- Read & align with your strategic plan
- Be attentive to emerging risks and A.I.
- Incorporate data analytics and continuous monitoring
- Focus on meeting expectations of board
- Continually promote cybersecurity practices
- Implement robust Corrective Action Plans
- Be intentional about enhancing your presentation skills



Be an agent of change



CUAV

Scan this QR code



Or go to

<https://talk.ac/robclarkjr>

and enter this code when prompted

TALK

Robert.Clark@howard.edu
RobClarkSpeaking@gmail.com
770.815.7922
[linkedin.com/in/robclarkjr/](https://www.linkedin.com/in/robclarkjr/)
www.RobClarkJr.com

