

MSI Presidential Leadership Summit

Managing the Institution's Most Critical Risks: An Enterprise Risk Management Approach to Managing Cyber and Fraud Risks

Dr. Michael Dean
Ms. Kathy Zelnik
Mr. Wally Coy
Ms. Stephanie Powell

U.S. Department of Education
FSA 2019 Presidential Leadership Summit

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

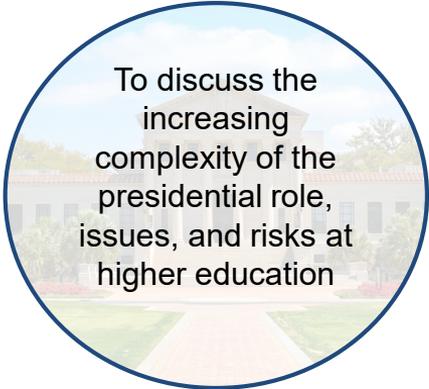
PROUD SPONSOR of
the AMERICAN MIND®

December 2019

Introduction

- Objectives
- Institutional Leadership and Risk Context
- Enterprise Risk Management: Enabling Strategy
- Managing Cybersecurity Risk
- Managing Fraud Risk

Objectives



To discuss the increasing complexity of the presidential role, issues, and risks at higher education



To discuss how Enterprise Risk Management may be used to enable strategy and manage risks institution-wide

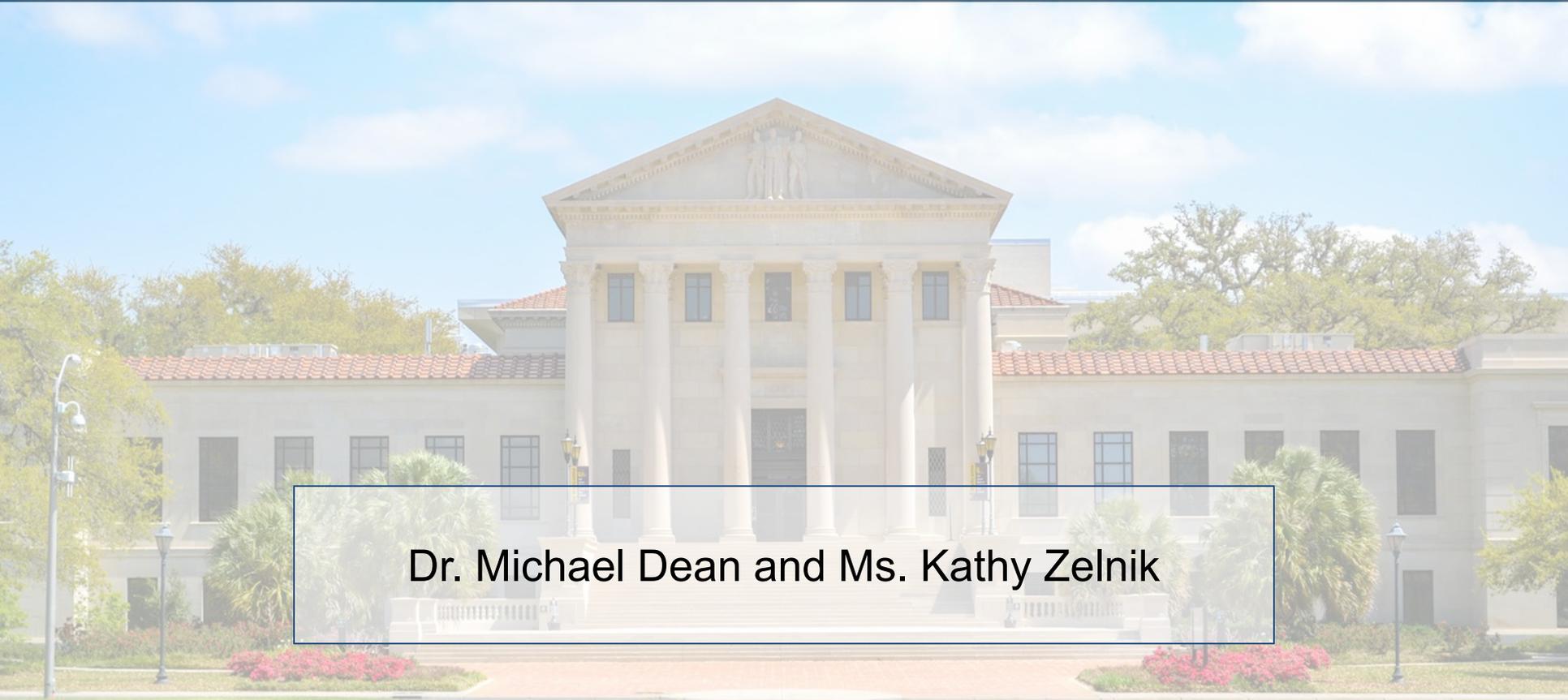


To improve cybersecurity risk knowledge and discuss management of cybersecurity risks



To improve fraud risk knowledge and discuss management of fraud risks

Institutional Leadership and Risk Context



Dr. Michael Dean and Ms. Kathy Zelnik

Institutional Leadership and Risk Context



College presidents find themselves in a setting that is unprecedented in its complexity.
American Council on Education (2018)

Institutional Leadership and Risk Context

Complexity and the Presidential Role

| 20-30 Years Ago | Today |
|------------------------------|-----------------------------|
| Fundraising | Fiscal Solvency |
| Athletics Performance | Severe Enrollment Pressures |
| Curriculum | Education Disruptors |
| Tradition Keeping | Outcomes |
| Budget Planning | Cybersecurity |
| Physical Plant | Sexual Assault |
| Routine Compliance | Athletics Scandals |
| | Active Shooters |
| | Evolving Compliance |
| Siloed Accountability | President First |

Institutional Leadership and Risk Context

Seven Critical Issues Facing
Higher Education
Risk and Insurance (2018)



- 1 Fiscal Solvency
- 2 Athletic Concussion Injury
- 3 Sexual Assault
- 4 Gender Equality Issues
- 5 Erosion of Public Trust in Higher Education
- 6 Campus Crisis Readiness
- 7 Cybersecurity

Institutional Leadership and Risk Context

Seven Challenges Facing Higher Education Forbes Magazine (2017)

- 1 Cost is turning off potential customers, alienating public
- 2 Increase in federal financial aid linked to increase in regulation
- 3 Less expensive approaches to certifying competence, disruption of traditional higher ed
- 4 Traditional role of colleges as a place for divergent ideas continually under attack
- 5 Slow economic growth and aging population reducing resources
- 6 The value of a college degree as a device to signal knowledge, intelligence, and skills is fraying
- 7 At large campuses intercollegiate athletics has become too costly, exploitive, and heightened public awareness of scandals

Institutional Leadership and Risk Context



Enterprise Risk Management (ERM) and Enabling

Kathy Zelnik



What is Enterprise Risk Management?

Risk:

The possibility that events will occur and affect the achievement of strategy and business objectives.

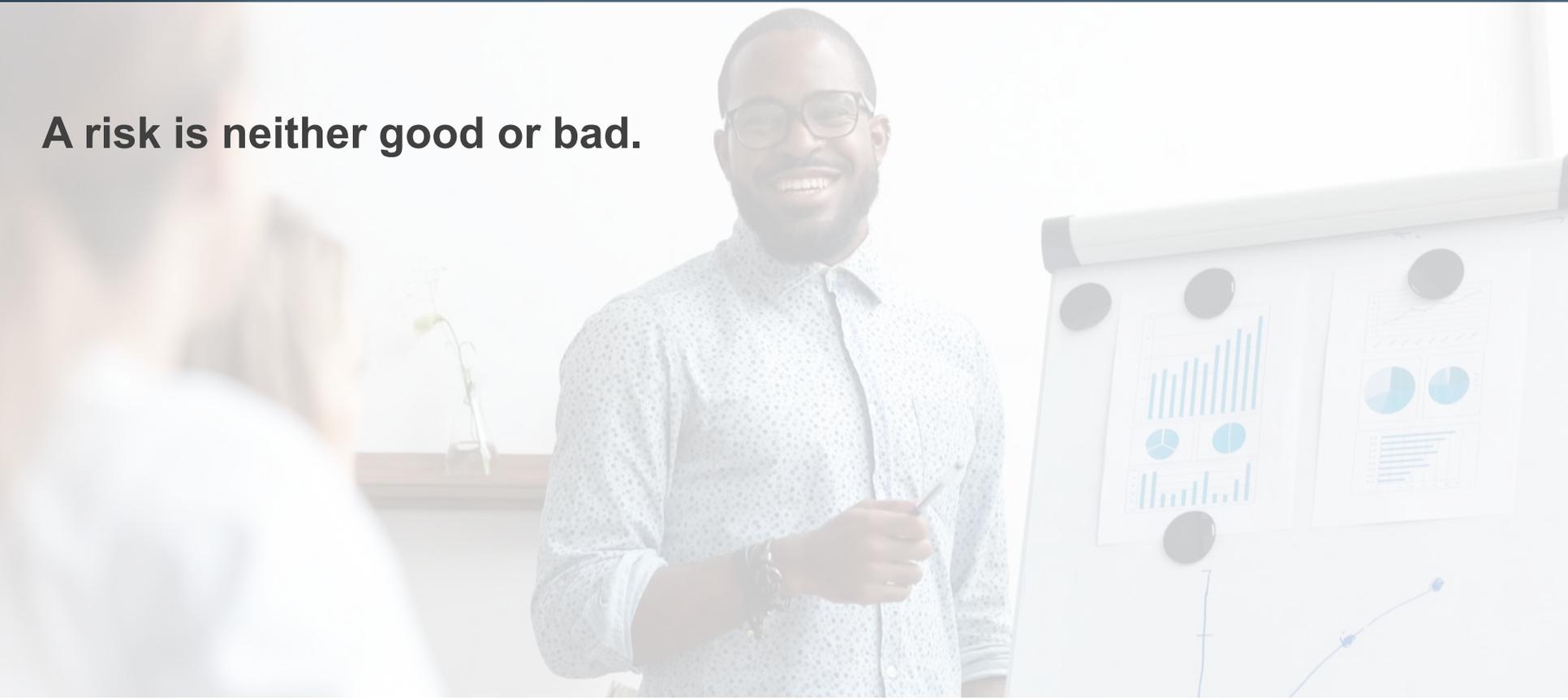
Enterprise Risk Management:

The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value.



Introduction to ERM

A risk is neither good or bad.



Why ERM?

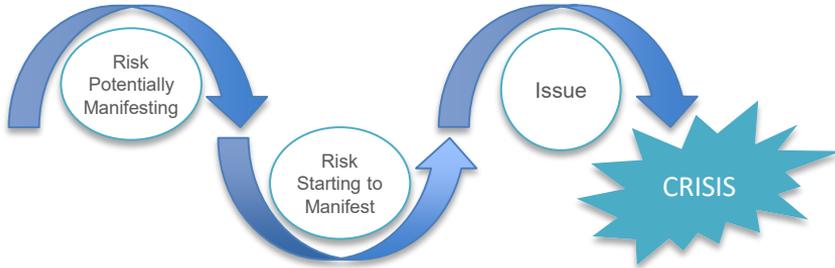
Without risk, there is no discovery, there's no new knowledge, there's no bold adventure... the greatest risk is to take no risk."

Why do cars have brakes? To let them go faster!

- June Rogers, widow of Challenger commander
Dick Scobee

Why ERM?

Avoid Crisis Management



Avoid a Bad Outcome



Achieve Better Results



ERM's Value: Improving Business Outcomes

- 1 Opens and improves the channels for **communication and dialogue** about opportunities and risks by providing transparency at the enterprise level.
- 2 **Increases positive outcomes** while reducing negative surprises.
- 3 Offers a comprehensive view of risk **across an organization** from both a “top-down” and “bottom-up” perspective.
- 4 Allows for more **informed decision-making**.
- 5 Encourages a more **proactive** approach to risk management resulting in “fewer surprises” that may negatively impact the organization’s mission and reputation.
- 6 Provides and organization with **standardized** tools to use in managing risk and sharing risk information.

ERM's Value: Improving Business Outcomes



Discussion of integrating strategy and risk is elevated through three different dimensions

- 1 The possibility of strategy not aligning with mission, vision, and core values
- 2 The implications from the strategy chosen
- 3 Risk to strategy and performance

Graphic from COSO's *Enterprise Risk Management – Integrating with Strategy and Performance*

Attributes of a Strong ERM Program

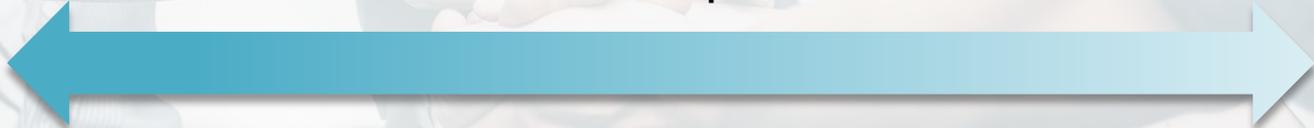


Graphic from COSO's *Enterprise Risk Management – Integrating with Strategy and Performance*

Where Does Risk Management Start?

At the top!

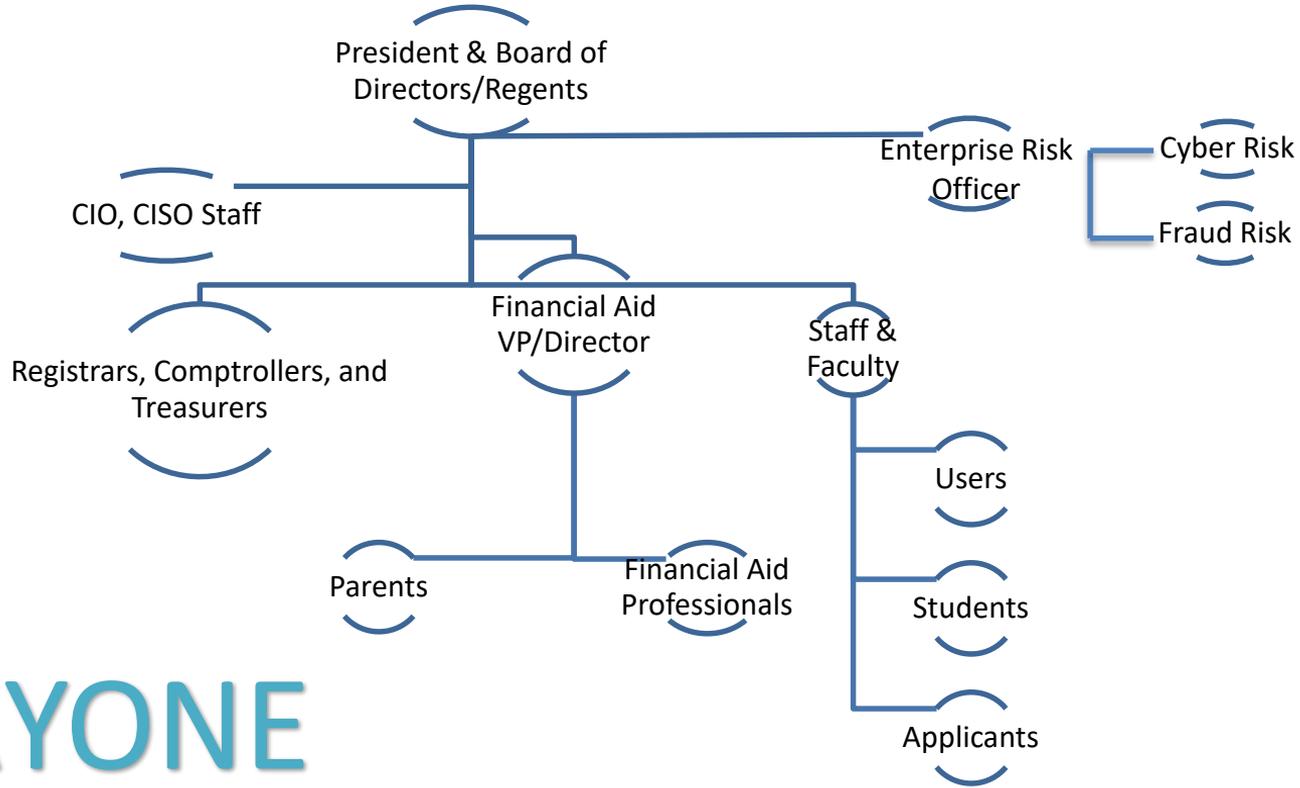
Risk Transparent



Risk “Secretive”

Risk Aware

Who is Responsible for Risk Management?



EVERYONE

Managing Cybersecurity Risk

Mr. Wally Coy, CRISC,
CISM, CISA, CISSP

First Some Definitions

From a cybersecurity perspective (i.e., Confidentially, Integrity, Availability of data, information, and/or information technology systems) the following definitions (based on NIST guidance) are generally accepted:

Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Vulnerability - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Risk (Information Security Risk) - The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

Risk Mitigation - Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Cybersecurity Risks

The consequences of a cyber breach can include:

Compromised
Personally Identifiable
Information (PII)

Corrupt data such as
financial transactions and
academic records

Denial of access to critical
applications, systems, and
services

Enabling possible identity
theft and fraud scenarios

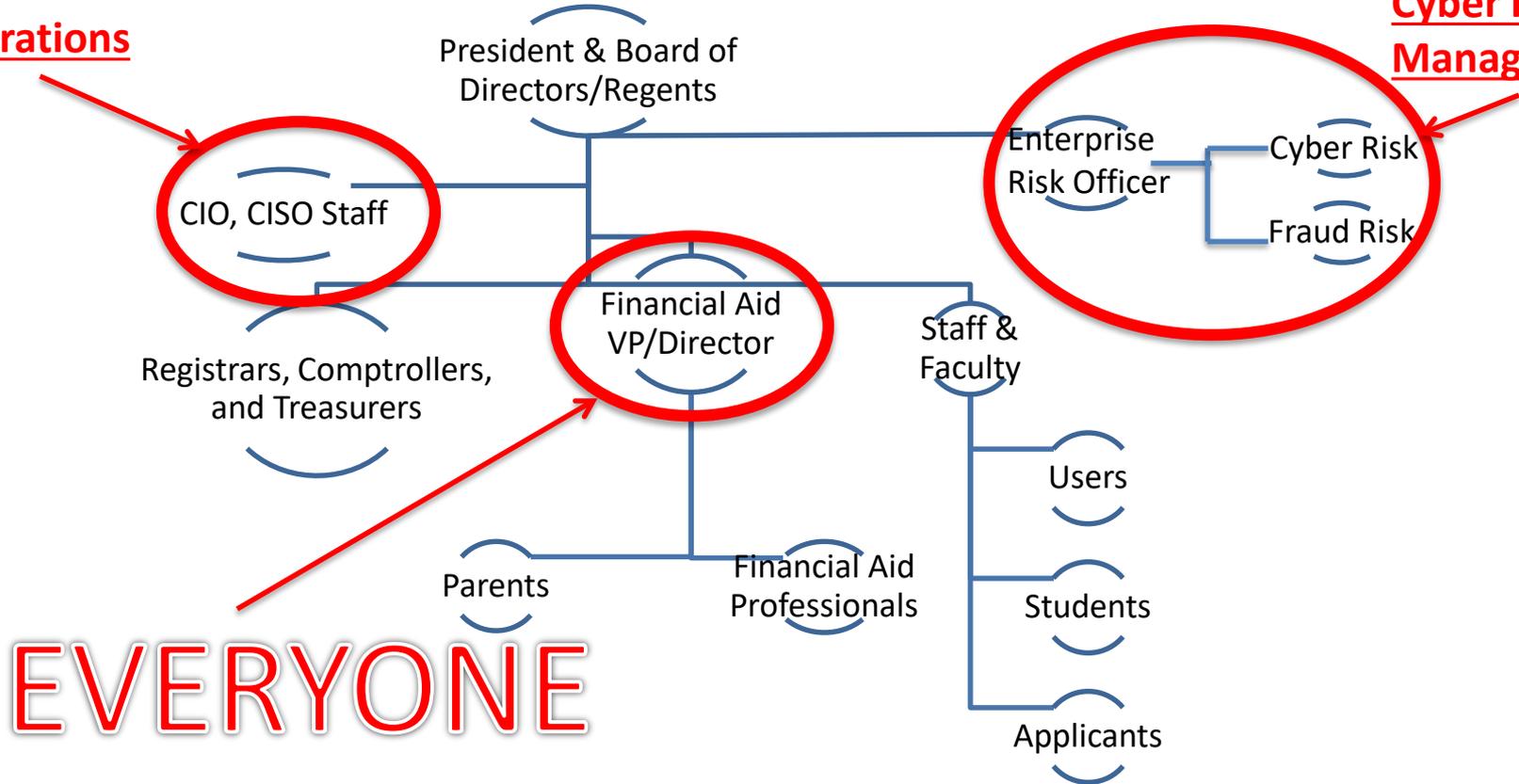
Potential reputational
damage to your institution

~ 90% of cybersecurity risks can be mitigated with good basic security controls or **“Cyber Hygiene” & User Education and Awareness**

Who is Responsible for Cyber Risk Management?

IT Operations

Cyber Risk Management



EVERYONE

Top 5 Cyber Threat Vectors



Cyber threats most likely will exploit vulnerabilities associated with:

1. Human Behavior
2. Network Connectivity
3. Endpoint Devices
4. Authentication
5. App Stores

Top 5 Phishing Attacks



1. **Smishing** – phishing using SMS texts

2. **Spy-Phishing** – phishing using keyloggers

3. **Vishing** – phishing using phone calls

4. **Pharming** – phishing using redirection to fake websites

5. **Watering Hole Attacks** – phishing using typical websites used by targets (e.g. students, administrators, academic staff)

Account Takeover (ATO) Attacks

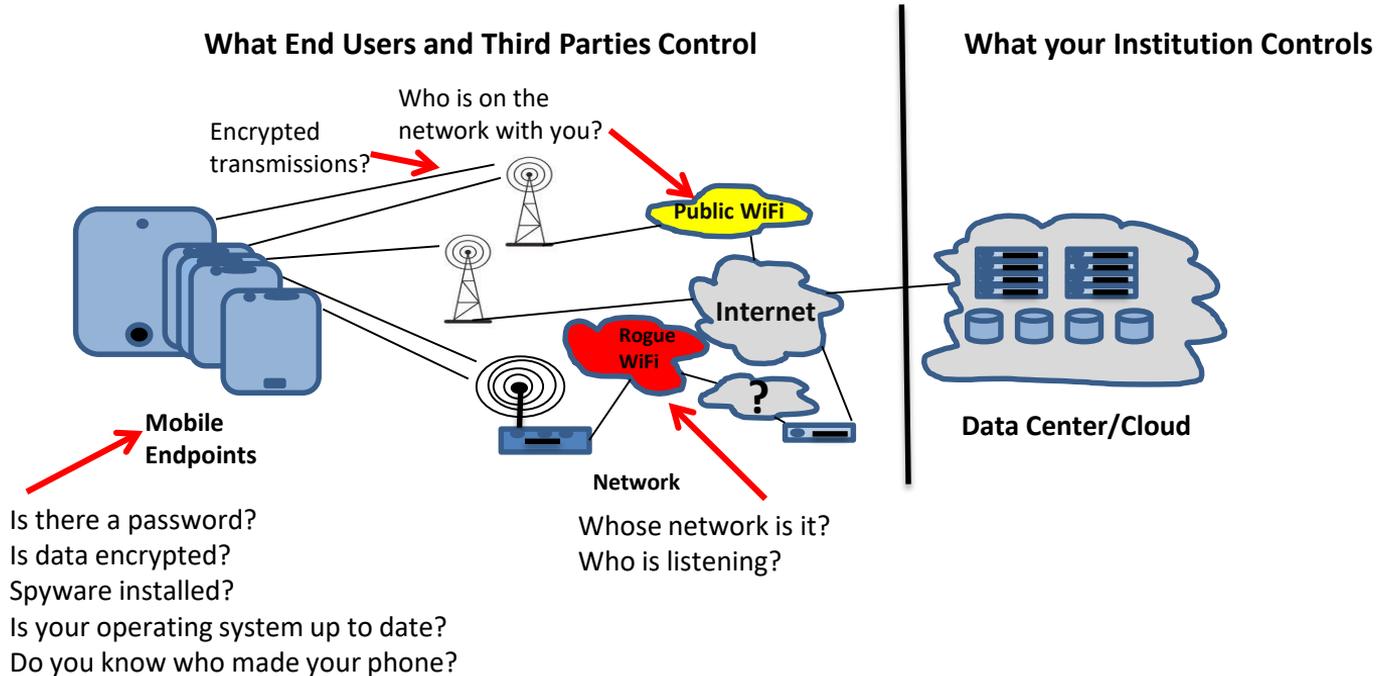
ATO attacks can be used to gain access to a user's email account (e.g., through phishing) and the attacker:

1. Establishes control of an account (persistence) without alerting the user or security administrators.
2. Conducts reconnaissance to determine how to exploit the account.
3. Exfiltrates sensitive information or steals funds and can repeat this process if user accounts credentials from other potentially higher-value targets were also compromised.

The attacker will potentially continue targeted email attacks and execute Business Email Compromise (BEC) and Vendor Email Compromise (VEC) to steal funds.

Mobile Endpoint Attack Surface

The primary cyber threat entry path is through endpoints your institution does not control (e.g., mobile phones, tablets, and personal computers).



Mobile User Behavior Vulnerabilities

Mobile User Behavior and Developer Practices Introduce Preventable Cybersecurity Vulnerabilities

For every 10,000 devices in an organization there is a ~95% chance that at least 1 device is infected with a malicious application that could be key stroke capture malware, ransomware, or other damaging spyware.*

50%

Do Not Use Passcodes

About half of mobile device users do not use passcodes to protect mobile devices which exposes the contents of the device if lost.

160

Unique IPs/Day

Mobile devices typically connect to an average of 160 unique IP addresses (Internet sites) a day potentially exposing devices to malicious sites and malware.

* Mobile Security Index 2019, Verizon

Mobile User Behavior Vulnerabilities (continued)

33%

Unencrypted

Over a third of mobile device communications is unencrypted potentially compromising PII of the user.

25%

**High Risk
Vulnerabilities**

A quarter of mobile applications have high risk security vulnerabilities that if exploited compromise the security of the device.

100%

Of Tested Apps

In a recent study of mobile banking applications all 30 apps analyzed had at least one security vulnerability which could result in the compromise of the device's security and users data.

If They Can't Phish you . . .

they'll try to just guess your password! Vulnerabilities introduced by human behavior are the most likely to be exploited and password security is the most likely culprit

New NIST “Digital Identity” guidelines* revise previous long-standing (and painful) password guidelines

- Less complex passwords
- Easy to remember longer “keyphases” with no preset expiration date
- Password hints and knowledge-based authentication (e.g., first pet) are **not** recommended
- 8 – 64 characters with all ASCII characters allowed
- 10 attempts before lockout
- Password checking against know password dictionaries

Instead of **G0T!gers#** use ***courage run spring play***, but many systems are not yet set up to allow such password so always follow your organizations security policy

The 25 most commonly used passwords of 2018**

1. 123456 (Unchanged)
2. password (Unchanged)
3. 123456789 (Up 5)
4. 12345678 (Down 1)
5. 12345 (Unchanged)
6. 111111 (New)
7. 1234567 (Up 1)
8. sunshine (New)
9. qwerty (Down 5)
10. iloveyou (Unchanged)
11. princess (New)
12. admin (Down 1)
15. welcome (Down 1)
14. 666666 (New)
15. abc123 (Unchanged)
16. football (Down 7)
17. 123123 (Unchanged)
18. monkey (Down 5)
19. 654321 (New)
20. !@#%* &* (New)
21. charlie (New)
22. aa123456 (New)
23. donald (New)
24. password1 (New)
25. qwerty123 (New)

* NIST Special Publication 800-63-3, Digital Identity Guidelines, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>

** <https://www.securitymagazine.com/articles/89919-the-25-passwords-leaked-online-in-2018>

Cybersecurity Vulnerability Mitigation

Cyber Hygiene:

- Documented and enforced security policy and controls
 - Two-factor authentication for admins and critical applications
 - Testing your cybersecurity - vulnerability scanning and penetration testing
 - Incident Response Plans
 - Contingency Plans (Business Continuity Plans)
- & User Education and Awareness – especially for “phishing” attacks



BE PREPARED

Detecting, Responding, and Recovering from a Breach

How you detect, respond to, and recover from a cyber breach is as **(or more)** important than how you protect (i.e., through cyber hygiene) your systems

Intrusion Prevention/Detection Systems

- Endpoints (PC and mobile)
- Networks
- In the cloud

Incident Response Plans

- Policy
- Procedures
- Notification
- “Playbooks”
- “Tabletop Exercises”

Contingency Plans

- Business Continuity Plans
- Disaster Recover Plan
- Backups
 - Local and offsite
 - Cloud-based backups
- Testing of backups

Cybersecurity Risk Management – Governance

Risk management starts at the top with the President & Board of Directors/Regents

- The most prominent and costly cybersecurity incidents and how they are managed (or not managed) are almost always attributable to failures in governance and inadequate communication of cybersecurity risks
- Are cybersecurity strategy and risks communicated in business language?
- Does your board have representation with technology or cybersecurity backgrounds?
- Do you have a cybersecurity strategy that is ready for board review and approval?
- Active participation (risk aware and risk informed) - is cybersecurity a regular agenda item for the president and board?

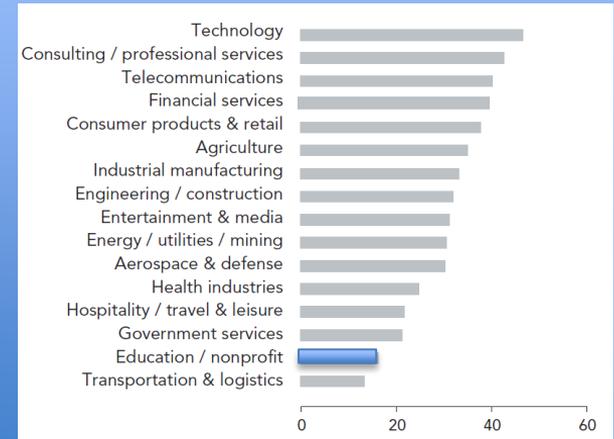


Cybersecurity Challenges

The education sector tends to budget less for cybersecurity than most of the other sectors in our economy. To overcome this challenge it is critical to have:

- Effective and efficient use of limited human and financial resource is critical
- A well-crafted cybersecurity strategy is key
- Formal collaboration with sector peers
- Executive leadership and board approval of the strategy
- A regular feedback loop - measurement of effectiveness against metrics

North American firms, by sector, with more than \$1 billion in gross revenue that budget \$10 Million or more for cybersecurity (percent)*



* Adapted from Office of Financial Research, Cybersecurity and Financial Stability: Risks and Resilience, February 15, 2017.

Elements of a Cybersecurity Program

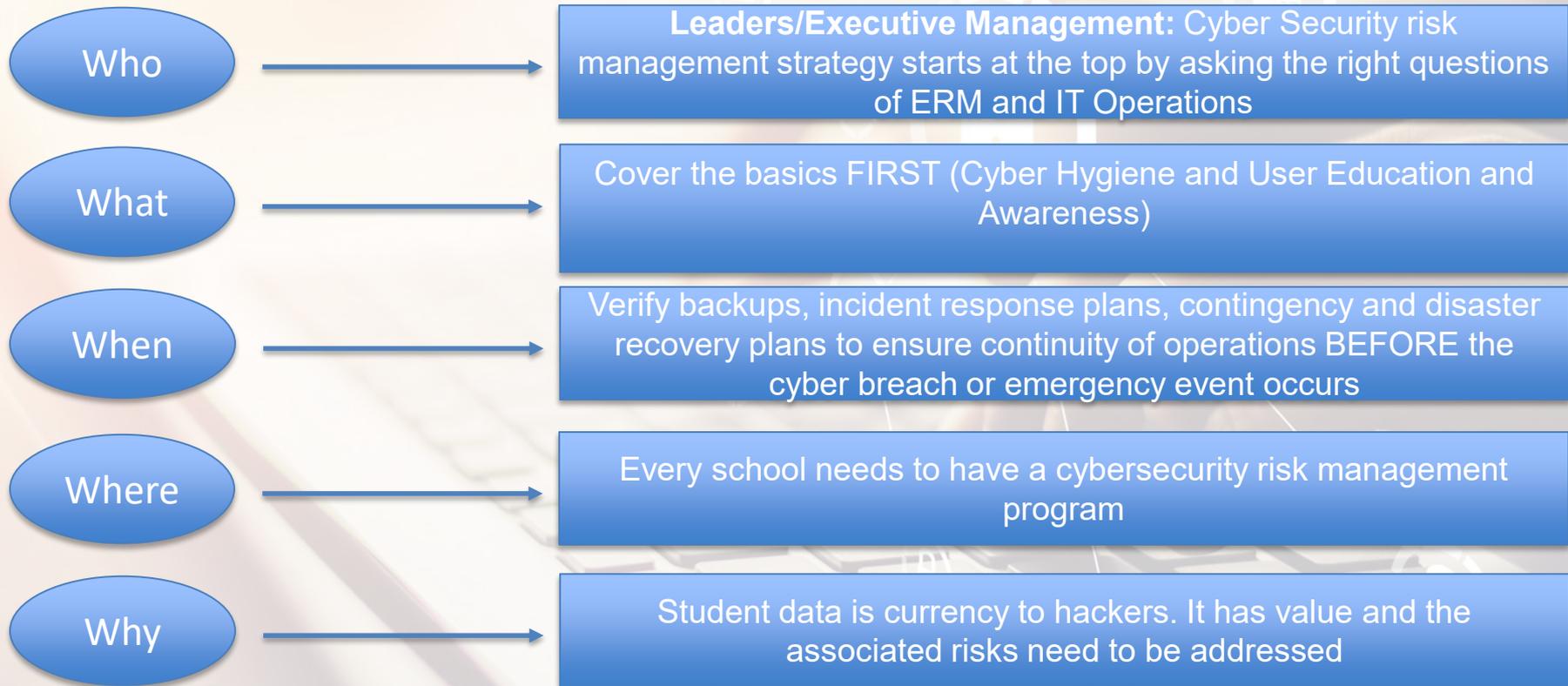
Use a recognized cybersecurity framework such as NIST*

- Develop an overall strategy based on a recognized cybersecurity framework (NIST is recommended).
 - You can't protect everything equally so identify the "crown jewels" or high value assets
- Develop security standards and baselines for your institution and third-party service providers.
- Assign a chief information security officer in charge of cybersecurity.
- Formally collaborate with others in the industry.
- Ensure active participation of executive leadership and the board of directors in your institution's cybersecurity strategy.

*NIST publications are free for industry use and are not subject to copyright in the United States. Below are links to some relevant cybersecurity guidance documents:

- NIST Special Publication 800-12, Revision 1, An Introduction to Information Security, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf>
- NIST Cybersecurity Framework, <https://www.nist.gov/cyberframework>
- NIST Special Publication 800-171, Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf>
- NIST Special Publication 800-171A, Assessing Security Requirements for Controlled Unclassified Information, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf>

Closing Points

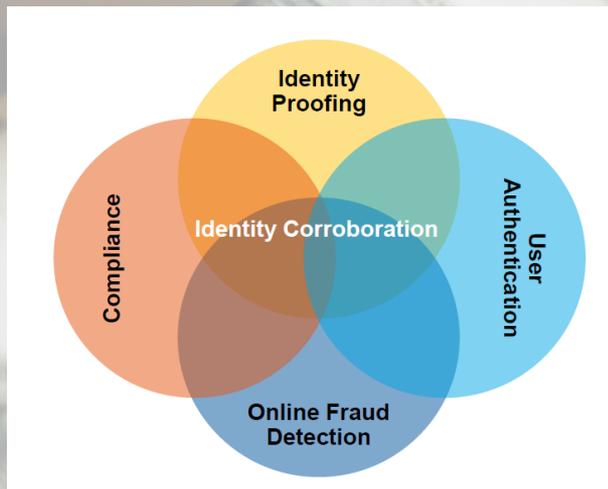


Cyber and Fraud Risk Management Work Together

Steal Data
"Cybercrime"



Steal Money
"Financial Crime"



Managing Fraud Risk

A close-up photograph of a hand holding a stack of US dollar bills. The focus is on a one hundred dollar bill, showing the portrait of Benjamin Franklin. The background is slightly blurred, showing other bills in the stack.

Stephanie Powell

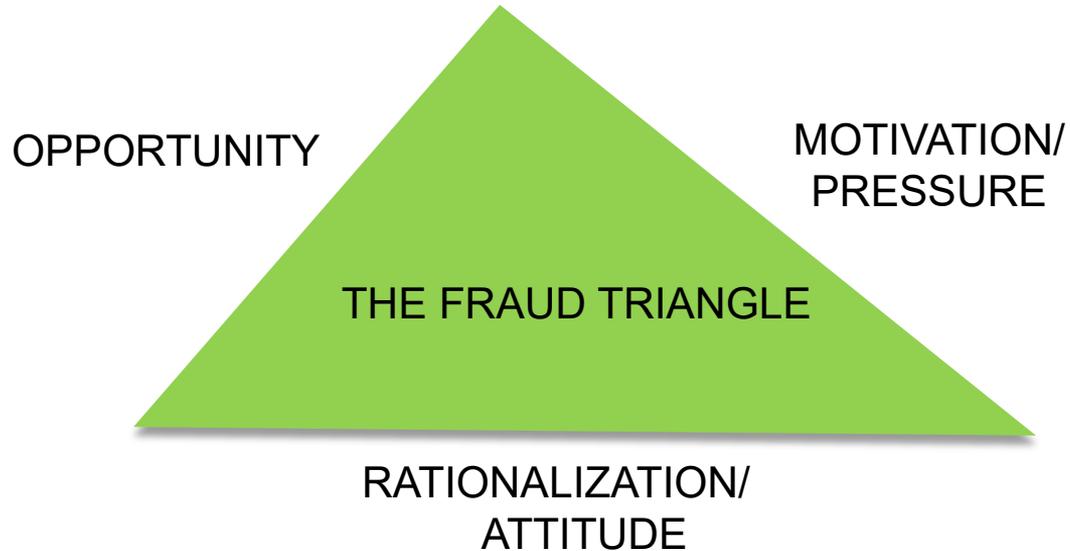
What is Fraud?

- **Financial**
- **Reward**
- **Acquired**
- **Using**
- **Deception**

“There is no kind of dishonesty into which otherwise good people more easily and frequently fall than that of defrauding the government.”

-Benjamin Franklin

What risk factors may lead to fraud?



Where are your fraud risks?



We should manage fraud risk, but is it required?

**Under 34 CFR 668.16(g)(1)
MUST refer to OIG:**

- Applicant
- Administrator

**if there is credible information
indicating fraud.**



Establish a Fraud Risk Management Program

Ask Strategic Questions

- Who is the senior-level leader who will take ownership of this program?
- How will you motivate people to collaborate across the various disciplines and share information?
- What are the tools and technology available on your campus?
- How will you measure success?
- How will you meet the challenges?



Fraud Risk Management Program

TONE AT THE TOP:

- Encourage staff to identify and report patterns of fraudulent behavior
- Stay vigilant and remain persistent
- Constantly monitor information for triggers of suspicion and request additional information based on reasonable suspicion
- Investigate allegations of fraud or abuse
- Ensure there are consequences

Assess Your Fraud Risks

Tailor your fraud risk assessment to your school:

- Who are the relevant stakeholders?
- What are your data sources?
- What analytic tools are available?
- What controls are in place?



What is Fraud Risk Management?

Prevention



Detection



FRAUD RISK MANAGEMENT PROGRAM

Suggestions for Fraud Prevention:

- Promote Fraud awareness activities around campus for both students and staff
- Communicate available reporting mechanisms across the entire community. (ED OIG Hotline: 1-800-MIS-USED)
- Support employee engagement activities
- Assess availability of data analytics

Differences Between OIG's Investigation Services and FSA's Program Compliance and Enforcement Offices

| OIG INVESTIGATION SERVICES | FSA |
|--|---|
| <ul style="list-style-type: none">• Investigates any fraud impacting ED programs or operations | <ul style="list-style-type: none">• Conducts compliance reviews, administrative investigations of violations of HEA |
| <ul style="list-style-type: none">• Works with federal and state prosecutors to take criminal and civil actions | <ul style="list-style-type: none">• Takes administrative actions authorized by the HEA and program regulations |
| <ul style="list-style-type: none">• Used risk-based decisions to improve outcomes | <ul style="list-style-type: none">• Reviewers and investigators have administrative authority only |
| <ul style="list-style-type: none">• Criminal investigators have statutory law enforcement authority to carry firearms and execute search and arrest warrants | <ul style="list-style-type: none">• Has program operating responsibilities |
| | <ul style="list-style-type: none">• Is required to send allegations of fraud to OIG |

Questions and Answers

