

# PARTNERING TO SAFEGUARD IHEs FROM CYBERSECURITY THREATS #20

Recommendations from the U.S Department of Homeland Security Cybersecurity and  
Infrastructure Security Agency (CISA)

Davon Tyler

U.S. Department of Education

2023 FSA Training Conference for Financial Aid Professionals

# AGENDA

---

- Threats facing Educational Institutions
- The effects of cyberattacks
- Feedback from Stakeholder Engagement
- CISA Recommendations
- Questions?

All links in this presentation will be in your handout.

001001010101100011  
001000100011110010  
100100010010001010  
0100079%0001010101  
110010001010100101  
010110101011000101  
110040,000,0001010  
010110101001011010  
110101100101100011  
011001001001000010  
110101001001010101  
100011001101001010  
100101101010010110

**79%** of higher education providers reported ransomware attacks in 2023

**MOVEit vulnerability** – 40 million people, 890 organizations impacted

# FROM THE HEADLINES

---

Schools Are a Top Target of Ransomware Attacks, and It's Getting Worse

Ransomware threat against colleges grows, survey finds

Data Breach Taps 30 Years of Sensitive Info at University of Minnesota

Colleges across the U.S. - say they've been swept up in the cyberattack exploiting

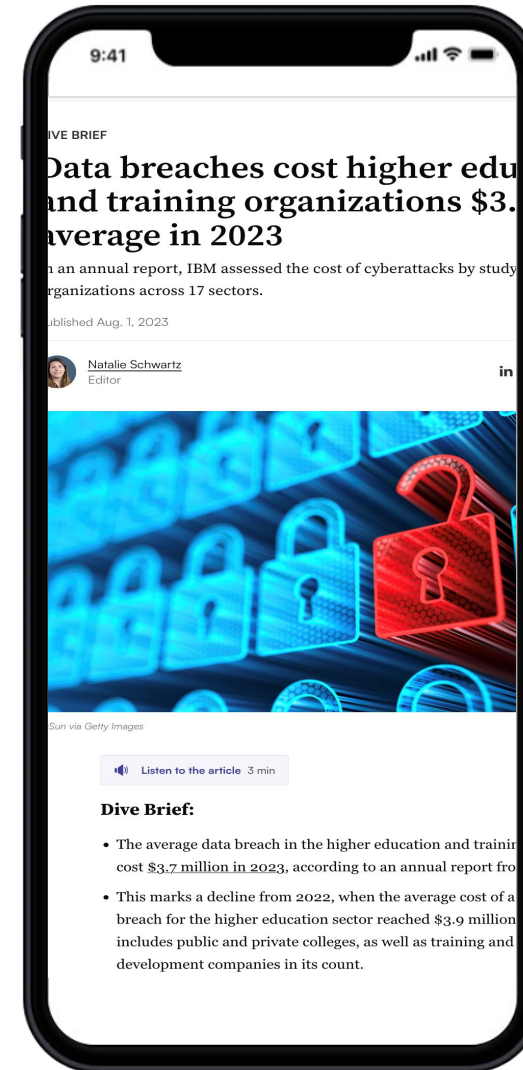
Cyberattacks Pose 'Existential Risk' to Colleges—and Sealed One Small College's Fate



# CONSEQUENCES

*74% of all data breaches were the result of a human element*

- Unauthorized disclosure of sensitive information
- Data breaches
- Loss of confidence\trust\reputation
- Mission impact & financial losses
- "Worst case scenario" School closure





# \$3.7 Million

---

## THE AVERAGE COST OF A DATA BREACH IN THE EDUCATION SECTOR

72% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 92% of breaches.

Top three attack methods are system intrusion, miscellaneous errors, and social engineering, i.e hacking and ransomware.



# CYBERSECURITY THREATS FACING IHE'S

---

- Student data breaches
- Data breaches involving teachers and school community members information
- Business email compromise (BEC) scams
- Online class and school meeting invasions
- Website and social media defacement
- Denial of service (DDoS) attacks
- Ransomware attacks

# THE EFFECTS OF CYBER ATTACKS ON EDUCATIONAL INSTITUTIONS

---



Monetary loss



Loss of learning



1,241 incidents in 2022

Source: 2022 Data Breach Investigations Report  
(DBIR)



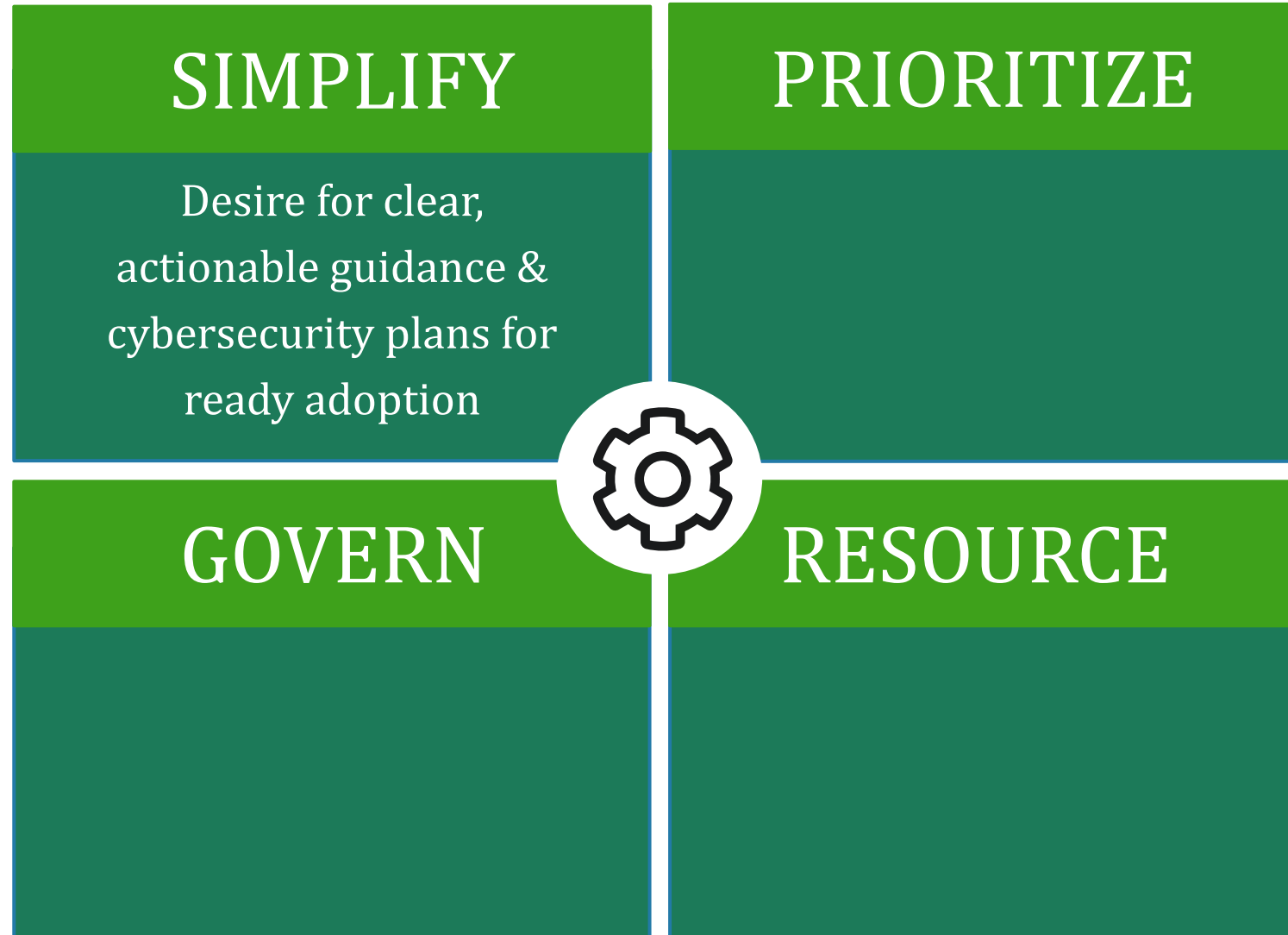
# FEEDBACK FROM STAKEHOLDER ENGAGEMENT

---

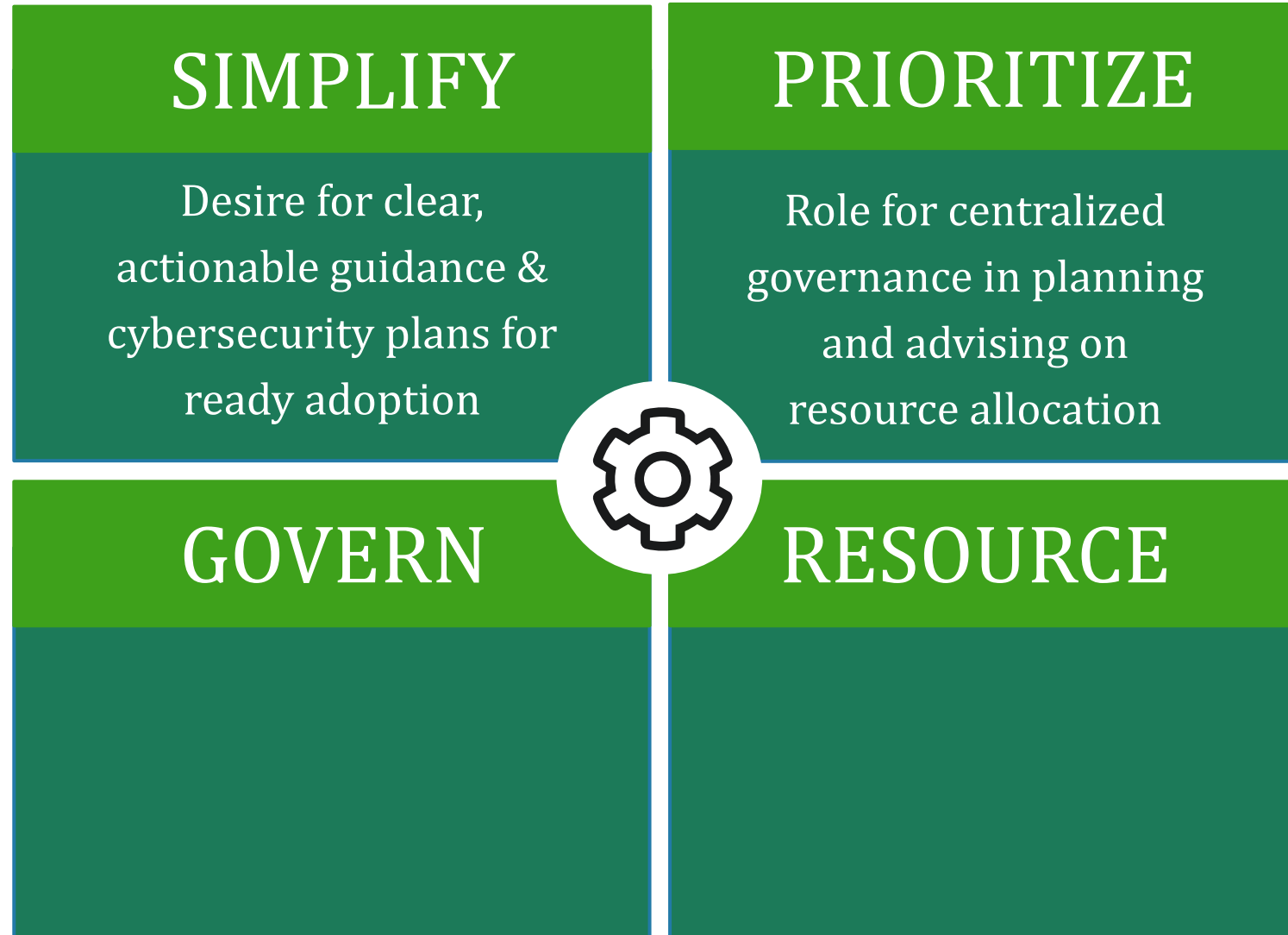
Challenge: Shortage of cybersecurity professionals



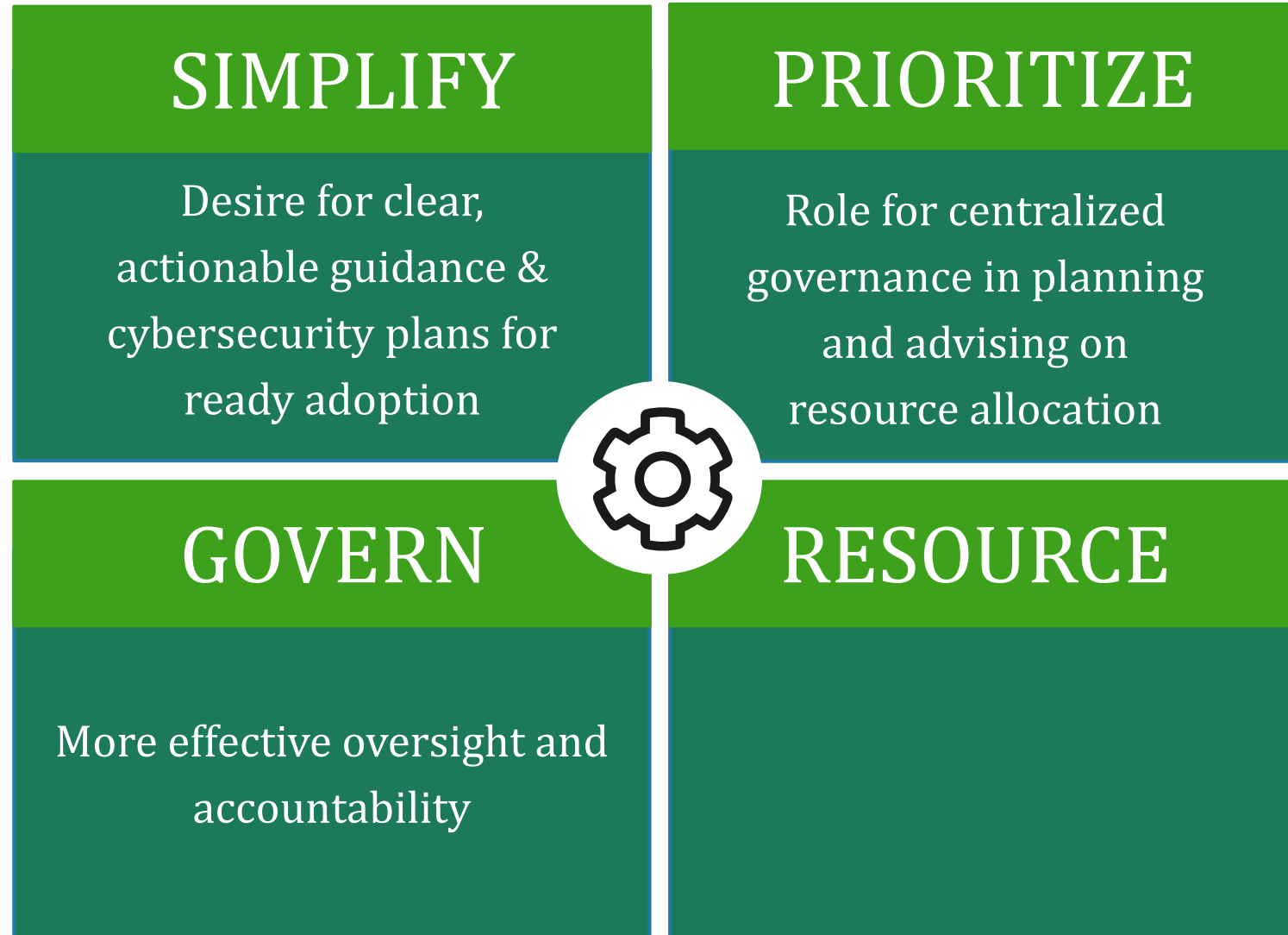
# FEEDBACK FROM STAKEHOLDER ENGAGEMENT



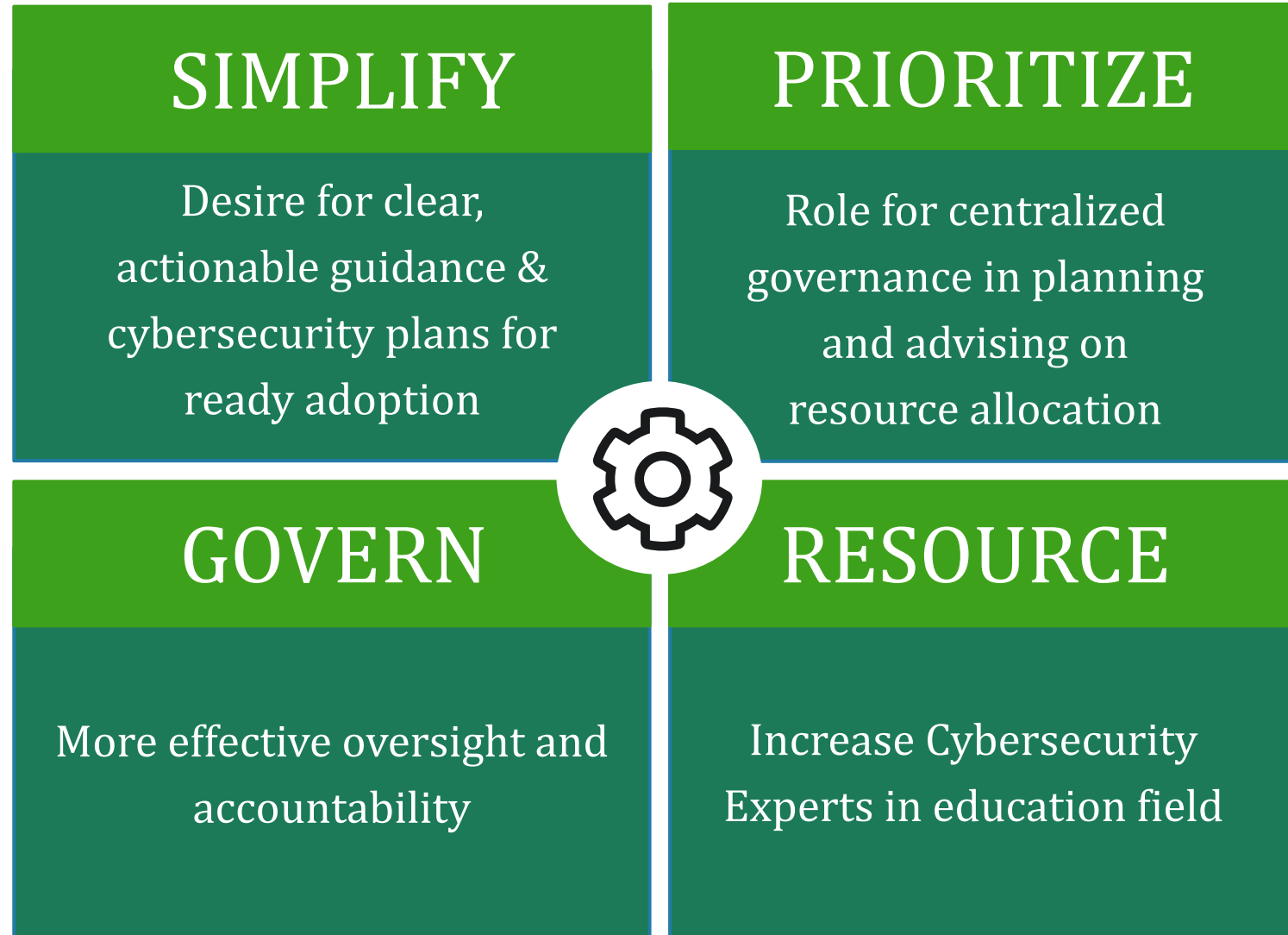
# FEEDBACK FROM STAKEHOLDER ENGAGEMENT



# FEEDBACK FROM STAKEHOLDER ENGAGEMENT



# FEEDBACK FROM STAKEHOLDER ENGAGEMENT





# CISA KEY FINDINGS BASED ON FEEDBACK FROM STAKEHOLDERS

---

# KEY FINDINGS

---

- 1 **Begin with a small number of prioritized investments.**
- 

- 2

---

- 3

# KEY FINDINGS

---

- 1** Begin with a small number of prioritized investments.
  - 2** Elevate cybersecurity risk management as a top priority for administrators, superintendents, and other leaders at every educational institution.
  - 3**
-

# KEY FINDINGS

---

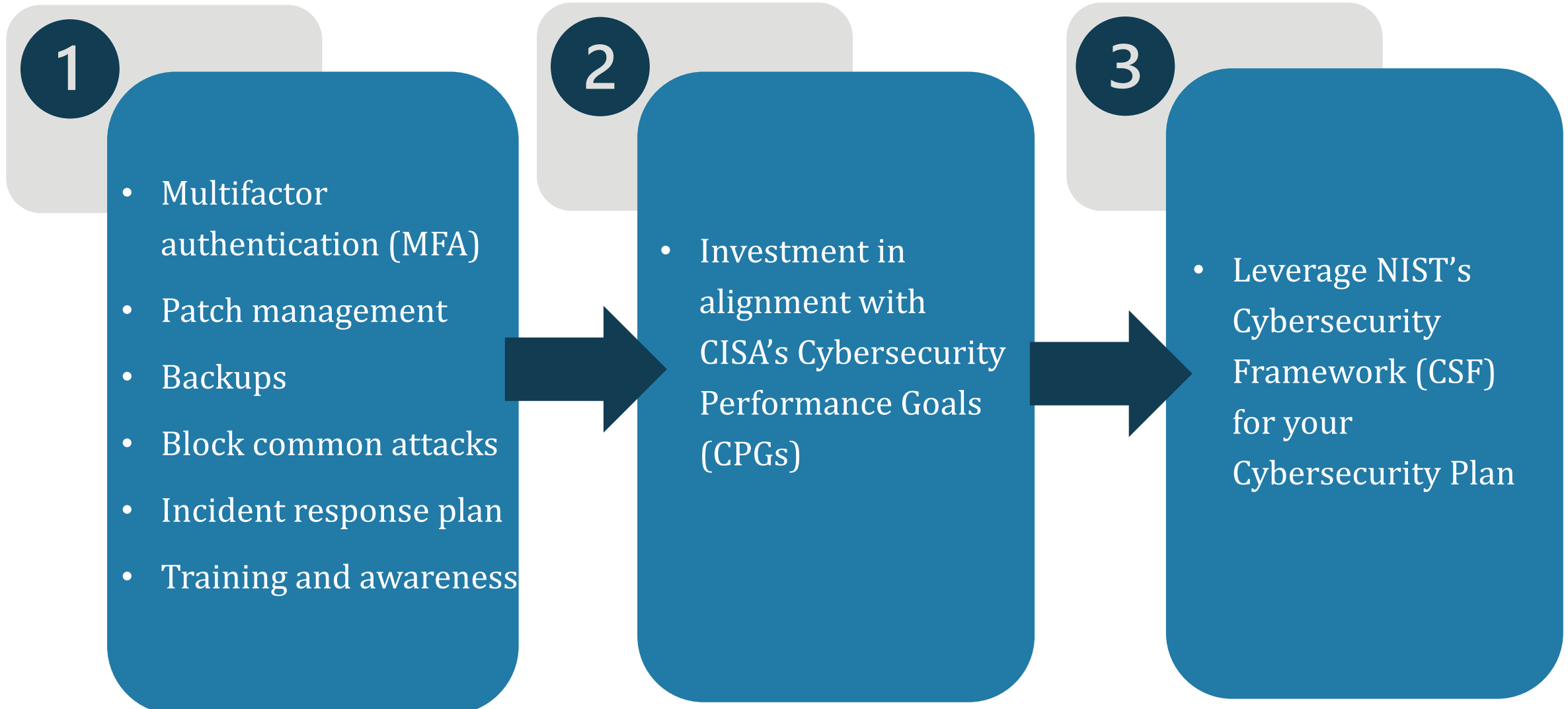
- 1** Begin with a small number of prioritized investments.
- 2** Elevate cybersecurity risk management as a top priority for administrators, superintendents, and other leaders at every educational institution.
- 3** Collaboration and information sharing with peers and partners to build awareness and sustain resilience.

# CISA RECOMMENDATIONS OVERVIEW

---



# IMPLEMENT MOST IMPACTFUL SECURITY MEASURES



# CISA RECOMMENDATIONS IN DETAIL

---

## RECOMMENDATION 1:

### Invest in the Most Impactful Security Measures

- ✓ Implement [multifactor authentication \(MFA\)](#)
- ✓ Prioritize [patch management](#)
- ✓ Perform and [test backups](#)
- ✓ Minimize exposure to [common attacks](#)
- ✓ Develop and exercise a [cyber incident response plan](#)
- ✓ Create a [training and awareness](#) campaign at all levels

## RECOMMENDATION 2:

**Recognize and actively address resource constraints**

- ✓ Work with your state or territory State Administrative Agency (SAA) to leverage the [State and Local Cybersecurity Grant Program \(SLCGP\)](#)
- ✓ Utilize [free or low-cost services](#) to make near-term improvements
- ✓ Expect and call for [technology providers](#) to enable strong security controls
- ✓ Migrate IT services to more secure [cloud versions](#)

## RECOMMENDATION 3:

### Focus on Collaboration and Information Sharing

- ✓ Join relevant collaboration groups, such as [MS-ISAC](#) (Multi-State Information Sharing and Analysis Center)
- ✓ Work with other [information-sharing organizations](#) such as fusion centers, state school safety centers, and other state and regional agencies, and associations.
- ✓ Build a strong and enduring relationship with [CISA](#) and FBI [regional](#) cybersecurity personnel.



# EXECUTIVE SUMMARY

---

“Change must come from the top down. Leaders must establish and reinforce a cybersecure culture. Information technology and cybersecurity personnel cannot bear the burden alone.”

# THE SAFEGUARDS RULE



Your institution is required to **develop, implement, and maintain** an information security program



Your Information Security Program protects your students' information with **administrative, technical, and physical** safeguards



**The information security plan strives to:**

- Ensure security and confidentiality
- Protect against anticipated threats or hazards
- Protect against unauthorized access

# THE PROGRAM IS SCALABLE



It must be appropriate for:



The size and  
complexity of  
your institution



The nature and  
scope of your  
activities

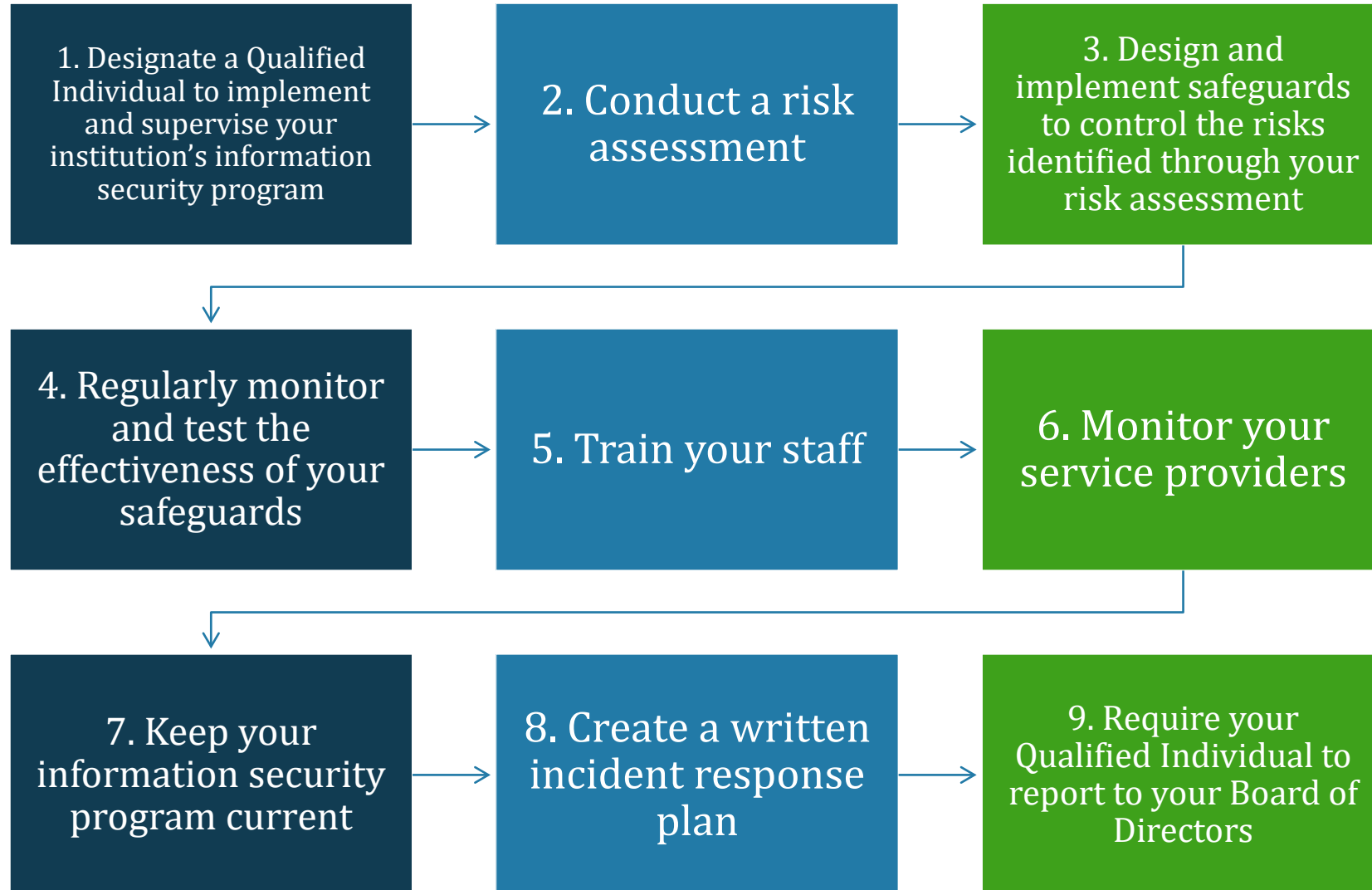


The sensitivity of  
the information

# MAJOR ELEMENTS OF YOUR CYBERSECURITY PLAN



# WHAT YOU NEED TO DO





# **YOUR INCIDENT RESPONSE PLAN & REDUCING RISK**



# YOUR INCIDENT RESPONSE PLAN COVERS

---

- ✓ The goals of your plan
- ✓ The internal processes your institution will activate in response to a security event
- ✓ Clear roles, responsibilities, and levels of decision-making authority
- ✓ Communications and information sharing both inside and outside your institution
- ✓ A process to fix any identified weaknesses in your systems and controls
- ✓ Procedures for documenting and reporting security events and your institution's response
- ✓ A post-mortem of what happened and a revision of your incident response plan and information security program based on what you learned

# RISK REDUCING STRATEGIES

**1** Implement and periodically review access controls

**5** Enable multi-factor authentication for anyone accessing personal formation

**2** Know what you have and where you have it

**6** Dispose of personal information securely

**3** Encrypt customer information on your system and when it's in transit

**7** Anticipate and evaluate changes to your information system or network

**4** Assess your apps

**8** Maintain a log of authorized users' activity and keep an eye out for unauthorized access



# NIST



## SP 800-171



Special Publication

The number or  
name of the  
standard

## TOPICS YOU ALREADY KNOW:

NIST  
SP 800-171

controls  
training  
inventory  
procedures  
management  
policies  
maintenance  
audit

# 14 CONTROL FAMILIES

## MANAGEMENT CONTROLS

Risk Assessment  
Awareness & Training  
Audit & Accountability

## PROCEDURAL CONTROLS

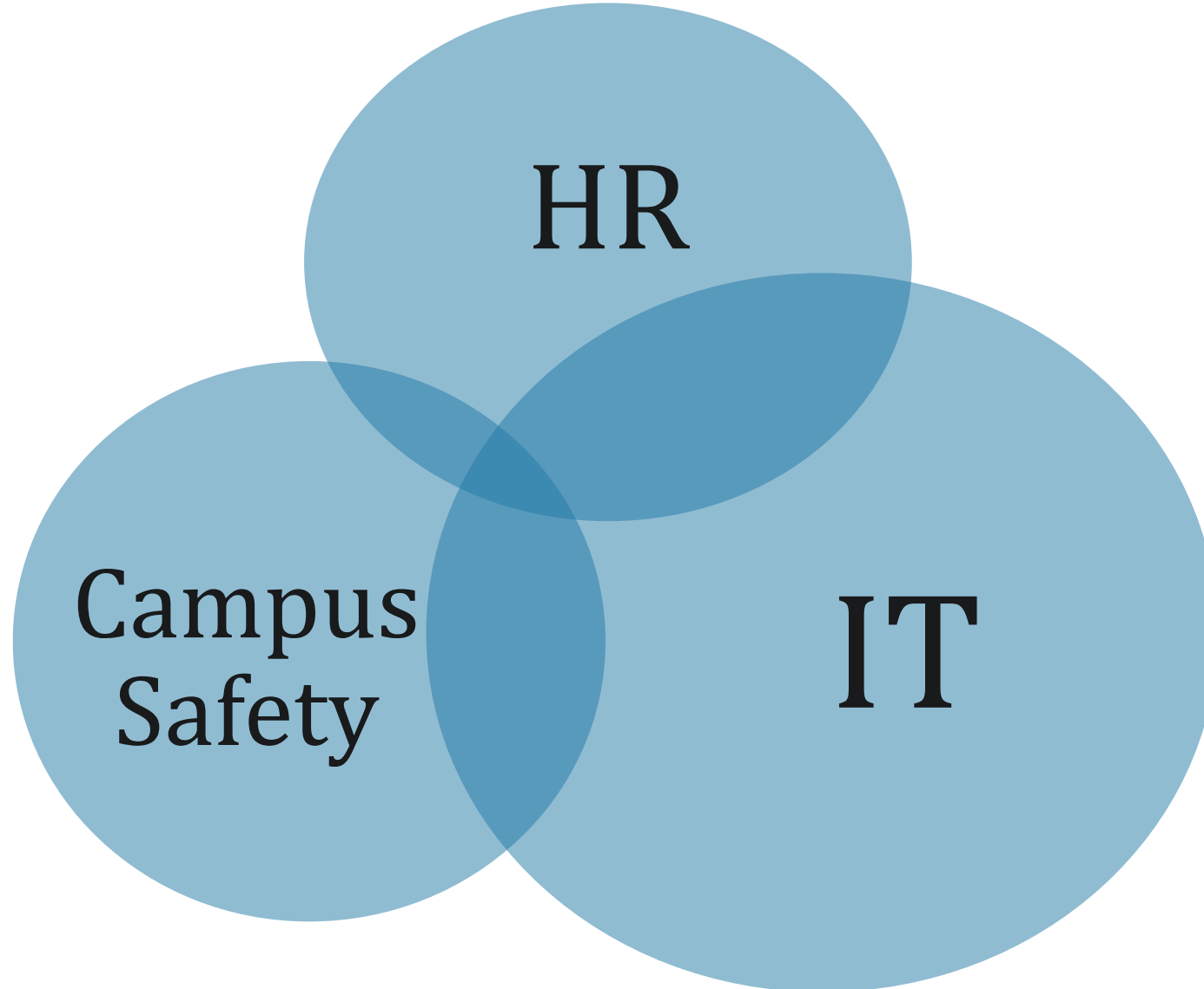
Access Control  
Configuration Management  
Identification &  
Authentication  
Maintenance  
System & Communications  
Protection  
System & Information  
Integrity  
Security Assessment

## OPERATIONAL CONTROLS

Incident Response  
Media Protection  
Physical Protections  
Personnel Security

**NIST**  
SP 800-171

# NIST SP 800-171 IS A TEAM SPORT



# IHE CYBERSECURITY NEWSLETTER

Actionable Information

Sent Quarterly to 20,000 Leadership, IT and Compliance Pros at IHEs

To sign up and receive FSA's new cybersecurity

newsletter, please email [FSASchoolCyberSafety@ed.gov](mailto:FSASchoolCyberSafety@ed.gov) with the subject line: "Send me the FSA Cybersecurity Newsletter for IHEs."





# QUESTIONS?

## Report breaches to:

- fsaschoolcybersafety@ed.gov
- OR use the Cybersecurity Breach Intake Form





---

**FSA CYBERSECURITY WEBSITE**  
**[HTTPS://FSAPARTNERS.ED.GOV/TITLE-IV-PROGRAM-ELIGIBILITY/CYBERSECURITY](https://fsapartners.ed.gov/title-iv-program-eligibility/cybersecurity)**

**CISA RESOURCES**  
**[HTTPS://WWW.CISA.GOV/CYBERSECURITY](https://www.cisa.gov/cybersecurity)**

**NIST CYBERSECURITY FRAMEWORK**  
**[HTTPS://WWW.NIST.GOV/CYBERFRAMEWORK](https://www.nist.gov/cyberframework)**

---