Information Security

A Primer for Business Leaders

AGH University

MARCH 22, 2018

AGH
CPAs & ADVISORS

Administration

NATIONAL REGISTRY OF
CPE
SPONSORS

SHRM
SHRM-CP | SHRM-SCP
RECERTIFICATION
PROVIDER
2018

HR CERTIFICATION INSTITUTE®
h™
APPROVED • 2018 • PROVIDER

If you need CPE or HR credit, please participate in all polls throughout the presentation.

Administration

A recording of today’s webinar will be emailed for your reference or to share with others.

Administration

For best quality, call in by phone instead of using your computer speakers.

Administration

To ask questions during the presentation, use the questions box on the right side of your screen.

Administration

Please provide your feedback at the end of today’s presentation.

Brian Johnson

Senior Vice President, Technology Services
CISA, CISM, CGEIT, CRISC, CPA

Allen, Gibbs & Houlik, L.C.

AGH
CPAs & ADVISORS

Message Objective:

By introducing information security principles that you can reliably use to understand and address your security needs…

Message Objective:

…you will be better prepared to protect and sustain your information systems and the processes that rely upon them.

Agenda:

1. The Leadership Gap
2. An IT Governance Framework
3. The Information Security Perspective

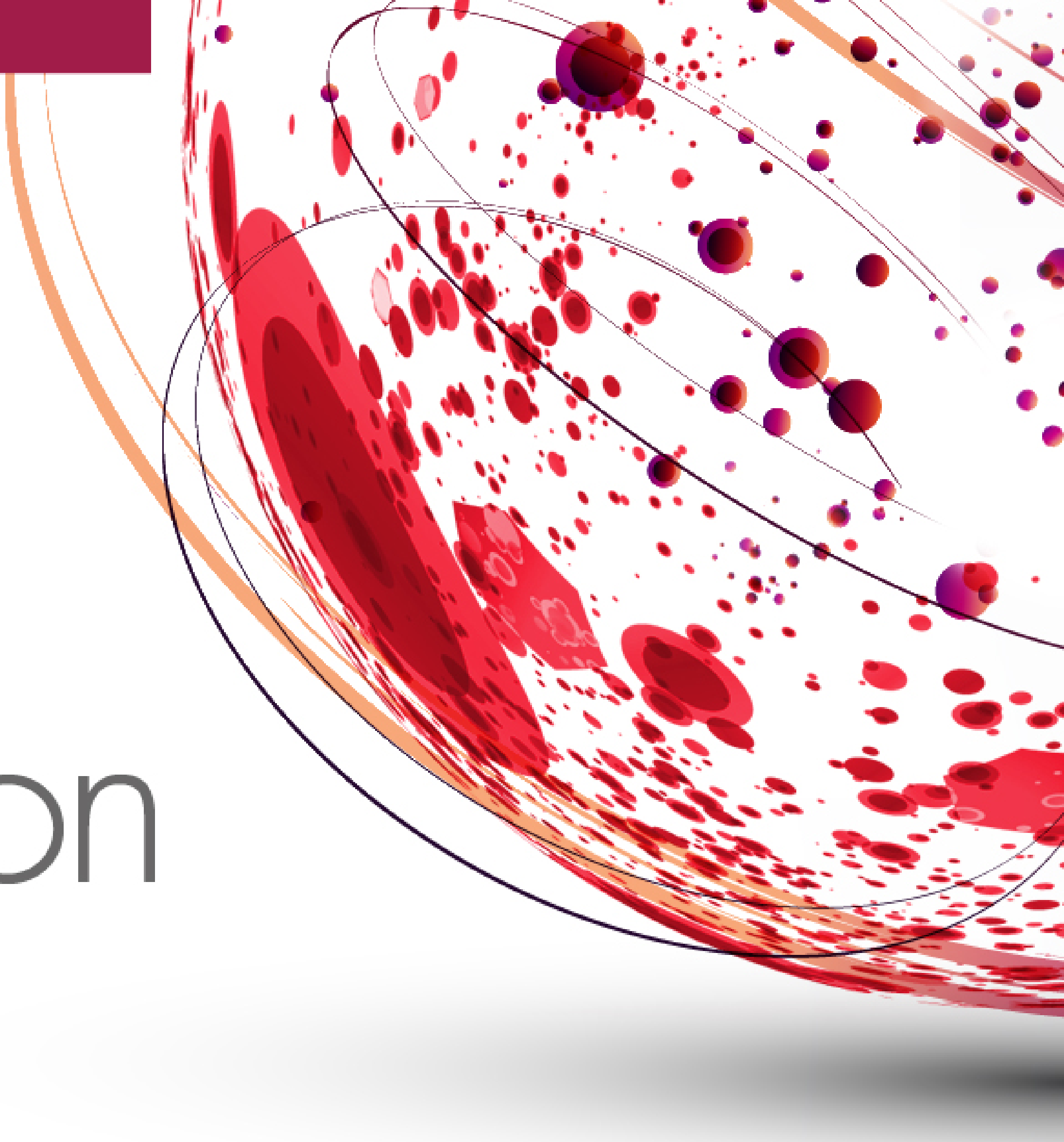
prim·er

/ˈprīmər/

noun

1. A resource that serves as an introduction for business leaders and managers who are new to information security.

Polling Question



Agenda:

1. The Leadership Gap
2. An IT Governance Framework
3. The Information Security Perspective

ISACA®

Trust in, and value from, information systems

Does ISACA conduct important primary research?

ISACA®

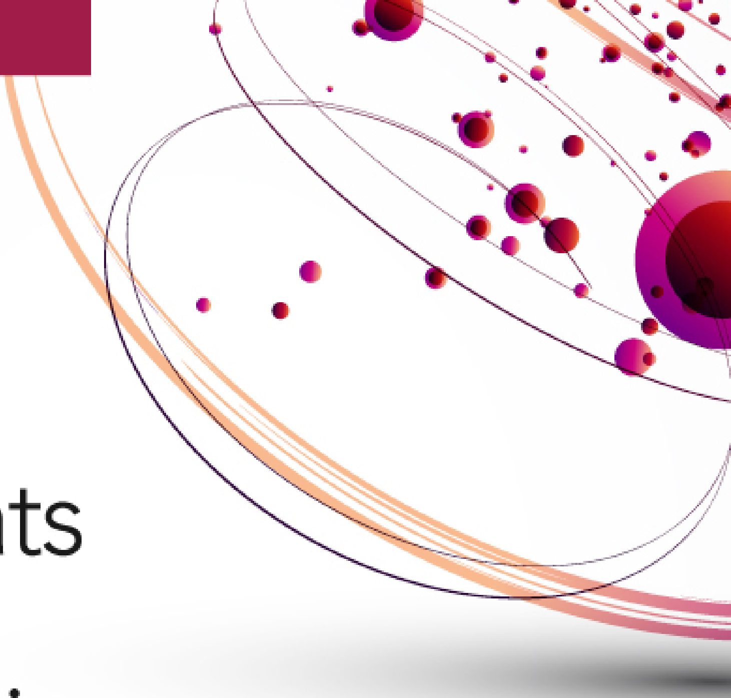
Trust in, and value from, information systems

ISACA, *Better Tech Governance Is Better for Business.*

BETTER TECH GOVERNANCE IS BETTER FOR BUSINESS

AN ISACA RESEARCH REPORT

ISACA®



The Assertion:

"Non-stop cyber-threats and ongoing digital transformation of business have elevated **governance of technology** into board-rooms across the globe."

ISACA, *Better Tech Governance Is Better for Business*, 2.

The Question:

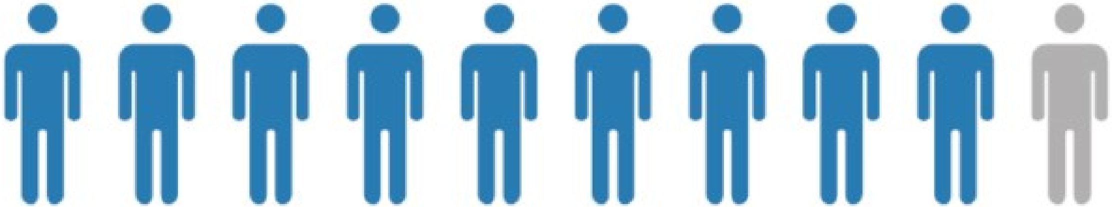
"How are senior leaders handling their growing responsibility for effective oversight of all things digital?"

ISACA, *Better Tech Governance Is Better for Business*, 2.

Key Findings

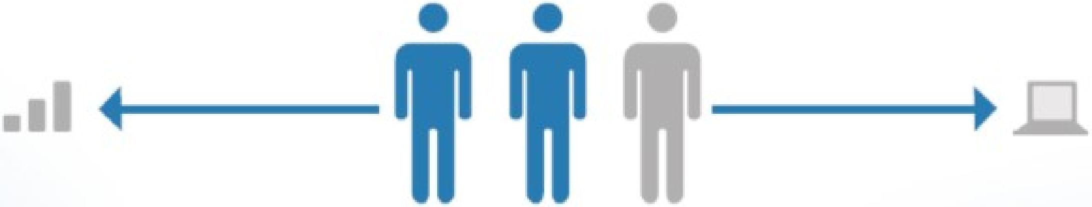
On the Plus Side:

9 in 10 senior leaders surveyed agree that **better governance** of information technology leads to **better** economic **outcomes** and more business agility.



Less Favorably:

More than two-thirds of all respondents say their company's top leaders need to **prioritize strengthening connections** between IT and business goals.



ISACA, *Better Tech Governance Is Better for Business*, 2.

On the Plus Side:

Two-thirds of organizations polled have **increased** spending on **risk management** in the past year.

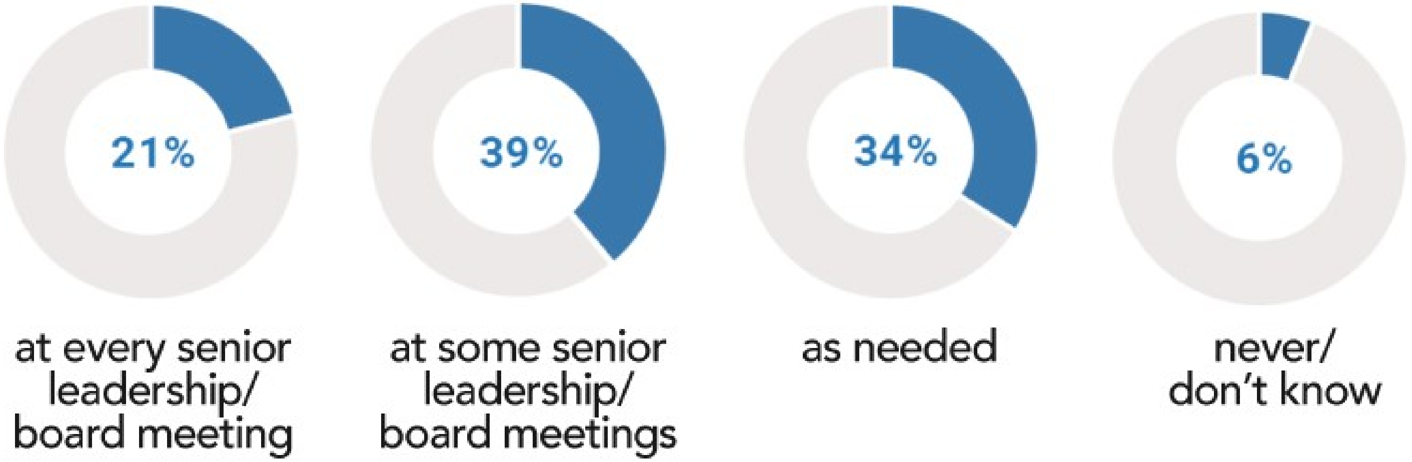
Less Favorably:

Barely more than half agree that their boards and executive teams are doing all they can to **safeguard** the organization's **digital assets.**

ISACA, *Better Tech Governance Is Better for Business*, 2.

Leadership in the Know...?

"How often is your senior **leadership briefed about** risk topics such as **cyber security** and disaster recovery/ business continuity?"



ISACA, *Better Tech Governance Is Better for Business*, 4.

Top 3 Challenges:

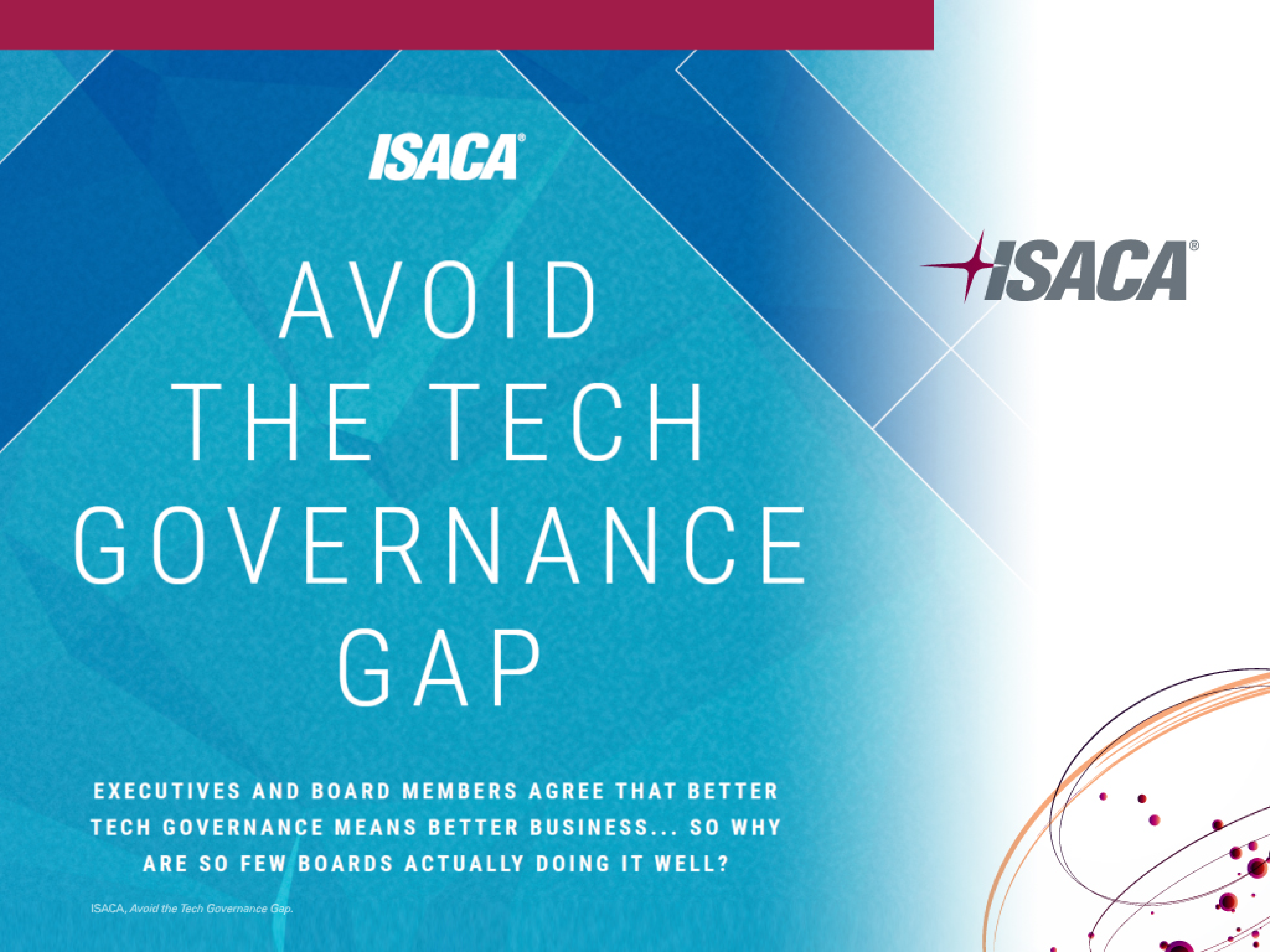
1. Cyber security policies and defenses	44%
2. Risk management priorities	36%
3. Alignment between IT objectives and overall enterprise objectives	35%

ISACA, *Better Tech Governance Is Better for Business*, 5.

Leadership Worries:

"Boardroom worries over increased internal and external threats are so great (61%) that almost half (48%) of leadership teams have prioritized investments in cyber-defense improvements over other programs."

ISACA, *Better Tech Governance Is Better for Business*, 5.



ISACA

ISACA

AVOID THE TECH GOVERNANCE GAP

EXECUTIVES AND BOARD MEMBERS AGREE THAT BETTER TECH GOVERNANCE MEANS BETTER BUSINESS... SO WHY ARE SO FEW BOARDS ACTUALLY DOING IT WELL?

ISACA, *Avoid the Tech Governance Gap.*

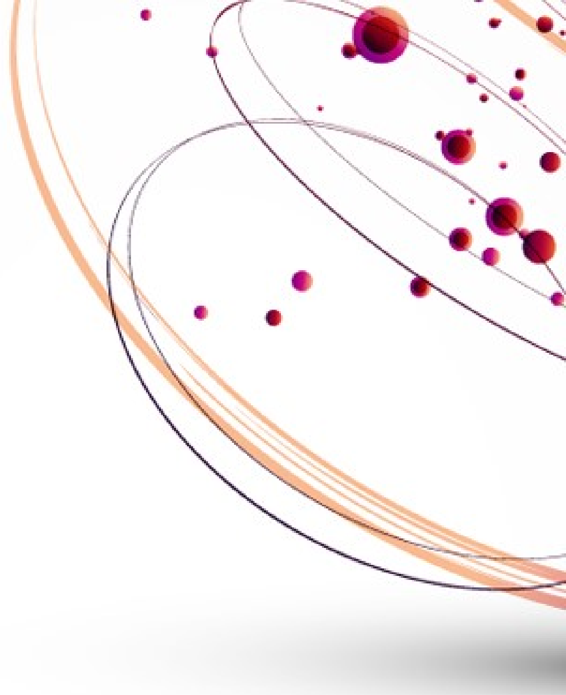
What Organizational Leaders Say:

Cyber security is #1 governance challenge

What Organizational Leaders Do:

JUST 15% to increase spending on data security training for board members

ISACA, *Avoid the Tech Governance Gap,* 1.

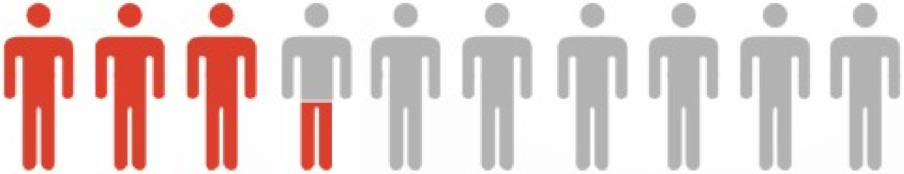


What Organizational Leaders Say:

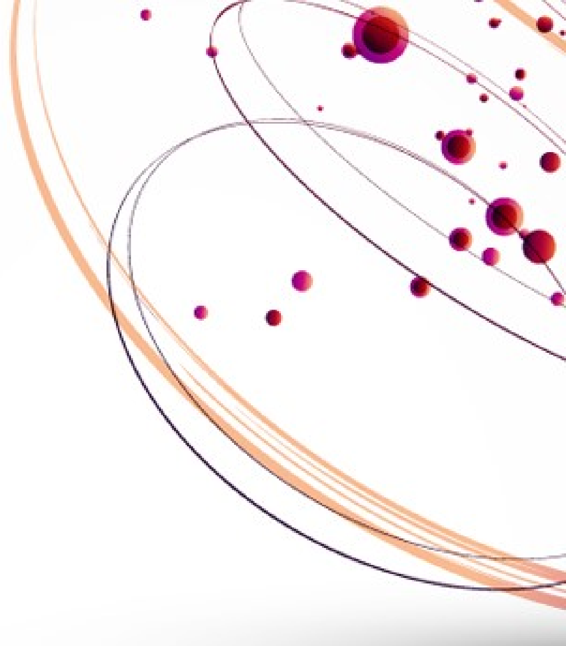
Risk management is #2 governance challenge

What Organizational Leaders Do:

Only 33% to fund increase in Enterprise Risk Management program

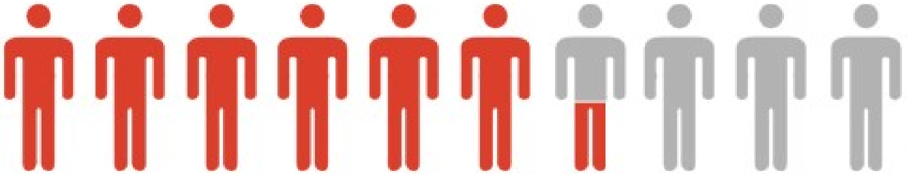


ISACA, *Avoid the Tech Governance Gap,* 1.

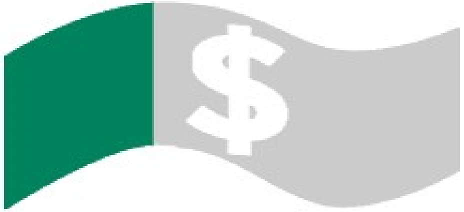


What Organizational Leaders Say:

64% believe internal threats are rising



What Organizational Leaders Do:



Only 35% to fund increase in data security training for employees

ISACA, *Avoid the Tech Governance Gap*, 1.

Takeaways

1 Analyze enterprise risks if security budget shrinks.

2 Ensure tech expertise is represented in boardroom.

3 Conduct continuous security awareness training.

4 Align tech investments with enterprise strategy.

5 Research and employ industry best practices and security controls.

ISACA, *Better Tech Governance is Better for Business*, 9.

Takeaways

1 Analyze enterprise risks if security budget shrinks.

awareness training.

4 Align tech investments with enterprise strategy.

5 Research and employ industry best practices and security controls.

ISACA, *Better Tech Governance is Better for Business*, 9.

Takeaways

1 Analyze enterprise risks if security budget shrinks

2 Ensure tech expertise is represented in boardroom.

4 Align tech investments with enterprise strategy.

5 Research and employ industry best practices and security controls.

ISACA, *Better Tech Governance is Better for Business*, 9.

Takeaways

1 Analyze enterprise risks if security budget shrinks.

2 Ensure tech expertise is represented

3 Conduct continuous security awareness training.

5 Research and employ industry best practices and security controls.

ISACA, *Better Tech Governance is Better for Business*, 9.

Takeaways

1 Analyze enterprise risks if security budget shrinks.

2 Ensure tech expertise is represented in boardroom.

4 Align tech investments with enterprise strategy.

practices and security controls.

ISACA, *Better Tech Governance is Better for Business*, 9.

Takeaways

1 Analyze enterprise risks if security budget shrinks.

2 Ensure tech expertise is represented in boardroom.

3 Conduct continuous security awareness training.

5 Research and employ industry best practices and security controls.

ISACA, *Better Tech Governance is Better for Business*, 9.

Polling Question

Okay, I'm following! But how do I bridge the tech governance gap?

Agenda:

1. The Leadership Gap
2. An IT Governance Framework
3. The Information Security Perspective

Another Assertion:

"Information is a key resource for all enterprises."

ISACA, *COBIT 5*, 13.

"From the time
that **information** is
created…

to the moment that
it is **destroyed…**

technology plays
a **significant role**."

ISACA, *COBIT 5*, 13.

“Information technology is increasingly advanced and has become pervasive in enterprises of all sizes, whether commercial, not-for-profit, or in the public sector.”

ISACA, *COBIT 5*, 13.

How can we create optimal **value** from information technology?

ISACA, *COBIT 5*, 13.

How can we create optimal **value** from information technology?

By **balancing** benefit realization with risk levels and resource use.

ISACA, *COBIT 5*, 13.

Value Creation

Risks & Resources

Benefits

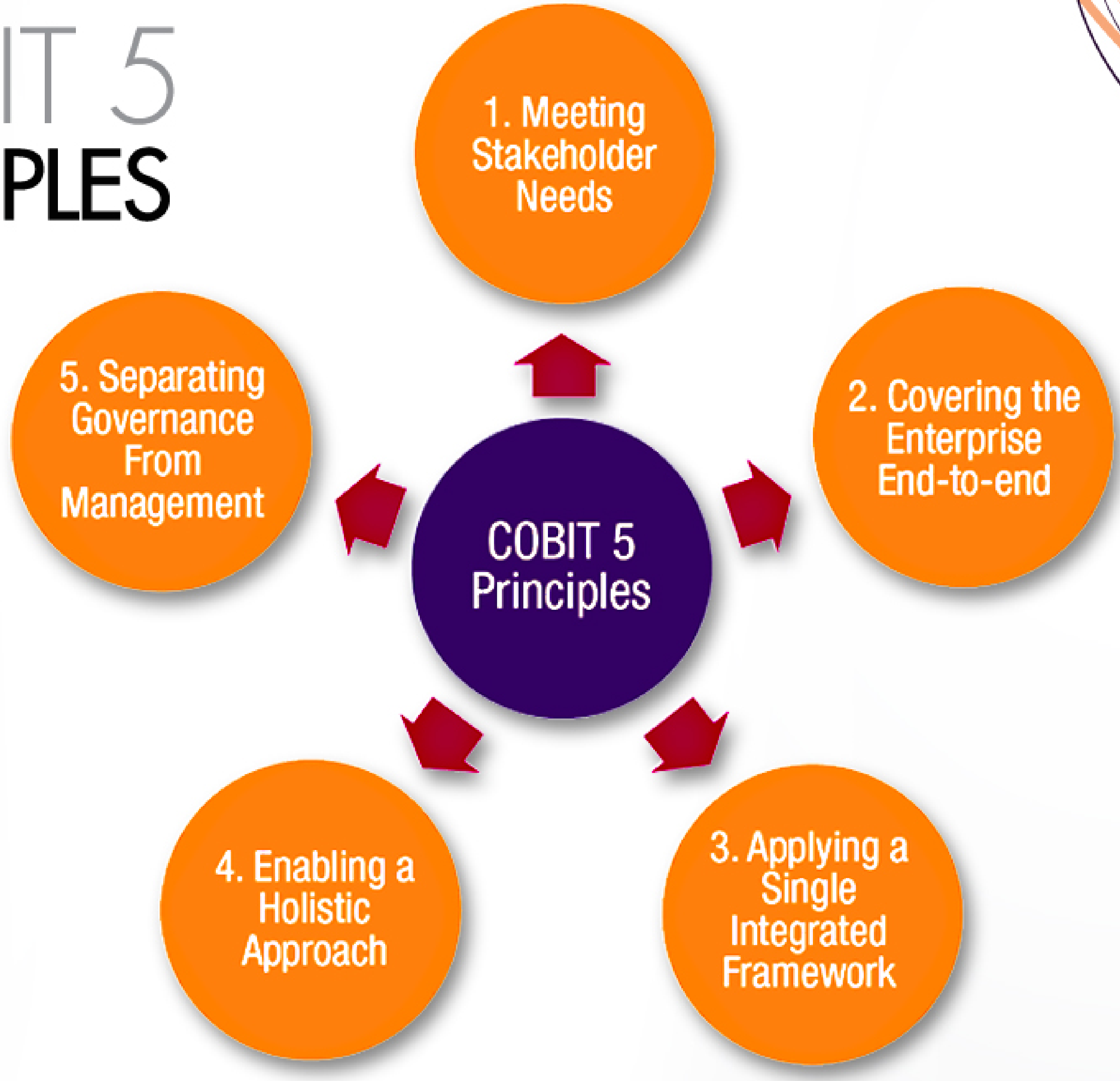
COBIT® 5

AN ISACA® FRAMEWORK

"The COBIT 5 framework is built on five basic **principles** and includes extensive guidance on **enablers** for **governance** and **management** of enterprise IT."

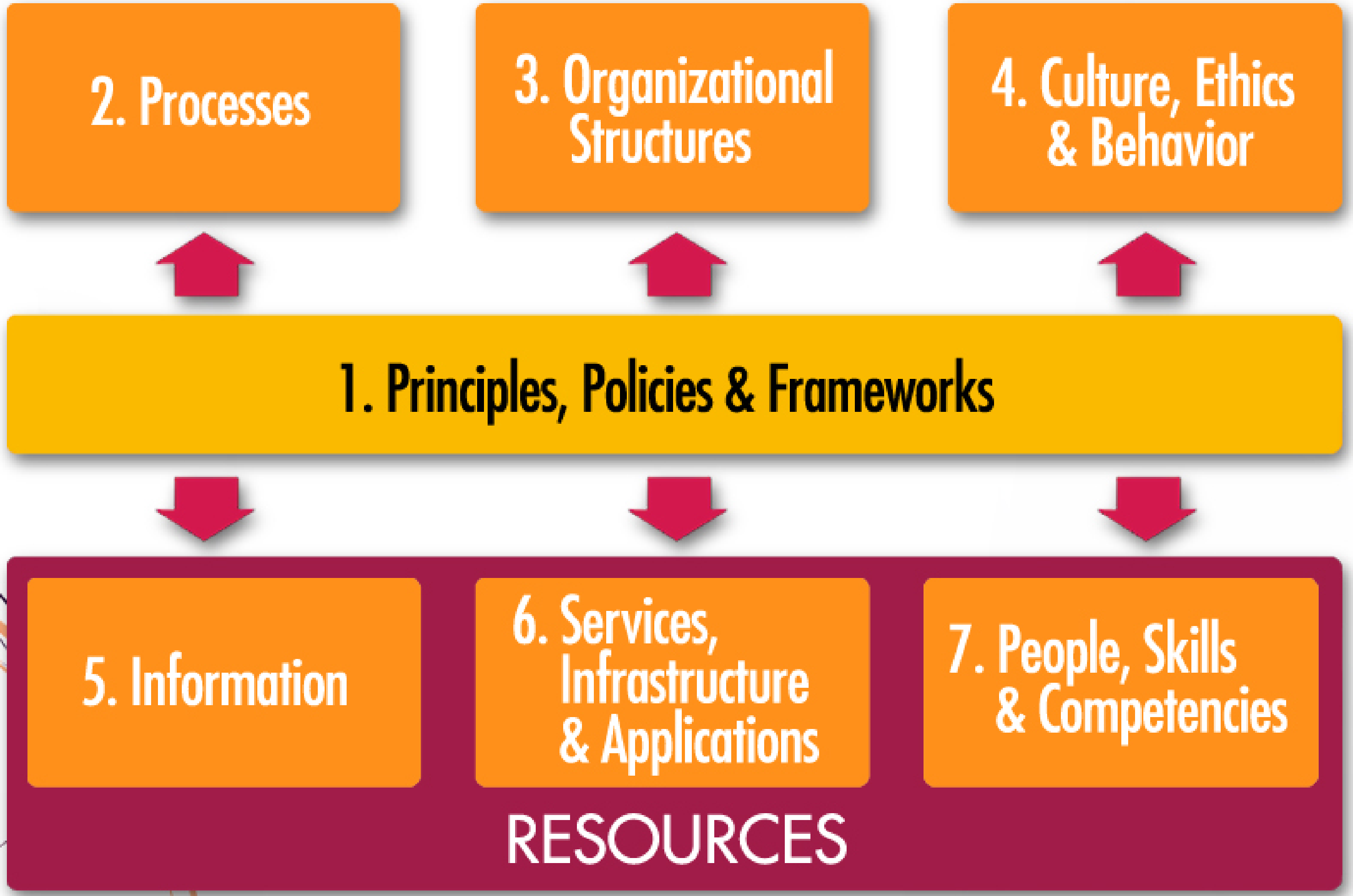
ISACA, *COBIT 5*, 11.

COBIT 5 PRINCIPLES


1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
COBIT 5 Principles
5. Separating Governance From Management
4. Enabling a Holistic Approach
3. Applying a Single Integrated Framework

ISACA, *COBIT 5*, fig. 2.

COBIT 5 ENTERPRISE ENABLERS



2. Processes

3. Organizational Structures

4. Culture, Ethics & Behavior

1. Principles, Policies & Frameworks

5. Information

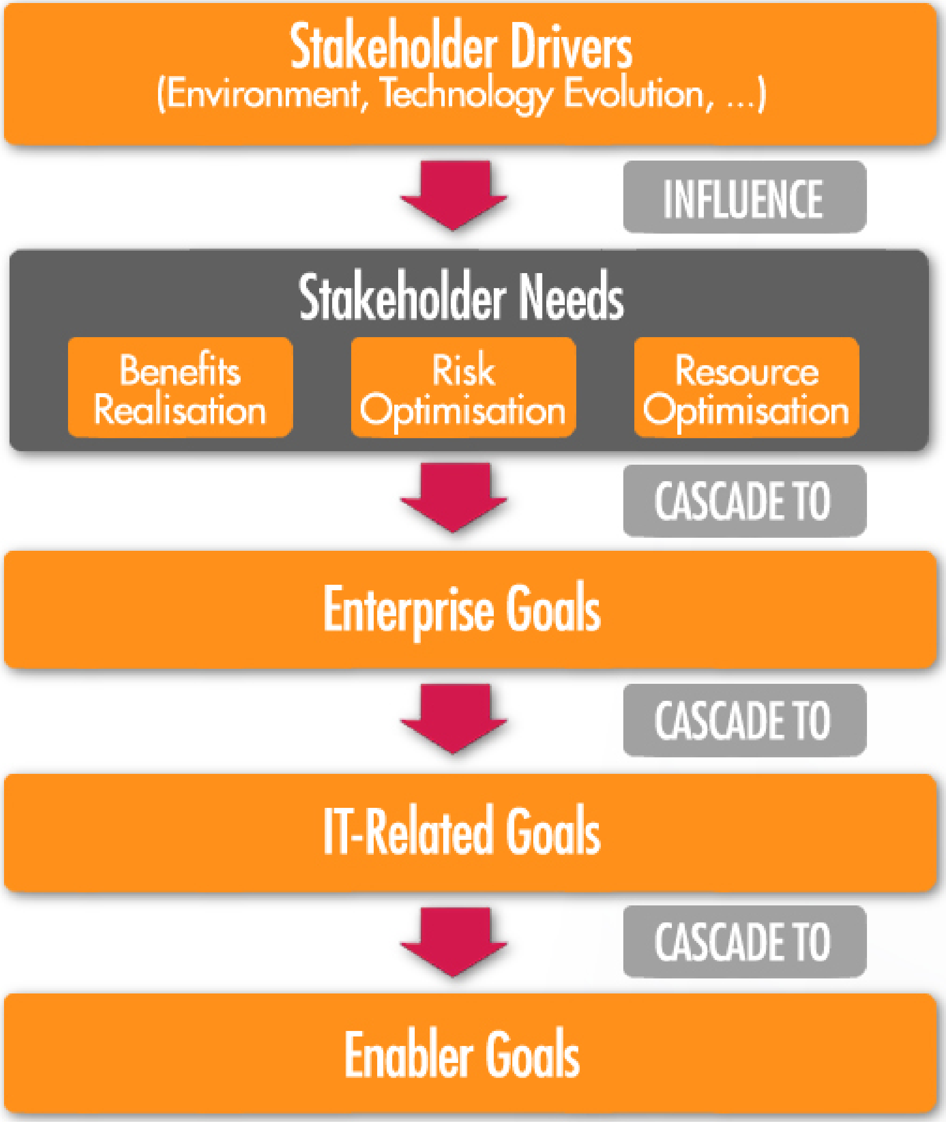
6. Services, Infrastructure & Applications

7. People, Skills & Competencies

RESOURCES

ISACA, *COBIT 5*, fig. 12.

COBIT 5 GOALS CASCADE OVERVIEW



Stakeholder Drivers
(Environment, Technology Evolution, ...)

INFLUENCE

Stakeholder Needs

Benefits Realisation

Risk Optimisation

Resource Optimisation

CASCADE TO

Enterprise Goals

CASCADE TO

IT-Related Goals

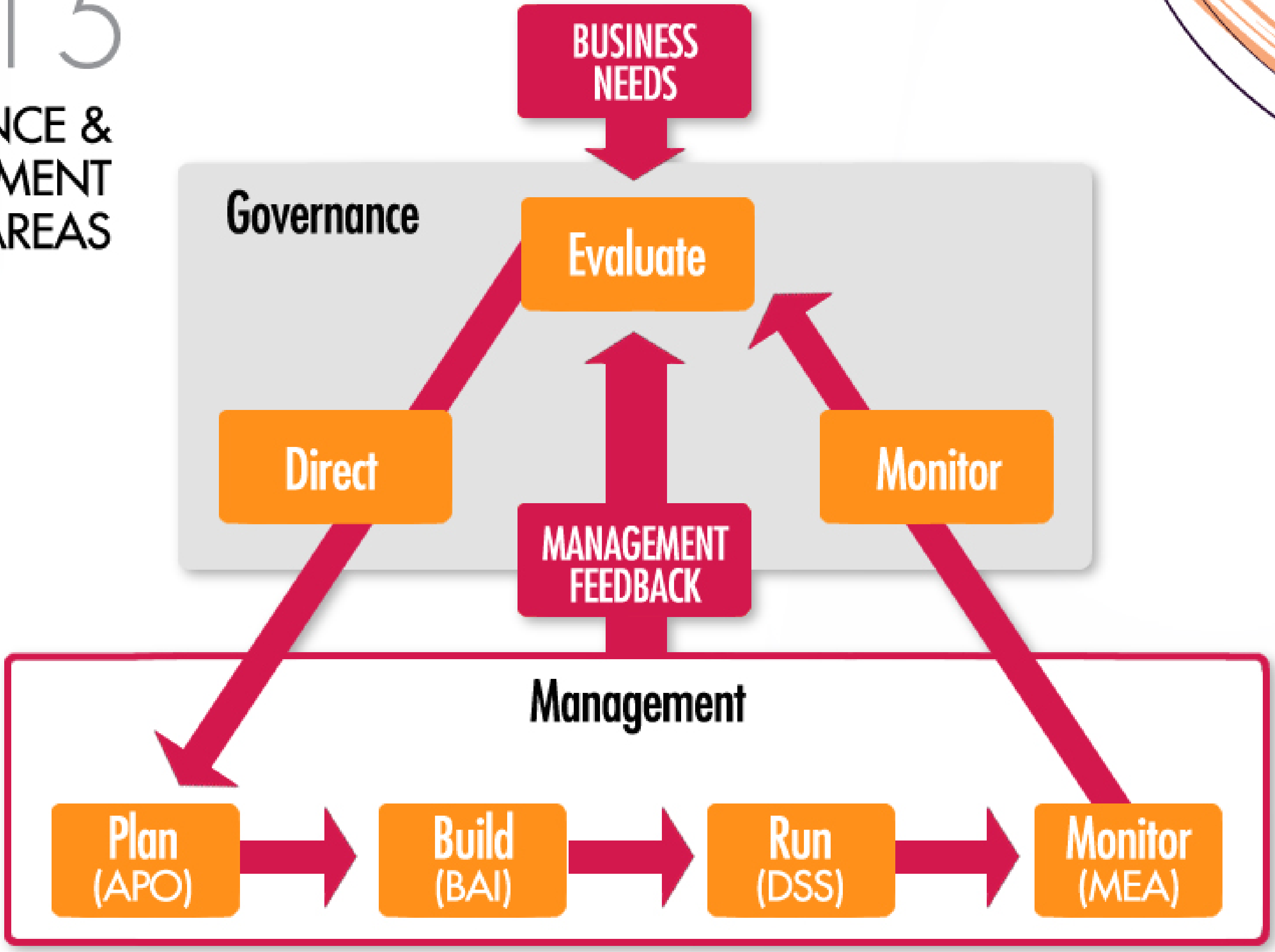
CASCADE TO

Enabler Goals

ISACA, *COBIT 5*, fig. 4.

COBIT 5

GOVERNANCE & MANAGEMENT KEY AREAS



ISACA, *COBIT 5*, fig. 15.

So, what should I expect from my enterprise and its executives?

Desired Outcomes

1 Maintain high-quality information to support business decisions.

2 Generate business value from IT-enabled investments, i.e., achieve strategic goals and realize business benefits through effective and innovative use of IT.

3 Achieve operational excellence through the reliable and efficient application of technology.

4 Maintain IT-related risk at an acceptable level.

5 Optimize the cost of IT services and technology.

6 Comply with ever-increasing relevant laws, regulations, contractual agreements and policies.

ISACA, *COBIT 5*, 13.

Desired Outcomes

1 Maintain high-quality information to support business decisions.

2 Generate business value from IT-enabled investments, i.e., achieve strategic goals and realize business benefits through effective

4 Maintain IT-related risk at an acceptable level.

5 Optimize the cost of IT services and technology.

6 Comply with ever-increasing relevant laws, regulations, contractual agreements and policies.

ISACA, *COBIT 5*, 13.

Desired Outcomes

1 Maintain high-quality information to support business decisions.

2 Generate business value from IT-enabled investments, i.e., achieve strategic goals and realize business benefits through effective and innovative use of IT.

6 Comply with ever-increasing relevant laws, regulations, contractual agreements and policies.

regulations, contractual agreements and policies.

ISACA, *COBIT 5*, 13.

Polling Question

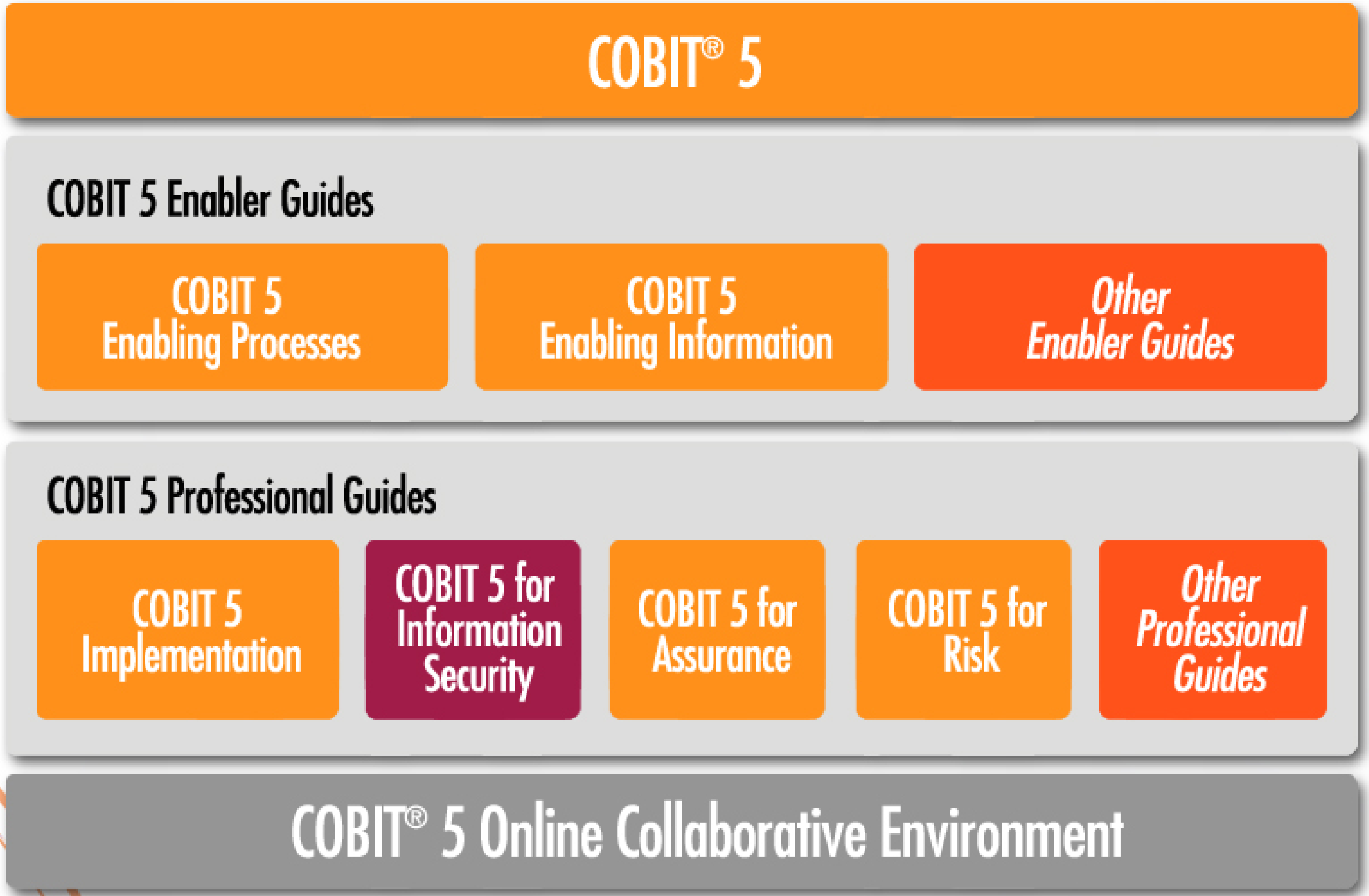
Agenda:

1. The Leadership Gap
2. An IT Governance Framework
3. The Information Security Perspective

COBIT® 5

FOR INFORMATION SECURITY

COBIT 5 PRODUCT FAMILY



COBIT® 5

COBIT 5 Enabler Guides

- COBIT 5 Enabling Processes
- COBIT 5 Enabling Information
- *Other Enabler Guides*

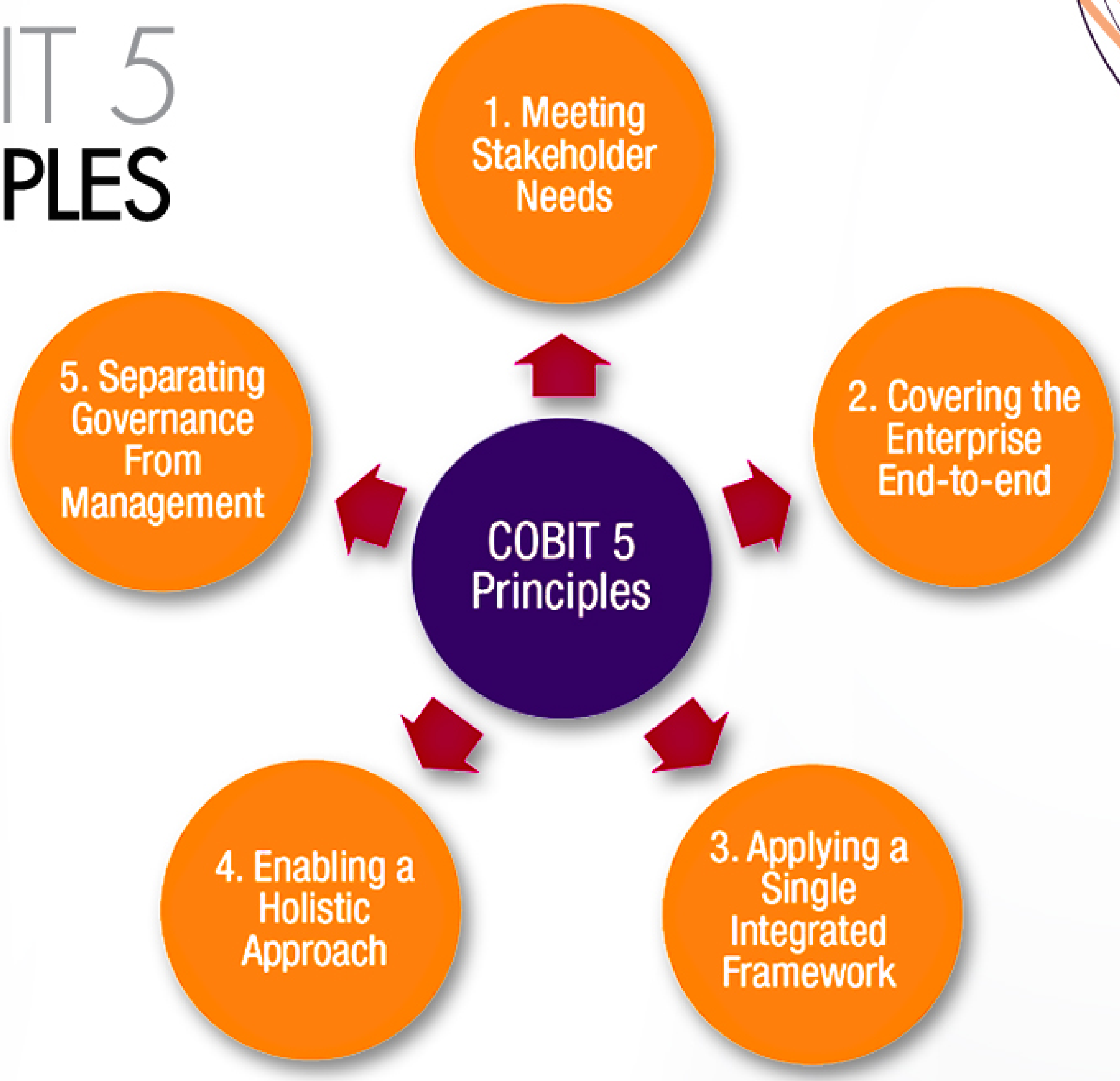
COBIT 5 Professional Guides

- COBIT 5 Implementation
- COBIT 5 for Information Security
- COBIT 5 for Assurance
- COBIT 5 for Risk
- *Other Professional Guides*

COBIT® 5 Online Collaborative Environment

ISACA, *COBIT 5 for Information Security*, fig. 1.

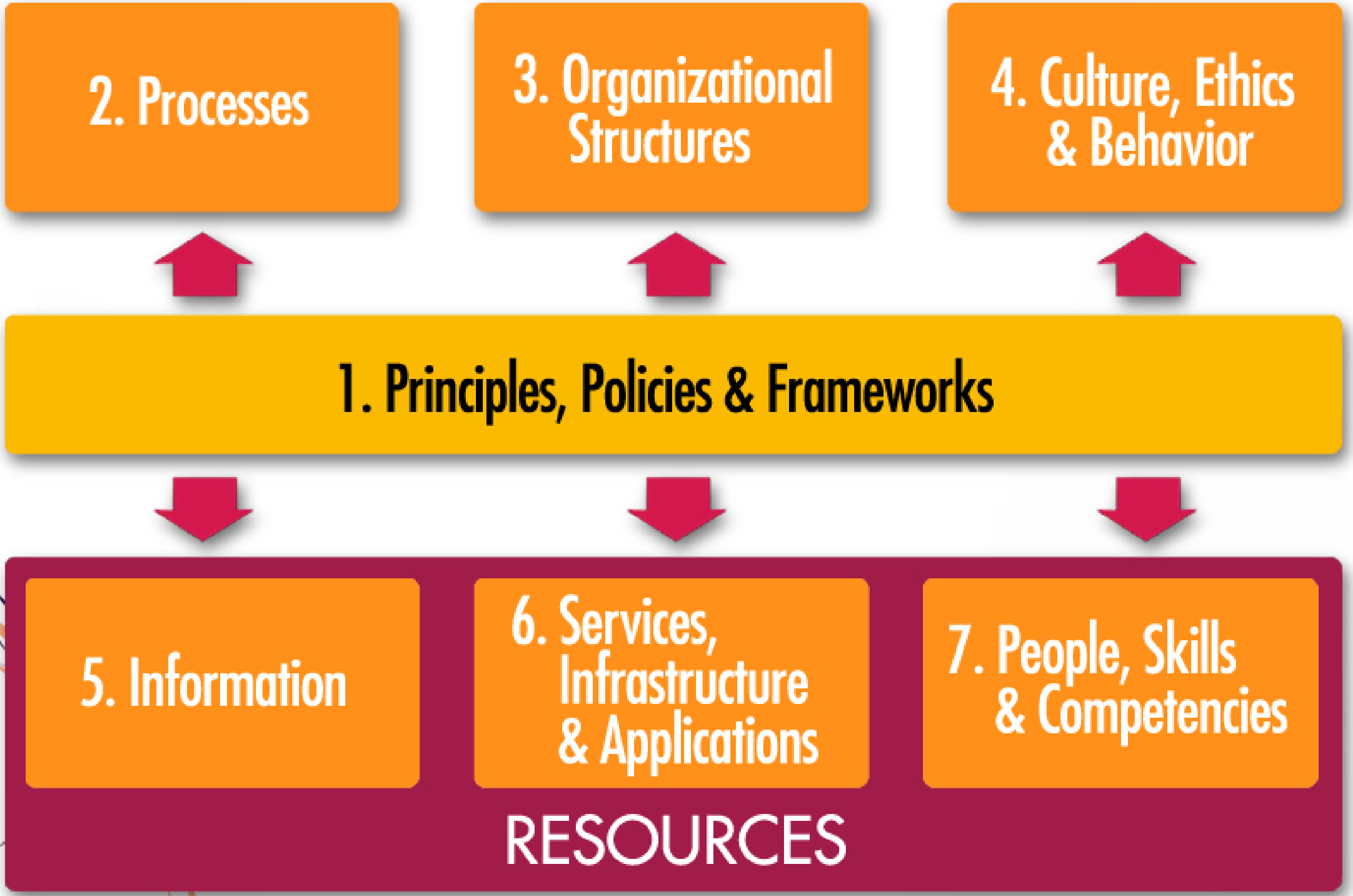
COBIT 5 PRINCIPLES



1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
COBIT 5 Principles
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management

ISACA, *COBIT 5*, fig. 2.

COBIT 5 ENTERPRISE ENABLERS



2. Processes

3. Organizational Structures

4. Culture, Ethics & Behavior

1. Principles, Policies & Frameworks

5. Information

6. Services, Infrastructure & Applications

7. People, Skills & Competencies

RESOURCES

ISACA, *COBIT 5*, fig. 12.

COBIT 5
FOR INFORMATION SECURITY & ENABLERS

COBIT 5 for Information Security provides specific guidance related to all enablers:

1. Information security **policies, principles and frameworks**
2. **Processes**, including information security-specific details and activities
3. Information security-specific **organizational structures**
4. In terms of **culture, ethics and behavior**, factors determining the success of information security governance and management
5. Information security-specific **information** types for enabling information security governance and management within the enterprise
6. **Service capabilities** required to provide information security and related functions to an enterprise
7. **People, skills and competencies** specific for information security

ISACA, *COBIT 5 for Information Security*, 26.

Information Security
DEFINED

ISACA defines information security as something that:

Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability)

ISACA, *COBIT 5 for Information Security,* 19.

Information Security
DEFINED

ISACA defines information security as something that:

"Confidentiality" means preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information.

ISACA, *COBIT 5 for Information Security*, 19.

Information Security
DEFINED

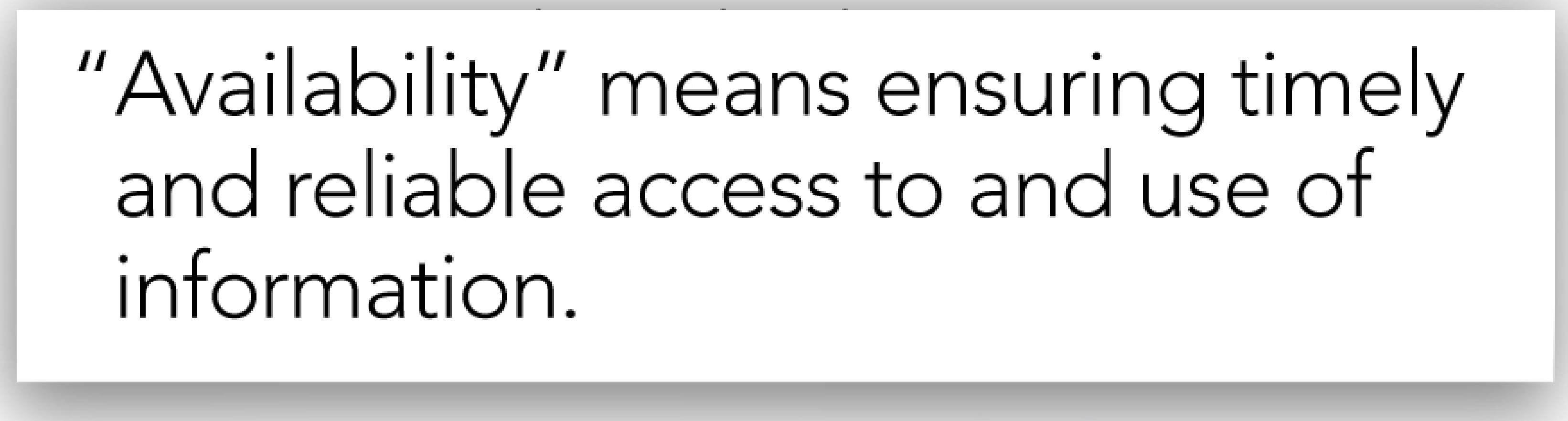
ISACA defines information security as something that:

"Integrity" means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

ISACA, *COBIT 5 for Information Security,* 19.

Information Security
DEFINED

ISACA defines information security as something that:



“Availability” means ensuring timely and reliable access to and use of information.

ISACA, *COBIT 5 for Information Security*, 19.

prin·ci·ple

/'prinsəpəl/

noun

1. An enabler of governance and of management. Comprises the values and fundamental assumptions held by the enterprise, the beliefs that guide and put boundaries around the enterprise's decision making, communication within and outside the enterprise, and stewardship—caring for assets owned by another.

ISACA, *Glossary*.

Information Security
PRINCIPLES

The principles are structured to enable three tasks:

1. Support the business
2. Defend the business
3. Promote responsible information security behavior

ISACA®
Trust in, and value from, information systems

Information Security Forum

(ISC)²®

ISACA, *COBIT 5 for Information Security,* 29.

Information Security
PRINCIPLES

1. Support the business

1.1 Focus on the business to ensure that information security is integrated into essential business activities.

1.2 Deliver quality and value to stakeholders to ensure that information security delivers value and meets business requirements.

ISACA, *COBIT 5 for Information Security*, 29.

Information Security
PRINCIPLES

1. Support the business *continued*

1.3 Comply with relevant legal and regulatory requirements to ensure that statutory obligations are met, stakeholder expectations are managed and civil or criminal penalties are avoided.

1.4 Provide timely and accurate information on security performance to support business requirements and manage information risks.

ISACA, *COBIT 5 for Information Security*, 29.

Information Security
PRINCIPLES

1. Support the business *continued*

1.5 Evaluate current and future information threats to analyze and assess emerging information security threats so that informed, timely action to mitigate risk can be taken.

1.6 Promote continuous improvement in information security to reduce costs, improve efficiency and effectiveness, and promote a culture of continuous improvement in information security.

ISACA, *COBIT 5 for Information Security,* 29.

Information Security
PRINCIPLES

2. Defend the business

2.1 Adopt a risk-based approach to ensure that risk is treated in a consistent and effective manner.

2.2 Protect classified information to prevent disclosure to unauthorized individuals.

ISACA, *COBIT 5 for Information Security*, 29.

Information Security
PRINCIPLES

2. Defend the business *continued*

2.3 Concentrate on critical business applications to prioritize scarce information security resources by protecting the business applications in which a security incident would have the greatest business impact.

2.4 Develop systems securely to build quality, cost-effective systems on which business people can rely.

ISACA, *COBIT 5 for Information Security,* 29.

Information Security
PRINCIPLES

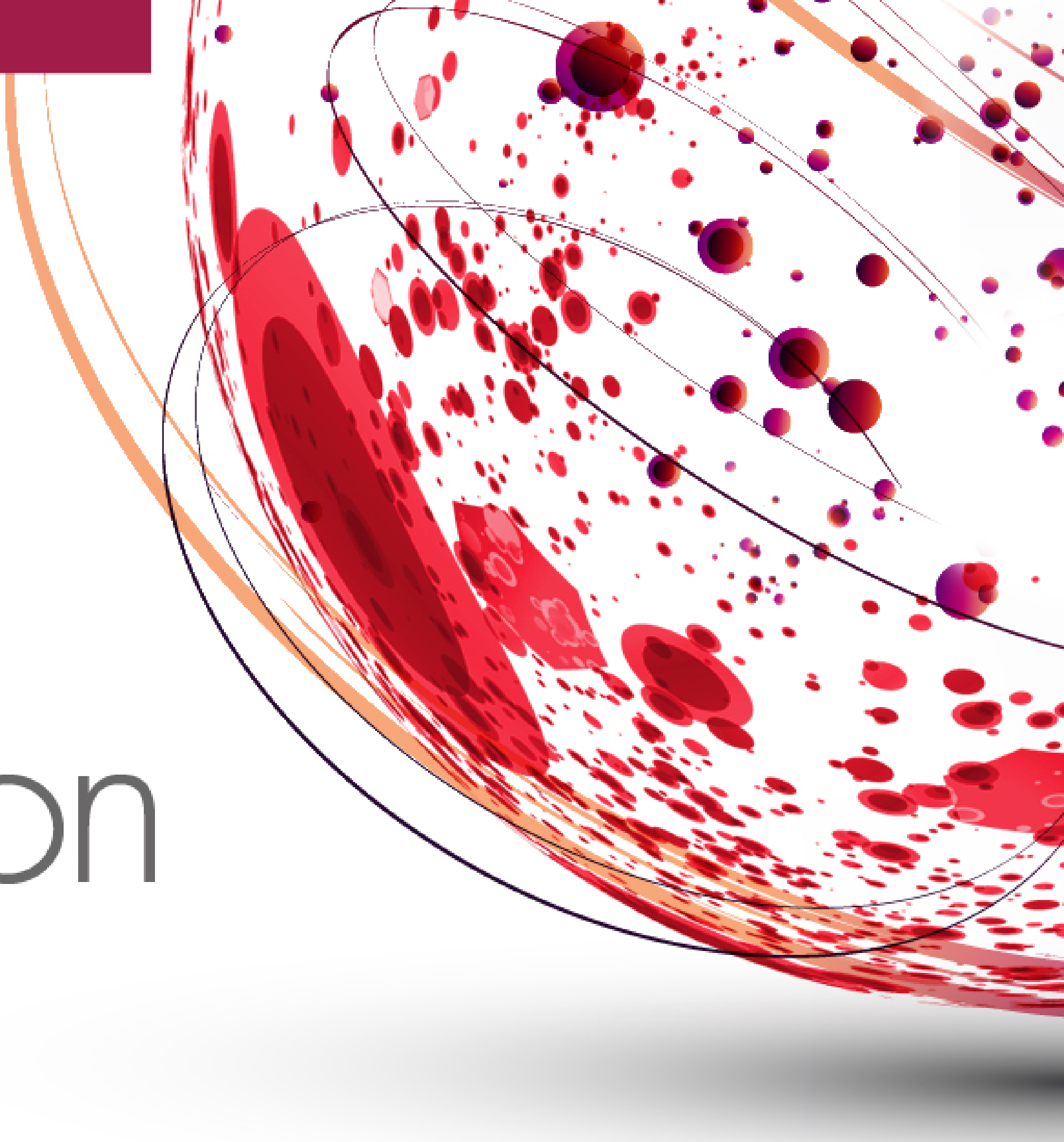
3. Promote responsible information security behavior

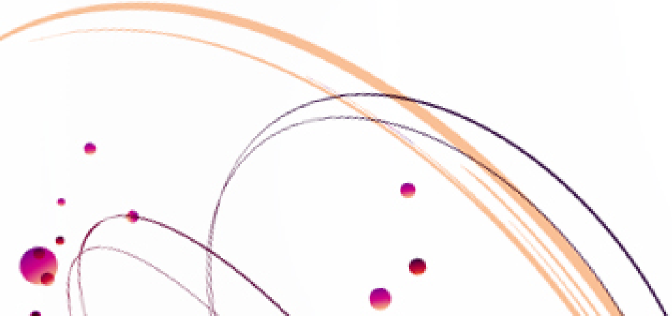
3.1 **Act in a professional and ethical manner** to ensure that information security-related activities are performed in a reliable, responsible, and effective manner.

3.2 **Foster a security-positive culture** to provide a positive security influence on the behavior of end users, reduce the likelihood of security incidents occurring, and limit their potential business impact.

ISACA, *COBIT 5 for Information Security*, 29.

Polling Question



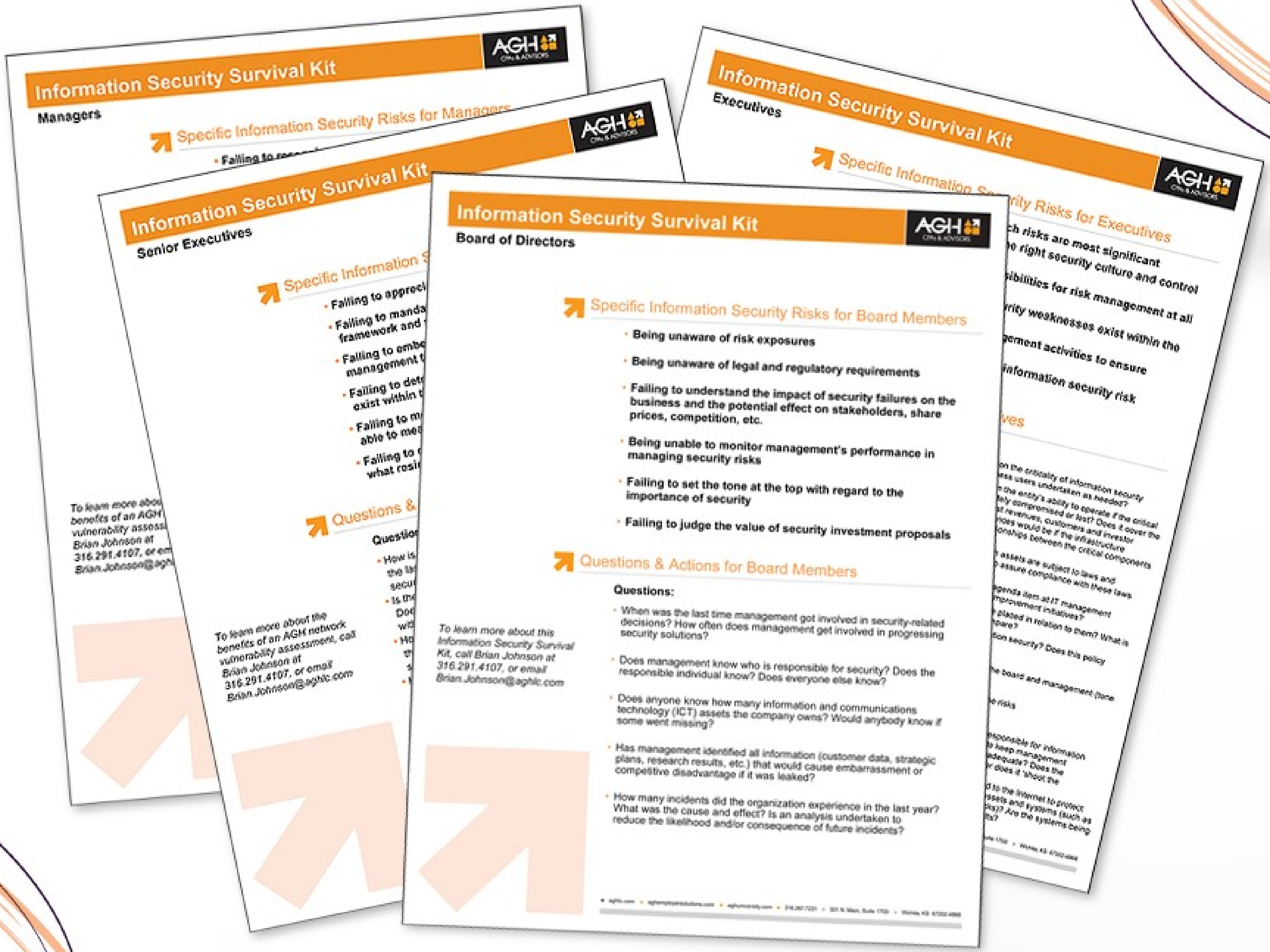


How can I introduce these principles?

COBIT
Security Baseline

An Information Security Survival Kit 2nd Edition

IT Governance Institute, *COBIT Security Baseline: An Information Security Survival Kit.*



Information Security Survival Kit

Managers

Specific Information Security Risks for Managers

Information Security Survival Kit

Senior Executives

To learn more about the benefits of an AGH network vulnerability assessment, call Brian Johnson at 316.291.4107, or email Brian.Johnson@aghlc.com

Information Security Survival Kit

Executives

Specific Information Security Risks for Executives

Information Security Survival Kit

AGH CPAs & ADVISORS

Board of Directors

Specific Information Security Risks for Board Members

- **Being unaware of risk exposures**
- **Being unaware of legal and regulatory requirements**
- **Failing to understand the impact of security failures on the business and the potential effect on stakeholders, share prices, competition, etc.**
- **Being unable to monitor management's performance in managing security risks**
- **Failing to set the tone at the top with regard to the importance of security**
- **Failing to judge the value of security investment proposals**

Questions & Actions for Board Members

Questions:

- When was the last time management got involved in security-related decisions? How often does management get involved in progressing security solutions?
- Does management know who is responsible for security? Does the responsible individual know? Does everyone else know?
- Does anyone know how many information and communications technology (ICT) assets the company owns? Would anybody know if some went missing?
- Has management identified all information (customer data, strategic plans, research results, etc.) that would cause embarrassment or competitive disadvantage if it was leaked?
- How many incidents did the organization experience in the last year? What was the cause and effect? Is an analysis undertaken to reduce the likelihood and/or consequence of future incidents?

To learn more about this Information Security Survival Kit, call Brian Johnson at 316.291.4107, or email Brian.Johnson@aghlc.com

aghlc.com • aghemployersolutions.com • aghuniversity.com • 316.267.7231 • 301 N. Main, Suite 1700 • Wichita, KS 67202-4868

IT Governance Institute, *COBIT Security Baseline: An Information Security Survival Kit.*

Agenda:

1. The Leadership Gap
2. An IT Governance Framework
3. The Information Security Perspective

Message Objective:

By introducing information security principles that you can reliably use to understand and address your security needs…

Message Objective:

…you will be better prepared to protect and sustain your information systems and the processes that rely upon them.

References

Information Security Forum. "Principles for Information Security Practitioners." Information Security Forum, 2010. https://www.isaca.org/Knowledge-Center/Standards/Documents/Principles-for-Info-Sec-Practitioners-poster.pdf.

———. "Principles for Information Security Practitioners: An Overview." Information Security Forum, 2010. https://www.isaca.org/Knowledge-Center/Standards/Documents/Principles-for-Info-Sec-Practitioners-overview.pdf.

ISACA. An Introduction to the Business Model for Information Security. Rolling Meadows, IL: ISACA, 2009. http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf.

———. "Avoid the Tech Governance Gap." Rolling Meadows, IL: ISACA, 2017. http://www.isaca.org/SiteCollectionDocuments/Better-Tech-Governance-Is-Better-for-Business-Infographic.pdf.

———. "Better Tech Governance Is Better for Business." Rolling Meadows, IL: ISACA, 2017. http://www.isaca.org/Knowledge-Center/Research/Documents/Better-Tech-Governance-Is-Better-for-Business-Report.pdf.

———. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, IL: ISACA, 2012.

———. COBIT 5 for Information Security. Rolling Meadows, IL: ISACA, 2012.

———. "Glossary," 2018. https://www.isaca.org/Pages/Glossary.aspx.

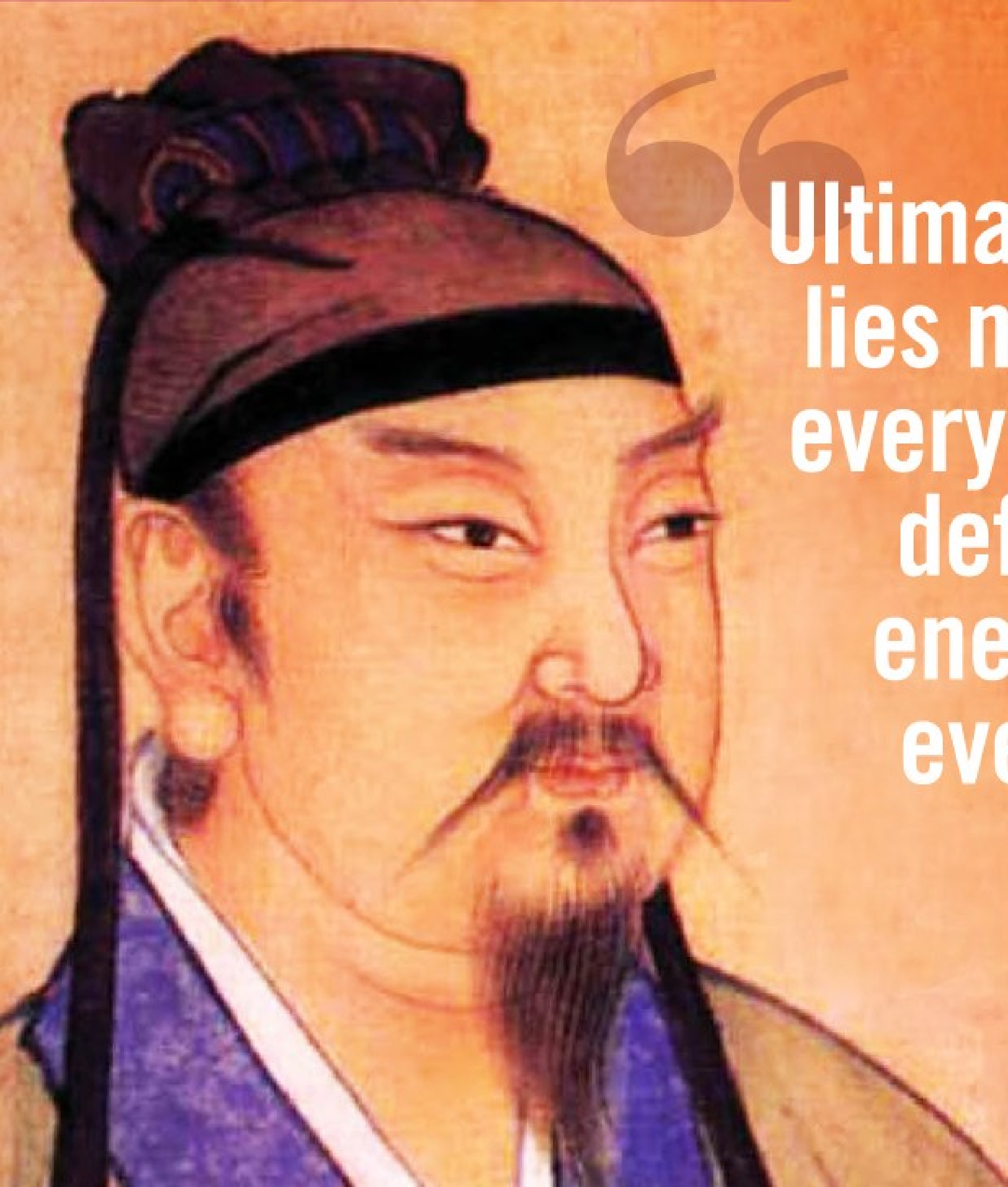
———. The Business Model for Information Security. Rolling Meadows, IL: ISACA, 2010. http://www.isaca.org/Knowledge-Center/BMIS/Documents/BMIS-22Sept2010-Research.pdf.

———. "The Business Model for Information Security Brochure." ISACA, 2009. http://www.isaca.org/Knowledge-Center/BMIS/Documents/BMISBrochure.pdf.

IT Governance Institute. COBIT Security Baseline: An Information Security Survival Kit. 2nd ed. Rolling Meadows, IL: IT Governance Institute, 2007. http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT-Security-Baseline-2ndEd-Research-18Sept07.pdf.

———. Information Security Governance: Guidance for Boards of Directors and Executive Management. 2nd ed. Rolling Meadows, IL: IT Governance Institute, 2006. http://www.isaca.org/Knowledge-Center/Research/Documents/Information-Security-Govenance-for-Board-of-Directors-and-Executive-Management_res_Eng_0510.pdf.

———. Information Security Governance: Guidance for Information Security Managers. Rolling Meadows, IL: IT Governance Institute, 2008. http://www.isaca.org/Knowledge-Center/Research/Documents/InfoSec-Guidance-for-Information-Security-Managers_res_Eng_0508.pdf.



> Ultimate excellence lies not in winning every battle, but in defeating the enemy without ever fighting.

– *Sun Tzu*

Questions?

brian.johnson@aghlc.com