Trust in, and value from, information systems

如何面对网络安全问题的挑战？
治理企业的IT是关键

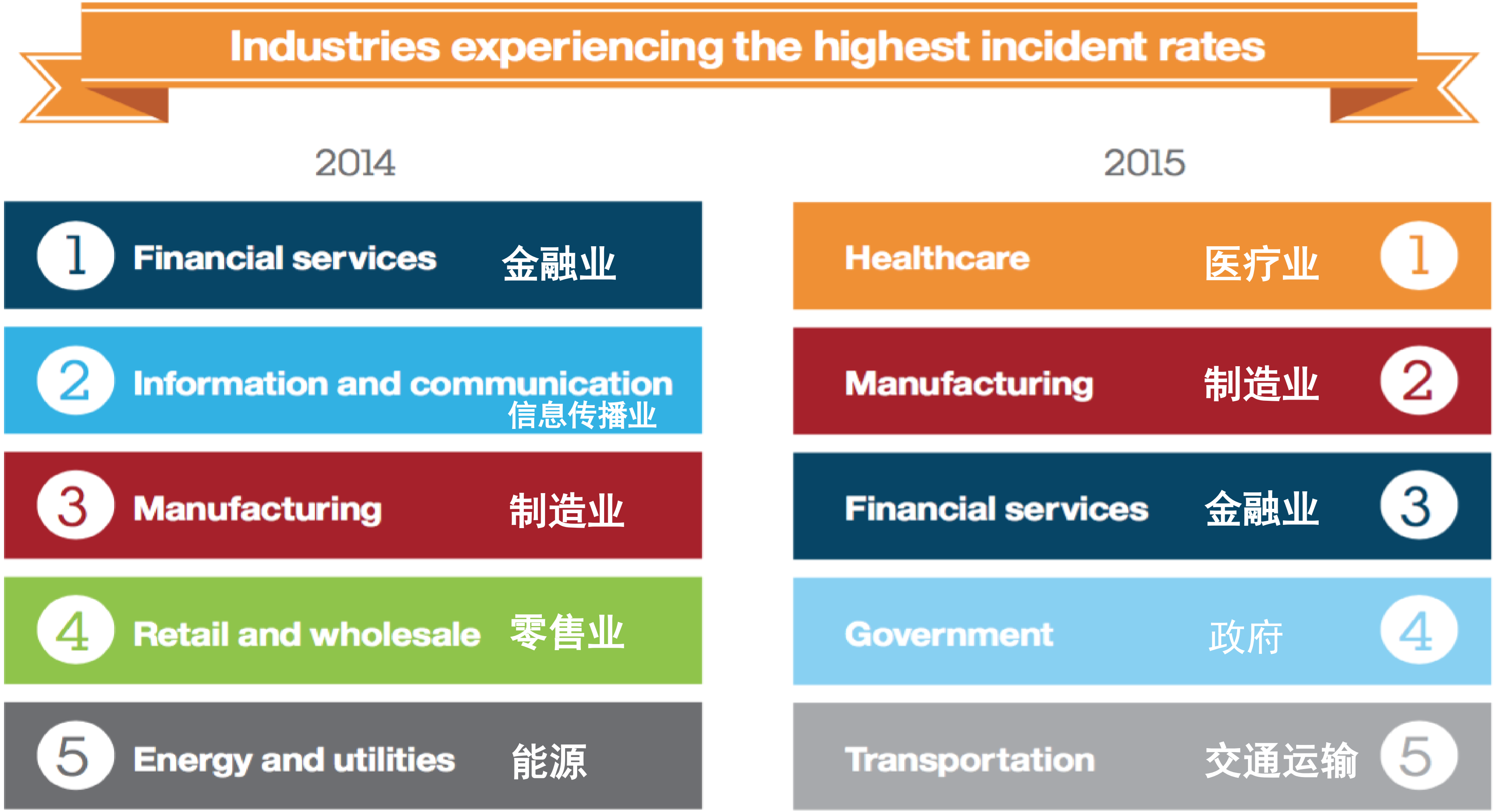
Leonard Ong, CISA, CISM, CRISC, CGEIT, CoBIT 5 Implementer & Assessor

14 July 2016

议程

1. 网络安全现状
2. 如何利用IT治理来解决网络安全问题？
3. 要点概述

不断更换的头号网络攻击对象



Industries experiencing the highest incident rates

	2014	2015
1	Financial services 金融业	Healthcare 医疗业
2	Information and communication 信息传播业	Manufacturing 制造业
3	Manufacturing 制造业	Financial services 金融业
4	Retail and wholesale 零售业	Government 政府
5	Energy and utilities 能源	Transportation 交通运输

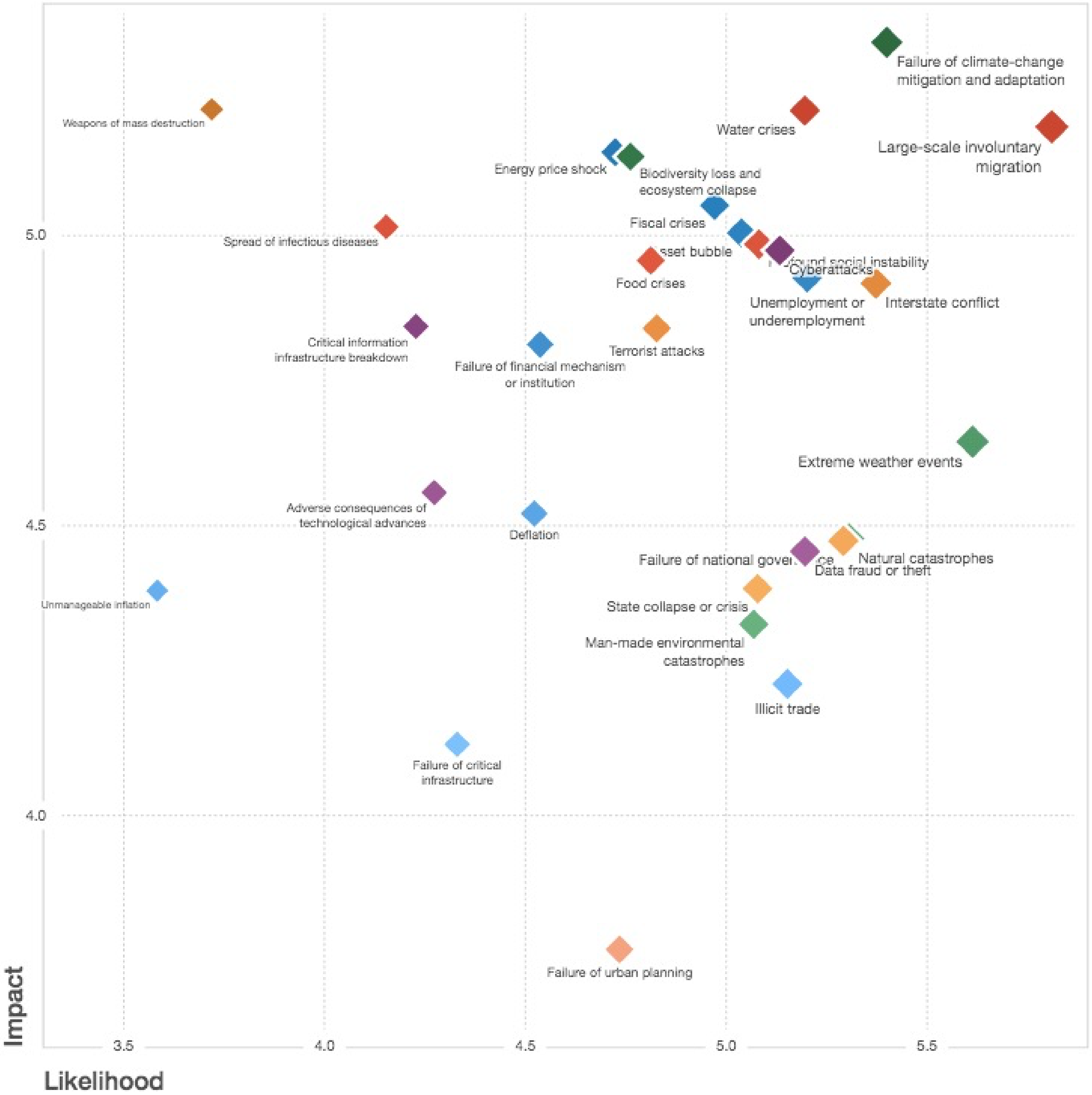
2016 IBM Cyber Security Intelligence Index

网络安全现状

— **KETAN DHOLAKIA, CISM, CRISC**
MANAGING PARTNER, MACLEAR
CHICAGO, ILLINOIS, USA
ISACA MEMBER SINCE 2007

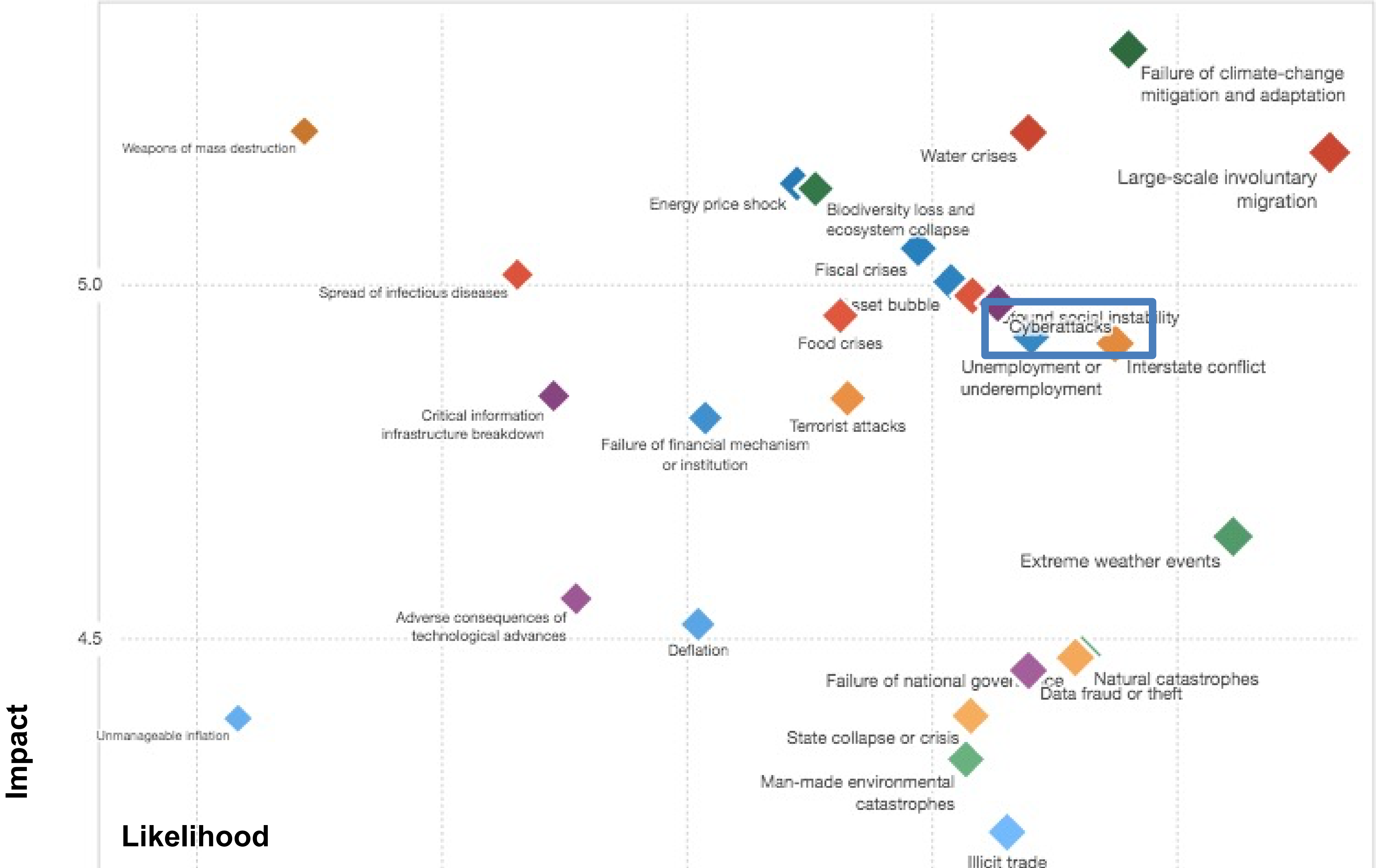
ACCOMPLISH MORE

全球网络风险概况 2016



ISACA®
Trust in, and value from, information systems

全球网络风险概况 2016



3,400+ RESPONDENTS WORLDWIDE

来自全球3400多名受访者

83% 将网络攻击视为前三大企业隐患之一，但只有

VIEW CYBERATTACKS AS ONE OF TOP 3 THREATS TO BUSINESS, BUT ONLY

38% 表示他们对未来可能的冲击做好了充分的准备

FEEL PREPARED FOR A SOPHISTICATED ATTACK

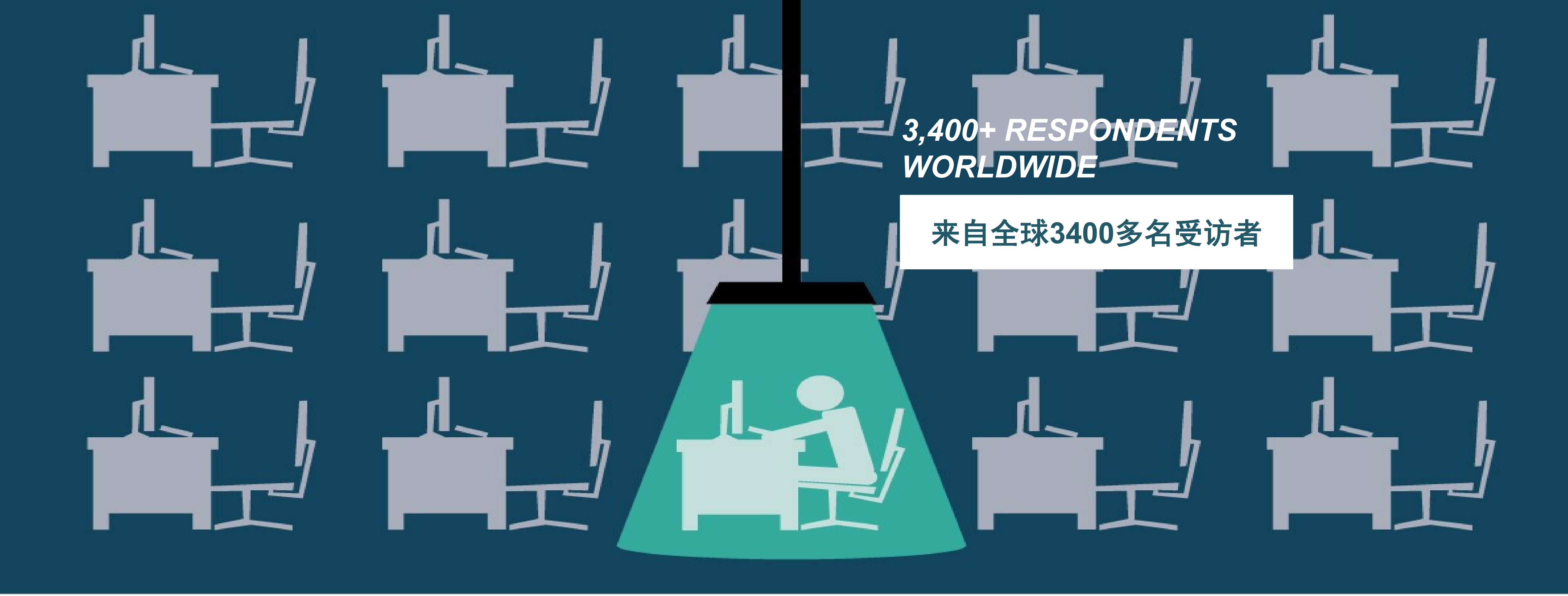
VISIT: WWW.ISACA.ORG/CYBERSECURITYREPORT

ISACA®

Trust in, and value from, information systems

CSX™

CYBERSECURITY NEXUS



3,400+ RESPONDENTS WORLDWIDE

来自全球3400多名受访者

86% 认为现有人才市场上网络安全技能短缺

SEE A CYBERSECURITY SKILLS SHORTAGE

VISIT: WWW.ISACA.ORG/CYBERSECURITYREPORT

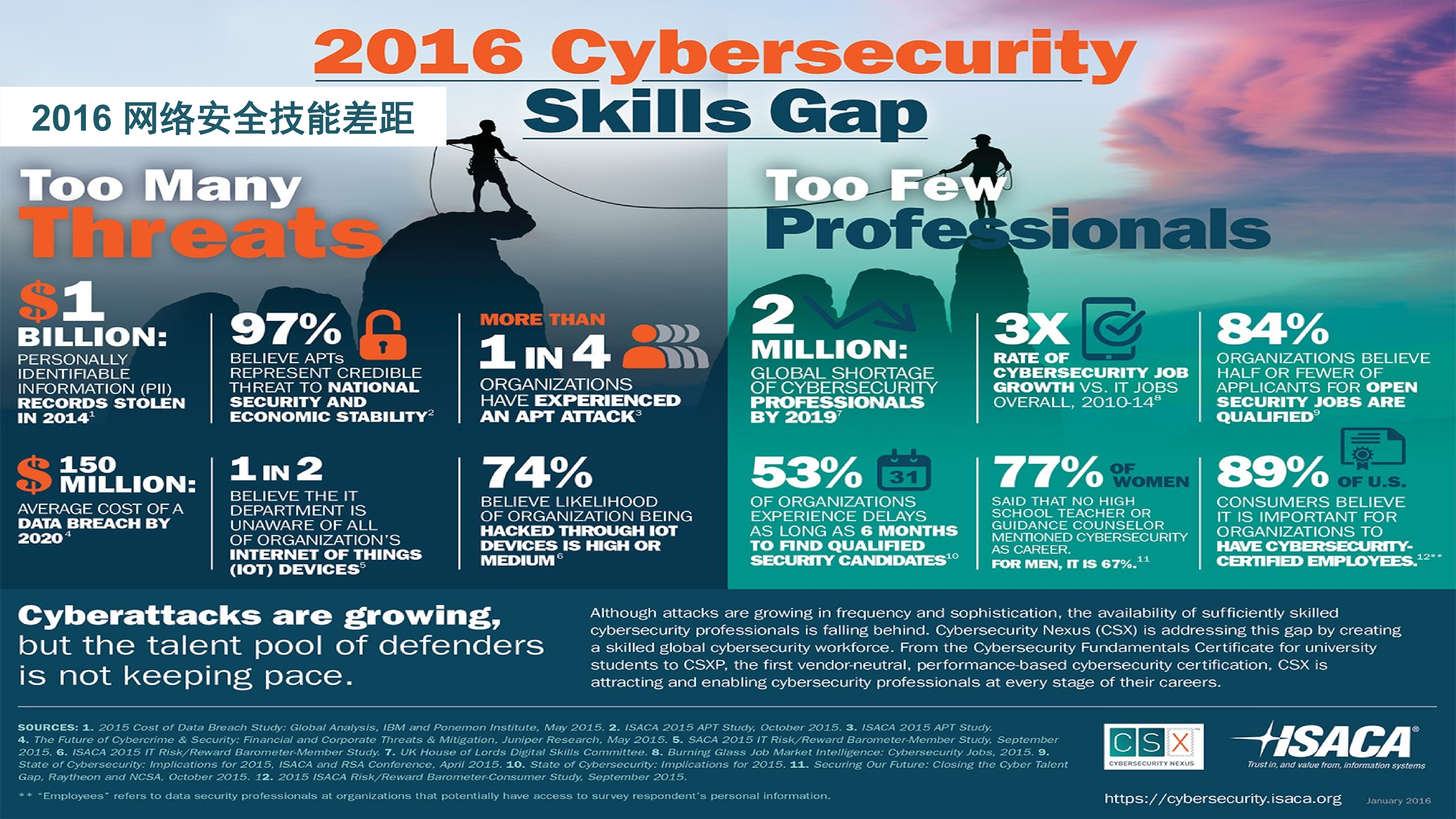
ISACA®

Trust in, and value from, information systems

CSX™

CYBERSECURITY NEXUS

2016 网络安全技能差距



2016 Cybersecurity Skills Gap

Too Many Threats

$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) **RECORDS STOLEN IN 2014**[1]

97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO **NATIONAL SECURITY AND ECONOMIC STABILITY**[2]

MORE THAN 1 IN 4 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[3]

$150 MILLION: AVERAGE COST OF A **DATA BREACH BY 2020**[4]

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S **INTERNET OF THINGS (IOT) DEVICES**[5]

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING **HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM**[6]

Too Few Professionals

2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY **PROFESSIONALS BY 2019**[7]

3X RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14[8]

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR **OPEN SECURITY JOBS ARE QUALIFIED**[9]

53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS **6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES**[10]

77% OF WOMEN SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. **FOR MEN, IT IS 67%.**[11]

89% OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO **HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.**[12**]

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

SOURCES: 1. *2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015.* **2.** *ISACA 2015 APT Study, October 2015.* **3.** *ISACA 2015 APT Study.* **4.** *The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015.* **5.** *SACA 2015 IT Risk/Reward Barometer-Member Study, September 2015.* **6.** *ISACA 2015 IT Risk/Reward Barometer-Member Study.* **7.** *UK House of Lords Digital Skills Committee.* **8.** *Burning Glass Job Market Intelligence: Cybersecurity Jobs, 2015.* **9.** *State of Cybersecurity: Implications for 2015, ISACA and RSA Conference, April 2015.* **10.** *State of Cybersecurity: Implications for 2015.* **11.** *Securing Our Future: Closing the Cyber Talent Gap, Raytheon and NCSA, October 2015.* **12.** *2015 ISACA Risk/Reward Barometer-Consumer Study, September 2015.*

** "Employees" refers to data security professionals at organizations that potentially have access to survey respondent's personal information.

CSX CYBERSECURITY NEXUS

ISACA® Trust in, and value from, information systems

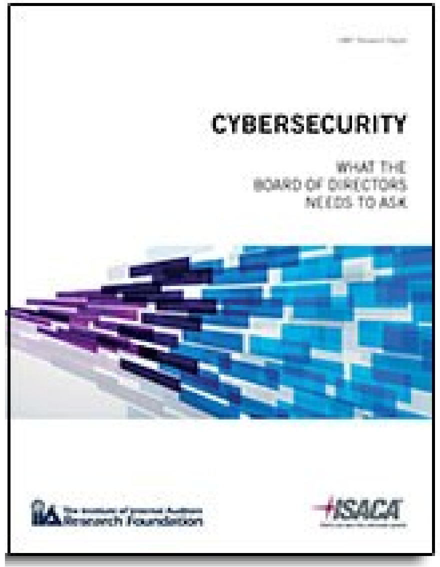
https://cybersecurity.isaca.org

January 2016

高层管理谈网络安全问题

- 65%董事成员表示网络安全风险处于高风险范围或已有所提高

只有14%表示他们参与了网络安全问题的处理，但有58%认为他们应该参与得更多。

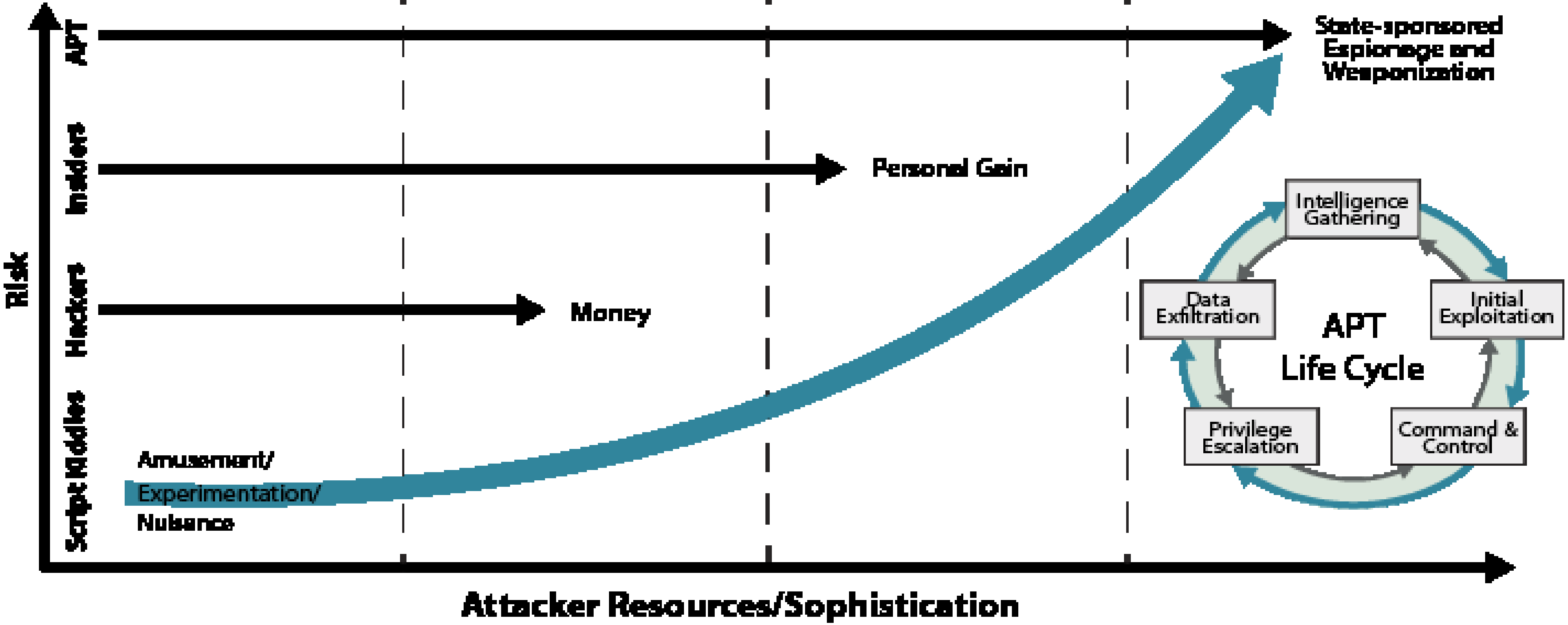


CYBERSECURITY

WHAT THE
BOARD OF DIRECTORS
NEEDS TO ASK

网络威胁的演变

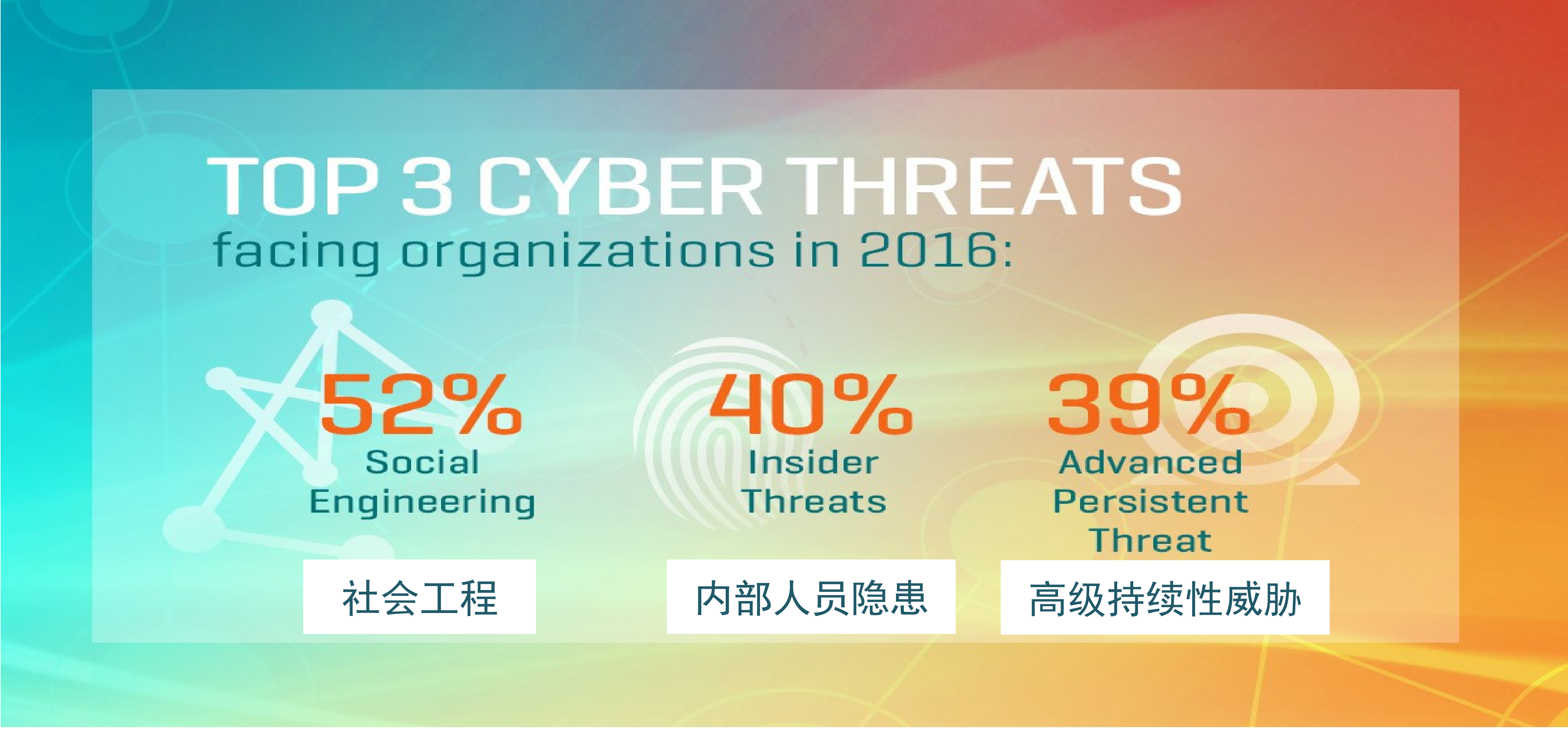
Unsophisticated Attackers (Script Kiddies)	Sophisticated Attackers (Hackers)	Corporate Espionage (Hackers)	State-sponsored Attacks Advanced Persistent Threat (APT)
You are attacked because you are on the Internet and have a vulnerability	You are attacked because you are on the Internet and have information of value	Your current or former employee seeks financial gain from selling your IP	You are targeted because of who you are, what you do, or the value of your IP



1980s/1990s → 2012

- > BrainBoot / Morris Worm
- > Polymorphic Viruses
- > Michelangelo
- > Concept Macro Virus
- > Melissa
- > "I Love You"
- > Anna Kournikova
- > Sircam
- > Code Red and Nimda
- > SQL Slammer
- > Blaster
- > Sobig
- > MyDoom
- > Netsky
- > Sasser
- > Storm botnet
- > Koobface
- > Conficker
- > Aurora
- > Mariposa
- > Stuxnet
- > WikiLeaks
- > Anonymous
- > LulzSec
- > Spy Eye / Zeus
- > Duqu
- > Flame

ISACA®
Trust in, and value from, information systems



TOP 3 CYBER THREATS

facing organizations in 2016:

52%
Social Engineering

社会工程

40%
Insider Threats

内部人员隐患

39%
Advanced Persistent Threat

高级持续性威胁

SOURCE:
ISACA'S JANUARY 2016 CYBERSECURITY SNAPSHOT, GLOBAL DATA,
WWW.ISACA.ORG/2016-CYBERSECURITY-SNAPSHOT

CSX™
CYBERSECURITY NEXUS

ISACA®
Trust in, and value from, information systems

JIMMY
Kimmel
LIVE!
abc
WEEKNIGHTS 11:35|10:35c

网络安全 与 IT治理

— **URMILLA PERSAD, CISA, CISM, CRISC**
IT AUDIT MANAGER, FIRST CITIZENS BANK LIMITED
PORT OF SPAIN, TRINIDAD & TOBAGO
ISACA MEMBER SINCE 2004

MORE **OPPORTUNITY**

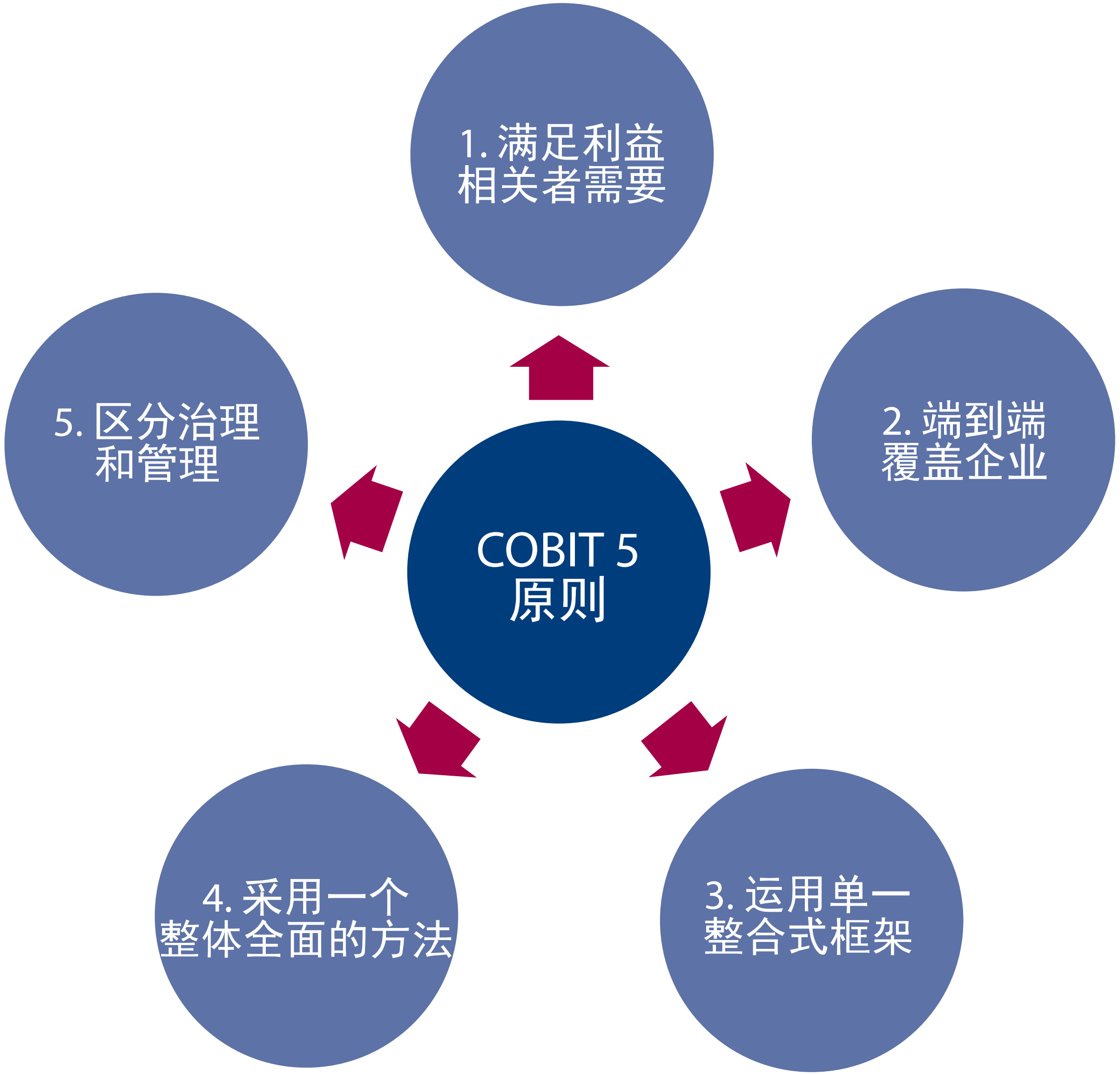
谁应该对网络安全问题负责？

- ✗ IT Security 计算机安全部门
- ✗ Enterprise Risk Management 企业风险管理部门
- ✗ Information Technology 信息科技部门
- ✗ Audit 审计部
- ✗ Business Leaders 企业领导
- ✗ Senior Management 高层管理
- ✓ Everyone 每个成员

How? When? What?

网络安全是企业的推动者

COBIT5 原则



COBIT 5
原则

1. 满足利益
相关者需要

2. 端到端
覆盖企业

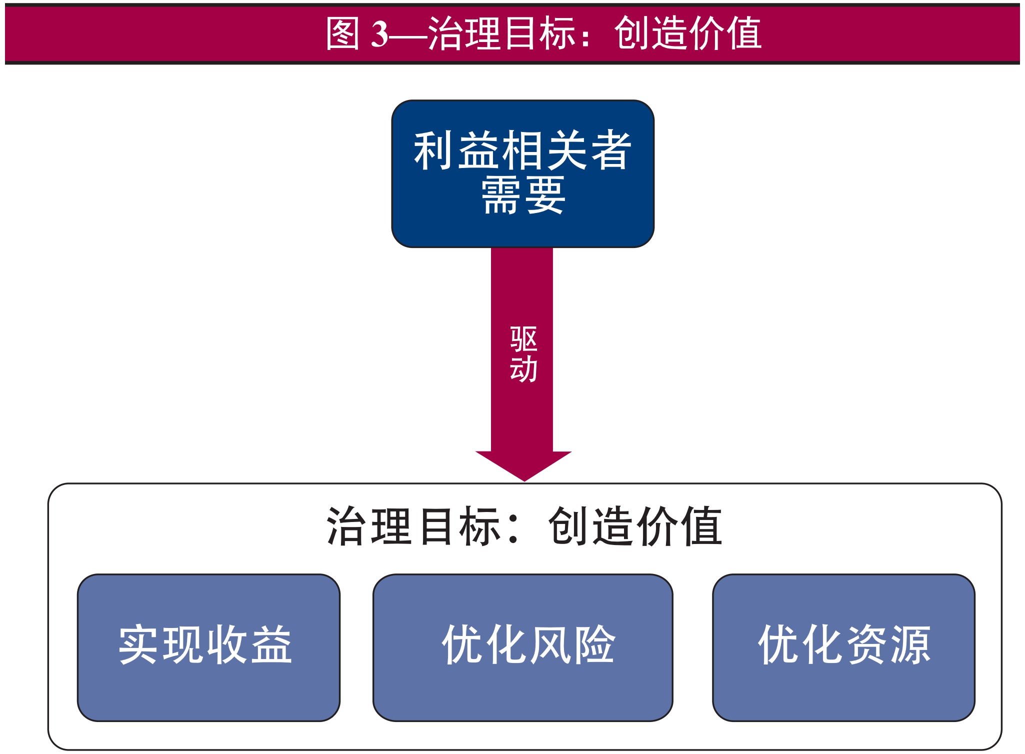
3. 运用单一
整合式框架

4. 采用一个
整体全面的方法

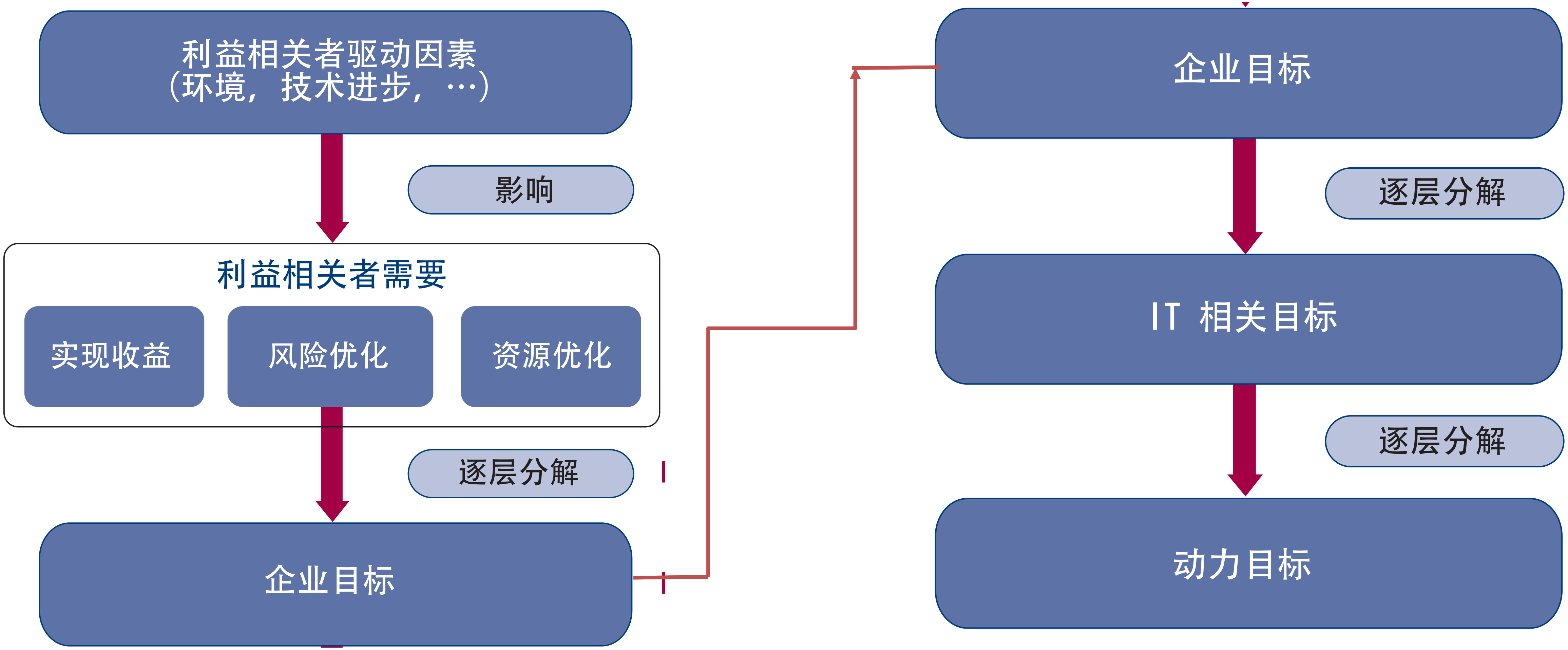
5. 区分治理
和管理

原则1：满足利益相关者需要

图 3—治理目标：创造价值



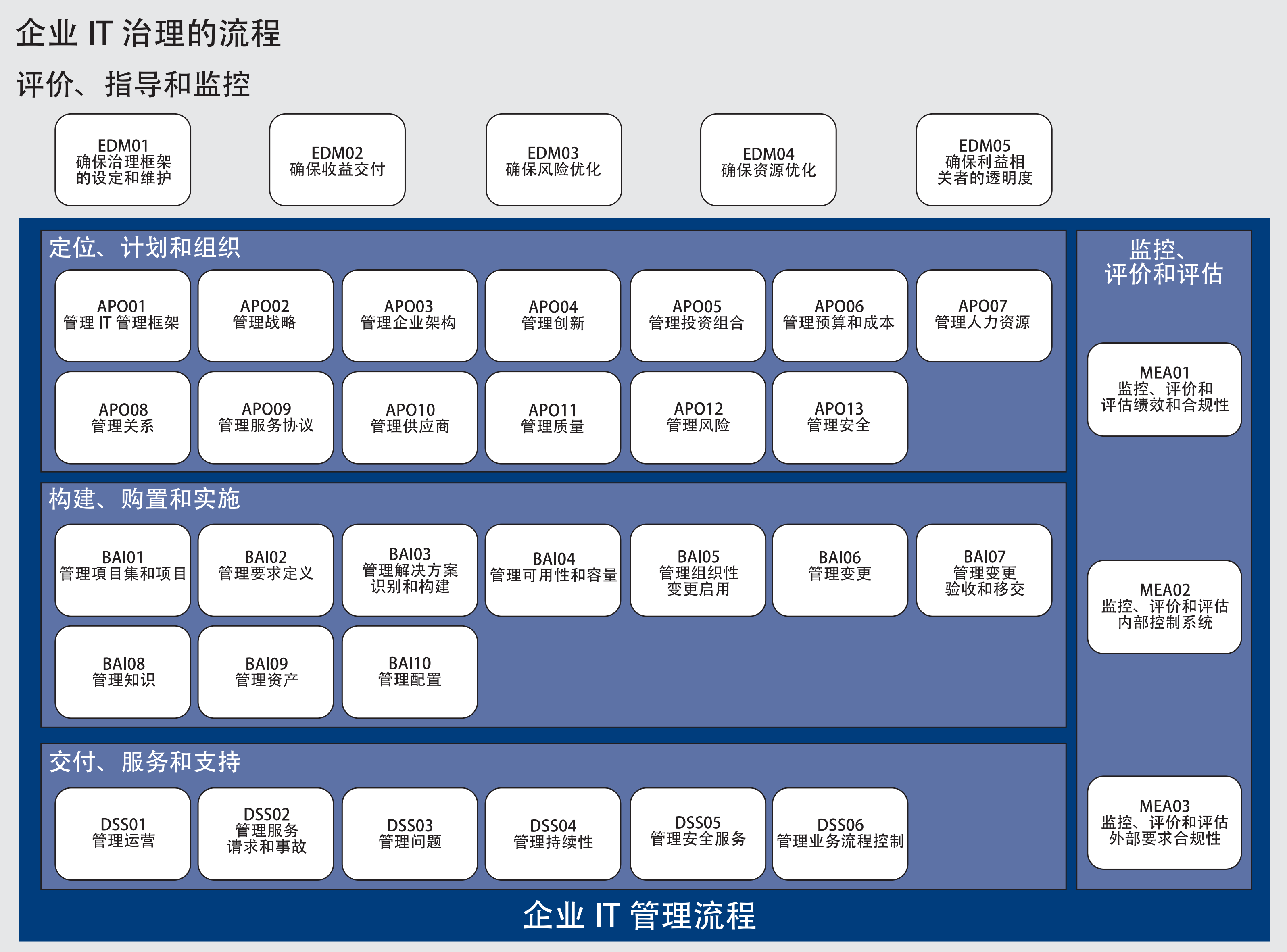
目标分层



ISACA®
Trust in, and value from, information systems

Pr Proprietary

原则2: 端到端覆盖企业



企业 IT 治理的流程

评价、指导和监控

- EDM01 确保治理框架的设定和维护
- EDM02 确保收益交付
- EDM03 确保风险优化
- EDM04 确保资源优化
- EDM05 确保利益相关者的透明度

定位、计划和组织

- APO01 管理 IT 管理框架
- APO02 管理战略
- APO03 管理企业架构
- APO04 管理创新
- APO05 管理投资组合
- APO06 管理预算和成本
- APO07 管理人力资源
- APO08 管理关系
- APO09 管理服务协议
- APO10 管理供应商
- APO11 管理质量
- APO12 管理风险
- APO13 管理安全

构建、购置和实施

- BAI01 管理项目集和项目
- BAI02 管理要求定义
- BAI03 管理解决方案识别和构建
- BAI04 管理可用性和容量
- BAI05 管理组织性变更启用
- BAI06 管理变更
- BAI07 管理变更验收和移交
- BAI08 管理知识
- BAI09 管理资产
- BAI10 管理配置

交付、服务和支持

- DSS01 管理运营
- DSS02 管理服务请求和事故
- DSS03 管理问题
- DSS04 管理持续性
- DSS05 管理安全服务
- DSS06 管理业务流程控制

监控、评价和评估

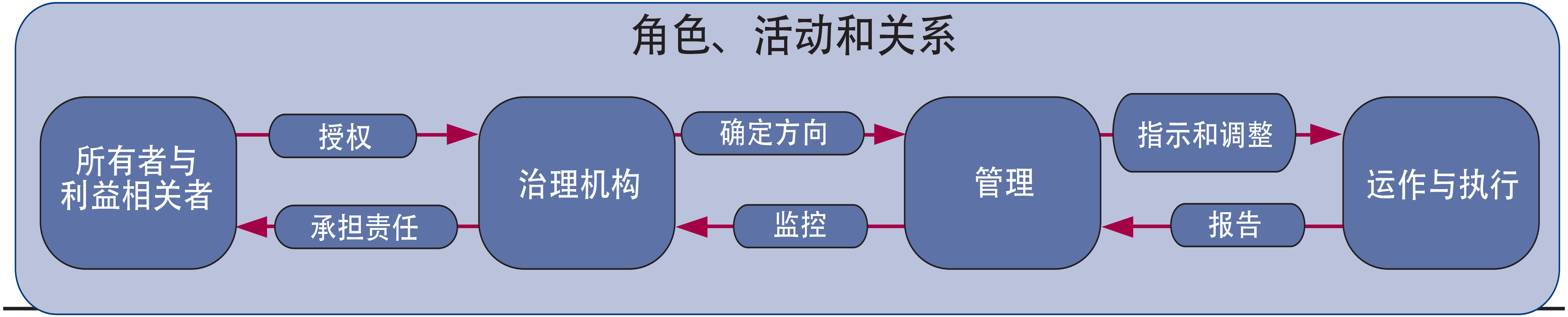
- MEA01 监控、评价和评估绩效和合规性
- MEA02 监控、评价和评估内部控制系统
- MEA03 监控、评价和评估外部要求合规性

企业 IT 管理流程

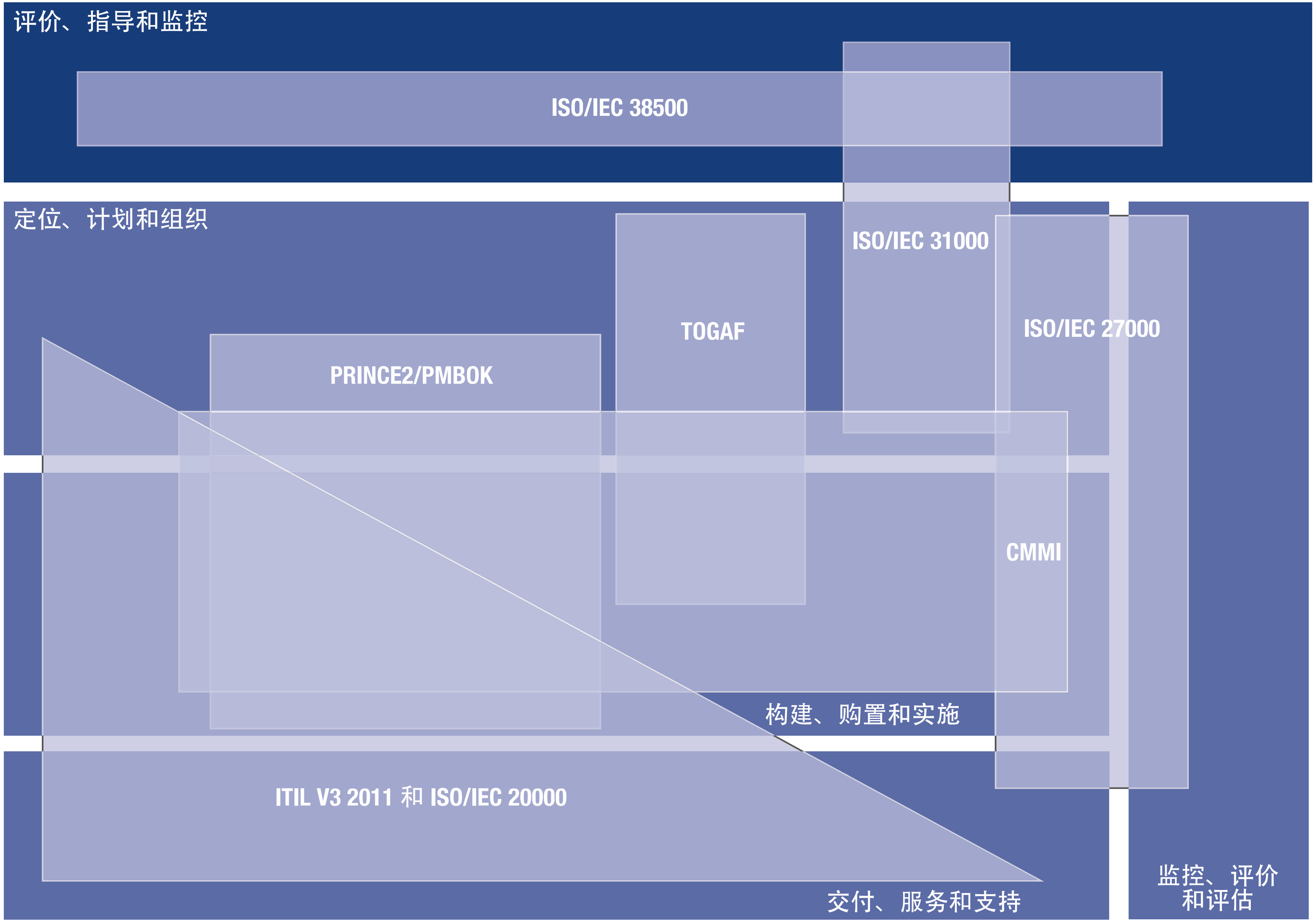
Pr Proprietary

ISACA®
Trust in, and value from, information systems

原则2: 端到端覆盖企业



原则3: 运用单一整合式框架


评价、指导和监控

ISO/IEC 38500

定位、计划和组织

ISO/IEC 31000

TOGAF

ISO/IEC 27000

PRINCE2/PMBOK

CMMI

构建、购置和实施

ITIL V3 2011 和 ISO/IEC 20000

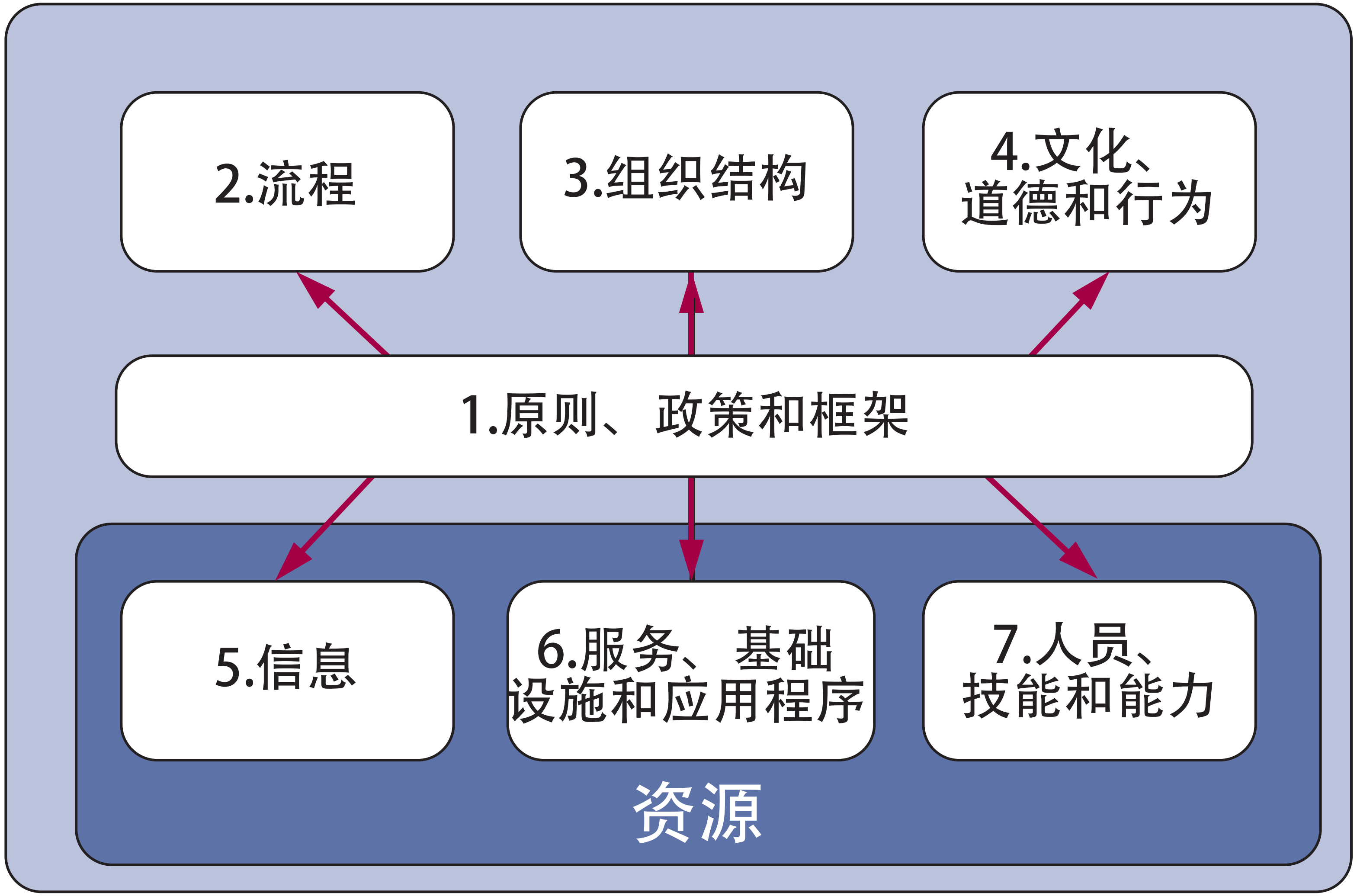
交付、服务和支持

监控、评价和评估

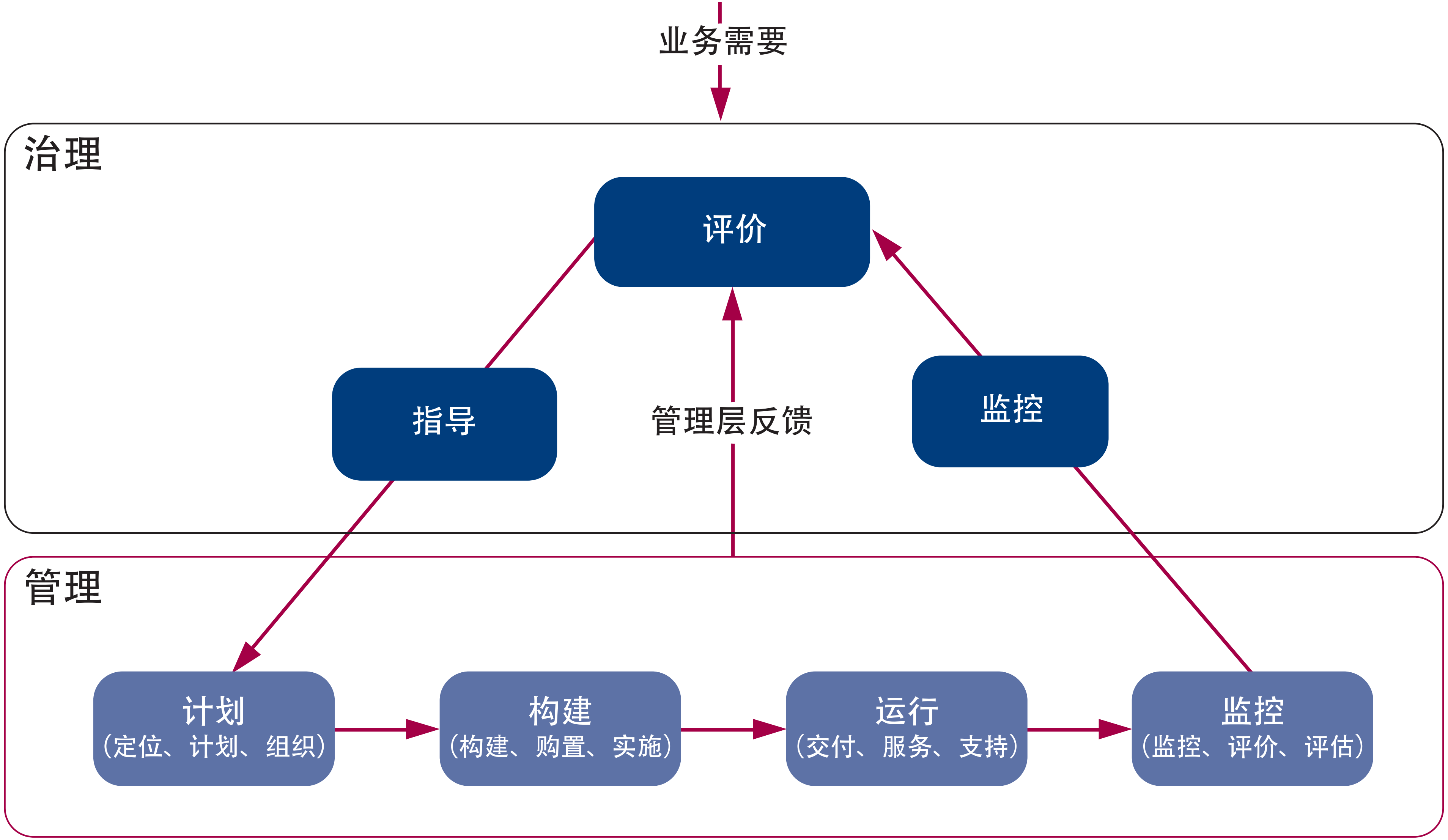
ISACA®
Trust in, and value from, information systems

Pr Proprietary

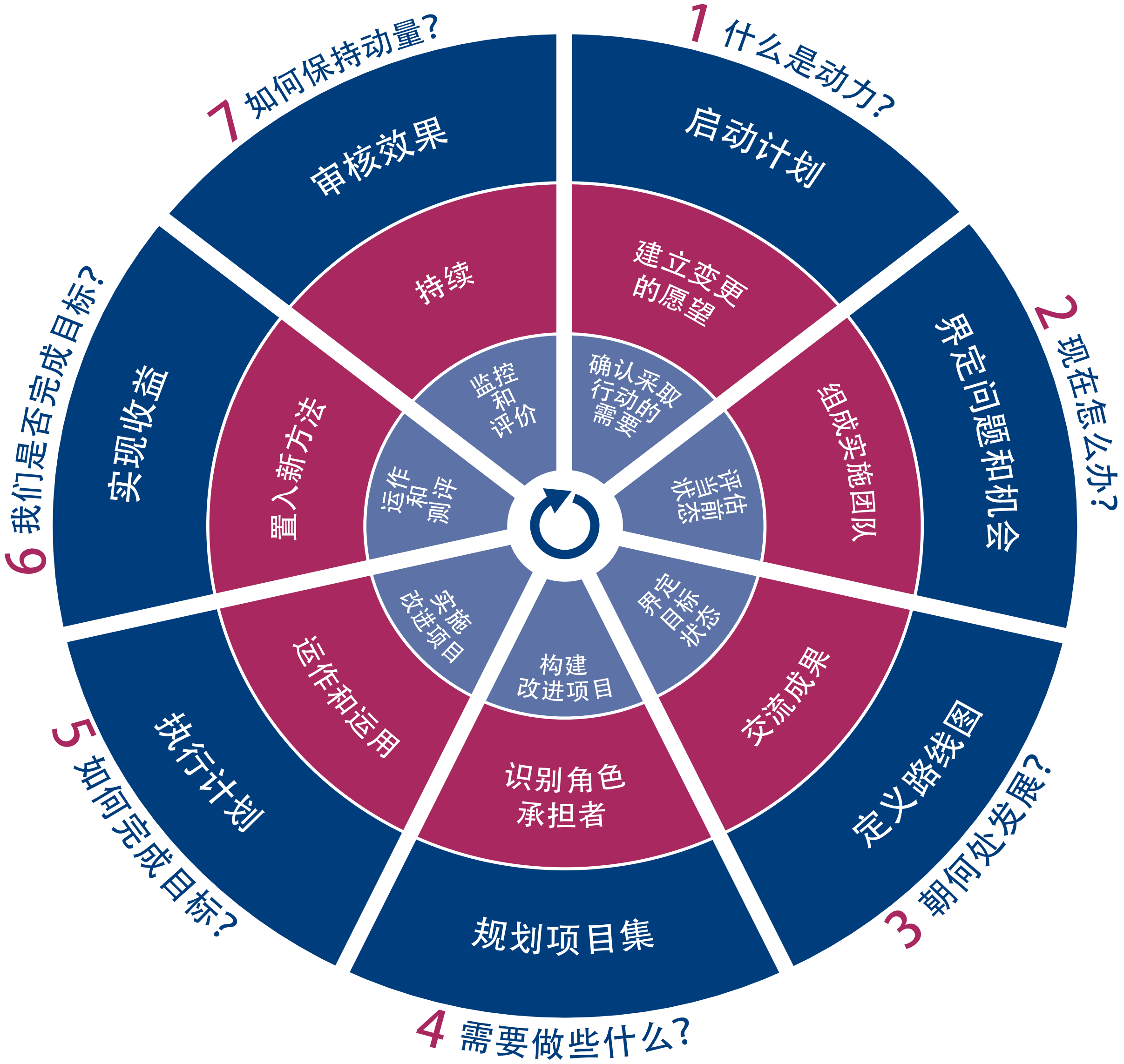
原则4: 采用一个整体全面的方法



原则5: 区分治理和管理


业务需要
治理
评价
指导
管理层反馈
监控
管理
计划
（定位、计划、组织）
构建
（构建、购置、实施）
运行
（交付、服务、支持）
监控
（监控、评价、评估）

实施生命周期的七个阶段

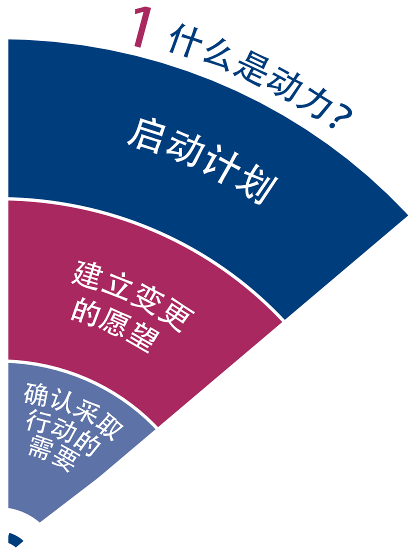


- 项目集管理（外环）
- 变更启动（中环）
- 持续改进生命周期（内环）

ISACA®
Trust in, and value from, information systems

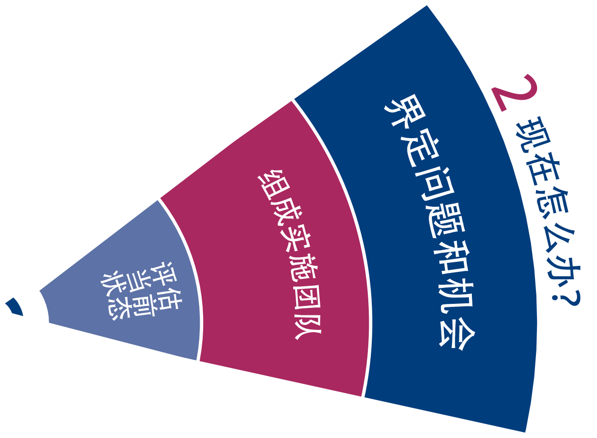
第一阶段：什么是动力？

- 识别和商定实施或改进计划的需求
- 确定痛点和触发事件
- 在行政管理层营造出变更的愿望



第二阶段:现在怎么办?

- 利用目标分层来界定实施计划的范围
- 考虑风险场景来突出需要关注的关键流程
- 进行当前状态的评估
- 通过执行一项流程能力评估来发现问题和缺陷
- 大规模计划予以架构



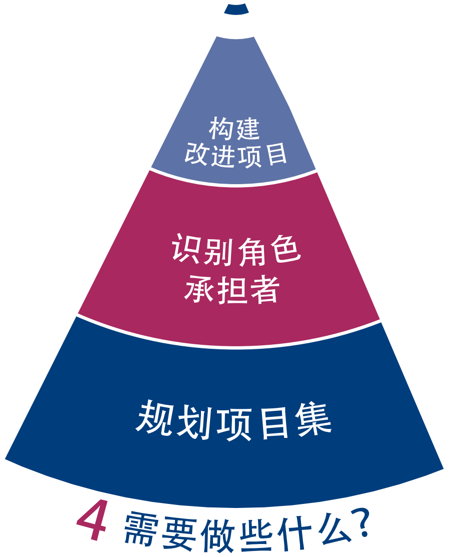
第三阶段:朝何处发展

- 设定实施目标
- 识别差距和潜在的解决方案
- 优先考虑较易于实现的和产生最大收益的计划

界定目标状态
交流成果
定义路线图
3 朝何处发展?

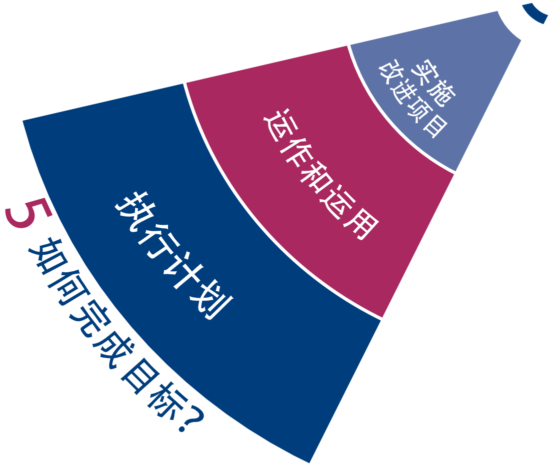
第四阶段: 需要做些什么？

- 界定合理的业务案例所支持的项目
- 开发一项实施变更计划



第五阶段: 如何完成目标?

- 解决方案应在日常实践中予以实施
- 界定衡量标准
- 形成监控机制以确保实现业务一致性

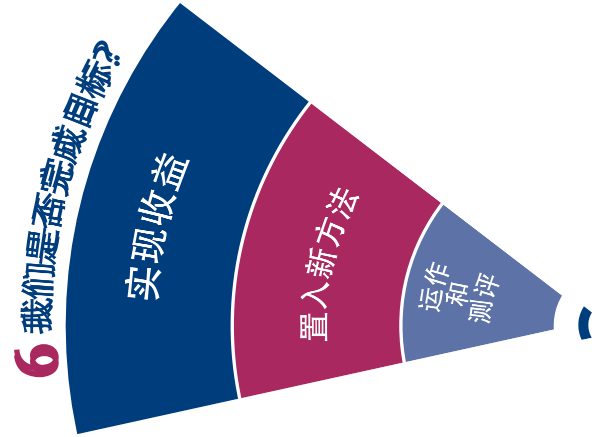


Proprietary

ISACA®
Trust in, and value from, information systems

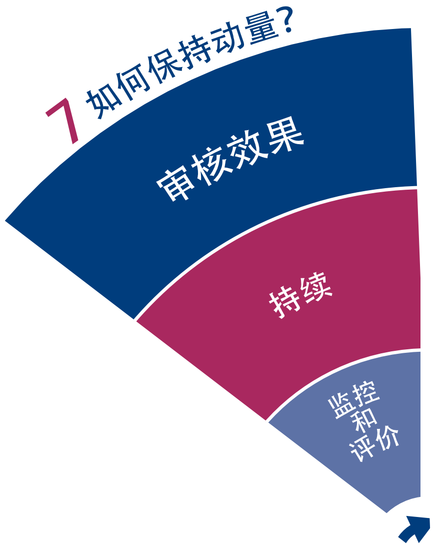
第六阶段: 我们是否完成目标？？

- 关注于新或改良的动力的持续运行
- 对于其预期收益实现的监控



第七阶段: 如何保持动量?

- 对计划的整体成功进行审验
- 确认进一步的需求
- 强化持续改进的要求



20 YEARS Est. 1996

COBIT 5

AN ISACA® FRAMEWORK

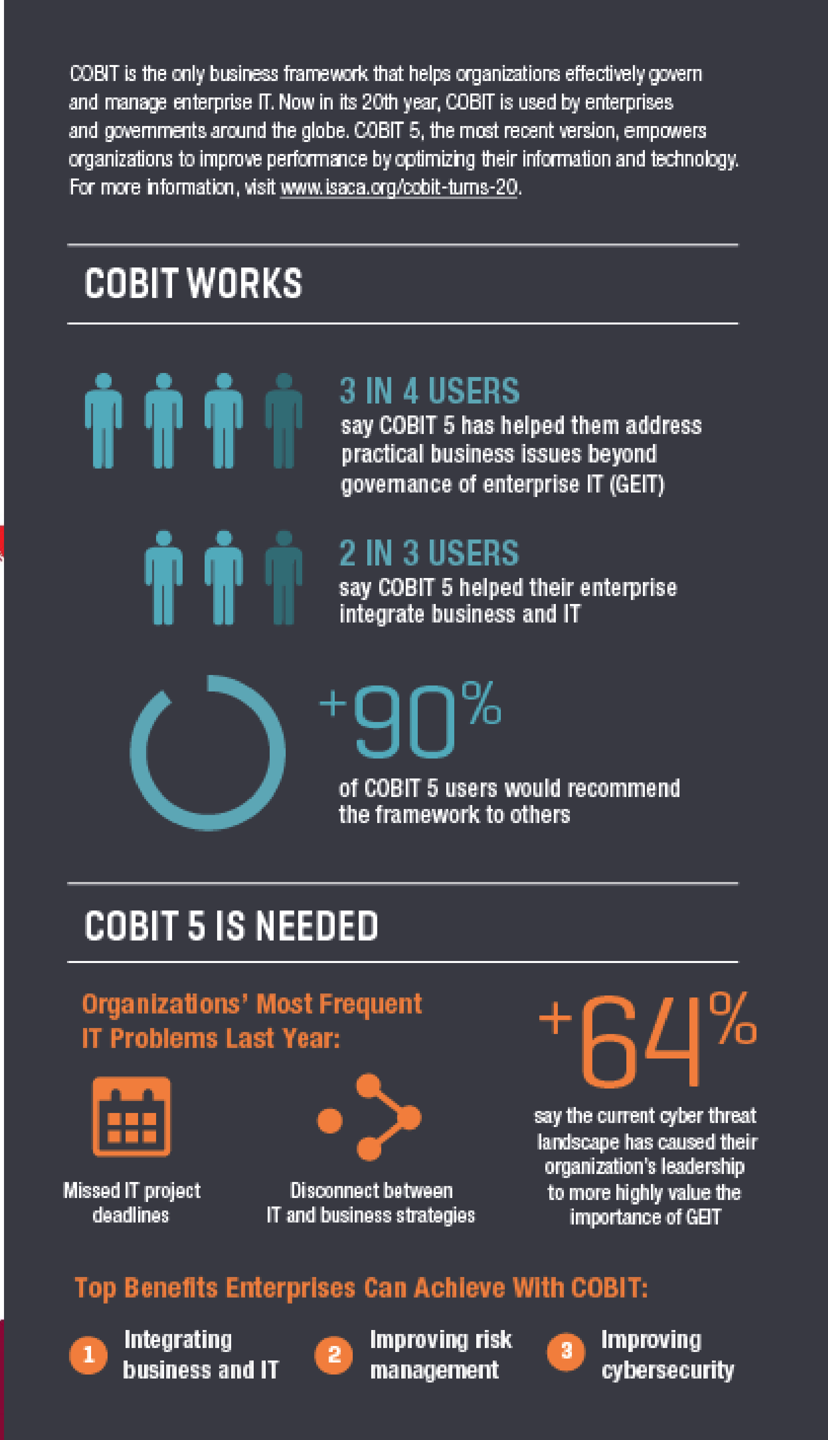
+610,000
downloads of COBIT 5 publications

+890,000
COBIT Online page views since its September 2014 launch

11,677
COBIT 5 exams taken in 2015

Nurture and continue to build COBIT training and usage globally and, where appropriate, leverage other valued frameworks

完善和继续在全球范围推广COBIT培训和使用，必要时将利用其它有价值的框架体系。



COBIT is the only business framework that helps organizations effectively govern and manage enterprise IT. Now in its 20th year, COBIT is used by enterprises and governments around the globe. COBIT 5, the most recent version, empowers organizations to improve performance by optimizing their information and technology. For more information, visit www.isaca.org/cobit-turns-20.

COBIT WORKS

3 IN 4 USERS
say COBIT 5 has helped them address practical business issues beyond governance of enterprise IT (GEIT)

2 IN 3 USERS
say COBIT 5 helped their enterprise integrate business and IT

+90%
of COBIT 5 users would recommend the framework to others

COBIT 5 IS NEEDED

Organizations' Most Frequent IT Problems Last Year:

Missed IT project deadlines

Disconnect between IT and business strategies

+64%
say the current cyber threat landscape has caused their organization's leadership to more highly value the importance of GEIT

Top Benefits Enterprises Can Achieve With COBIT:

1 Integrating business and IT

2 Improving risk management

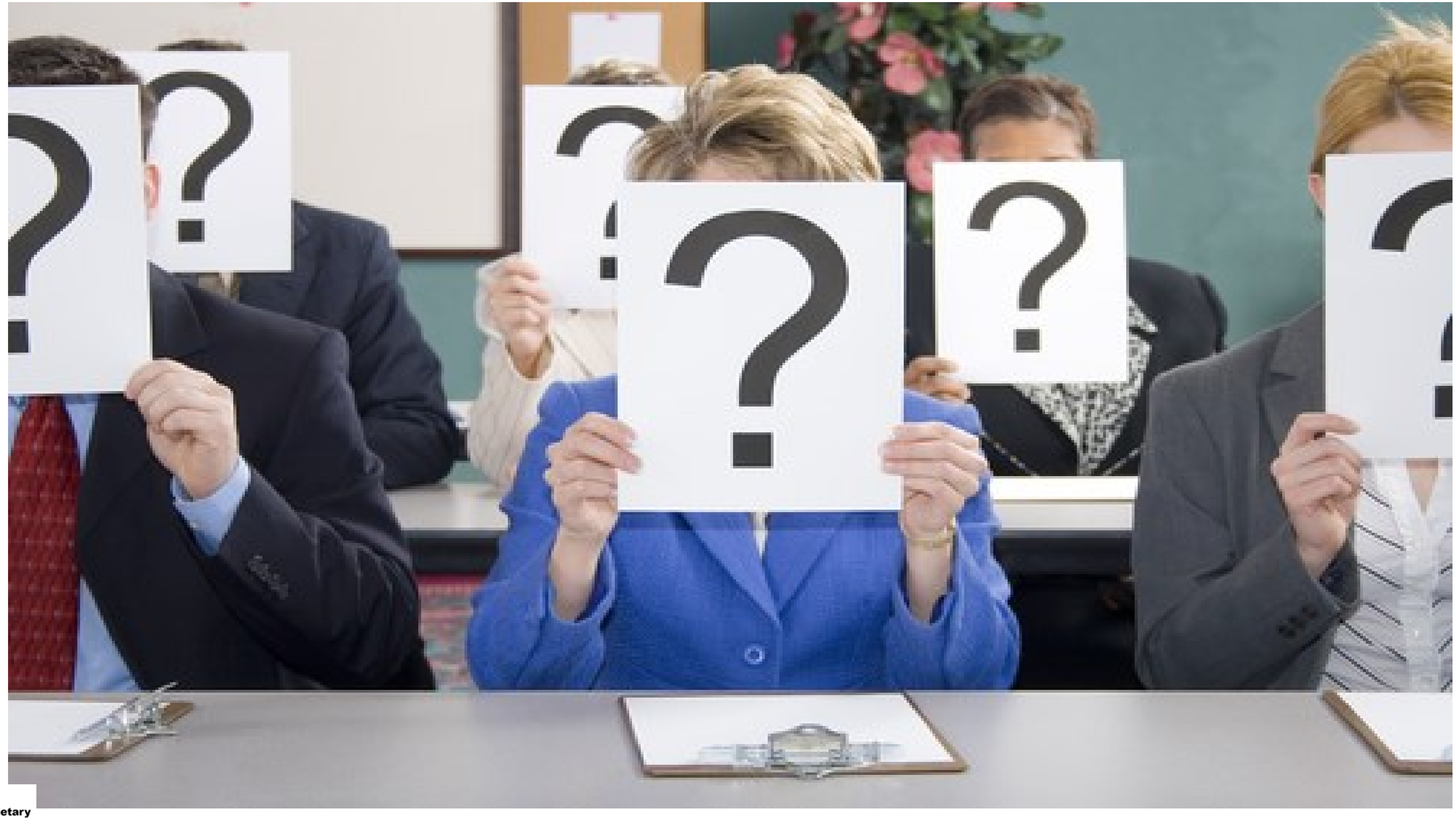
3 Improving cybersecurity

Pr Proprietary

要点概述

- 网络攻击将越来越频繁而其造成的财政损失也将越来越多。
- 网络攻击带来到损失与影响是不良的。
- 企业IT治理可以有效地自上而下地帮助企业调整网络安全的管理。
- 网络安全可以成为企业的竞争优势，促进企业的提高。

DISCUSSIONS



Trust in, and value from, information systems

Pr Proprietary