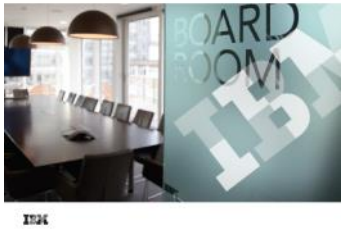
# 检查清单到架构

*CISO 从合规性到以风险为基础的网络安全方案转变的洞察*

# CISO 评估为安全管理层记录了重要和新兴问题的大事年表，同时指明了要贯彻执行的最佳做法

## 2012




### 找到战略入口

为安全管理层建立了三个原型，即响应者、保护者和影响者，并探索他们的特点。

## 2013


### 为安全管理层确立新标准

为安全管理层确定达到影响者地位的实际措施：通过业务实践、技术和测量。

## 2014


### 为未来巩固加强

尝试定义安全管理层发展的下一个阶段，为未来提供建议。

# 在 2015 年，我们更进一步地了解到 CISO 如何开发网络安全策略，以及如何确定安全投资的优先级

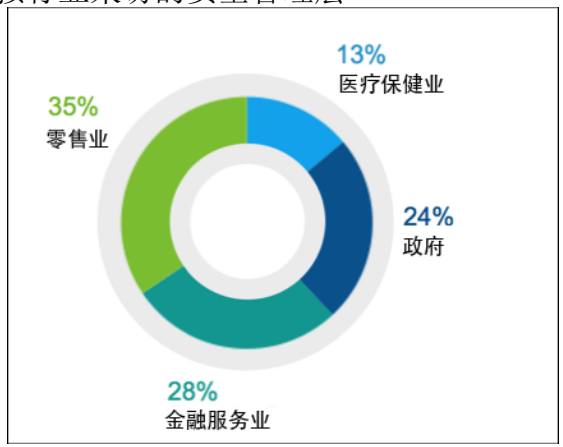
- 网络安全风险的优先级属于企业最高管理层级别，其用于安全措施的资金不断增长，反映出挑战的严峻性
- 历史上，网络安全投资决策通常基于“检查清单”方法，以满足合规性需求
- 安全管理层现在将其方案转变为以风险为基础，通过使用定制的架构，来确定风险，并确定安全投资的优先级

## 关于本报告

这份 IBM Center for Applied Insights 报告是在“识别公司如何管理网络安全投资”的基础之上做出的。这项研究由 IBM 发起，由网络安全的达尔文迪森研究院 (Darwin Deason Institute for Cyber Security) 进行，该机构隶属于得克萨斯州达拉斯市的南卫理工会大学莱尔工程学院。

深入的采访是以半结构化的方法进行的，其目的在于探索最高的网络安全风险、如何判定风险、网络安全活动的组织支持，以及如何确定投资优先级。

按行业采访的安全管理层



# 在转变到以风险为基础的方案时，CISO 所面临的最大挑战

**以“策略”为重点**

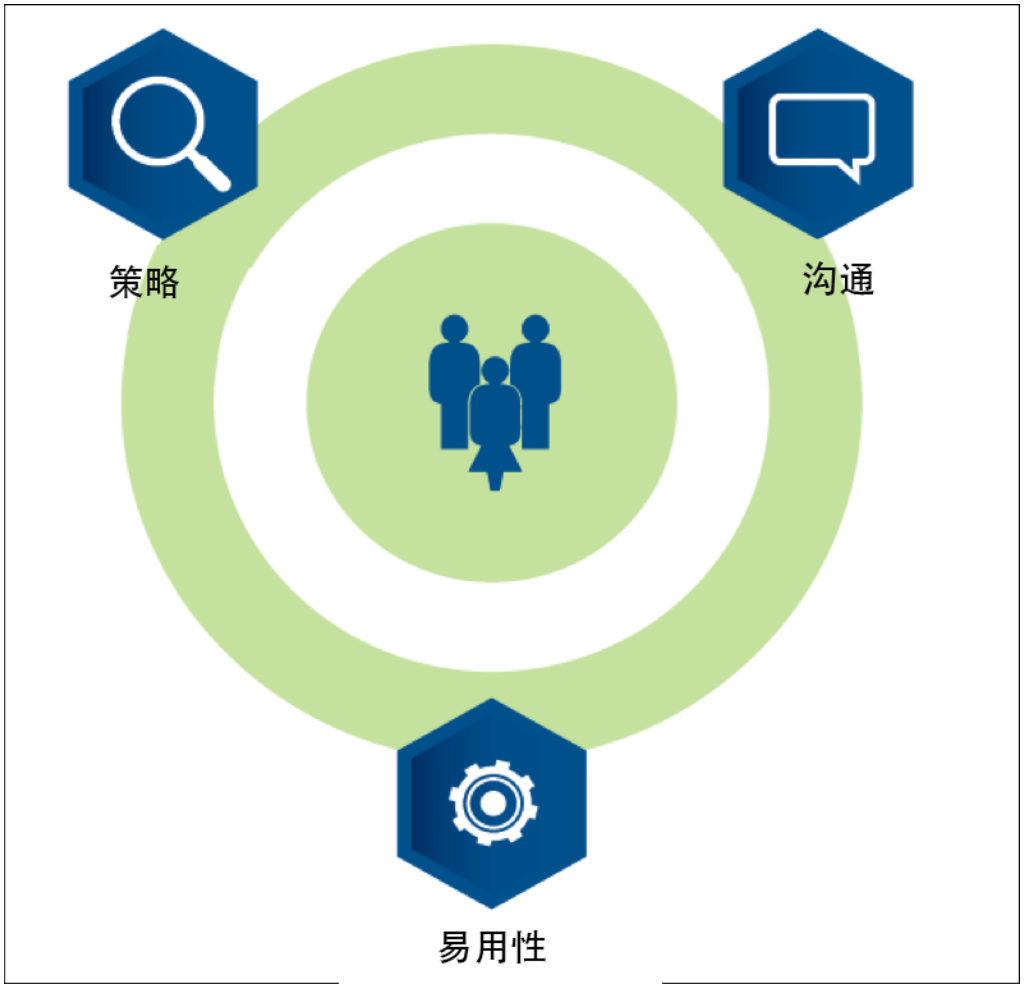
*如何从以合规性为基础的安全方案转变为以风险为重点的方案*

**就优先级进行沟通**

*如何能够与最高管理层就风险问题进行最佳的沟通，并管理期望值*

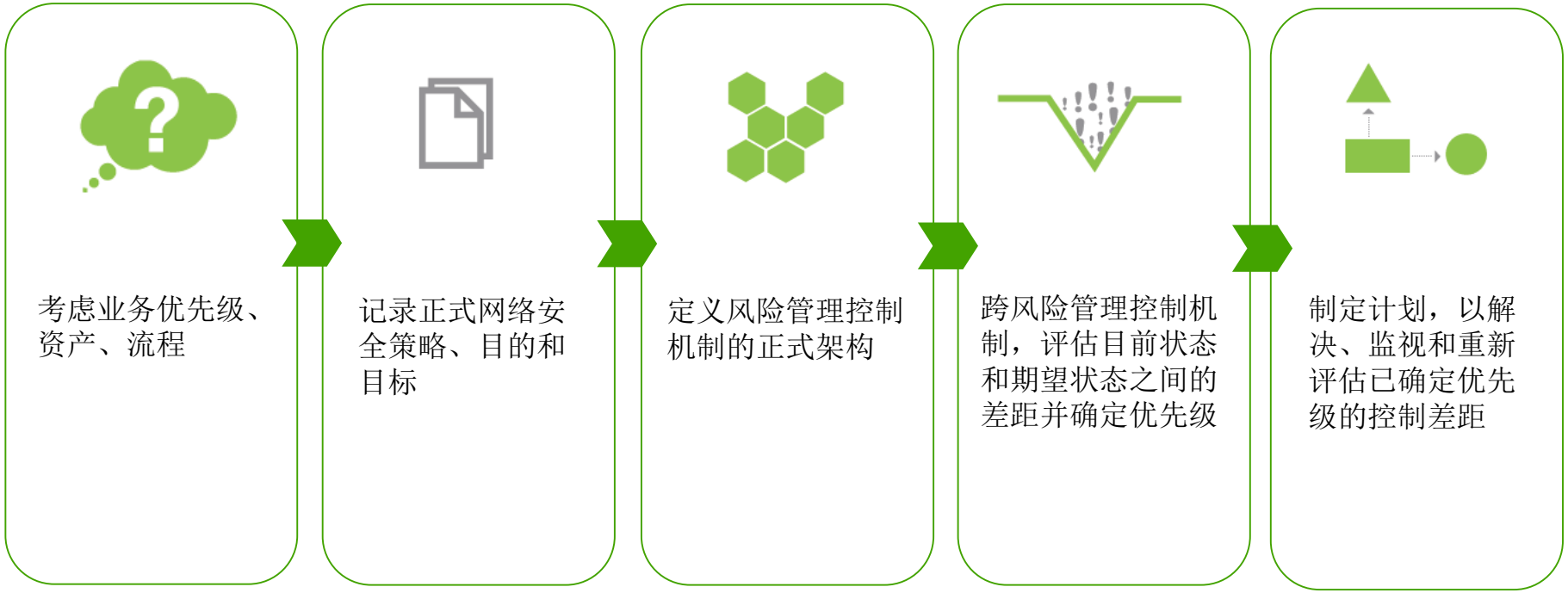
**使网络安全策略易于使用**

*是否具有实现正确控制机制以获得成功所需的技能、资源和工具*

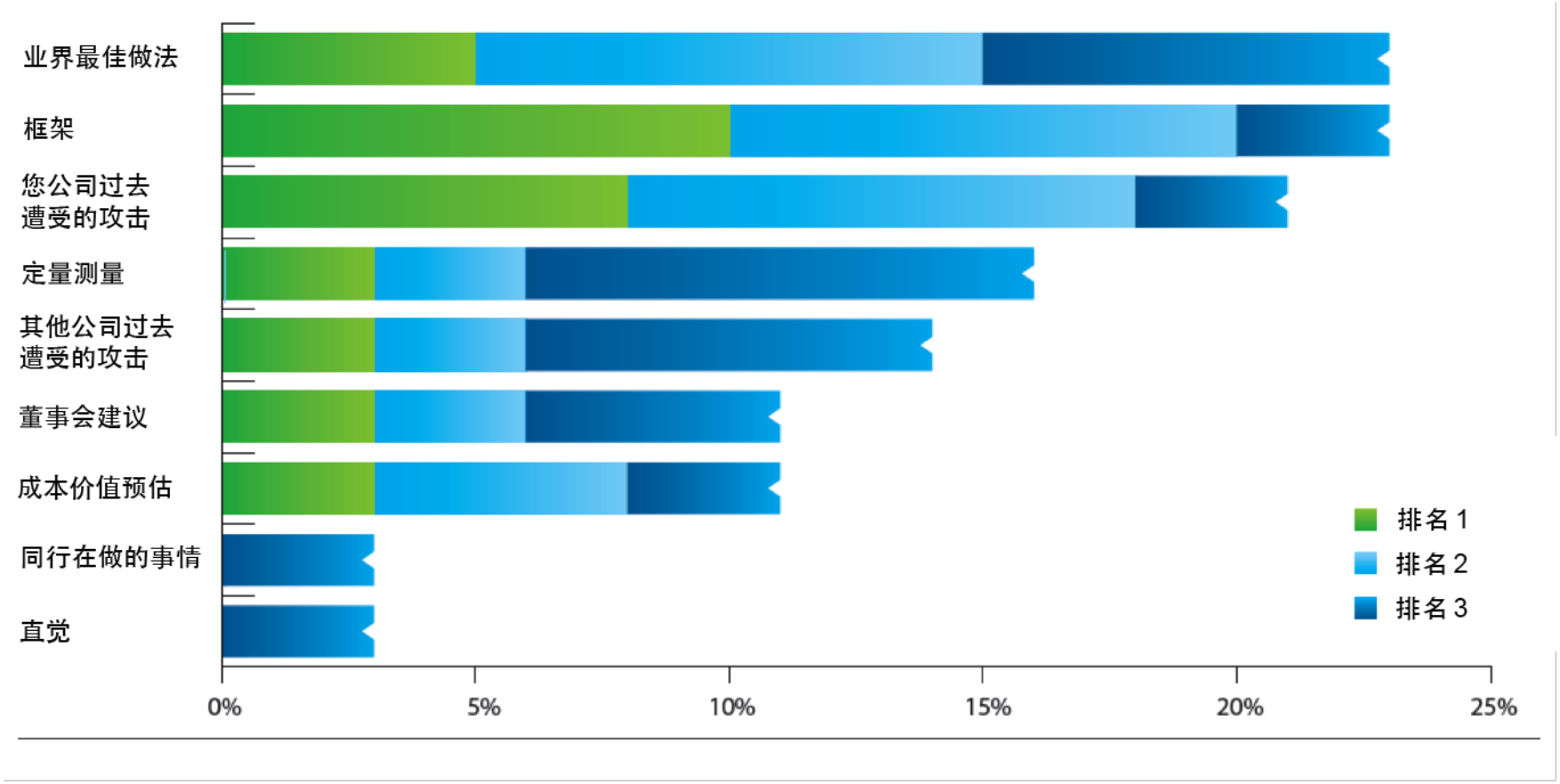


# CISO 日益转向使用架构，作为选择评估风险并确定威胁优先级的策略工具

网络安全方案的关键要素：



# 架构、公司过去遭受的攻击和业界最佳实践被列为风险管理的前三大网络安全优先级确定方法



# 定制的架构助力超越合规性，转到以风险为基础的策略

以安全合规性为重点的传统方法无法确保组织为潜在安全隐患做出最好的准备

- 架构为风险评估提供最佳基础，以完全且一致地评估安全挑战并确定差距
- 公司开发自己的网络风险架构，这样更可能对其组织真正的风险有更深入的了解

*“安全必须以事实为依据且具有说服力，在就其观点与背后的一些想法进行印证时，能够站得住脚，而不是一拍脑袋‘我想要做这些事情，因为明摆着这会是下一个安全问题，而且很酷’。”*
*-- 零售业 CISO*

# 架构有助于增加与企业最高管理层的协作，就优先级问题进行沟通

- 架构对于 CISO 来说，是一种非常有效的沟通工具，可将网络安全传达给上级管理层以获得支持
- 85% 的 CISO 报告上级管理层增加了对网络安全工作的支持
- 88% 的 CISO 报告其安全预算已经增加
- 25% 的 CISO 曾调查，认为自己支出适当的那些人也使用架构作为策略工具

*“资深管理层领导让我用他们能够听得懂的话、用项目和用钱来清楚地阐述什么是安全策略。”*
*-- 零售业 CISO*

# 架构提供实现网络安全策略的指导

- 感知“风险降低”和“合规性”仍然位居榜首，以确保满足基线安全目标
- 人才短缺使得许多 CISO 开始寻求外部支持，以补充技能和资源
- CISO 依赖于对等网络、第三方信息和第三方情报数据

*“关键是开发新技能集的能力，使人们可以适应不断变化的环境，而不是教授网络安全中的最新例程。”*
*-- 美国管理信息安全副教授*

# 为了应对人才短缺的问题，安全管理层和学术机构可以采用协作方法来发展技能

- 对学生进行培训，通过将业务组件集成到技术课程（反之亦然），让他们成为技术和业务之间的促进者
- 创建整体课程，模拟真实世界状况和安全管理层的挑战
- 培养全能专家，使用预测和行为分析，以了解攻击，并领先一步

*“网络安全已经得到发展，相应地教育也已得到发展。以前是以技术为主，加上动手实践，现在转变为融入更多管理层和策略。”*
*-- 美国管理安全信息方案主管*

来源：塑造安全问题解决者：2015 年 IBM Center for Applied Insights 的“为未来巩固加强的学术洞察”

# 制定以风险为基础的网络安全方案的要点

## 制定

**超越合规性转到以风险为基础的策略**

定制架构，实现对组织真正风险的策略性评估，同时强调网络安全的优先级。

## 指导

**增加与企业最高管理层的协作**

使用架构作为有效的沟通工具，以更为易用的方法，将网络安全策略传达给利益相关者，以获得支持。

## 交付

**运用架构驱动的网络安全洞察**

运用正确的技能、第三方情报和业界最佳做法，以实现源自架构的指导。

**www.ibm.com/ibmcai/ciso**
**www.ibm.com/security/ciso**

本报告中所述的调查结果不应解释为获得了南卫理公会大学网络安全的达尔文迪森研究院 (Darwin Deason Institute for Cyber Security) 的支持。网络安全的达尔文迪森研究院对本报告中提供的观点既不同意也不反对。



IBM Corporation
New Orchard Road
Armonk, NY 10504

创作于美利坚合众国
2014 年 12 月