Formalizing IT Risk Management and Governance

Virtual Executive Briefing
10 August 2017

CEB Information Risk Leadership Council

CEB is now Gartner®

A Framework for Member Conversations

The mission of Gartner's CEB Leadership Councils is to help executives and their teams harness their growth potential by taking insights from the best companies to save time and make better decisions. When we bring leaders together, it is crucial that our discussions neither restrict competition nor improperly share inside information. All other conversations are welcomed and encouraged.

Confidentiality and Intellectual Property

These materials have been prepared by Gartner, Inc. and/or its affiliates ("Gartner") for the exclusive and individual use of our CEB Leadership Council member companies. These materials contain valuable confidential and proprietary information belonging to Gartner, and they may not be shared with any third party (including independent contractors and consultants) without the prior approval of Gartner. Gartner retains any and all intellectual property rights in these materials and requires retention of the copyright mark on all pages reproduced.

Legal Caveat

Gartner is not able to guarantee the accuracy of the information or analysis contained in these materials. Furthermore, Gartner is not engaged in rendering legal, accounting, or any other professional services. Gartner specifically disclaims liability for any damages, claims, or losses that may arise from a) any errors or omissions in these materials, whether caused by Gartner or its sources, or b) reliance upon any recommendation made by Gartner.

THE FACILITATOR FOR TODAY'S VIRTUAL BRIEFING

Chris J. Mixter is a Principal Executive Advisor with CEB, Now Gartner, advising the firm's Infrastructure, Information Security, and Project Management members. Chris spends half his time deeply involved in the development of new best-practices, tools, and data across these domains, and the other half facilitating Executive Forums and on-site workshops for member companies. Prior to joining CEB in 2001, Chris worked for BB&T Bank in North Carolina. Chris graduated from Wake Forest University with a degree in Politics.

PARTIAL LIST OF PARTICIPANTS

AUTODESK.

BOMBARDIER
the evolution of mobility

ETS®

GE

KAISER PERMANENTE®

Manulife

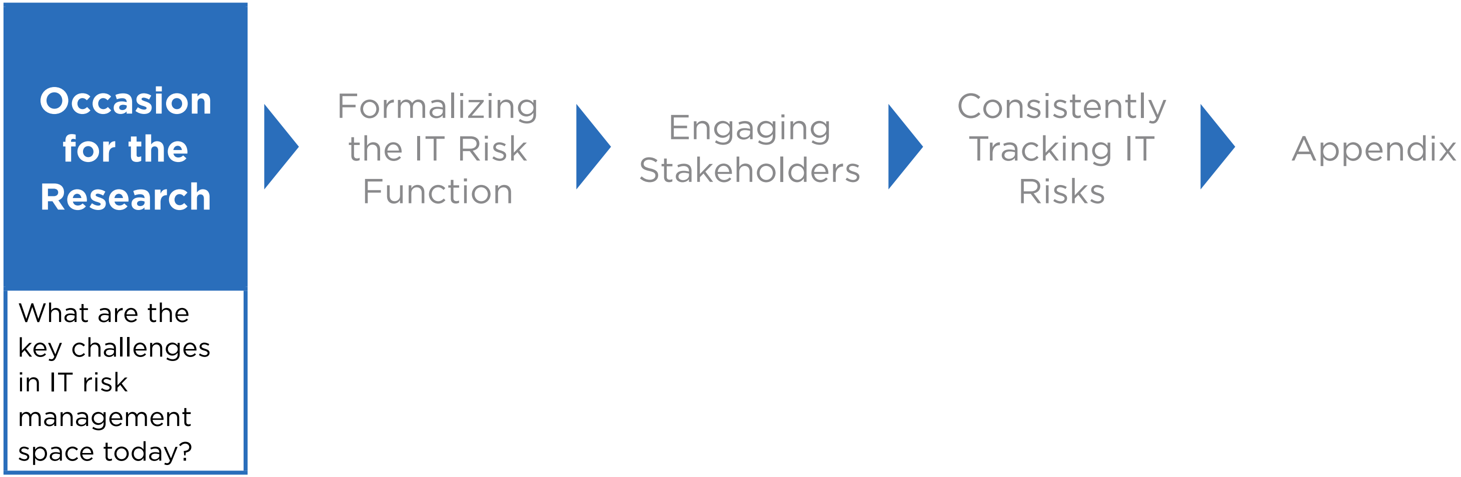
Micron

Microsoft

tyco

ROADMAP FOR THE PRESENTATION

Key Practitioner Questions



Occasion for the Research

What are the key challenges in IT risk management space today?

Formalizing the IT Risk Function

Engaging Stakeholders

Consistently Tracking IT Risks

Appendix

DEFINITION OF IT RISK

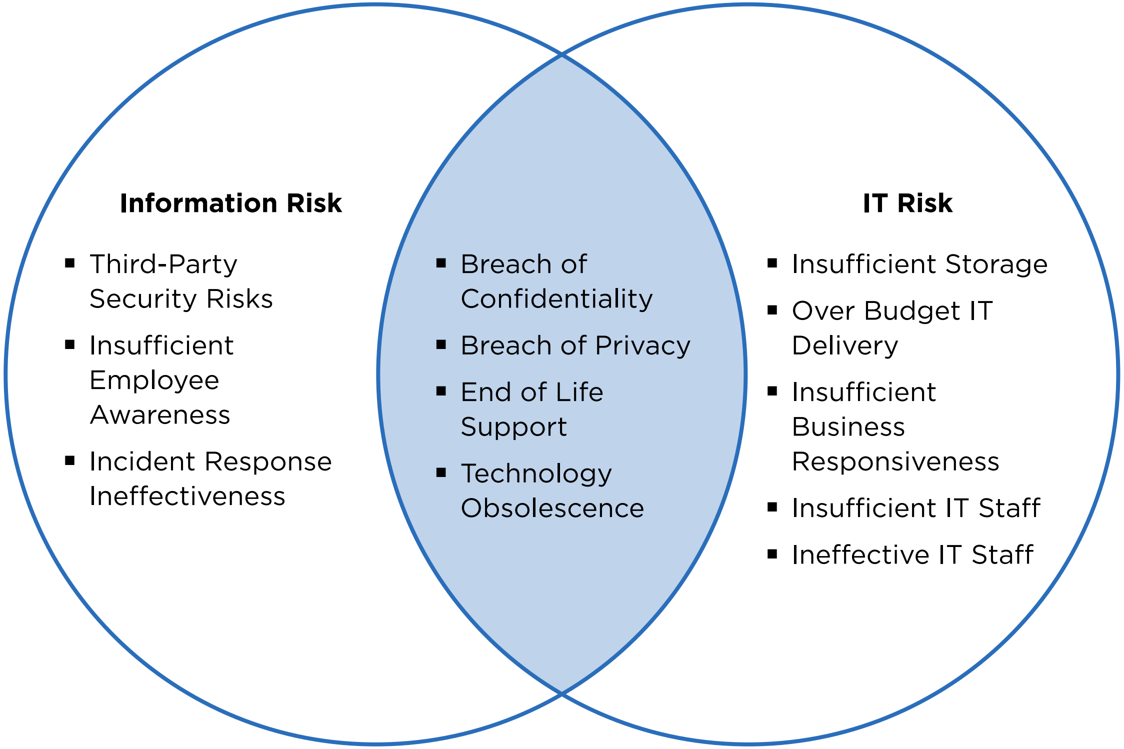
Definition of IT (or Technology) Risk

IT Risk is the potential for unexpected results associated with the use, ownership, and adoption of information technology. Risks manifest as unrealized or reduced business value in the following ways: Unsuccessful pursuit of business opportunities, unidentified business opportunities, destroyed value (tangible or intangible), excess cost.

Source: CEB analysis.

IT RISK ≠ INFORMATION RISK

IT Risk Has Overlap with Information Risk, but Includes Other Risks
Schematic



Information Risk

- Third-Party Security Risks
- Insufficient Employee Awareness
- Incident Response Ineffectiveness

- Breach of Confidentiality
- Breach of Privacy
- End of Life Support
- Technology Obsolescence

IT Risk

- Insufficient Storage
- Over Budget IT Delivery
- Insufficient Business Responsiveness
- Insufficient IT Staff
- Ineffective IT Staff

Source: CEB analysis.

CYBER RISK CAN OVERSHADOW LARGER RISKS

No Fortune 1000 company has gone out of business from a cyber attack or an IT system failure, but dozens have disappeared after being too slow to adapt to technology-driven changes in their business models.

Source: CEB analysis.

THE IT RISK TAXONOMY

CEB's IT Risk Taxonomy
Illustrative

IT Risk Type

IT Talent (Employees and Contractors)

- Shortfall of Staff
- Unpreparedness of Staff for a New Role
- Ineffectiveness of Staff

IT Capacity

- Limitations of the Network/Bandwidth
- Insufficient Storage
- Insufficient Computing Power
- Inability to Scale Other IT Capabilities

IT Reliability and Quality

- Loss of Integrity
- Loss of Availability
- Unacceptable Latency
- Vendor Support
- End of Life Support/Obsolescence

Information Security and Privacy

- Breach of Confidentiality
- Breach of Privacy

IT Legal and Compliance

- Audit Findings and Remediation Costs Fines
- Civil Lawsuits
- Criminal Charges
- Regulators Prevent Doing Business

IT Delivery

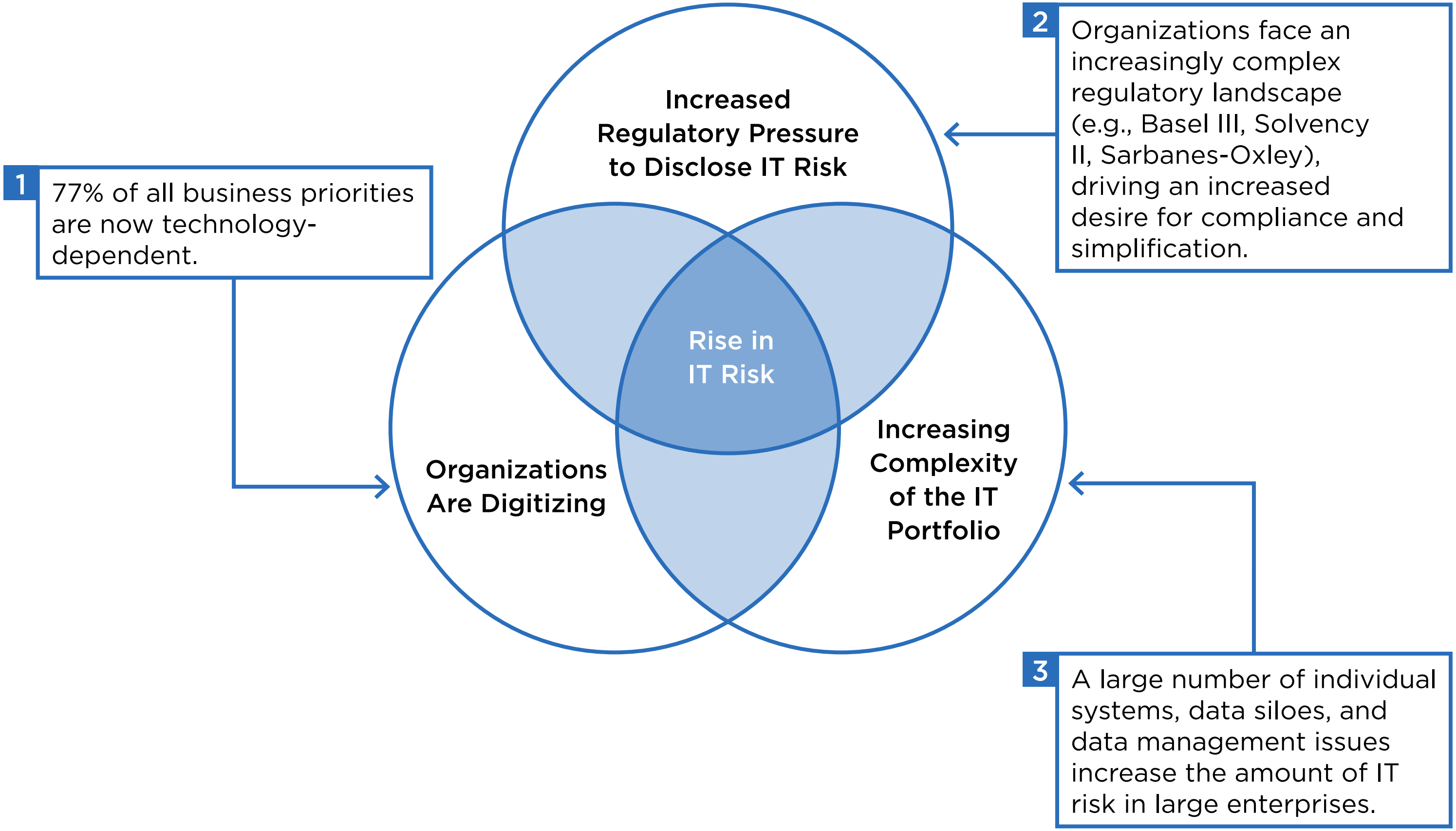
- Late Delivery
- Over Budget
- Unrealized Business Benefits
- Under-Adoption

IT Business Enablement

- Insufficiently Responsive to Business Needs
- Impact to Employee Productivity
- Damage to Company Reputation or Brand
- Missed Technology-Related Innovation and Opportunity Identification
- Excess Operational Cost

Source: CEB analysis.

KEY MAGNIFIERS OF IT RISK


Increased Regulatory Pressure to Disclose IT Risk
Rise in IT Risk
Organizations Are Digitizing
Increasing Complexity of the IT Portfolio

1 77% of all business priorities are now technology-dependent.

2 Organizations face an increasingly complex regulatory landscape (e.g., Basel III, Solvency II, Sarbanes-Oxley), driving an increased desire for compliance and simplification.

3 A large number of individual systems, data siloes, and data management issues increase the amount of IT risk in large enterprises.

Source: CEB analysis.

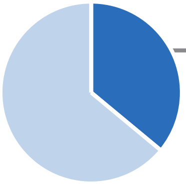
BARRIERS TO MANAGING RISK EFFECTIVELY

Three Main Challenges to Effectively Managing IT Risk

Percentage of Heads of IT Risk Who Cited Each Reason as Top Challenge

1 Formalizing the IT Risk Function

A lack of a formal entity that governs IT risk holds organizations back from knowing who should be managing risk when.

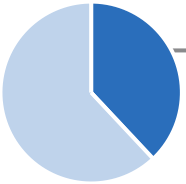


36%
Cite This as the Top Challenge

Key Practitioner Question:
How are IT Risk functions typically structured and organized at other large organizations?

2 Engaging Stakeholders

IT Risk functions struggle to engage senior business and/or IT stakeholders and control owners to make decisions on or actively manage IT risk.

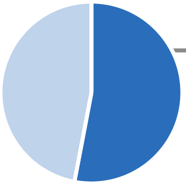


38%
Cite This as the Top Challenge

Key Practitioner Question:
How do I get senior stakeholders and owners of IT risks to actively participate in managing IT risks?

3 Consistently Tracking IT Risks

IT Risk functions struggle to evaluate and establish metrics to consistently track IT risk.



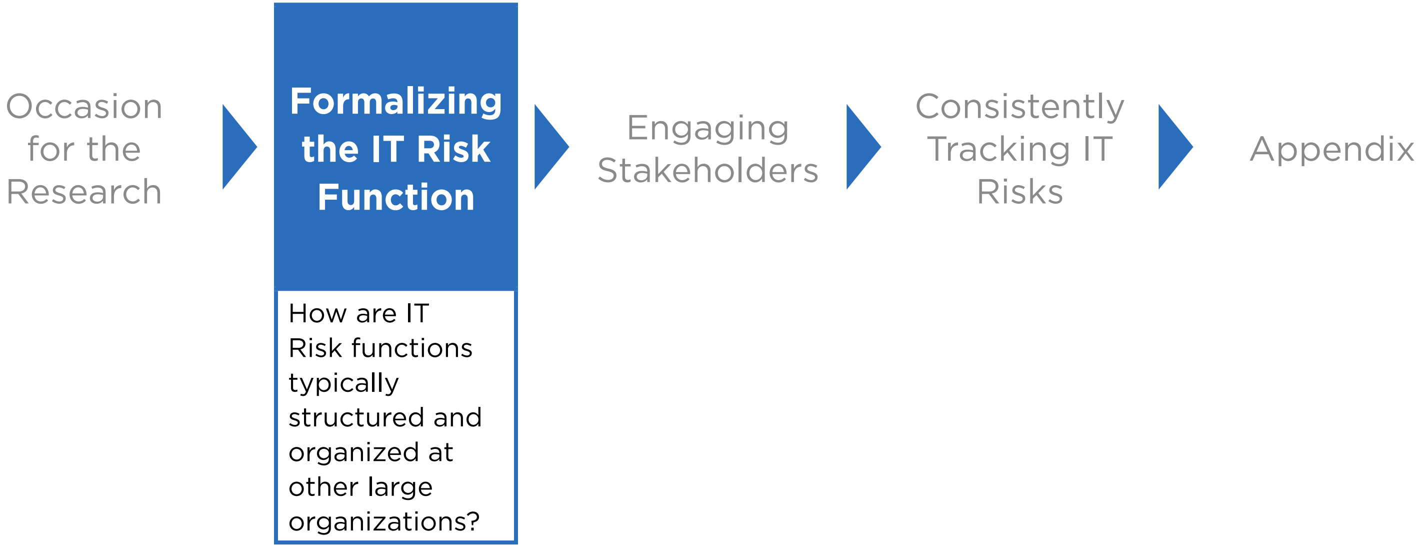
53%
Cite This as the Top Challenge

Key Practitioner Question:
How do I effectively track IT risks?

Source: CEB 2017 IT Risk Survey.

ROADMAP FOR THE PRESENTATION

Key Practitioner Questions



Occasion for the Research

Formalizing the IT Risk Function

How are IT Risk functions typically structured and organized at other large organizations?

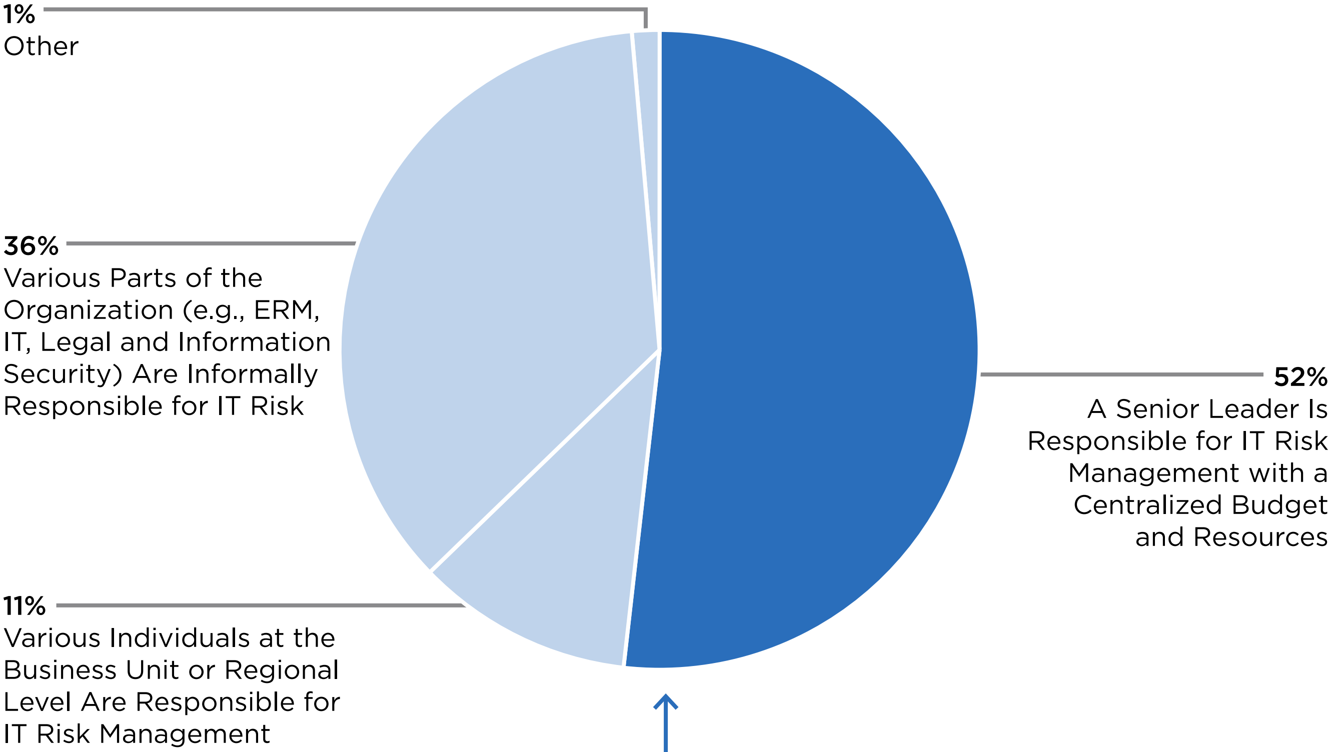
Engaging Stakeholders

Consistently Tracking IT Risks

Appendix

MAJORITY IS CENTRALIZING IT RISK MANAGEMENT

Ownership of IT Risk
Percentage of Respondents



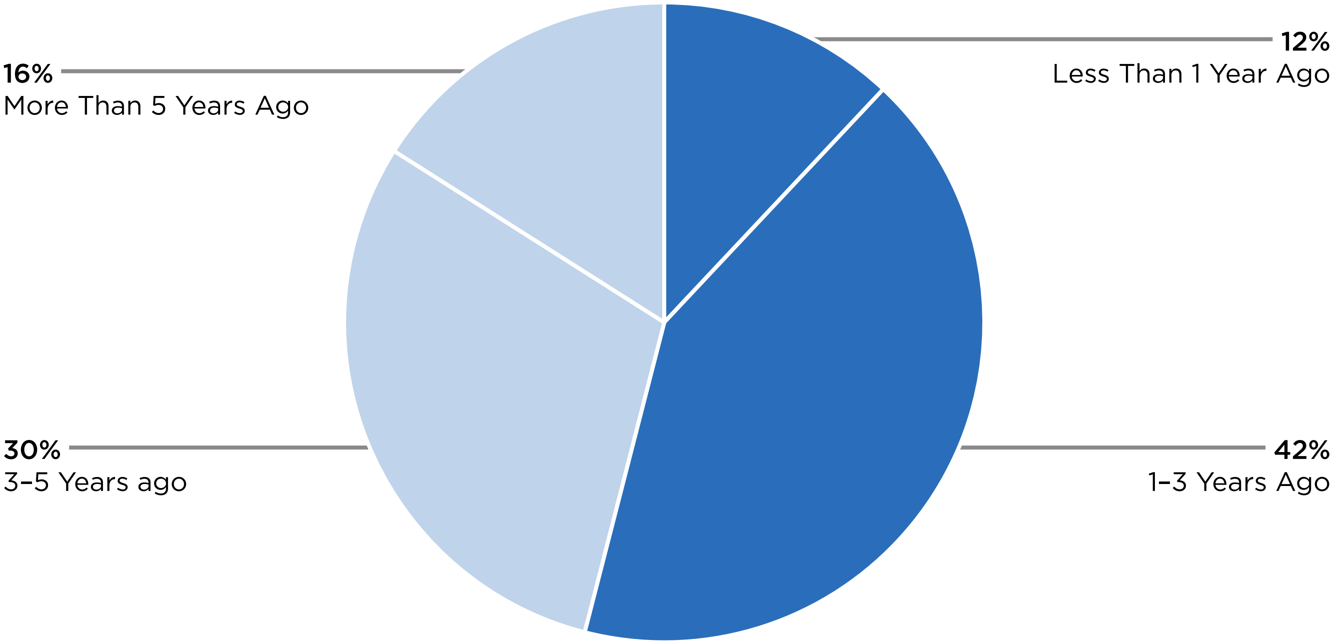
90% of organizations that have formal IT risk functions are highly or moderately digitized (See Appendix for the definition).

n = 81.

Source: CEB 2017 State of IT Risk Survey.

BUT MANY HAVE DONE SO RECENTLY

Timing for Establishment of a Formal IT Risk Function
Percentage of Respondents Who Report Having a Formal Function



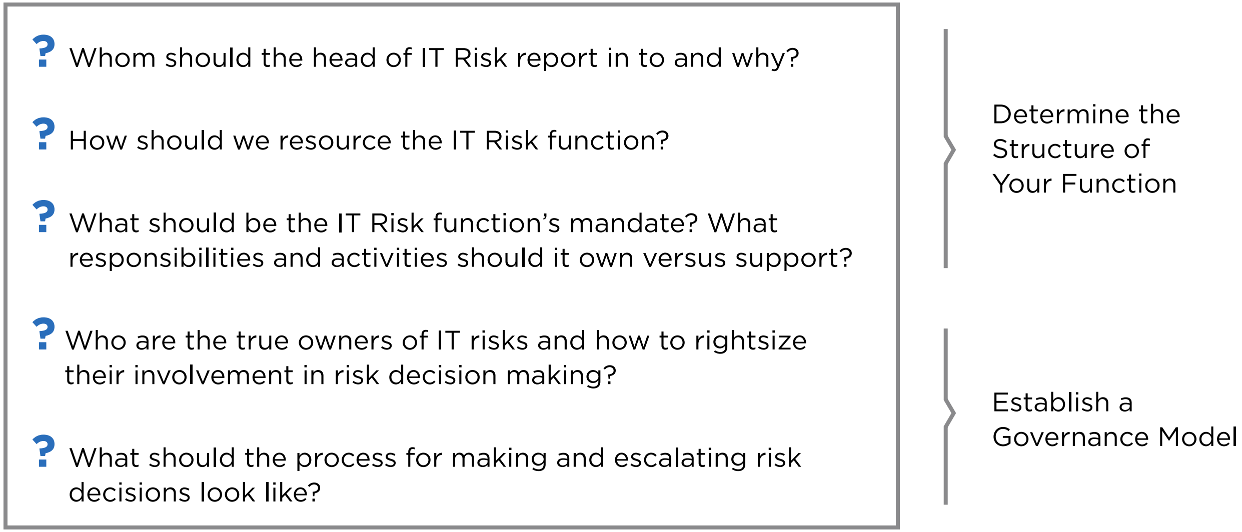
Organizations that have had IT risk functions the longest tend to be in highly regulated, highly digitized industries (e.g., finance, technology, pharmaceuticals).

n = 43.

Source: CEB 2017 State of IT Risk Survey.

DESIGN ELEMENTS OF AN IT RISK FUNCTION

Key Questions to Set Up the IT Risk Function



? Whom should the head of IT Risk report in to and why?

? How should we resource the IT Risk function?

? What should be the IT Risk function's mandate? What responsibilities and activities should it own versus support?

Determine the Structure of Your Function

? Who are the true owners of IT risks and how to rightsize their involvement in risk decision making?

? What should the process for making and escalating risk decisions look like?

Establish a Governance Model

Source: CEB analysis.

DESIGN ELEMENTS OF AN IT RISK FUNCTION

Key Questions to Set Up the IT Risk Function

- ? Whom should the head of IT Risk report in to and why?
- ? How should we resource the IT Risk function?
- ? What should be the IT Risk function’s mandate? What responsibilities and activities should it own versus support?

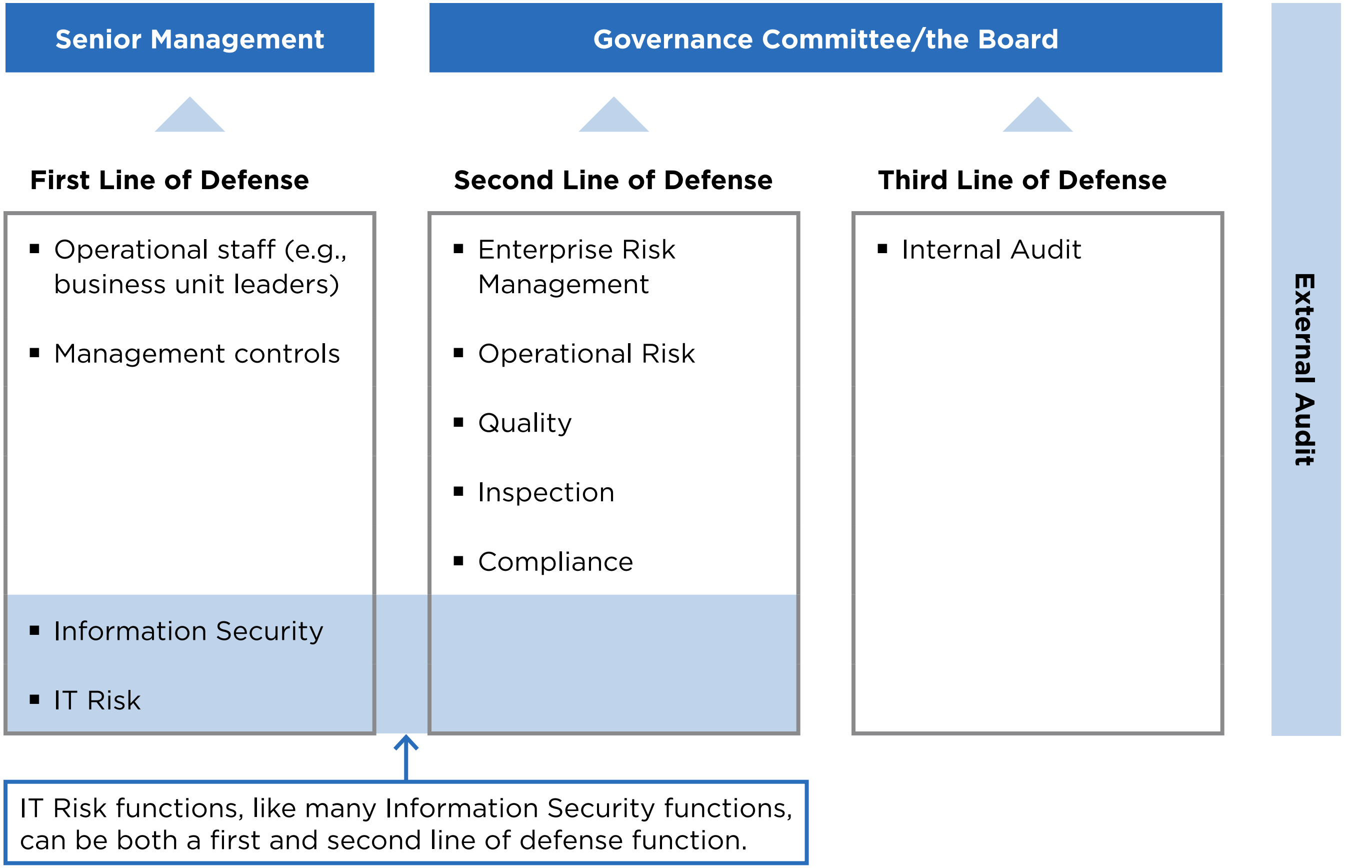
Determine the Structure of Your Function

The focus for today’s conversation.

Source: CEB analysis.

IT RISK IN THE THREE LINES OF DEFENSE MODEL

Schematic



Senior Management

Governance Committee/the Board

First Line of Defense

- Operational staff (e.g., business unit leaders)
- Management controls
- Information Security
- IT Risk

Second Line of Defense

- Enterprise Risk Management
- Operational Risk
- Quality
- Inspection
- Compliance

Third Line of Defense

- Internal Audit

External Audit

IT Risk functions, like many Information Security functions, can be both a first and second line of defense function.

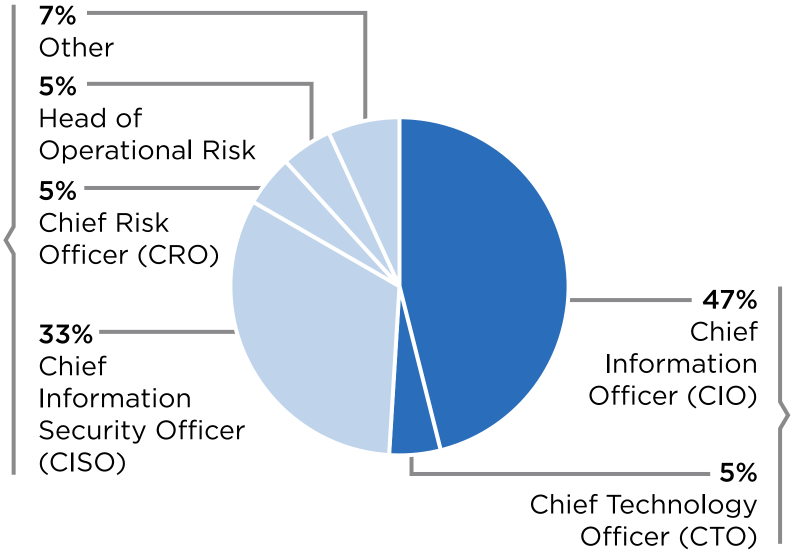
Source: Chartered Institute of Internal Auditors; CEB analysis.

THE MAJORITY OF FUNCTIONS REPORT INTO IT…

Direct Manager of the Head of IT Risk
Percentage of Respondents Who Report Having a Formal Function

Benefits of Reporting Outside of IT:

- Greater integrity in evaluating and managing IT risks.
- Greater exposure and awareness for IT risk management in the organization.



Benefits of Reporting into IT:

- Greater visibility into IT risks
- Easier to coordinate IT risk management efforts.

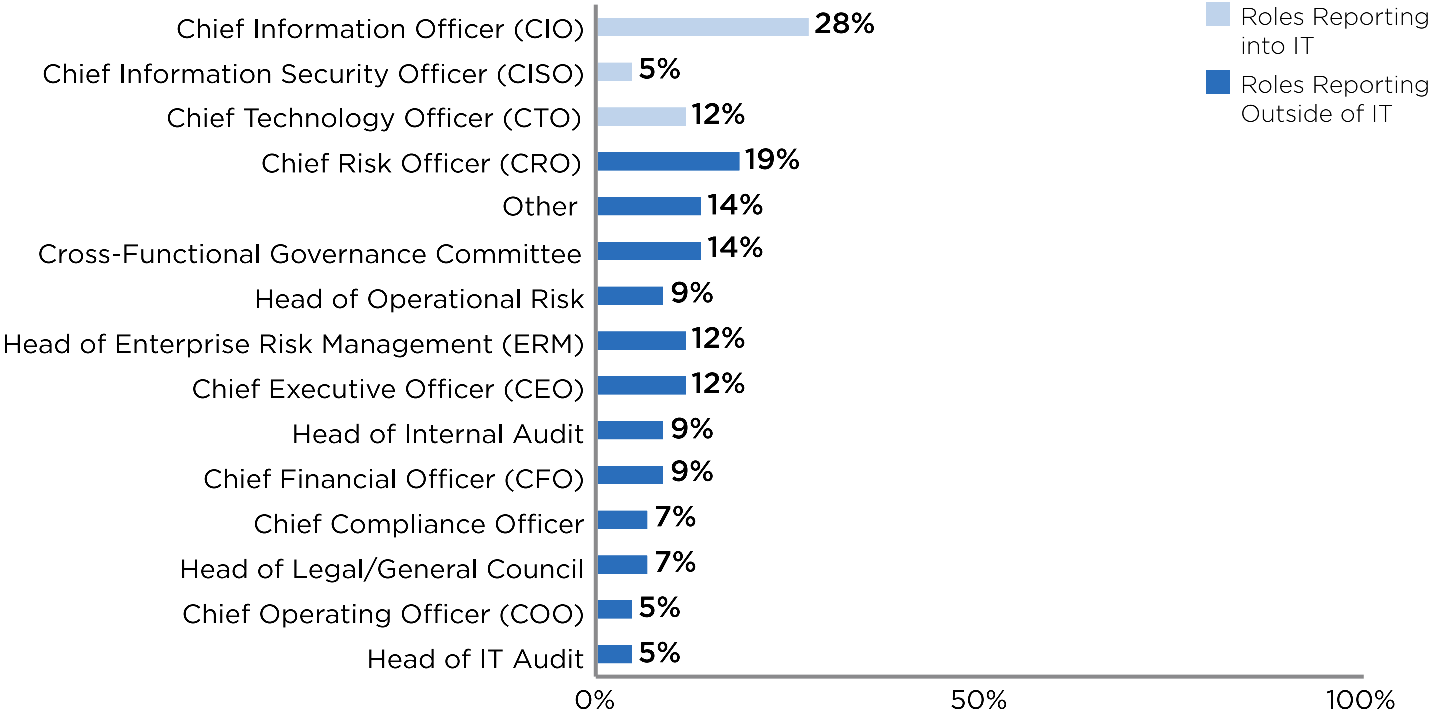
n = 43.

Source: CEB 2017 State of IT Risk Survey.

…WITH INDIRECT REPORTING OUTSIDE OF IT

Indirect Manager(s) of Head of the IT Risk

Percentage of Respondents Who Report Having a Formal Function; Multiple Responses Allowed



n = 43.

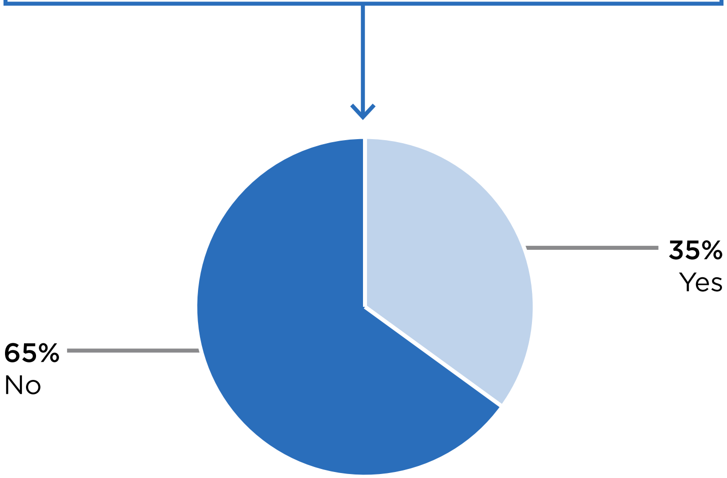
Source: CEB 2017 State of IT Risk Survey.

MOST HAVE STAFF, BUT LACK FORMAL BUDGETS

Dedicated Budget of a Formal IT Risk Function

Percentage of Respondents Who Report Having a Formal Function

The average CAPEX and OPEX combined IT Risk function budget for the 2017 fiscal year is $3,750,000.



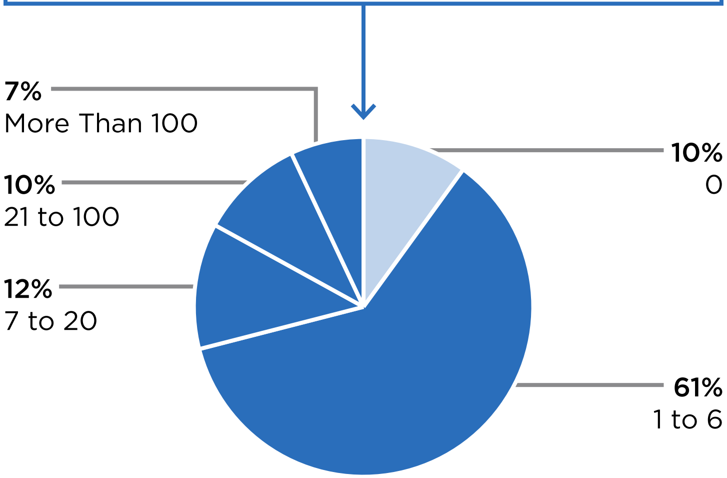
n = 43.

Source: CEB 2017 State of IT Risk Survey.

Full-Time IT Risk Employee

Percentage of Respondents Who Report Having a Formal Function

Functions without dedicated staff rely on employees who’s primary job function is not to manage and/or oversee IT risk.



n = 43.

Source: CEB 2017 State of IT Risk Survey.

THREE CORE MANDATES OF IT RISK FUNCTIONS

1. Ensure IT risk owners are effectively evaluating and registering IT risks using the appropriate processes and scales.

2. Own and directly manage IT risks, including logging, evaluation, and controls implementation.

3. Coordinate IT risk management and oversight that is dispersed across different parts of the organization.

Source: CEB analysis.

THREE DISTINCT IT RISK FUNCTION PROFILES

The Three IT Risk Function Profiles at a Glance

	Oversight	Oversight and Execution	Facilitator
Goal	Create guidelines and policies for registering and evaluating IT risk and monitor their implementation.	Execute and oversee all IT risk management efforts.	Primarily own coordination of IT risk efforts across the organization, along with supporting IT risk activities for which there is no "true" owner.
Activities	▪ Define IT risk policies and management guidelines ▪ Evaluate or monitor implementation of IT risk controls	▪ Remediate IT risks, including implementing necessary controls ▪ Create IT risk remediation plans	▪ Apart from IT risk awareness efforts for IT and business employees, little to no ownership of IT risk activities ▪ Participation in IT risk activities varies depending on the needs of the company
Areas of Maturity	High maturity in facilitating reporting, tracking progress, and acting on IT risks.	High maturity in reporting, tracking progress, and acting on IT risks.	Developing maturity in coordinating IT risk efforts across the organization, reporting, tracking progress, and acting on IT risks.
Reporting and Resourcing	Reports outside of IT more frequently than other function profiles and is more likely than not to have dedicated resources.	Typically reports into the CIO and has dedicated resources.	Typically reports into the CISO or the CIO and does not have dedicated resources.
Sample Industries	▪ Finance ▪ Pharmaceuticals	▪ Technology	▪ Retail ▪ Power ▪ Oil and Gas
Sample Size	21 Organizations	11 Organizations	10 Organizations

Source: CEB 2017 State of IT Risk Survey.

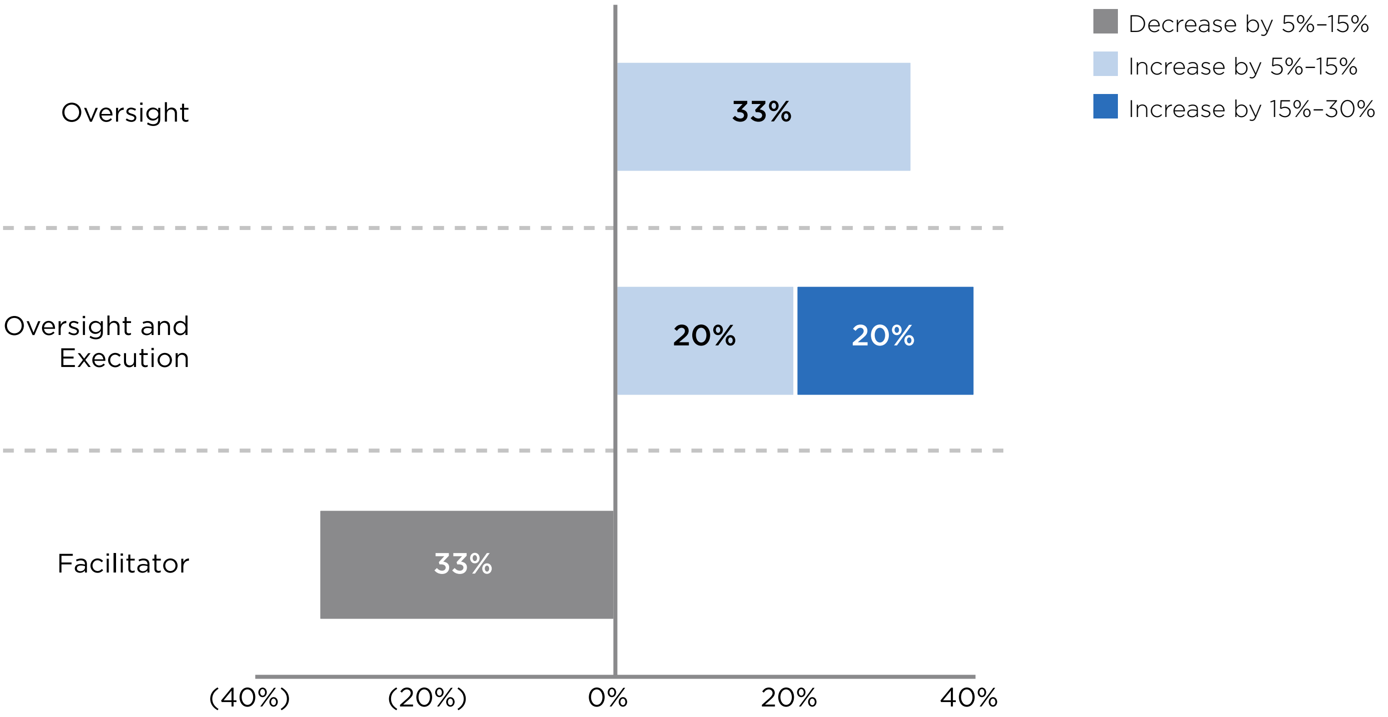
WHOM SHOULD I REPORT IN TO AND WHY?

HOW SHOULD I RESOURCE MY FUNCTION?

WHAT SHOULD BE MY FUNCTION'S MANDATE?

TWO PROFILES WILL LIKELY GET MORE FUNDING

Projected Budget Increase in the Next 12 Months for IT Risk Functions
Percentage of Formal IT Risk Functions

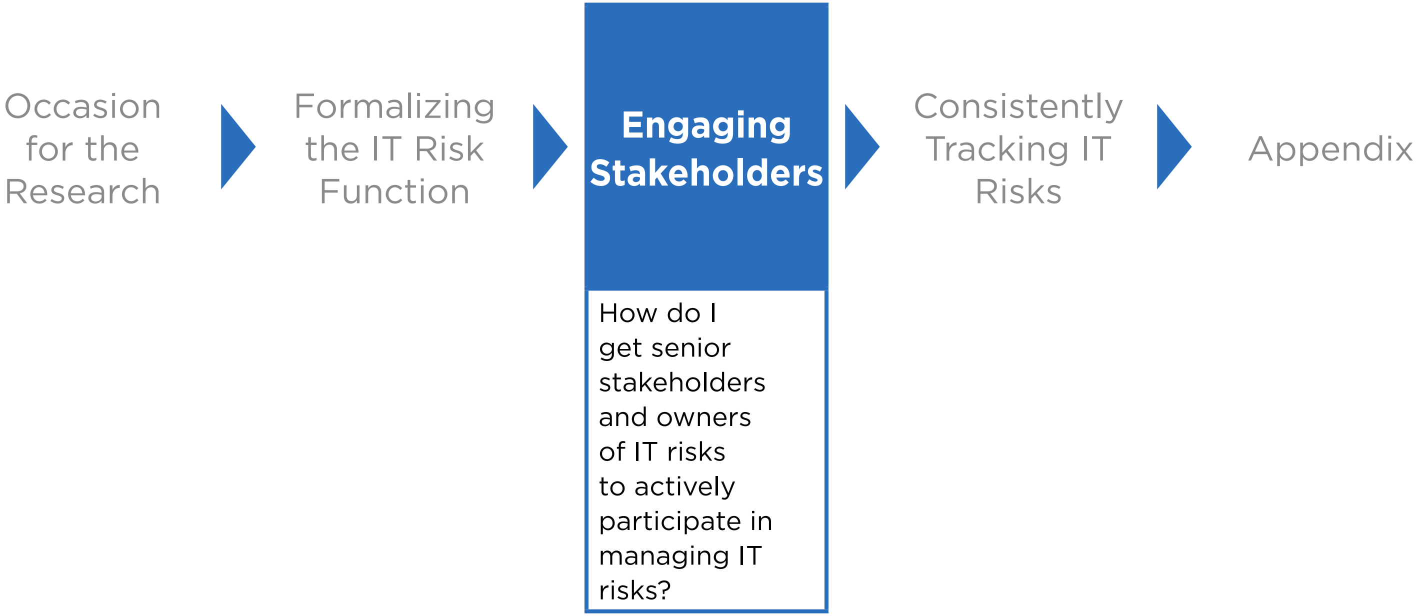


n = 43.

Source: CEB 2017 State of IT Risk Survey.

ROADMAP FOR THE PRESENTATION

Key Practitioner Questions



Occasion for the Research

Formalizing the IT Risk Function

Engaging Stakeholders

How do I get senior stakeholders and owners of IT risks to actively participate in managing IT risks?

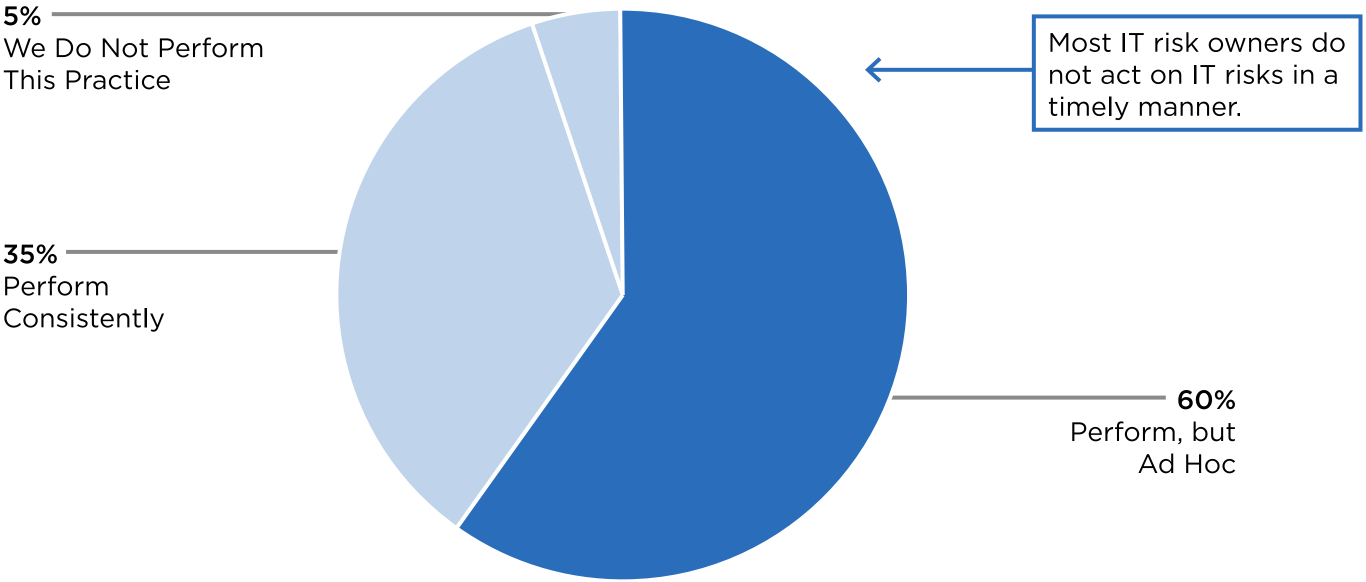
Consistently Tracking IT Risks

Appendix

FUNCTIONS STRUGGLE TO ENGAGE STAKEHOLDERS

Degree to Which IT Risks, Threats, and Opportunities Are Acted Upon in a Timely Manner by IT Risk Owners

Percentage of Respondents Who Have Formal IT Risk Functions



Most IT risk owners do not act on IT risks in a timely manner.

n = 43.

Source: CEB 2017 State of IT Risk Survey.

> "It's difficult for us to communicate the importance of being robust in our management of IT risk. There's no burning platform; people say: 'One of these days we should really expand the scope of IT risk,' but there is no feeling of urgency."
>
> Head of IT Risk
> Education Company

DEFINE IT RISK USING A TAXONOMY

IT Risk Taxonomy
Illustrative

IT Risk Type

IT Talent (Employees and Contractors)

- Shortfall of Staff
- Unpreparedness of Staff for a New Role
- Ineffectiveness of Staff

IT Capacity

- Limitations of the Network/Bandwidth
- Insufficient Storage
- Insufficient Computing Power
- Inability to Scale Other IT Capabilities

IT Reliability and Quality

- Loss of Integrity
- Loss of Availability
- Unacceptable Latency
- Vendor Support
- End of Life Support/Obsolescence

Information Security and Privacy

- Breach of Confidentiality
- Breach of Privacy

IT Legal and Compliance

- Audit Findings and Remediation Costs Fines
- Civil Lawsuits
- Criminal Charges
- Regulators Prevent Doing Business

IT Delivery

- Late Delivery
- Over Budget
- Unrealized Business Benefits
- Under-Adoption

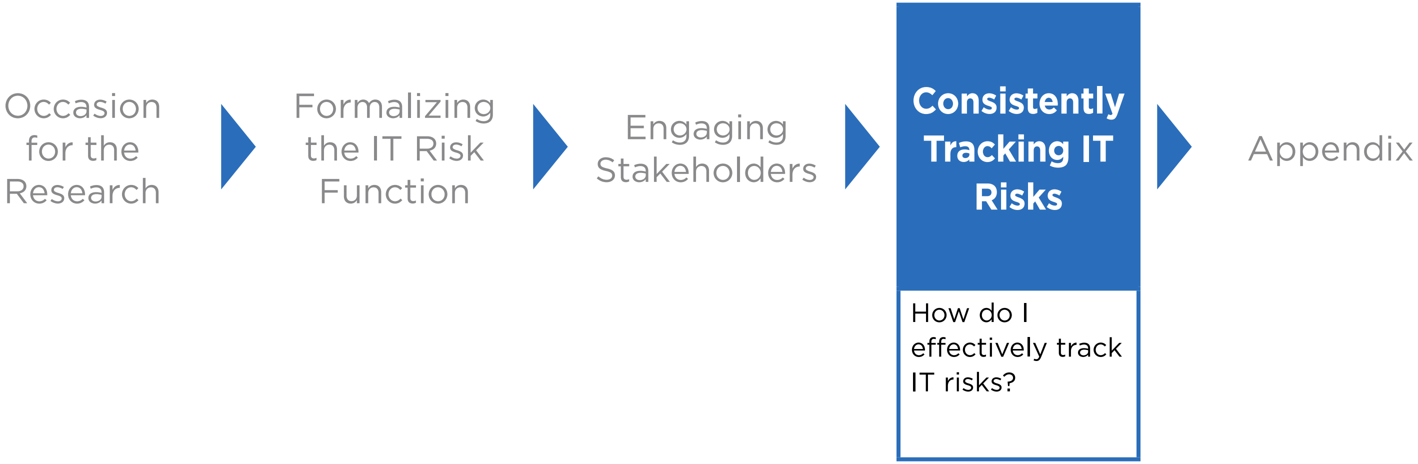
IT Business Enablement

- Insufficiently Responsive to Business Needs
- Impact to Employee Productivity
- Damage to Company Reputation or Brand
- Missed Technology-Related Innovation and Opportunity Identification
- Excess Operational Cost

Source: CEB analysis.

ROADMAP FOR THE PRESENTATION

Key Practitioner Questions



Occasion for the Research

Formalizing the IT Risk Function

Engaging Stakeholders

Consistently Tracking IT Risks

How do I effectively track IT risks?

Appendix

MEASURING IT RISK IS A CHALLENGE

Selected Excerpts from Conversations with Practitioners

> "We need metrics to help communicate how we are treading our desired risk tolerance level to our board. We also need to show that we are mitigating risks, how quickly are we closing gaps, and our recovery time."
>
> Head of IT Risk
> Financial Industry

> "A big challenge is obtaining qualitative and quantitative data to measure technology risk. Take obsolescence: how do we measure and report on that?"
>
> Head of IT Risk
> Pharmaceutical Industry

> "We are working on a standardized process for risk owners to measure and report on IT risks. Right now the process is not at all explicit, which makes it difficult to know how much risk you have and to compare risks across categories."
>
> Head of IT Risk
> Technology Industry

Source: CEB analysis.

DEVELOP UNIFIED RISK-REPORTING STANDARDS

Vodafone's Line-of-Sight Report
Illustrative

Report Section	What It Includes	How It Helps Senior Leaders
Section 1: Risk Overview	■ Essential risk background information (e.g., definition, impact, likelihood, ownership, oversight body, quantification of scenarios)	■ Gives context on why this is a principal risk that the organization needs to focus on ■ Provides insight into the risk owner's assessment on how comfortable the organization feels with the current level of risk exposure
Section 2: Risk Tolerance	■ Desired/target risk tolerance ■ Current position in relation to target tolerance	■ Defines the organization's level of comfort with the current risk exposure and where they currently stand in relation to that
Section 3: Risk Metrics	■ List of key risk metrics (KRI) ■ Assessment on whether the organization needs to do more or less to manage the risk	■ Indicates whether the risk is within the desired risk-tolerance level and whether relevant action plans deliver
Section 4: Action Plans	■ List of current actions plans to achieve target tolerance level	■ Demonstrates what measures the organization takes to address the current risk exposure
Section 5: Risk Mitigation and Assurance	■ Material controls in place ■ Overview of assurance oversight across the three lines of defense	■ Informs how the risk is managed in the first line of defense and the level of ongoing oversight provided by the second and third lines
Section 6: Assurance Results	■ Results of assurance activities testing the controls' effectiveness across the three lines defense	■ Indicates how effective the material controls are and whether there is a need for improvement

Source: Vodafone; CEB analysis.

vodafone

ROADMAP FOR THE PRESENTATION

Key Practitioner Questions

Occasion for the Research

Formalizing the IT Risk Function

Engaging Stakeholders

Consistently Tracking IT Risks

Appendix

- Survey demographics
- Summary results

SURVEY DEMOGRAPHICS

Industry	Percentage of Organizations
Financial Services	**10%**
Energy & Utilities	**6%**
Real Estate	**1%**
Insurance	**15%**
Education	**2%**
Transportation Services	**2%**
Electronics	**4%**
Banking	**6%**
Industrial Manufacturing	**2%**
Pharmaceuticals	**11%**
Beverages	**1%**
Government	**9%**
Construction	**1%**
Consumer Services	**1%**
Computer Software	**2%**
Retail	**6%**
Health Care	**5%**
Leisure	**1%**
Business Services	**2%**
Aerospace & Defense	**4%**
Chemicals	**2%**
Food	**1%**
Telecommunications Services	**1%**
Consumer Products Manufacturers	**1%**

Region	Percentage of Organizations
NA	**74%**
EMEA	**16%**
APAC	**10%**

Revenue	Percentage of Organizations
< $3 billion	**30%**
$3–$10 billion	**12%**
$10–$25 billion	**32%**
> $25 billion	**26%**

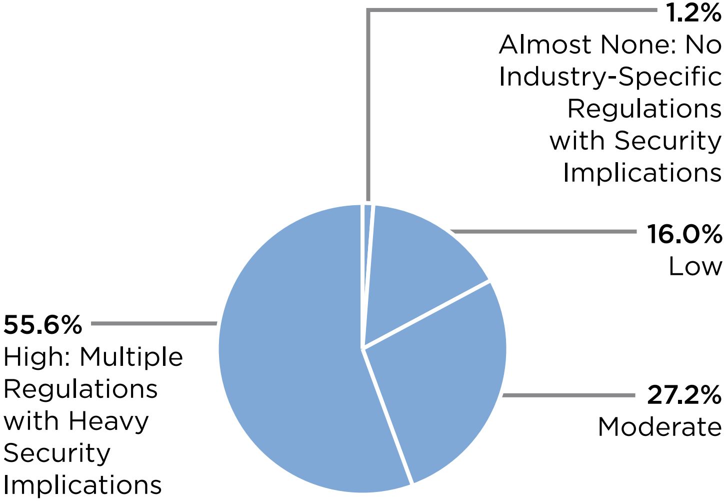
n = 81.

Source: CEB 2017 IT Risk Survey.

SURVEY DEMOGRAPHICS

Amount of Regulatory Burden Experienced by Organizations

Percentage of Respondents

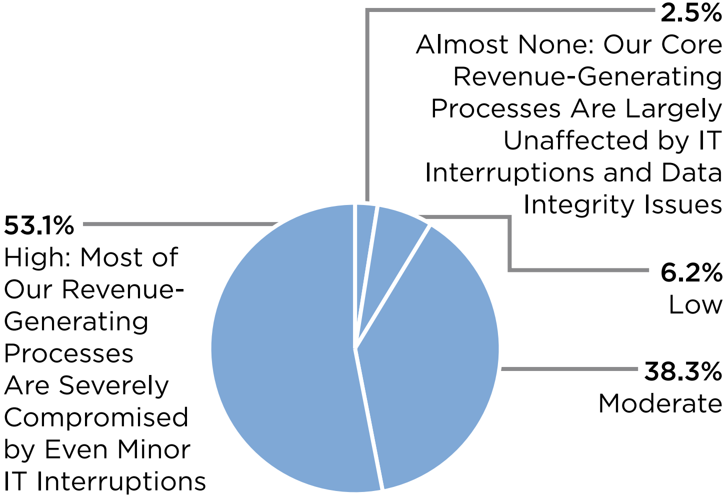


n = 81.

Source: CEB 2017 State of IT Risk Survey.

Technology-Intensiveness of Business Processes

Percentage of Respondents



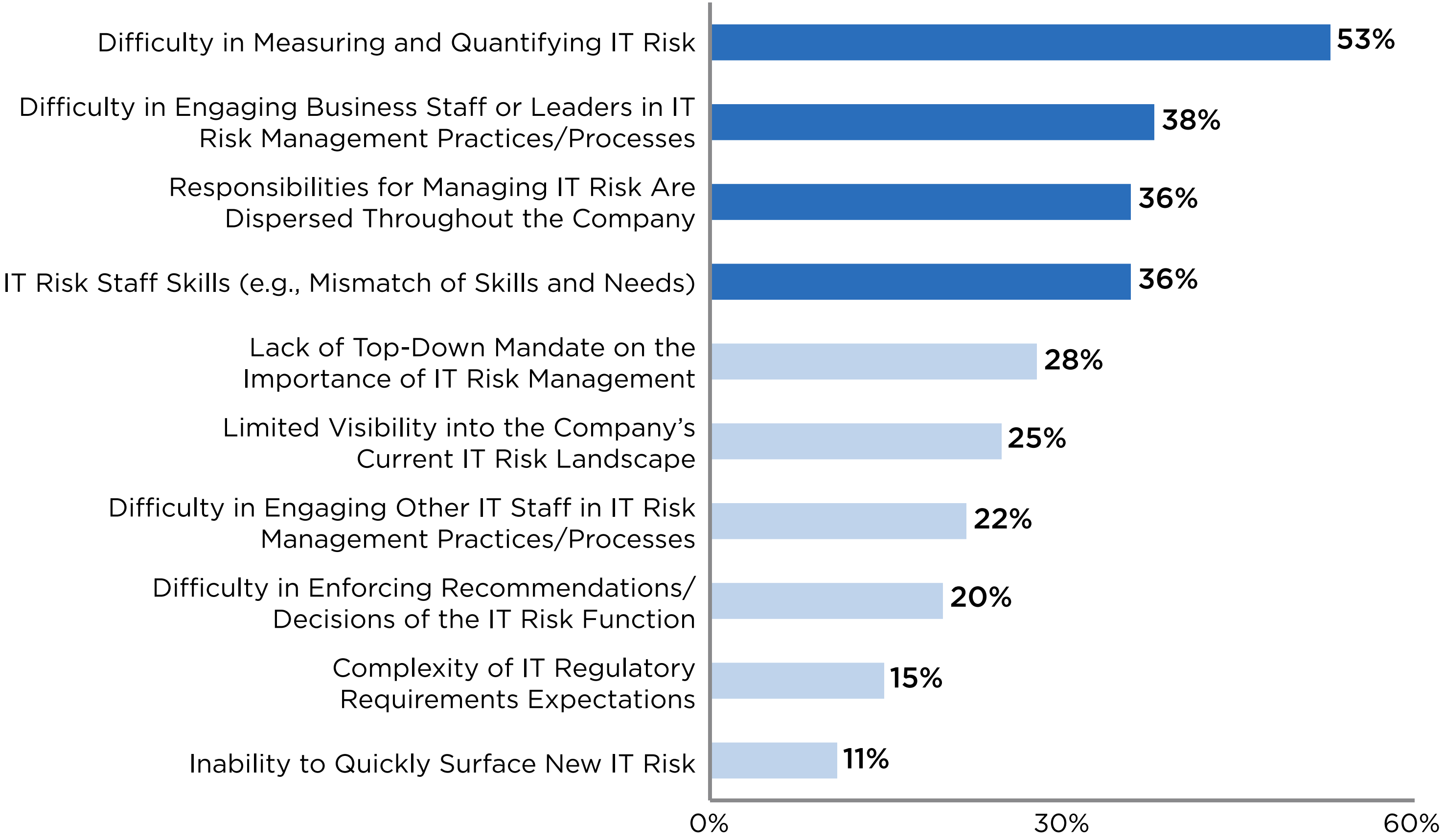
n = 81.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY RESULTS

Barriers to Building Effective IT Risk Management Practices

Percentage of Respondents Who Report Having a Formal Function



n = 81.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

Responsibility for Managing IT Risks

Percentage of Respondents Who Report Having a Formal Function

IT Risk Taxonomy Category	IT Risk	Percentage Selected
Business Enablement	Impact to Employee Productivity	14%
	Missed Technology-Related Innovation and Opportunity Identification	19%
	Excess Operational Cost	23%
	Insufficient Responsiveness to Business Needs	28%
	Damage to Company Reputation or Brand	51%
IT Capacity	Insufficient Storage	9%
	Insufficient Computing Power	9%
	Limitations of the Network/Bandwidth	16%
	Inability to Scale Other IT Capabilities	30%
IT Delivery	Under-Adoption	16%
	Over Budget	21%
	Unrealized Business Benefits	21%
	Late or Incomplete Delivery	23%
IT Legal and Compliance	Civil Lawsuits	7%
	Criminal Charges	9%
	Legal Fines or Penalties	16%
	IT Audit Findings and Remediation Costs	79%

n = 43.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

Responsibility for Managing IT Risks

Percentage of Respondents Who Report Having a Formal Function

IT Risk Taxonomy Category	IT Risk	Percentage Selected
IT Reliability and Quality	Unacceptable Latency	19%
	Vendor Support	37%
	End of Life Support/Obsolescence	40%
	Loss of Availability	58%
	Loss of Integrity	65%
IT Talent (Employees and Contractors)	Unpreparedness of Staff for a New Role	14%
	Ineffectiveness of Staff	19%
	Shortfall of Staff	28%
Security and Privacy	Breach of Privacy	65%
	Breach of Confidentiality	81%

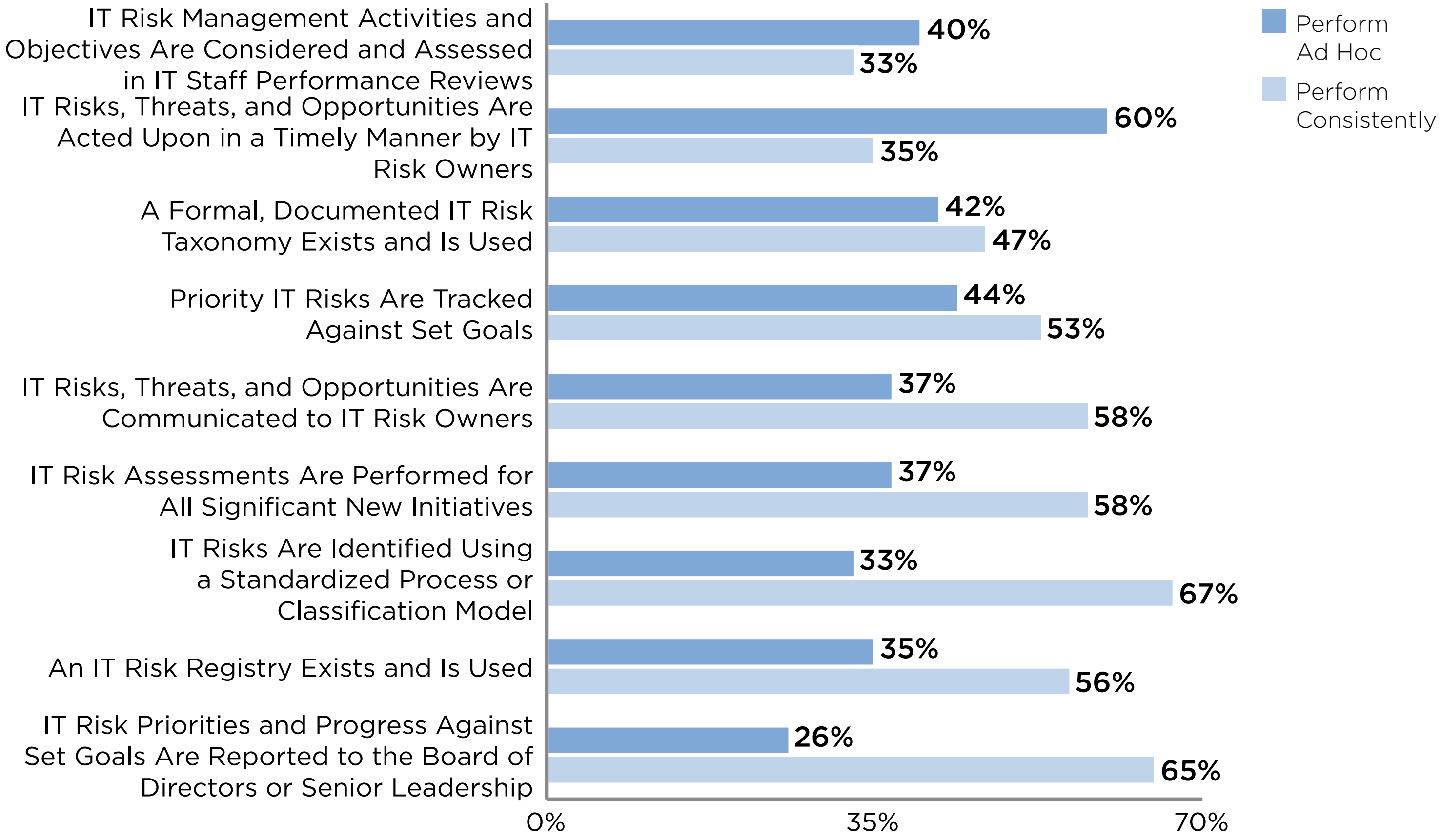
n = 43.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

Maturity in Conducting IT Risk Management Activities

Percentage of Respondents Who Report Having a Formal Function

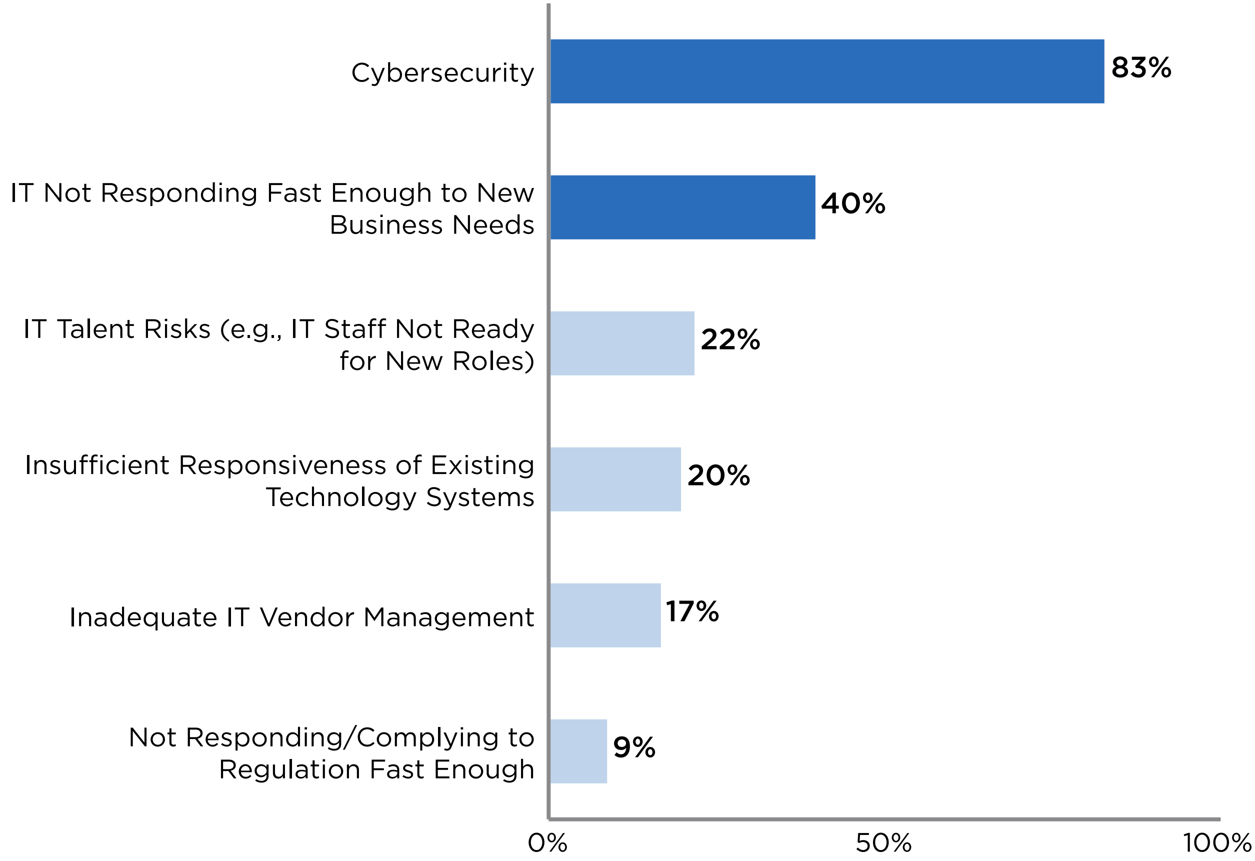


n = 43.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

Biggest IT Risks Facing Respondents' Organizations Today
Percentage of Respondents Selecting Risk: Two Responses Allowed



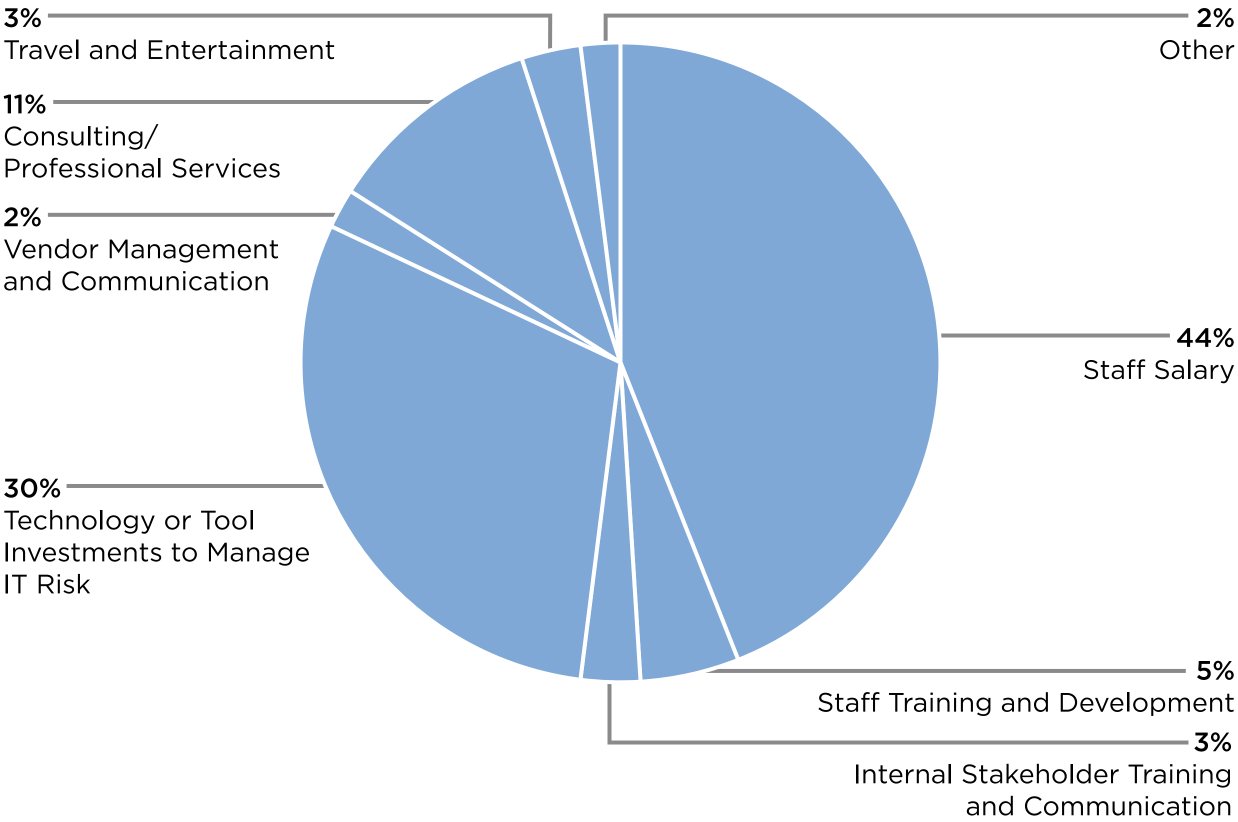
n = 81.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

Distribution of a Budget for a Formal IT Risk Function

Percentage of Respondents Who Report Having a Formal Function and a Dedicated Budget



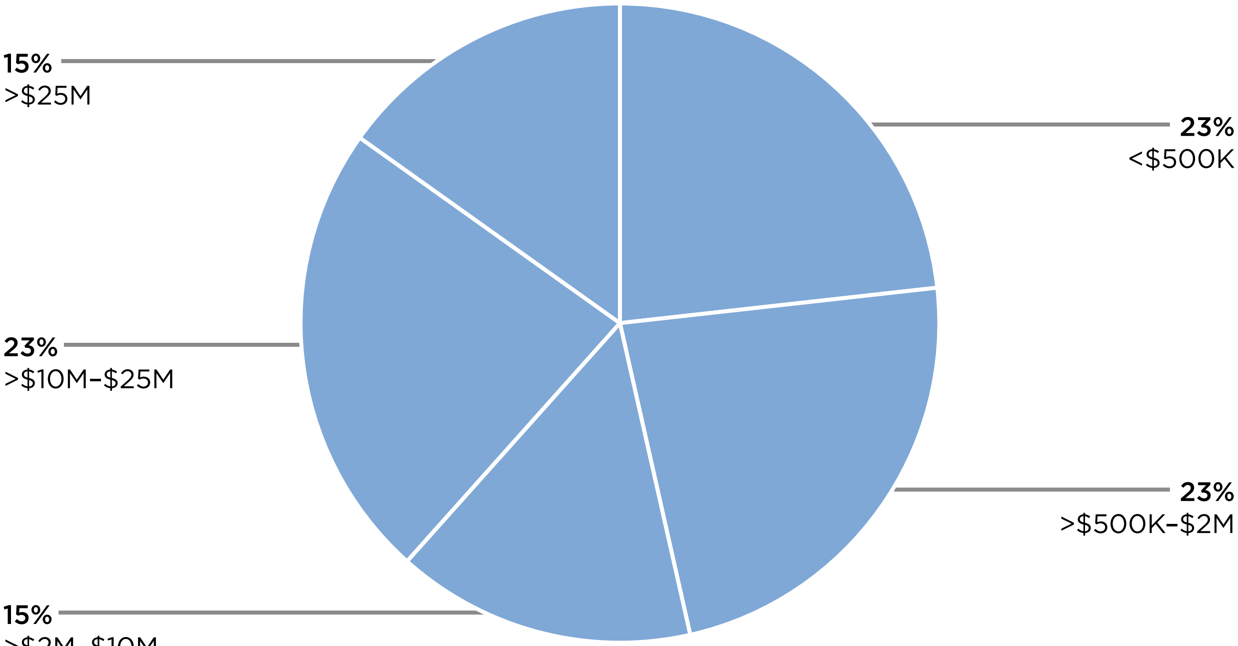
n = 15.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

IT Risk Function's 2017 Budget in $US

Percentage of Respondents Who Report Having a Formal Function and a Dedicated Budget



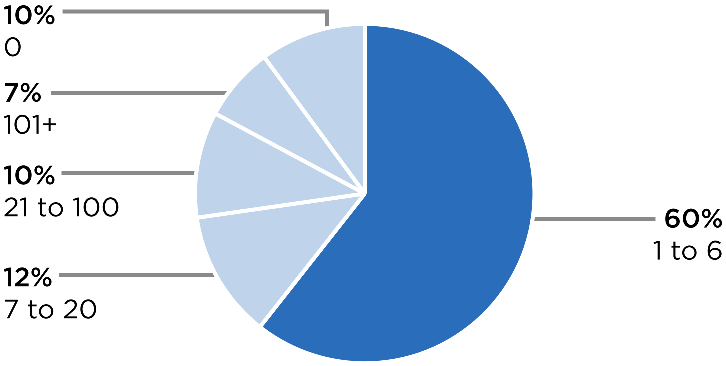
n = 13.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

Total Number IT Risk Employees in 2017 or the Current Fiscal Year
Percentage of Respondents

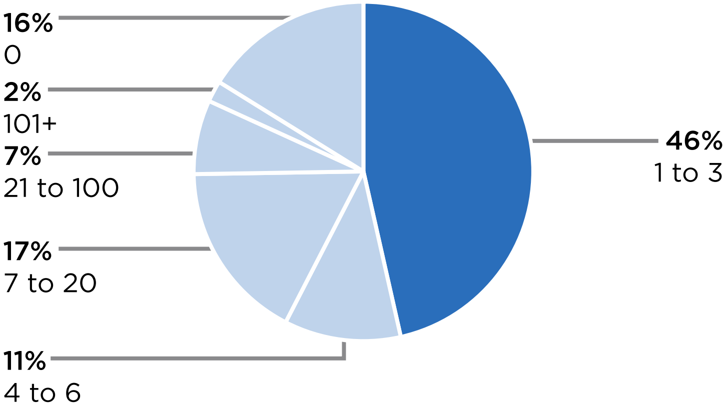
Number of full-time (i.e., those dedicating more than 50% of their time to IT risk activities and including the head of IT risk) IT risk employees



n = 81.

Source: CEB 2017 State of IT Risk Survey.

Number of part-time (i.e., those dedicating less than 50% of their time to IT risk activities and including the head of IT risk) IT risk employees



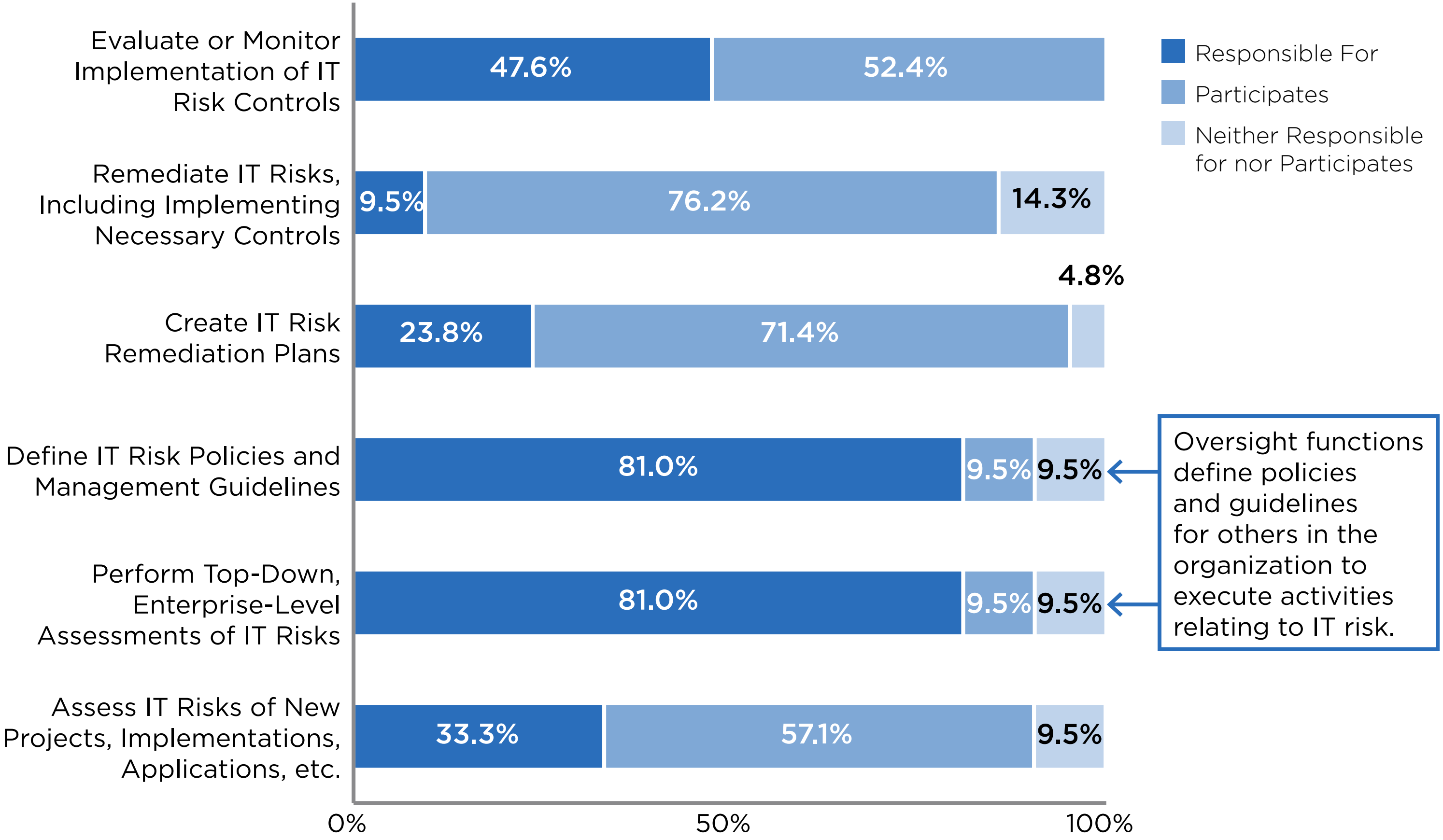
n = 81.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

Ownership of IT Risk Activities for Oversight Functions

Percentage of Respondents Who Report Having a Formal IT Risk Function



Oversight functions define policies and guidelines for others in the organization to execute activities relating to IT risk.

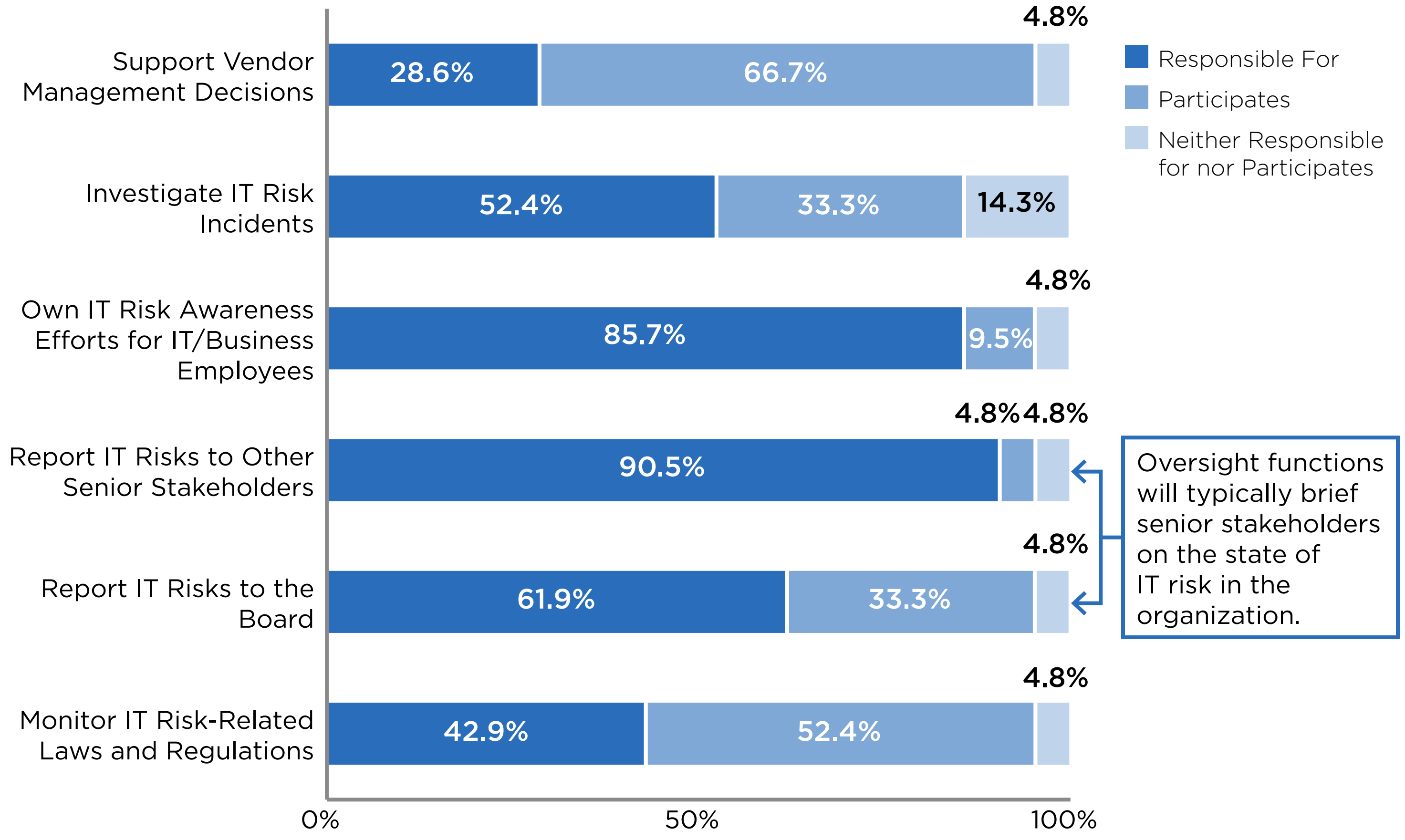
n = 43.

Source: CEB State of IT Risk Survey.

SUMMARY (CONTINUED)

Ownership of IT Risk Activities for Oversight Functions

Percentage of Respondents Who Report Having a Formal IT Risk Function



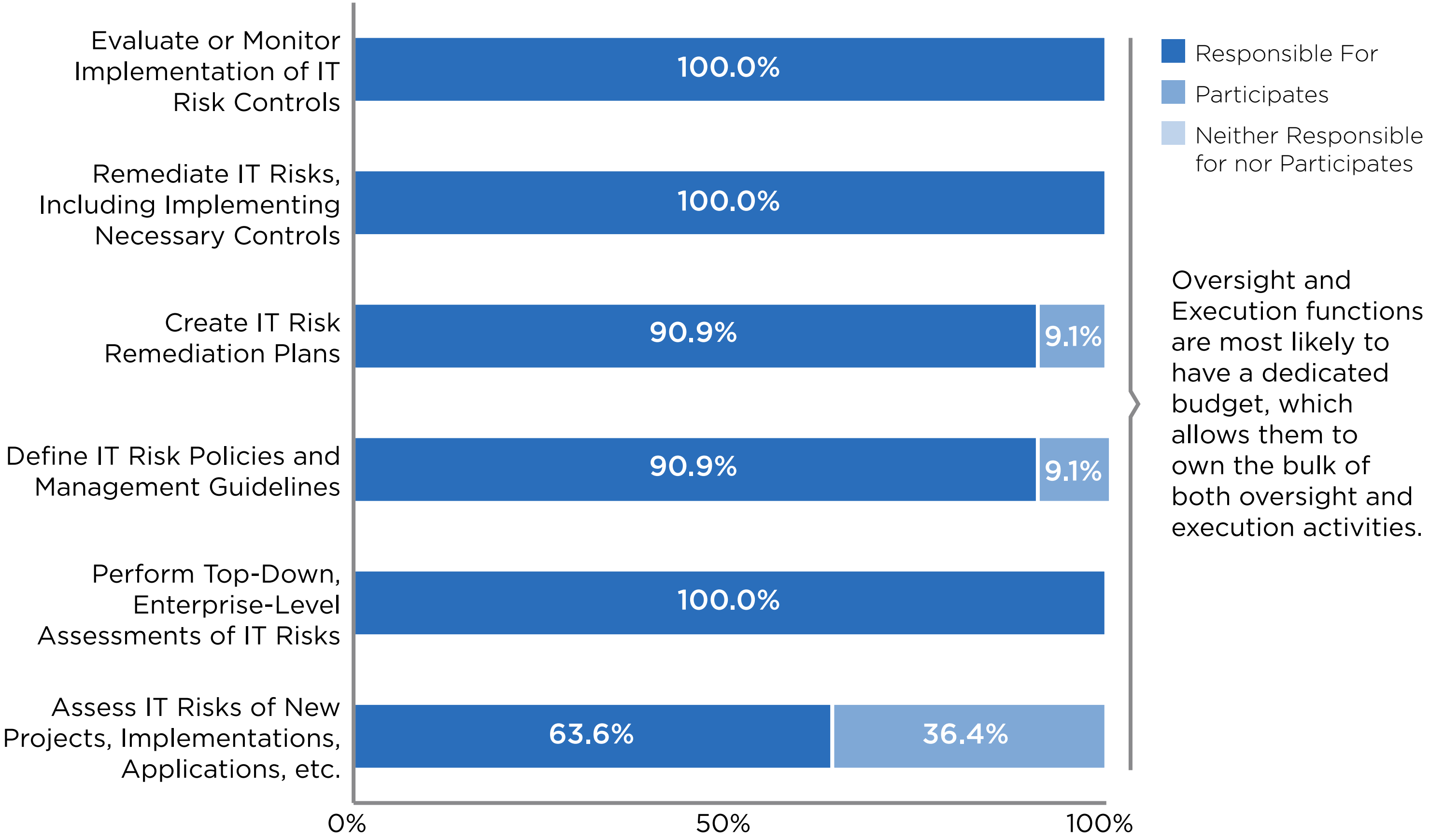
Oversight functions will typically brief senior stakeholders on the state of IT risk in the organization.

n = 43.

Source: CEB State of IT Risk Survey.

SUMMARY (CONTINUED)

Ownership of IT Risk Activities for Oversight and Execution Functions
Percentage of Respondents Who Report Having a Formal IT Risk Function



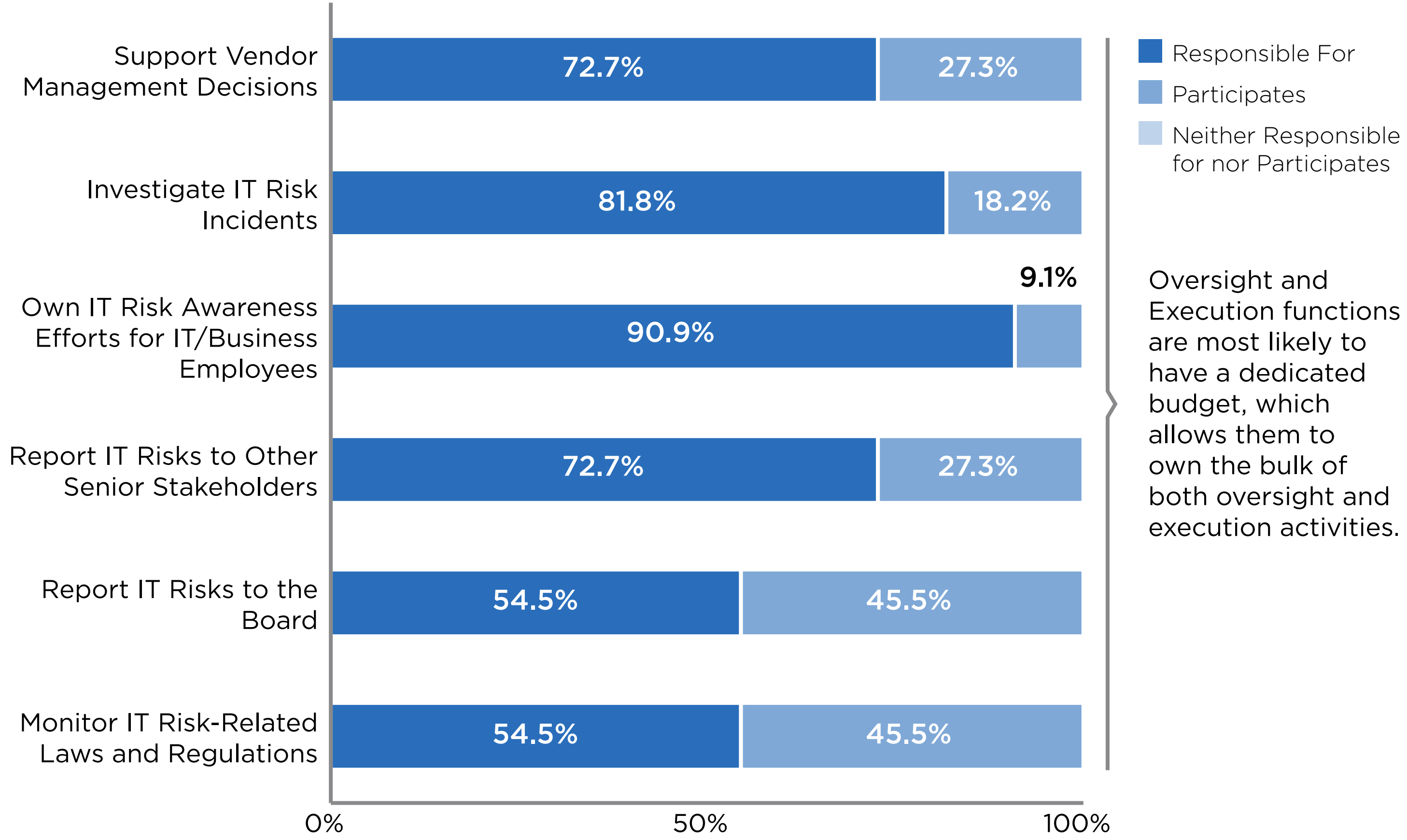
Oversight and Execution functions are most likely to have a dedicated budget, which allows them to own the bulk of both oversight and execution activities.

n = 43.

Source: CEB State of IT Risk Survey.

SUMMARY (CONTINUED)

Ownership of IT Risk Activities for Oversight and Execution Functions
Percentage of Respondents Who Report Having a Formal IT Risk Function



Oversight and Execution functions are most likely to have a dedicated budget, which allows them to own the bulk of both oversight and execution activities.

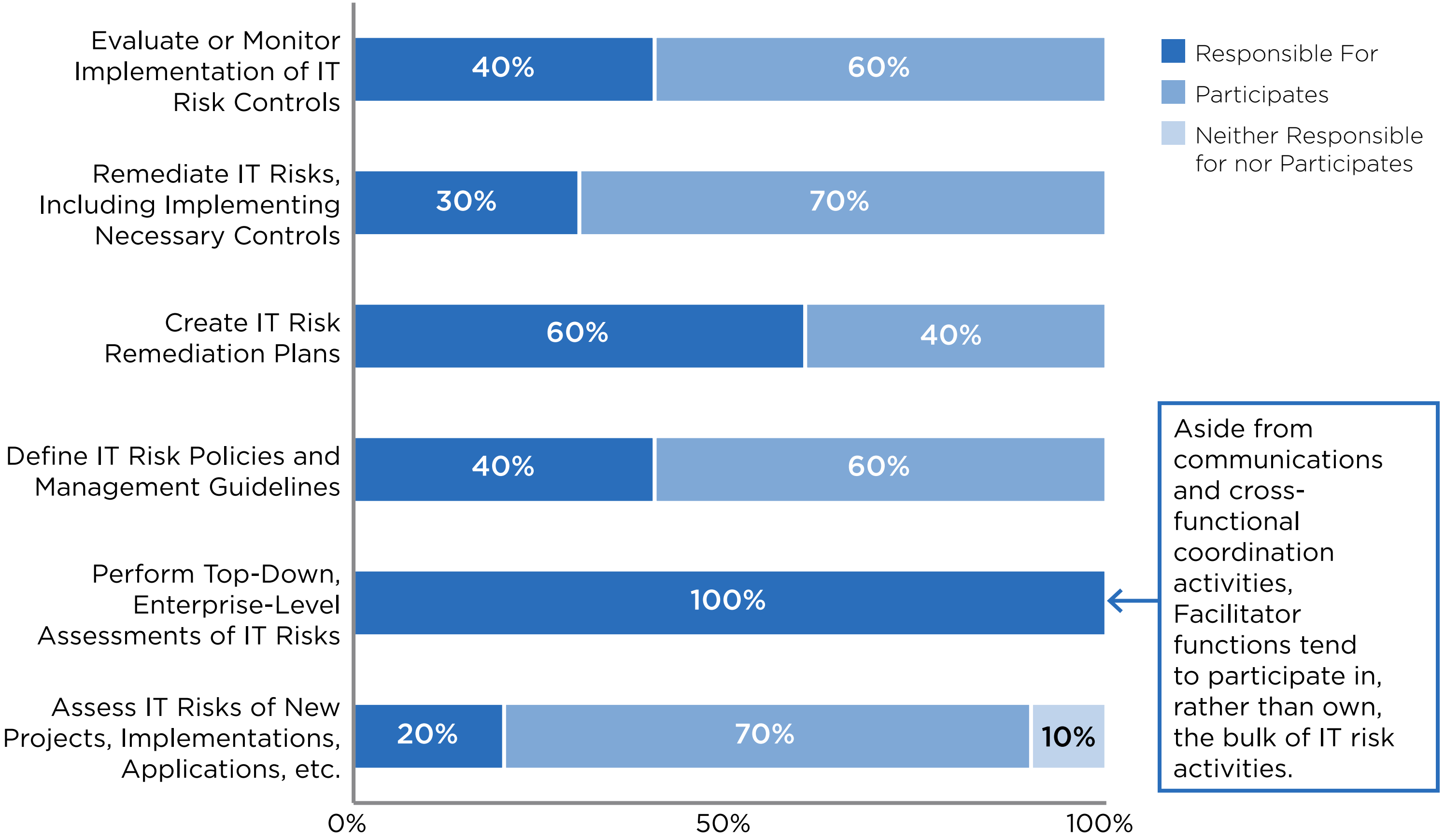
n = 43.

Source: CEB State of IT Risk Survey.

SUMMARY (CONTINUED)

Ownership of IT Risk Activities for Facilitator Functions

Percentage of Respondents Who Report Having a Formal IT Risk Function



Aside from communications and cross-functional coordination activities, Facilitator functions tend to participate in, rather than own, the bulk of IT risk activities.

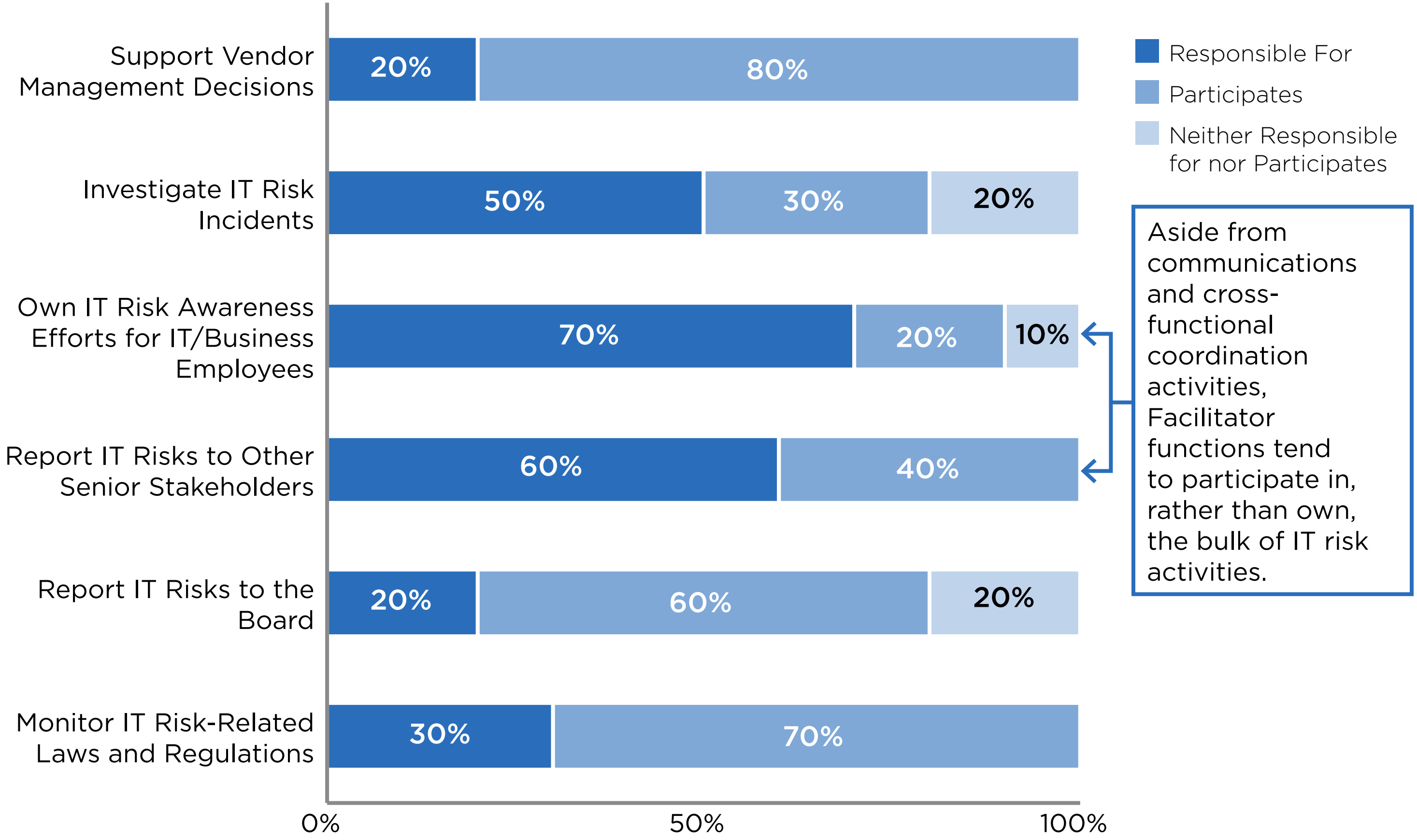
n = 43.

Source: CEB State of IT Risk Survey.

SUMMARY (CONTINUED)

Ownership of IT Risk Activities for Facilitator Functions

Percentage of Respondents Who Report Having a Formal IT Risk Function



Aside from communications and cross-functional coordination activities, Facilitator functions tend to participate in, rather than own, the bulk of IT risk activities.

n = 43.

Source: CEB State of IT Risk Survey.

SUMMARY (CONTINUED)

Surveyed Organizations’ Level of Technology Dependency
Percentage of Respondents Who Report Having a Formal IT Risk Function

	Profile					
	Oversight		Oversight and Execution		Facilitator	
Almost None: Our core revenue-generating processes are largely unaffected by IT interruptions and data integrity issues	0	0%	0	0%	0	0%
Low	2	10%	0	0%	1	10%
Moderate	2	10%	4	36%	5	50%
High: Most of our revenue-generating processes are severely compromised by even minor IT interruptions and data integration	17	81%	7	64%	4	40%

Organizations most dependent on technology tend to have the most mature IT Risk function profile.

n = 42.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

IT Risk Function Responsibilities According to Their Profile

Percentage of Respondents Who Report Having a Formal Function

Activities		Profile					
		Oversight		Oversight and Execution		Facilitator	
Monitor IT Risk-Related Laws and Regulations	Neither Responsible for nor Participates	1	5%	0	0%	0	0%
	Participates	11	52%	5	45%	7	70%
	Responsible For	9	43%	6	55%	3	30%
Report IT Risks to the Board	Neither Responsible for nor Participates	1	5%	0	0%	2	20%
	Participates	7	33%	5	45%	6	60%
	Responsible For	13	62%	6	55%	2	20%
Report IT Risks to Other Senior Stakeholders	Neither Responsible for nor Participates	1	5%	0	0%	0	0%
	Participates	1	5%	3	27%	4	40%
	Responsible For	19	90%	8	73%	6	60%
Own IT Risk Awareness Efforts for IT/Business Employees	Neither Responsible for nor Participates	1	5%	0	0%	1	10%
	Participates	2	10%	1	9%	2	20%
	Responsible For	18	86%	10	91%	7	70%
Investigate IT Risk Incidents	Neither Responsible for nor Participates	3	14%	0	0%	2	20%
	Participates	7	33%	2	18%	3	30%
	Responsible For	11	52%	9	82%	5	50%

n = 43.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

IT Risk Function Responsibilities According to Their Profile
Percentage of Respondents Who Report Having a Formal Function

Activities		Profile					
		Oversight		Oversight and Execution		Facilitator	
Support Vendor Management Decisions (e.g., Review and Negotiate IT Risk Provisions in Vendor Contracts)	Neither Responsible for nor Participates	1	5%	0	0%	0	0%
	Participates	14	67%	3	27%	8	80%
	Responsible For	6	29%	8	73%	2	20%
Assess IT Risks of New Projects, Implementations, Applications, etc.	Neither Responsible for nor Participates	2	10%	0	0%	1	10%
	Participates	12	57%	4	36%	7	70%
	Responsible For	7	33%	7	64%	2	20%
Perform Top-Down, Enterprise-Level Assessments of IT Risks (e.g., Identify Top 5–10 IT Risks)	Neither Responsible for nor Participates	2	10%	0	0%	0	0%
	Participates	2	10%	0	0%	0	0%
	Responsible For	17	81%	11	100%	10	100%

n = 43.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

IT Risk Function Responsibilities According to Their Profile
Percentage of Respondents Who Report Having a Formal Function

Activities		Profile					
		Oversight		Oversight and Execution		Facilitator	
IT Risk Functions Level of Involvement—Define IT Risk Policies and Management Guidelines	Neither Responsible for nor Participates	2	10%	0	0%	0	0%
	Participates	2	10%	1	9%	6	60%
	Responsible For	17	81%	10	91%	4	40%
Create IT Risk Remediation Plans	Neither Responsible for nor Participates	1	5%	0	0%	0	0%
	Participates	15	71%	1	9%	4	40%
	Responsible For	5	24%	10	91%	6	60%
Remediate IT Risks, Including Implementing Necessary Controls	Neither Responsible for nor Participates	3	14%	0	0%	0	0%
	Participates	16	76%	0	0%	7	70%
	Responsible For	2	10%	11	100%	3	30%
Evaluate or Monitor Implementation of IT Risk Controls	Neither Responsible for nor Participates	0	0%	0	0%	0	0%
	Participates	11	52%	0	0%	6	60%
	Responsible For	10	48%	11	100%	4	40%

n = 43.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

Direct Manager of Heads of IT Risk

Percentage of Respondents Who Report Having a Formal Function

	Profile					
	Oversight		Oversight and Execution		Facilitator	
Chief Executive Officer (CEO)	0	0%	0	0%	0	0%
Chief Information Officer (CIO)	11	52%	5	45%	4	40%
Chief Technology Officer (CTO)	0	0%	2	18%	0	0%
Chief Information Security Officer (CISO)	5	24%	3	27%	6	60%
Head of IT Audit	0	0%	0	0%	0	0%
Head of Legal/General Council	0	0%	0	0%	0	0%
Chief Risk Officer (CRO)	2	10%	0	0%	0	0%
Head of Enterprise Risk Management (ERM)	0	0%	0	0%	0	0%
Head of Operational Risk	0	0%	1	9%	0	0%
Chief Compliance Officer	0	0%	0	0%	0	0%
Chief Financial Officer (CFO)	0	0%	0	0%	0	0%
Chief Operating Officer (COO)	0	0%	0	0%	0	0%
Head of Internal Audit	0	0%	0	0%	0	0%
Cross-Functional Governance Committee	0	0%	0	0%	0	0%
Other, Please Specify:	3	14%	0	0%	0	0%

"Other" answers included the Chief Control Officer and Technology Risk and Compliance VP.

n = 42.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

Dotted Line Reporting for Heads of IT Risk

Percentage of Respondents Who Report Having a Formal Function

		Profile					
		Oversight		Oversight and Execution		Facilitator	
Chief Executive Officer (CEO)	Not Selected	19	90%	8	73%	10	100%
	Selected	2	10%	3	27%	0	0%
Chief Information Officer (CIO)	Not Selected	15	71%	9	82%	7	70%
	Selected	6	29%	2	18%	3	30%
Chief Technology Officer (CTO)	Not Selected	18	86%	11	100%	8	80%
	Selected	3	14%	0	0%	2	20%
Chief Information Security Officer (CISO)	Not Selected	21	100%	11	100%	8	80%
	Selected	0	0%	0	0%	2	20%
Head of IT Audit	Not Selected	20	95%	11	100%	9	90%
	Selected	1	5%	0	0%	1	10%
Head of Legal/General Council	Not Selected	18	86%	11	100%	10	100%
	Selected	3	14%	0	0%	0	0%

n = 42.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

Dotted Line Reporting for Heads of IT Risk
Percentage of Respondents Who Report Having a Formal Function

		Profile					
		Oversight		Oversight and Execution		Facilitator	
Chief Risk Officer (CRO)	Not Selected	17	81%	10	91%	8	80%
	Selected	4	19%	1	9%	2	20%
Head of Enterprise Risk Management (ERM)	Not Selected	17	81%	11	100%	9	90%
	Selected	4	19%	0	0%	1	10%
Head of Operational Risk	Not Selected	19	90%	10	91%	9	90%
	Selected	2	10%	1	9%	1	10%
Chief Compliance Officer	Not Selected	18	86%	11	100%	10	100%
	Selected	3	14%	0	0%	0	0%
Chief Financial Officer (CFO)	Not Selected	18	86%	11	100%	9	90%
	Selected	3	14%	0	0%	1	10%
Chief Operating Officer (COO)	Not Selected	21	100%	9	82%	10	100%
	Selected	0	0%	2	18%	0	0%

n = 42.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

Dotted Line Reporting for Heads of IT Risk

Percentage of Respondents Who Report Having a Formal Function

		Profile					
		Oversight		Oversight and Execution		Facilitator	
Head of Internal Audit	Not Selected	18	86%	10	91%	10	100%
	Selected	3	14%	1	9%	0	0%
Cross-Functional Governance Committee	Not Selected	17	81%	9	82%	10	100%
	Selected	4	19%	2	18%	0	0%

n = 42.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

IT Risk Function Maturity

Percentage of Respondents Who Report Having a Formal Function

Maturity Activities		Profile					
		Oversight		Oversight and Execution		Facilitator	
IT Risk Priorities and Progress Against Set Goals Are Reported to the Board of Directors or Senior Leadership	We Do Not Perform This Practice	1	5%	1	9%	2	20%
	Perform, but Ad Hoc	3	14%	3	27%	4	40%
	Perform Consistently	17	81%	7	64%	4	40%
IT Risks Are Identified Using a Standardized Process or Classification Model	We Do Not Perform This Practice	0	0%	0	0%	0	0%
	Perform, but Ad Hoc	4	19%	4	36%	6	60%
	Perform Consistently	17	81%	7	64%	4	40%
Priority IT Risks Are Tracked Against Set Goals	We Do Not Perform This Practice	0	0%	0	0%	1	10%
	Perform, but Ad Hoc	7	33%	5	45%	6	60%
	Perform Consistently	14	67%	6	55%	3	30%
IT Risk Management Activities and Objectives Are Considered and Assessed in IT Staff Performance Reviews	We Do Not Perform This Practice	5	24%	2	18%	5	50%
	Perform, but Ad Hoc	8	38%	6	55%	2	20%
	Perform Consistently	8	38%	3	27%	3	30%

🟦 Function Profile Most Mature in Performing or Facilitating IT Risk Activity in the Organization

n = 42.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

IT Risk Function Maturity

Percentage of Respondents Who Report Having a Formal Function

Maturity Activities		Profile					
		Oversight		Oversight and Execution		Facilitator	
IT Risk Assessments Are Performed for All Significant New Initiatives	We Do Not Perform This Practice	0	0%	0	0%	2	20%
	Perform, but Ad Hoc	8	38%	4	36%	3	30%
	Perform Consistently	13	62%	7	64%	5	50%
IT Risks, Threats, and Opportunities Are Communicated to IT Risk Owners	We Do Not Perform This Practice	1	5%	0	0%	1	10%
	Perform, but Ad Hoc	6	29%	4	36%	6	60%
	Perform Consistently	14	67%	7	64%	3	30%
IT Risks, Threats, and Opportunities Are Acted Upon in a Timely Manner by IT Risk Owners	We Do Not Perform This Practice	0	0%	1	9%	1	10%
	Perform, but Ad Hoc	12	57%	5	45%	8	80%
	Perform Consistently	9	43%	5	45%	1	10%
A Formal, Documented IT Risk Taxonomy Exists and Is Used	We Do Not Perform This Practice	2	10%	0	0%	3	30%
	Perform, but Ad Hoc	5	24%	7	64%	5	50%
	Perform Consistently	14	67%	4	36%	2	20%

🟦 Function Profile Most Mature in Performing or Facilitating IT Risk Activity in the Organization

n = 42.

Source: CEB 2017 State of IT Risk Survey.

SUMMARY (CONTINUED)

IT Risk Function Maturity

Percentage of Respondents Who Report Having a Formal Function

Maturity Activities		**Profile**					
		Oversight		**Oversight and Execution**		**Facilitator**	
An IT Risk Registry Exists and Is Used	We Do Not Perform This Practice	1	5%	1	9%	1	10%
	Perform, but Ad Hoc	5	24%	5	45%	5	50%
	Perform Consistently	15	71%	5	45%	4	40%

🟦 Function Profile Most Mature in Performing or Facilitating IT Risk Activity in the Organization

n = 42.

Source: CEB 2017 State of IT Risk Survey.

CEB INFORMATION RISK SERVICE UPDATES

Upcoming Events

Fusion Teams: How Digitization Work Gets Done	24 August
IT Operating Model for Digital Webinar Series: Adaptive Skills and Mindset	7 September

CEB's Annual Executive Retreat: Adapting Information Security for the Digital Era

Digitization offers Information Security unprecedented opportunities to enable business growth by guiding appropriate risk taking. But at the same time, digital transformation—especially Agile and DevOps—is causing strain on Information Security's status quo. CISOs must make significant shifts to adapt security's governance processes and skill sets to adapt the function.

Join us to learn how your peers are transforming security's governance processes and skill sets for digital business enablement.

2017 Dates: 6–7 September (New York), 12 October (London), 2–3 November (Palo Alto)

New Diagnostics and Tools

CEB Ignition™ Diagnostic for Information Risk — Always Available

Identify maturity gaps and prioritize areas for improvement based on over 20 years of our in-depth research into what defines high performing IT teams.

Security Activity-Skill Alignment Matrix Tool — Always Available

The Security Activity-Skill Alignment Matrix Tool helps you improve your strategic workforce planning by documenting required skills and competencies across different security activities.

Information Security Controls Mapping Tool — Always Available

Use our updated controls mapping tool to track alignment to ISO 27002, NIST 800-53, NIST CSF, and now NIST 800-171.