REPORT

# Evolving Resiliency Strategies Report

## Achieving the Right Level of Resilience

BC Management

Castellan

# Contents


5 Executive Summary

7 Program Resiliency Strategies

23 Program Characteristics

26 Demographics

30 BCM Research Overview

32 Advisory Board & Distributing Organizations

39 About BC Management

40 About Castellan

# Study Partner

Castellan

## ABOUT CASTELLAN

As the largest provider of business continuity management solutions – spanning consulting, software, managed services, and staffing – Castellan is uniquely positioned to help clients find the right balance of risk tolerance and resilience to protect their employees, brand, and bottom-line. Leveraging a proprietary proven process for driving business continuity success, Castellan partners with clients to establish a clear vision, drive real results, and provide on-going support from their community of business continuity experts. Castellan helps clients replace uncertainty with confidence.

For more information, visit castellanbc.com.

## ABOUT THE REPORT

This report focuses on the evolving strategies and approach to resiliency planning. Within this report you'll find data points highlighting what disruptions the program addresses when day-to-day management exceeds control, the executives who care most about the program and are involved in the governance committee, and what investment strategies are planned for 2022. The data highlighted throughout this report was gathered in BC Management's Evolving Resiliency Strategies Study between October 13, 2021 through December 10, 2021.

### This report is available as a complimentary report.

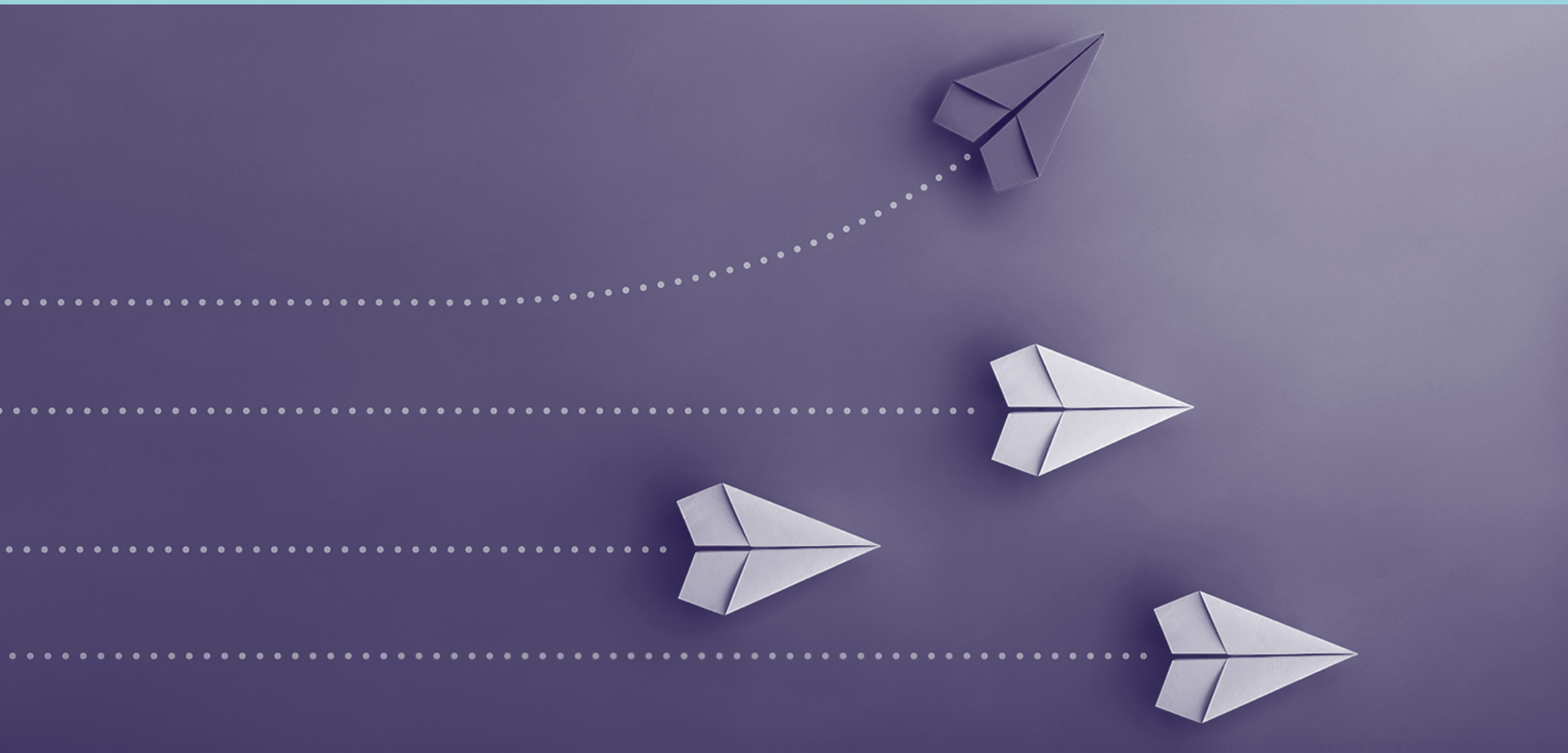
As a thank you to all of our study respondents we provided each participant with a complimentary, customized BCM Peer Benchmarking Data Dashboard, of which all study participants could choose their top three preferences by either industry or organizational gross annual revenues. If you haven't participated in this study and you'd like to receive a customized dashboard, you may still participate via our on-line study. Our dashboards highlight a tremendous amount of data points that are not included within this complimentary report.

### Like our research analytics?

Be sure to visit our website to download other complimentary reports and sign up for our study alerts. All study participants will receive customized peer dashboards for the corresponding studies they contribute to.

Please feel free to direct any inquiries to info@bcmanagement.com. We hope you enjoy this report.

# Executive Summary



# Executive Summary

We want to thank all of those who responded to the survey, our International Research Advisory Board, and everyone from the BC Management/Castellan Solutions team for their efforts in developing this valuable report.

This complimentary report highlights key findings and trends within resiliency planning for the previous year in addition to evolving resiliency strategies for the coming year. Those who confidentially participated in our study also received a customized BCM Peer Resilience Management Dashboard, which provides a full data review customized to either industry or by organizational revenues. And although this report included a more thorough assessment by different industries (financial, government, healthcare, insurance, and technology), we encourage you to participate in our Evolving Resiliency Strategies Study if you'd like to receive a more in-depth, customized data assessment within a dashboard.

This study, the first of its kind, highlighted some very intriguing data findings. One is that executive engagement and cyber response planning surged in 2021, followed by integrating resilience management programs with other risk disciplines. Executives showed increased scrutiny of resilience management capabilities and became actively involved in program updates, resulting in increased financial support of resiliency planning (via staffing, software automation, and technology), increased exercise participation, and elevated awareness across the organization. Looking forward into 2022, the data highlighted that many organizations are planning to keep their increased investment strategies in line to 2021 while focusing more on increasing situational awareness and threat intelligence in addition to technology resilience/ recoverability. Those organizations noting immature programs are planning to invest quite a bit more in their resilience management strategies in the next year.

The data findings also indicated that most resilience management programs address technology disruptions (88%), pandemic or a public health emergency (87%), and health/safety issues (82%), while only 52% of organizations noted that their program addresses supply chain disruptions and

## HIGHLIGHTS

**65%** of all respondents noted **increased executive engagement in 2021.**

**81%** of organizations with **mature programs** were more likely to address **operational resilience** within their program compared to those with **immature programs (65%).**

**80%** of respondents indicated that the **Chief Information Security Officer** cares most about the program (engaged or very engaged) followed by the **Chief Risk Officer (77%).**

**72%** of resilience management programs address **cyber attacks** when the impact exceeds day-to-day leadership control, but what about **credit and liquidity issues?** Only 14% address each of these issues.

### 2022 INVESTMENT STRATEGIES WILL BE FOCUSED IN:

**Technology Resilience/ Recoverability**

**Situational Awareness/ Threat intelligence**

only 42% of all organizations focus on supply chain continuity/resiliency planning. When taking a cross section of the data based on level of program maturity, we discovered that only 38% of immature programs and 64% of mature programs address this potential crisis in their programs. Although supply chain has traditionally operated independently of resiliency planning, we would expect that this will likely be an area of focused improvement in the coming years, especially after all the significant supply chain issues that impacted organizations since the start of the pandemic.

Our Evolving Resiliency Strategies Study also assessed how the program is prioritized and scoped, which has shifted in the last five years. Previously, a majority of plans were more location-based covering multiple functions within that location, likely to address different scenarios that might impact that one location from major life safety issues to natural events (weather related, earthquakes, etc.). Many organizations have been shifting their focus on the department, processes, or business functions (76%) to address when cyber attacks or reputation/brand issues may exceed day-to-day management control. Additionally, remote working, distributed workforce strategies, and planning philosophies, especially driven by the COVID pandemic, have also motivated organizations to be more strategic in their resilience management approach by incorporating enterprise risk management to develop targeted plans focused on the product, service, process, or output. There is still room for improvement, though, as few programs address liquidity, credit, product (recall, quality, delivery), or major publicly known audit finding issues.

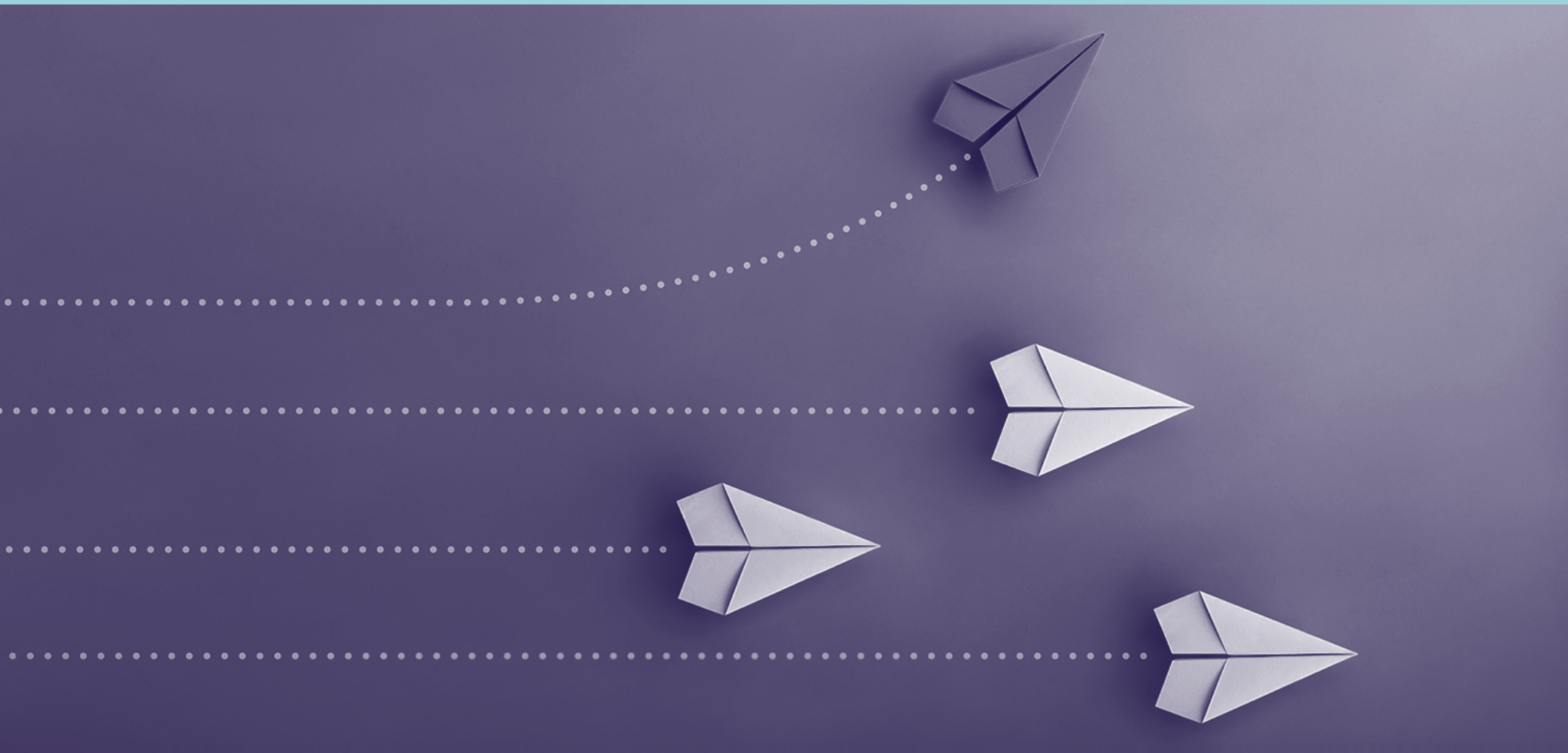
And, while the data findings indicated increased executive scrutiny and support in resilience management initiatives, it's important to note which executives care most about an organization's resiliency capabilities. Our BCM Trends data assessment (collected between 2009 to 2020) has indicated a shift away from Information Technology (27% to 16%) in favor of placing the program within Risk Management (11% to 22%). The data from our Evolving Resiliency Strategies Study also reported the Chief Information Security Officer (CISO) being the most engaged (80%) in resiliency planning, followed by the Chief Risk Officer (CRO) – 77%, and the Chief Security Officer (CSO) – 75%. The executives who were the least engaged included the Chief Administrative Officer (CAO) – 42%, Chief Financial Officer (CFO) – 53%, and the Chief Compliance Officer (CCO) – 55%. The findings also highlighted that the CRO (45%), CIO/CTO – Chief Information/Technology Officer (44%), and CISO (41%) are most likely to sit on a resiliency program governance committee, while the CMO/CCO – Chief Marketing/Communications Officer, CAO, and CHRO – Chief Human Resources Officer were less likely to be involved in the program's governance committee (13%, 15%, 28% respectively). We would expect the CHRO to become more involved in the future, though, especially when considering the severe impacts, the COVID pandemic and The Great Resignation has had on the workforce.

Since 2001, we have been fortunate to have received more than 25,000 responses from more than 50 countries that have supported over 45 industry leading surveys. Each of these reports created new insights and allowed for new trends to be identified in program maturity, compensation, and professional career growth while supporting the larger resiliency profession. We hope you find this report valuable in assessing your own program's resiliency strategies and that you utilize many of the resources that are imbedded within this report. And as always, we're here to help you in achieving the right level of resiliency.  Please do not hesitate to contact us with any questions you might have.

**Cheyene Marling, Hon MBCI**
**Managing Director,**
BC Management

cmarling@bcmanagement.com

# Program Resiliency Strategies



## How has the Strength of Your Resilience Management Program Changed Over the Past 12 Months?

| | Doesn't apply | Not sure | Decreased | Remain the same | Increased |
|---|---|---|---|---|---|
| Executive engagement | 3% | 4% | 6% | 22% | **65%** |
| Program integration w/ other risk disciplines | 4% | 4% | 2% | 38% | **51%** |
| Cyber response | 4% | 5% | 0% | 27% | **64%** |
| Third-party resilience management | 8% | 7% | 1% | **42%** | **42%** |
| Supply chain resiliency | 15% | 6% | 1% | **39%** | **38%** |
| Program governance | 2% | 3% | 5% | **47%** | **43%** |
| Program metrics - ability to resonate and drive continual improvements | 6% | 5% | 5% | **44%** | **40%** |
| Program automation | 13% | 2% | 2% | **54%** | 29% |

## How Have Your Executives Shown an Interest in Elevating Your Program's Maturity in the Last Year?

### TOP CATEGORIES FOR OPEN RESPONSES

**23%** **Increased executive/board updates & participation**

**21%** **Increased financial support of the program** (majority in increased staffing (74%) followed by software/ automation or technology (32%))

**12%** **Attention to program strategic recommendations**

**10%** **Increased exercises**

**10%** **Increased awareness/training and driving employee** involvement from executive level

Exceeds 100% due to multiple increased financial support.

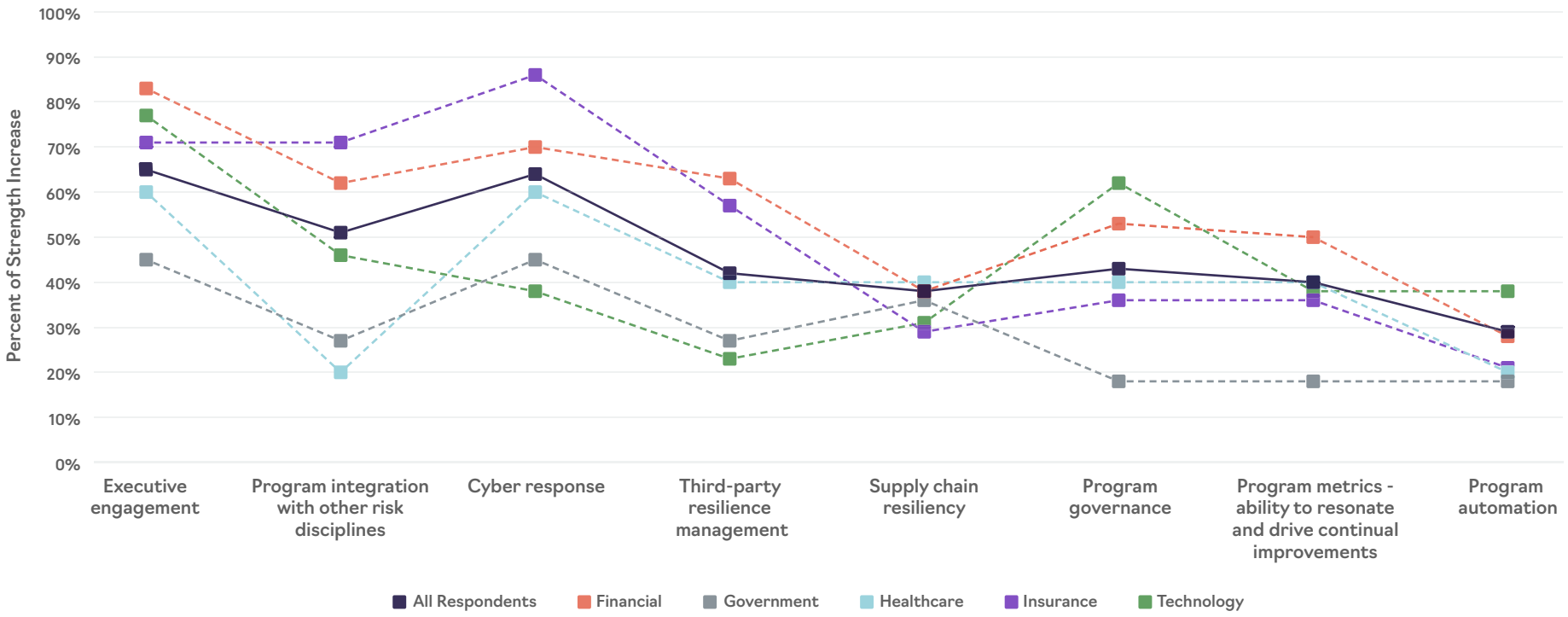
> Because of COVID their awareness has increased along with their support. We are focusing on Cyber and Ransomware due an increase in occurrences in the news.

> By providing governance/oversight for the program, asking questions, and listening to presentations and metrics discussions.

> Cyber response initiatives have increased drastically. Each executive has teams involved in creating business sustainment plans.

## How has the Resilience Management Program Increased in Strength in the Past 12 Months by Industry?

(Data Highlighted by Top Industries Based on Study Participation)




## INSIGHTS

- Our data shows that **executive engagement** and **cyber response** have surged this year (65% and 64%, respectively, of all respondents noted an increase), followed by program integration with other risk disciplines (51% all respondents). Technology organizations indicated the greatest increase in program automation (38%) while also maintaining the level of their cyber response (46% remain the same).
- Supply chain resiliency was almost evenly split between an increase in program strength and remaining the same (30-40% depending on the industry). Financial and insurance industries showed increased scrutiny over **third-party resilience management** (63% and 57%, respectively) while government entities have been less concerned with program governance or metrics in comparison to the other industries (noting only an 18% in increased program strength for both).

## How are the Investment Strategies in Your Program Evolving Over the Next 12 Months?

| | Doesn't apply | Not sure | Decreased | Remain the same | Increased |
|---|---|---|---|---|---|
| Full-time, permanent staff | 4% | 2% | 6% | **61%** | 27% |
| Emergency notification system | 5% | 2% | 1% | **68%** | 24% |
| Software automation | 10% | 4% | 1% | **53%** | 32% |
| Situational awareness and threat intelligence | 4% | 4% | 1% | 41% | **51%** |
| Technology to improve resilience/ recoverability | 3% | 5% | 1% | 39% | **53%** |
| Consulting - business focused | 19% | 4% | 4% | **50%** | 24% |
| Consulting - IT focused | 19% | 4% | 4% | **46%** | 27% |

## INSIGHTS

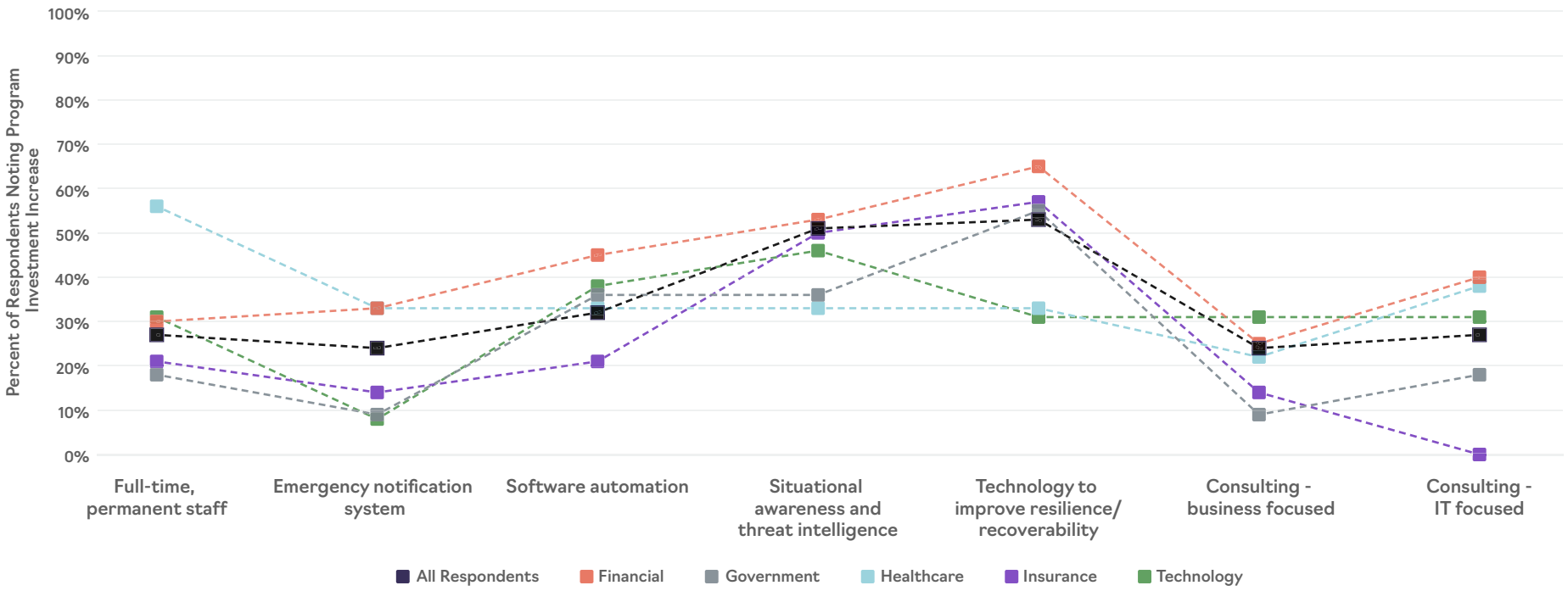
- Many organizations are continuing to keep their program investment strategies in line with 2021, with the exception of increasing **situational awareness and threat intelligence** along with **technology resilience/recoverability.** The data also showed that those organizations with immature programs were planning on investing more in their resilience management program in 2022.

### INVESTMENT STRATEGIES

Companies with **immature programs are increasing investment** in the following resilience management strategies in 2022:

1. **Situational awareness**: 53%
2. **Business consulting:** 40%
3. **Software automation:** 40%
4. **Full-time, permanent staff:** 38%
5. **IT consulting:** 38%
6. **Emergency notification system:** 35%

## How are the Investment Strategies in the Resilience Management Program Evolving Over the Next 12 Months by Industry? (Data Highlighted by Top Industries Based on Study Participation)

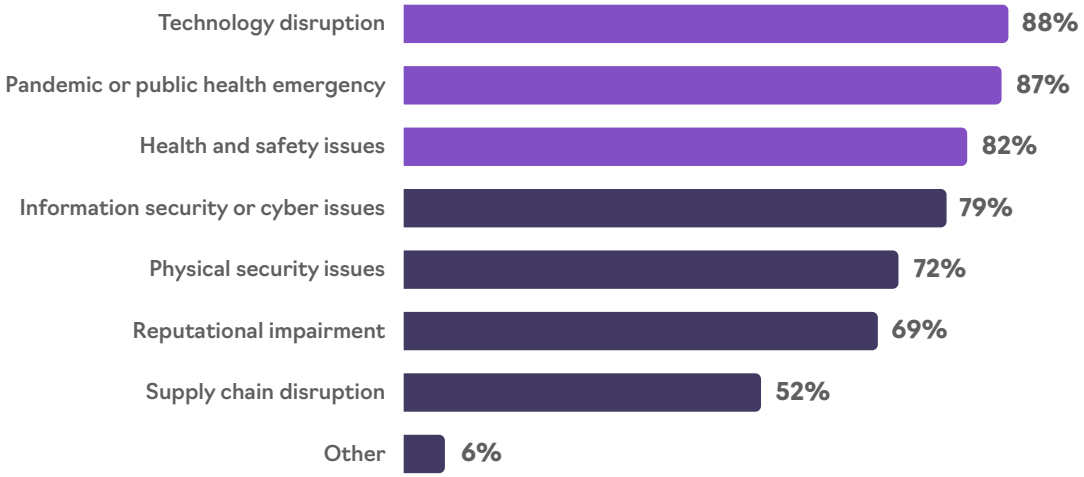



### INSIGHTS

- Although a majority of the respondents indicated significant program investments in both situational awareness/threat intelligence and technology resilience/recoverability, financial and insurance organizations led the pack. **60% of healthcare organizations plan to hire resiliency personnel** while the other industries are falling in line with the hiring trends over the last 2 years, which is between 20-30% increase in staffing.
- Financial, technology, government, and healthcare organizations are driven to increase **software automation** compared to all the respondents as a whole. Lastly, the data is showing a preference to investing in **IT consulting** versus business consulting, which aligns to the surge in situational awareness/threat intelligence and technology resilience/ recoverability.

## Which of these Crisis or Disruption-Related Issues does Your Program Address?

(Exceeds 100% due to Multiple Selections)




## INSIGHTS

- The data highlighted that the resilience management program is less likely to address **supply chain (52%)** and **reputational impairment (69%)** disruption-related issues. When assessing a cross section of the data by program maturity we discovered that only 38% and 45% of organizations with immature programs addressed these disruption-related issues, respectively within their program. Those organizations with mature resilience management programs were well ahead noting 64% and 81%, respectively, addressing these crises in the program.

## PLANNING RESOURCES

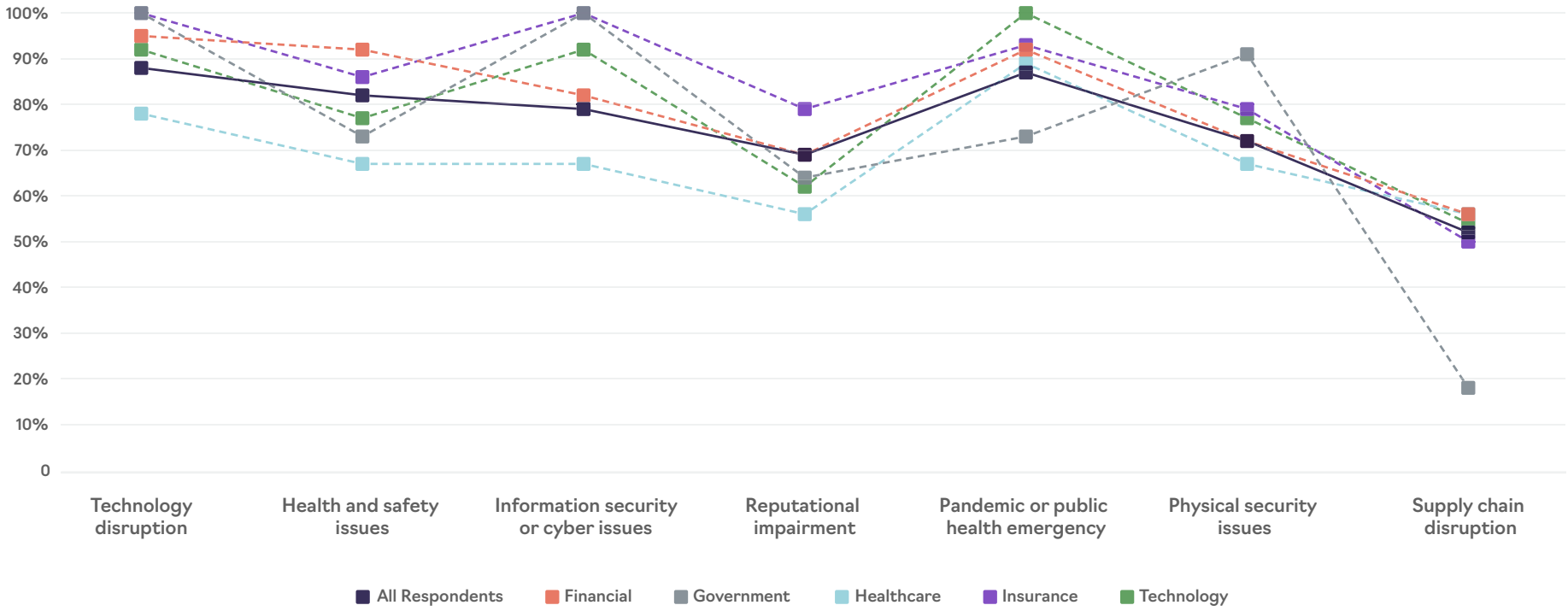
### Need help defining your plausible scenarios?

Castellan offers a **Plausible Scenario Builder** to help you define plausible scenarios and prepare to activate them for stress testing, as well as clarify the connection between operational resilience and business continuity.

GET THE GUIDE

## Crisis or Disruption-Related Issues Addressed in the Program by Industry

(Data Highlighted by Top Industries Based on Study Participation)




### INSIGHTS

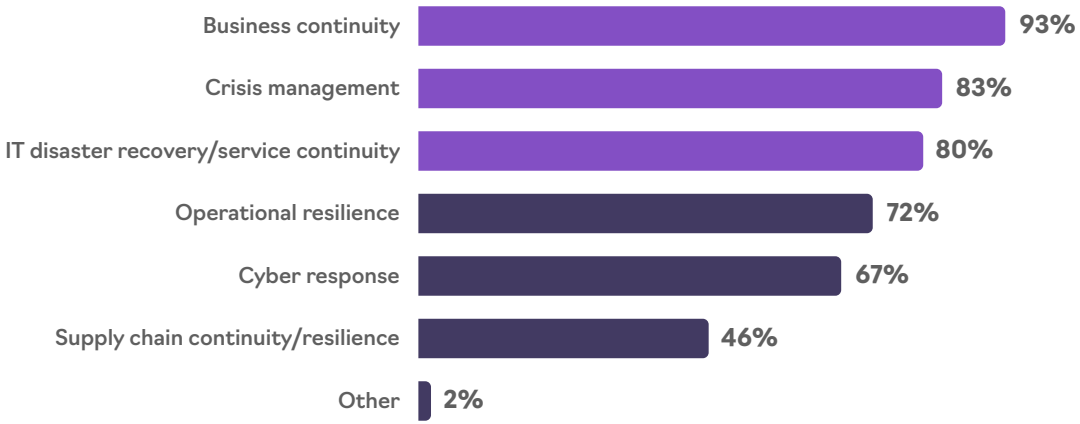
→ Additionally, when assessing this data point by industry we discovered that government entities were less likely to address supply chain disruptions with only 18% addressing this potential issue in their program. **Insurance organizations were more likely to address reputational impairment (79%).**

### PRO TIP

**Establish "impact tolerance"** that identifies how the inability of performing your key business services will impact your customers, your partners, the marketplace, or your company's viability. Each issue can be considered a "plausible scenario" for you to address when building the resilience management program. Input should be provided by various departments, including customer-facing areas, product development, marketing and communications.

## Which of the Following Topics are Addressed by Your Program?

(Exceeds 100% due to Multiple Selections)




> Over the last two years (since the start of the pandemic), we have seen some significant supply chain issues, which has resulted in organizations reconsidering how they handle business continuity planning for supply chain. Oftentimes, there may be business decisions that outweigh business continuity risk when it comes to supply chain (specifically, the decision to work with single- or sole source providers). However, due to the issues resulting from the pandemic, many organizations are starting to incorporate business continuity planning into their supply chain decisions. We are seeing more supplier business continuity program assessments and less single- or sole-sourced vendors. Supply chain is one area that has traditionally operated independently of business continuity. However, I believe this will become more integrated into business continuity programs as a result of the last two years.
>
> — Ashley Helmick (Advisory Board)

## INSIGHTS

- Cyber response and supply chain resiliency were less likely to be addressed in the resilience management program. While these topics might be positioned elsewhere within the organization, it is important to break down the silos for enterprise operational resiliency.
- When assessing a cross section of the data by program maturity we discovered that there was a differentiating factor between immature and mature resiliency programs. **Organizations with mature programs were more likely to include operational resilience (81%) and supply chain resilience (59%)** compared to those with immature programs (65% and 38%, respectively).

## CYBER RESOURCES

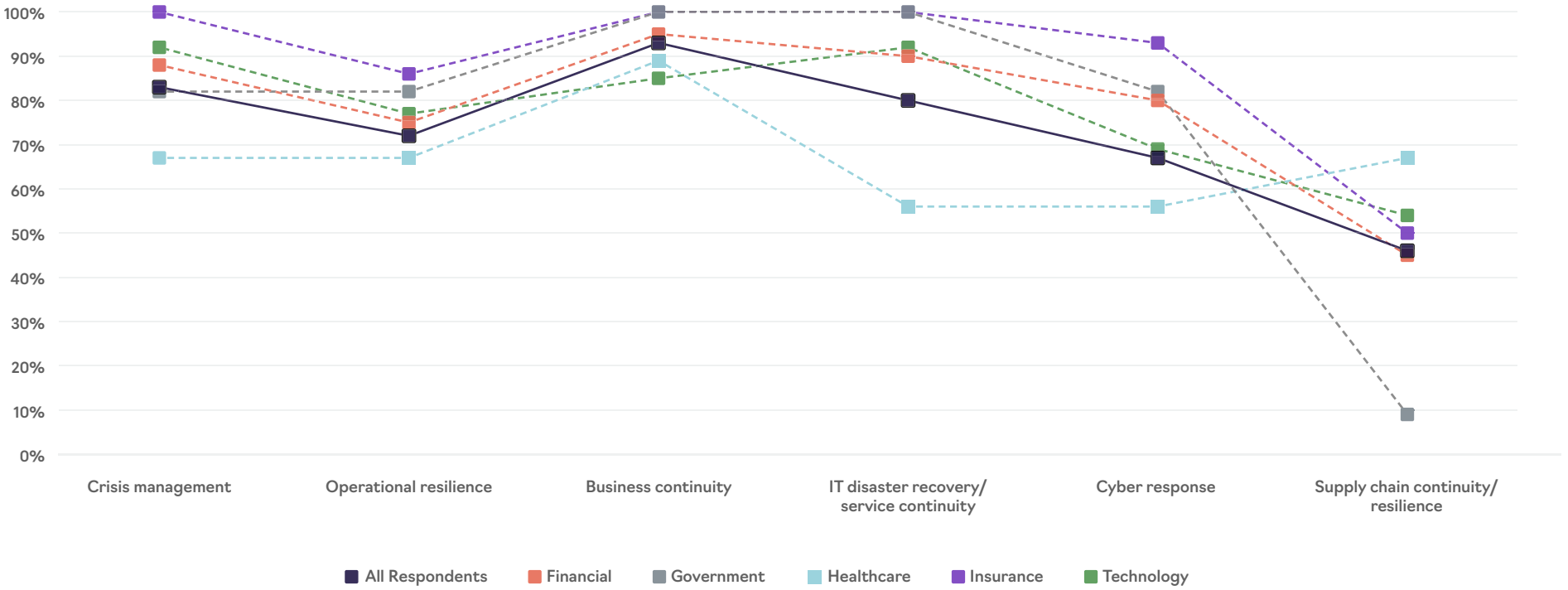
### Need assistance building your cyber resilience capability?

Castellan has developed a **Cyber Response Builder** that will help you proactively build your cyber resilience capabilities to anticipate, respond to, and recover from cyber attacks.

GET THE GUIDE

## Topics Addressed in the Resilience Management Program by Industry

(Data Highlighted by Top Industries Based on Study Participation)




### INSIGHTS

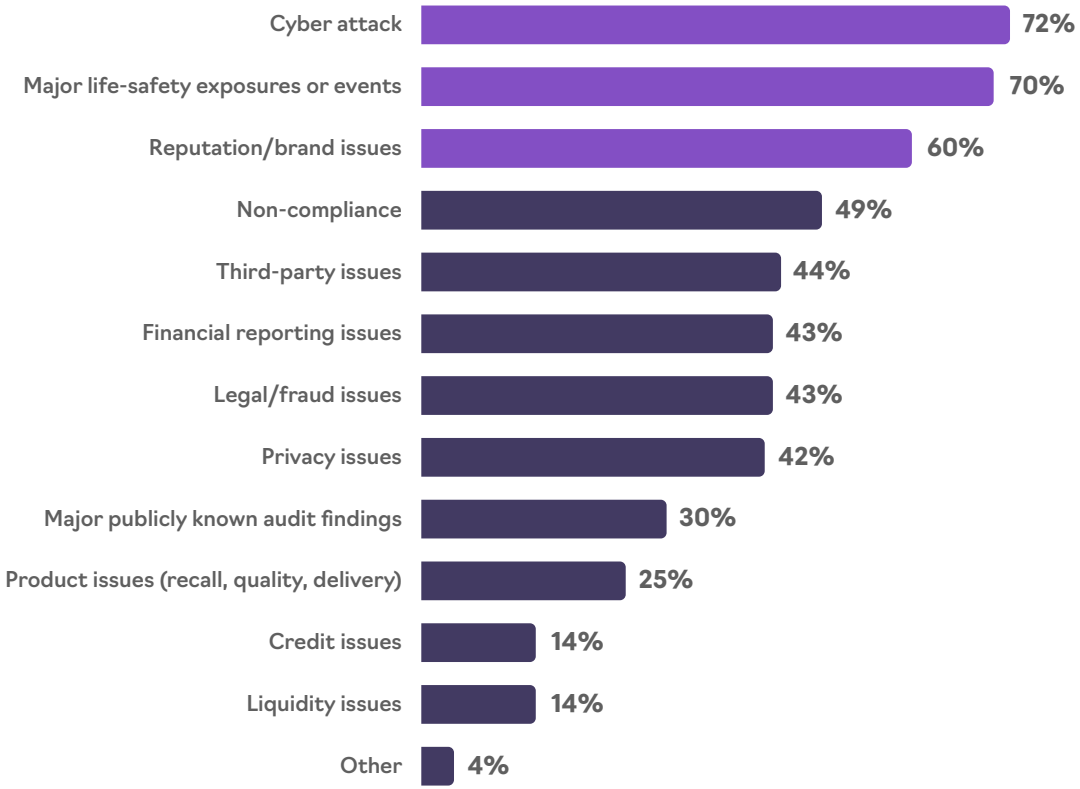
→ Additionally, when reviewing topics addressed in the resilience management program by industry, we discovered that insurance organizations were more likely to address all topics within the program while healthcare entities were less likely.

### PRO TIP

**Integration and alignment are key.** In the past, many of these topics were addressed separately ("siloed" approach). Many BC/DR plans did not address cyber response, and visa-versa. One key lesson learned from response measures taken by organizations early in COVID 19, is the dependency on suppliers, vendors and third party service providers. Moreover, it became clear over the past two-years, that building an effective resilience management program requires integration/alignment of all areas.

## Which of these Issues, when the Impact Exceeds Day-to-Day Management Control, does Your Program Address?

(Exceeds 100% due to Multiple Selections)



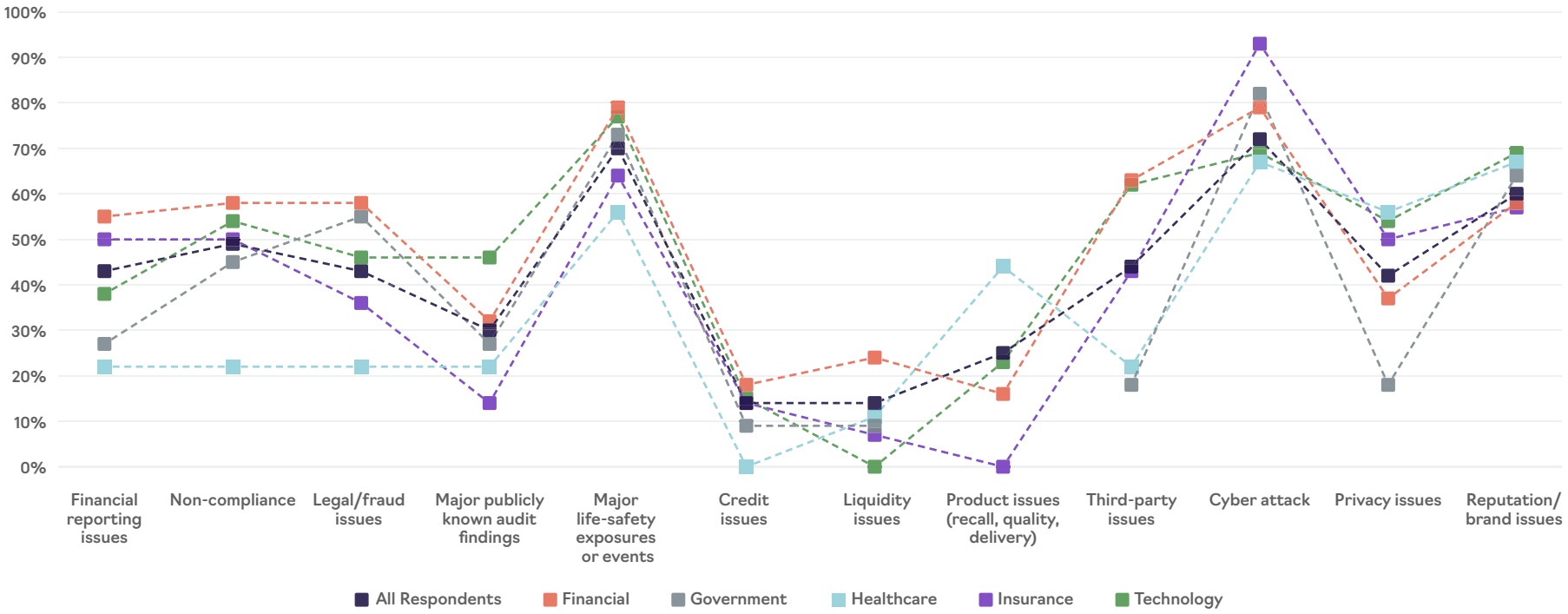

### INSIGHTS

→ **Cyber attacks, major life-safety exposures, and reputation/brand issues seem to be the most common crises addressed when day-to-day management exceeds control.** The data; however, highlighted several opportunities for program improvement, especially in credit and liquidity issues.

> In many organizations, Organizational Resilience programs have evolved from robust business continuity programs that traditionally considered disaster scenarios related to major life-safety exposures and natural events (weather related, earthquake, etc.). The COVID-19 pandemic encouraged the areas of enterprise risk management and business continuity to work together with the Human Resources areas at a more strategic level. The growing threat of cyber-attacks represents a new opportunity for organizational resilience professionals to integrate the areas of information technology and thus strengthen their programs.
>
> — Ing. Jorge Escalera (Advisory Board)

## Issues Addressed when Impact Exceeds Day-to-Day Management Control by Industry

(Data Highlighted by Top Industries Based on Study Participation)



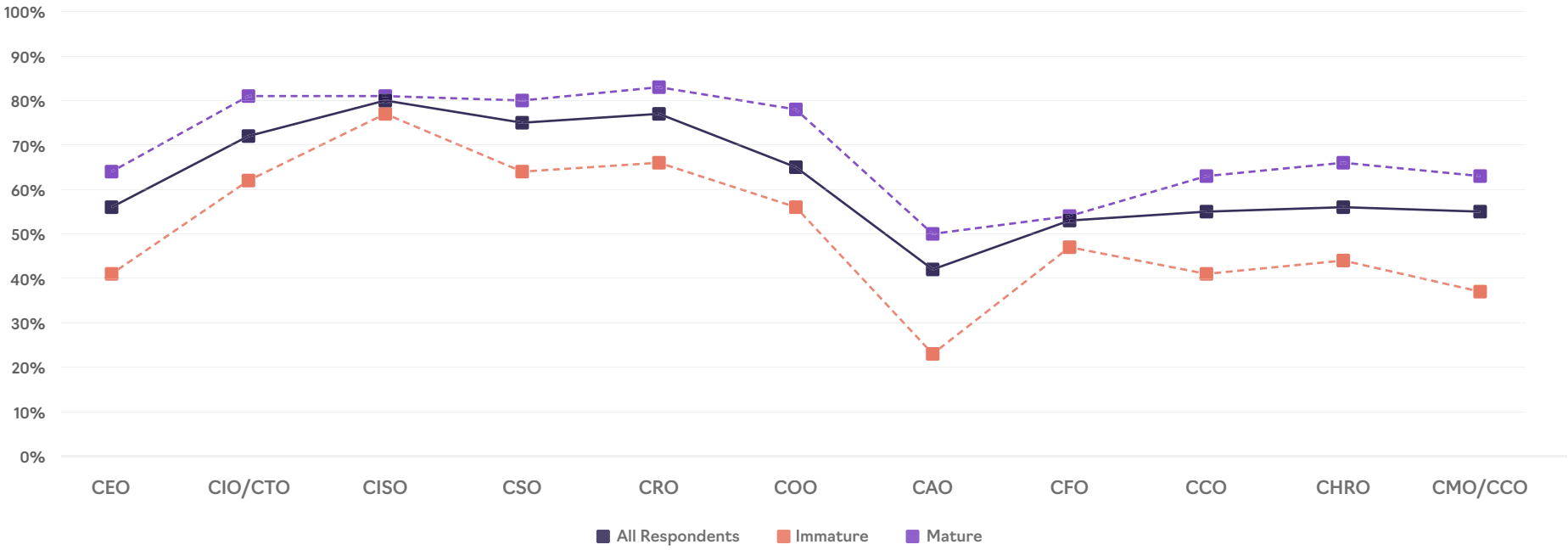

### PRO TIP

**Learn how your program compares to your peers.** Confidentially participate in our study to receive a Resilience Management dashboard, which is a dynamic peer data assessment customized by industry or organizational revenues.

PARTICIPATE IN OUR STUDY

## Which Executives Care Most about Your Program by Program Maturity (Self-Rating)?

Rating from 1 to 5 with 1 meaning "Very Little Engagement" and 5 meaning "Very Engaged".




### INSIGHTS

- Executive engagement drives program maturity; therefore, it shouldn't be surprising that organizations with more mature programs indicate higher executive engagement.
- Our trending data (collected 2009-2020) highlights that the program has shifted away from Information Technology (27%-16%) to Risk Management (11%-22%).

### WHICH EXECUTIVES CARE MOST ABOUT THE PROGRAM?

Percent of all respondents noting "very engaged" or "engaged".

1. **Chief Information Security Officer (CISO):** 80%
2. **Chief Risk Officer (CRO):** 77%
3. **Chief Security Officer (CSO):** 75%
4. **Chief Information/ Technology Officer (CIO/CTO):** 72%

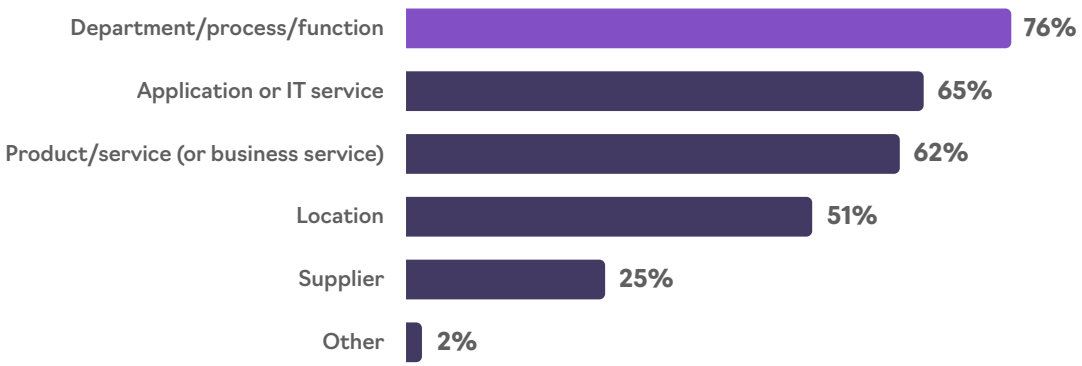
### WHICH EXECUTIVES CARE LEAST ABOUT THE PROGRAM?

Percent of all respondents noting "very engaged" or "engaged".

1. **Chief Compliance Officer (CCO):** 55%
2. **Chief Marketing/ Communications Officer (CMO/CCO):** 55%
3. **Chief Financial Officer (CFO):** 53%
4. **Chief Administrative Officer (CAO):** 42%

## How have You Prioritized/Scoped Your Program?

(Exceeds 100% due to Multiple Selections)




> The industry has recently seen a shift in how programs are scoped and plans are formulated - where even 5 years ago the majority of plans were location-based but covering multiple functions within that location. Today, due to factors such as remote working, more distributed workforce strategies and a change in planning philosophy it is far more common to base planning initiatives on processes or functions that may be distributed throughout the world. This transformation not only allows for a more targeted resiliency plan based on a more linear approach to a product, process or output but it also builds in inherent resiliency where before the loss of a single location would result in the complete loss of a process.
>
> — Kevin Cunningham (Advisory Board)


## RESILIENCE RESOURCES

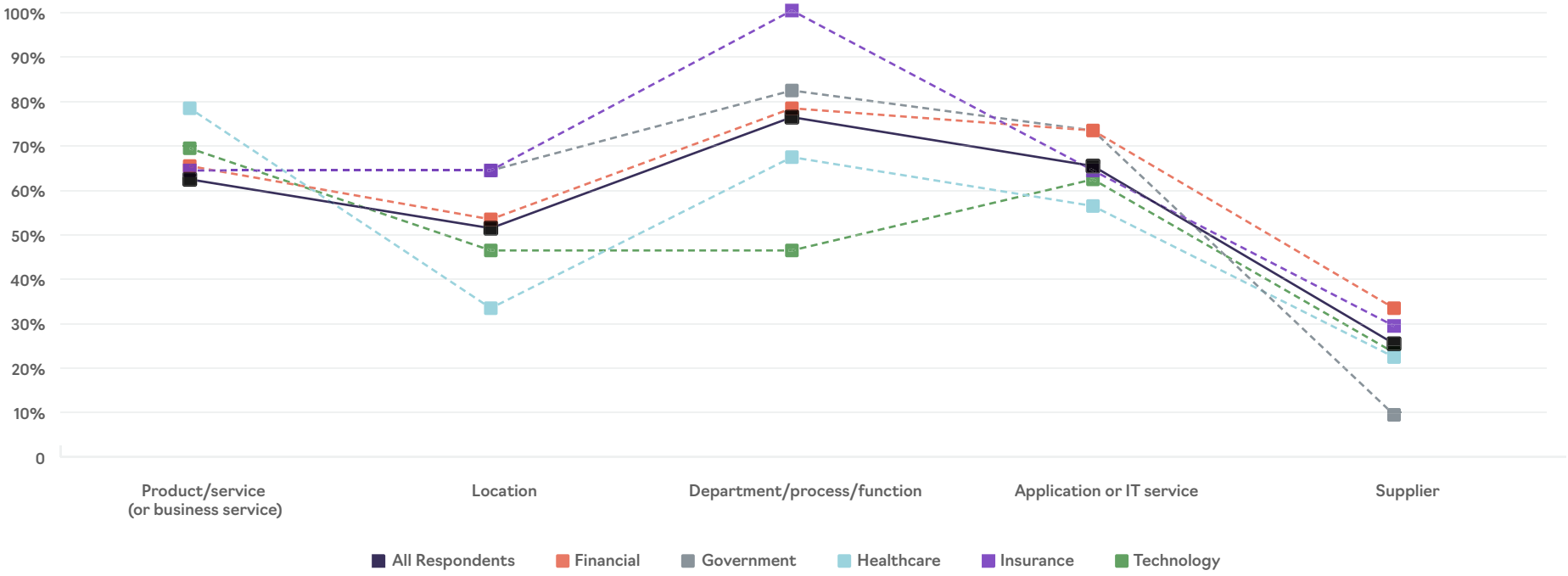
### Not sure how to get started with operational resilience?

Castellan's **Getting Started with Operational Resilience** guide will give you clarity on where to begin and help increase engagement with executive leadership through the five-step framework.

GET THE GUIDE

## How is the Resilience Management Program Prioritized/Scoped by Industry

(Data Highlighted by Top Industries Based on Study Participation)




### INSIGHTS

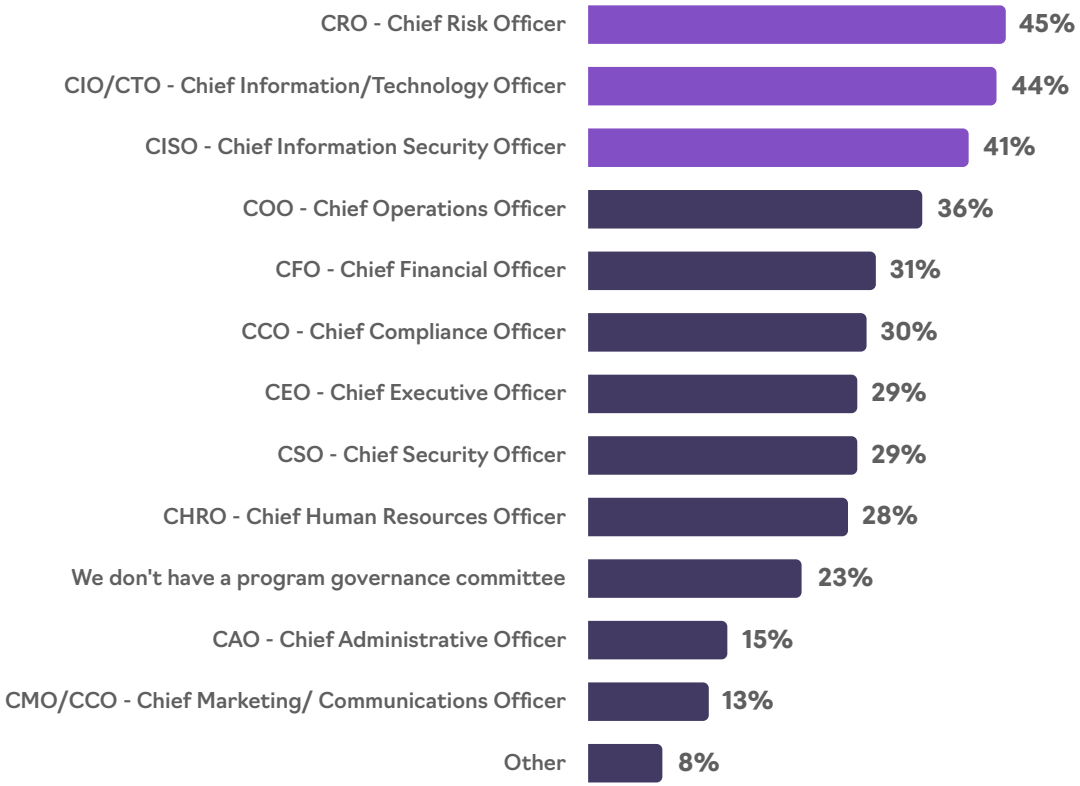
- Most organizations prioritize their resilience management program based on **departments/processes/functions** (76%); however, when we assess this data point by industry, we discovered a large variance within the findings. Organizations in the insurance industry noted 100%, while technology firms indicated only 46%.

### PRO TIP

**Prioritize with a "Frame discussion".** The process to prioritize your resilience management program has a number of considerations, as demonstrated in the chart. The type of industry will dictate which factors are considered most critical to scope your program. Soliciting input from senior leadership is a good start. Castellan recommends facilitating a "frame" discussion among the SLT and key stakeholders to establish the foundation for resiliency.

## Who Sits on Your Program's Governance Committee?

(Exceeds 100% due to Multiple Selections)




### Need Help Increasing Executive Engagement?

**Castellan's Executive Support Amplifier** gives you a five step framework for building (and keeping!) executive support for your business continuity program.

GET THE GUIDE

## INSIGHTS

- 23% of all respondents and 31% of organizations with immature programs don't have a program governance committee in place, while organizations with mature programs are more likely to have several different executives involved in the governance committee **(Chief Information/ Technology Officer (57%), Chief Risk Officer (57%), Chief Information Security Officer (50%), and Chief Security Officer (45%).**

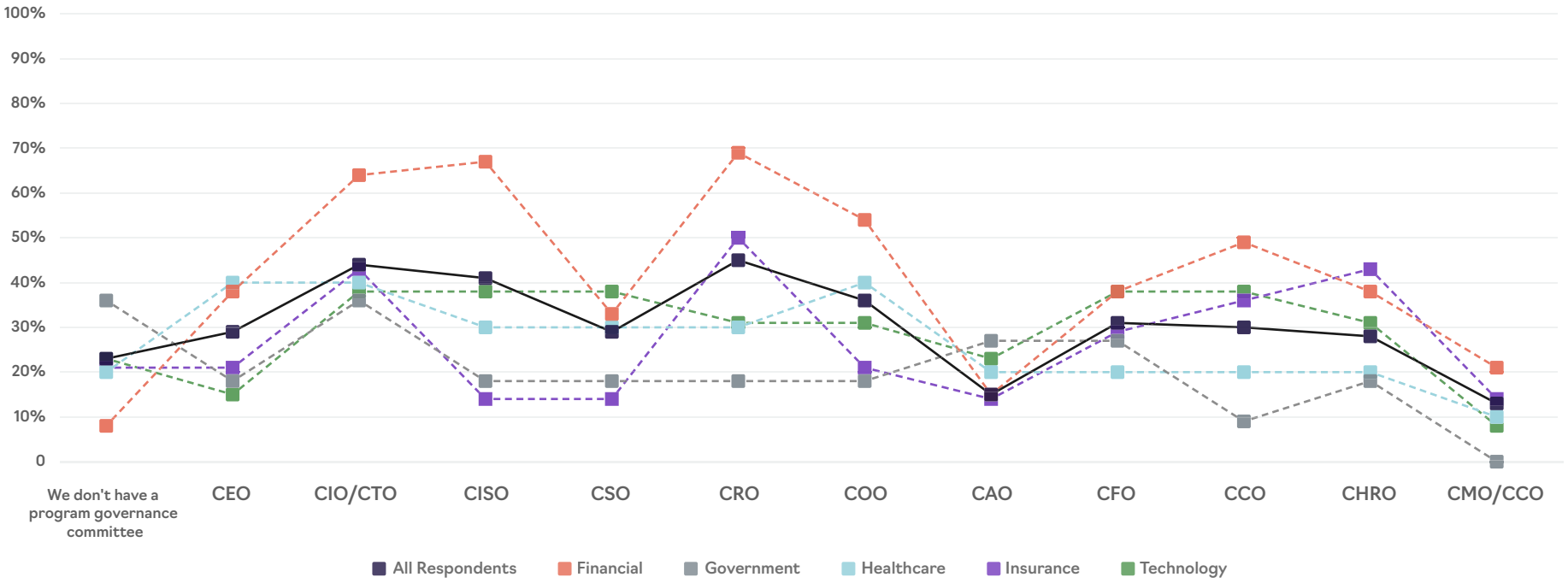
> Across Europe, United Kingdom and Ireland, Operational Resilience regulations in the finance sector have been published recently, with the aim of making company boards responsible for Operational Resilience. This too has had a positive impact on the increased level of senior leadership engagement.
>
> — Nicola Lawrence (Advisory Board)

**Regulators/Regulations:**

- European: DORA (Digital Operational Resilience Act)
- UK: Regulations published jointly by the Bank of England, Financial Conduct Authority (FCA), and the Prudential Regulation Authority (PRA)
- Ireland: Central Bank of Ireland

## Executives Included in the Program's Governance Committee by Industry

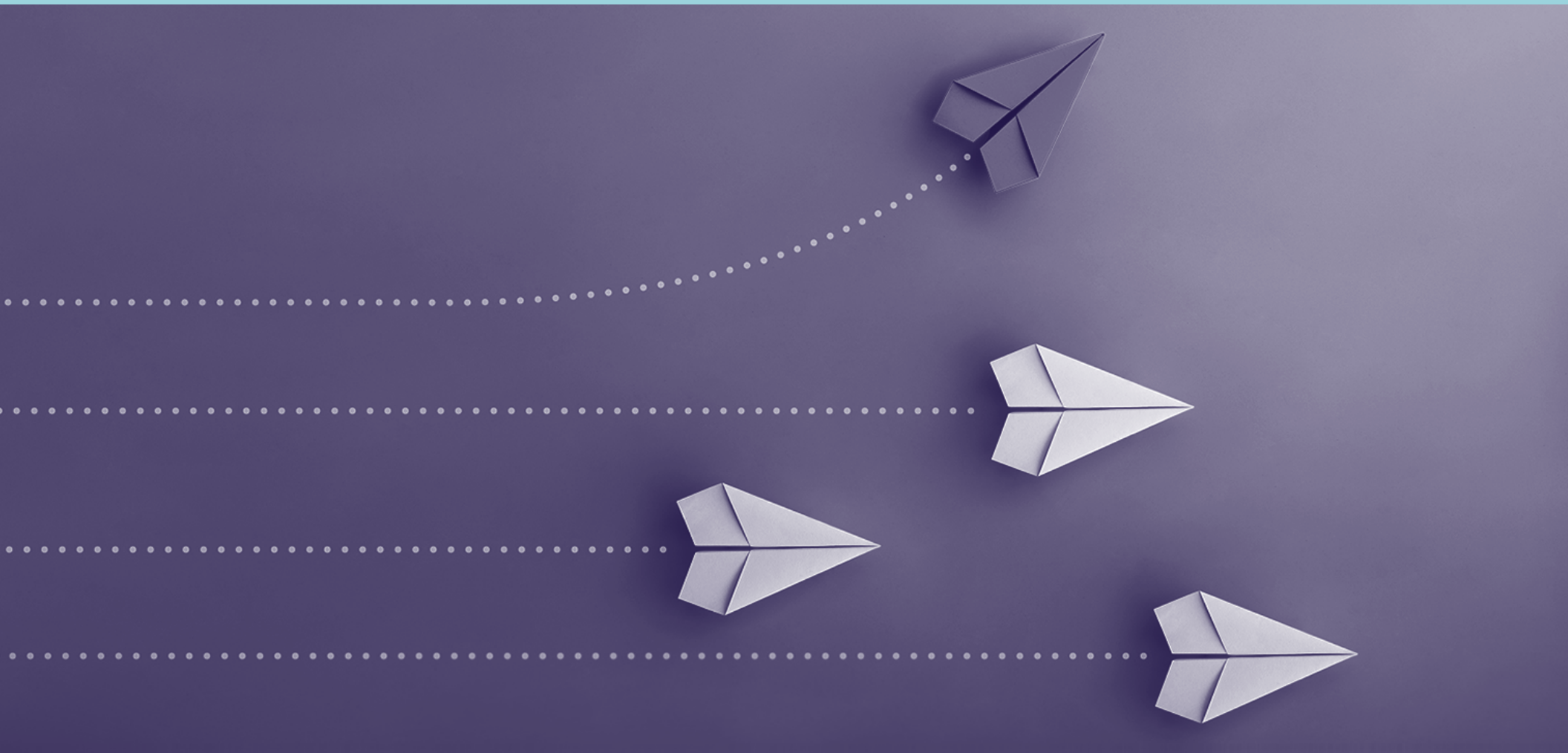
(Data Highlighted by Top Industries Based on Study Participation)



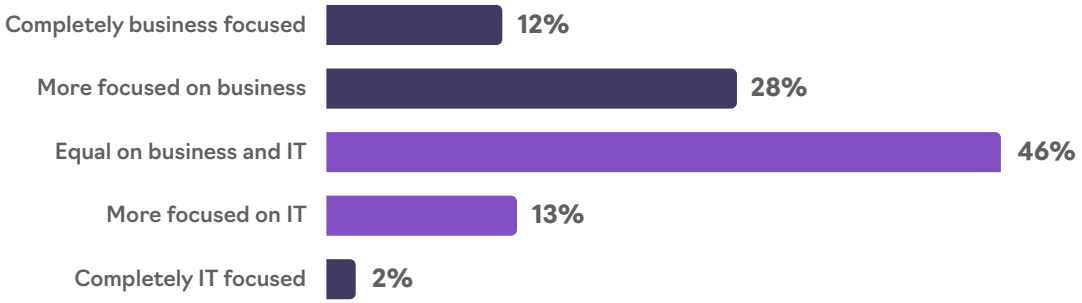

## INSIGHTS

- **Financial and insurance** organizations are more likely to include the Chief Risk Officer, 69% and 50%, respectively.
- 36% of **government** entities include the Chief Information/Technology Officer, while another 36% indicated that they do not have a governance committee.
- **Healthcare** organizations noted 40% each for Chief Executive Officer, Chief Information/Technology Officer, and Chief Operations Officer.
- **Technology** firms noted 38% each for Chief Information/Technology Officer, Chief Information Security Officer, Chief Security Officer, Chief Financial Officer, and Chief Compliance Officer.

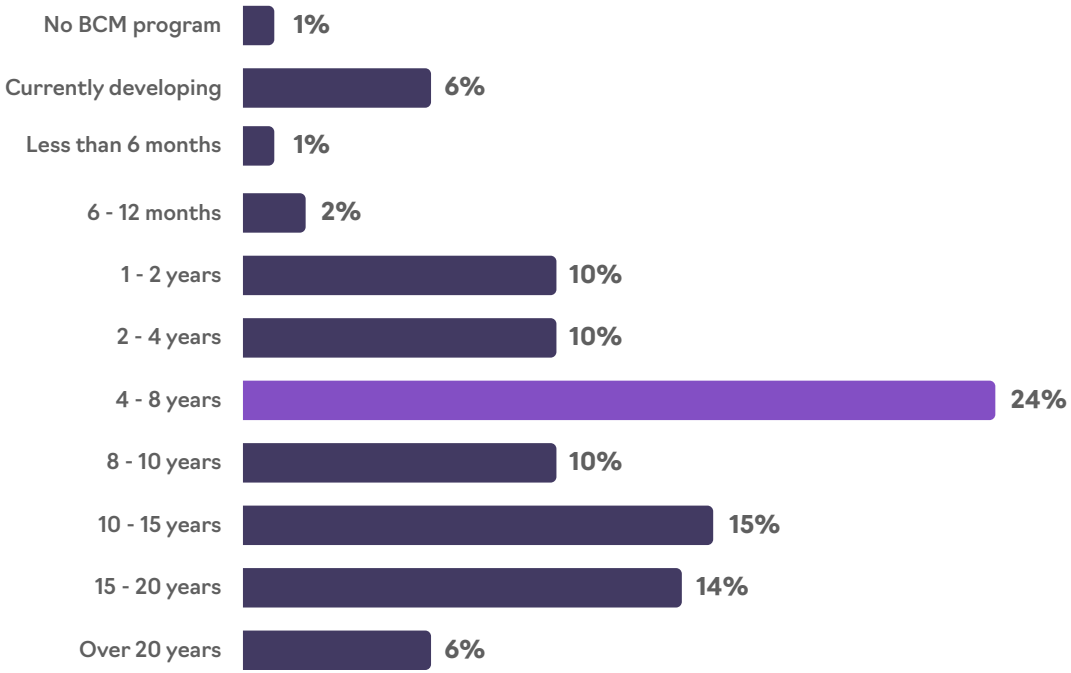
# Program Characteristics



## Program Definition (Manage or Work Within)




## Length of Program Existence (With or Without Your Involvement)




## DATA HIGHLIGHTS

### PROGRAM DEFINITION

**25%** of organizations with **immature programs** noted that their program was **completely or more focused on IT planning initiatives** while 12% of those organizations with mature programs noted the same.

**31%** of technology firms also indicated that their programs were **completely or more focused on IT planning initiatives.**

### LENGTH OF PROGRAM EXISTENCE

**28%** of organizations who noted an immature resilience management program indicated that their program is either **currently being developed or it was developed within the last year.**

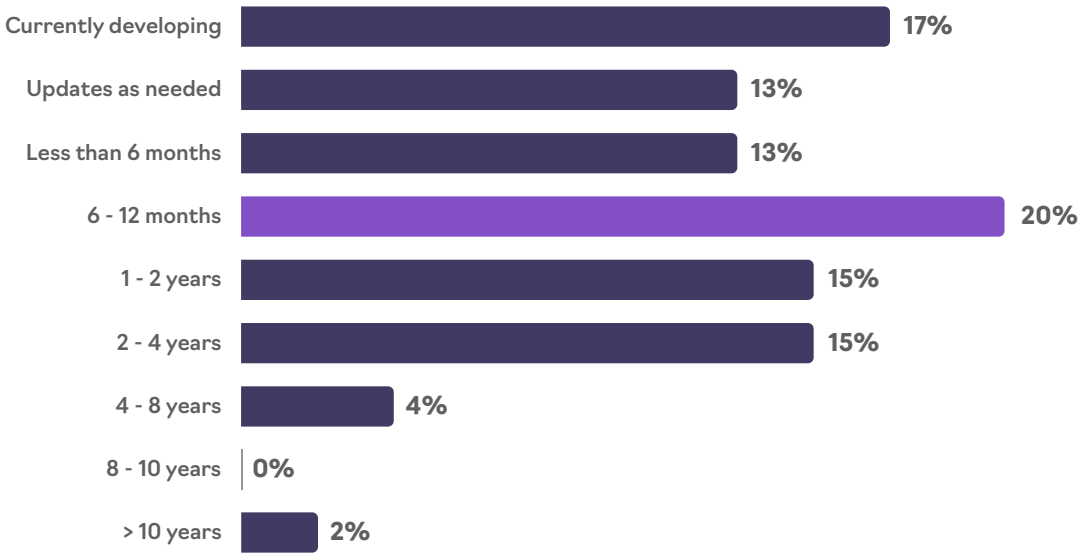
**52%** of organizations with mature programs noted that their **resilience management program was developed over 10 years ago.**

**Organizations with higher annual gross revenues also indicated more longevity with their program.**

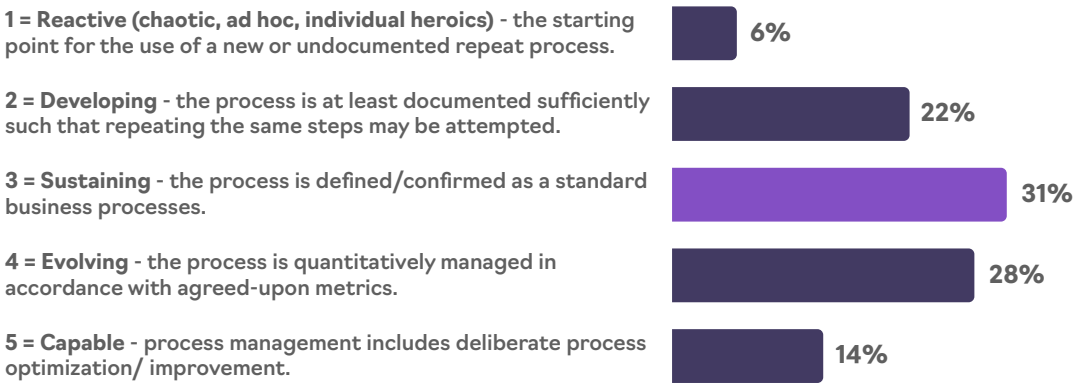
**10%** of organizations with less than $50M USD in annual gross revenues noted a program existence of 10+ years.

**60%** of organizations with $10B+ USD revenues developed their program 10+ years ago.

## Last End-to-End Program Review and/or Refresh




## Program Maturity – Self Rating




## DATA HIGHLIGHTS

### PROGRAM REVIEW/REFRESH

**40%** of organizations with immature programs are currently developing the program.

**45%** of organizations with mature programs have conducted an end-to-end review or refresh of their program in the last year.

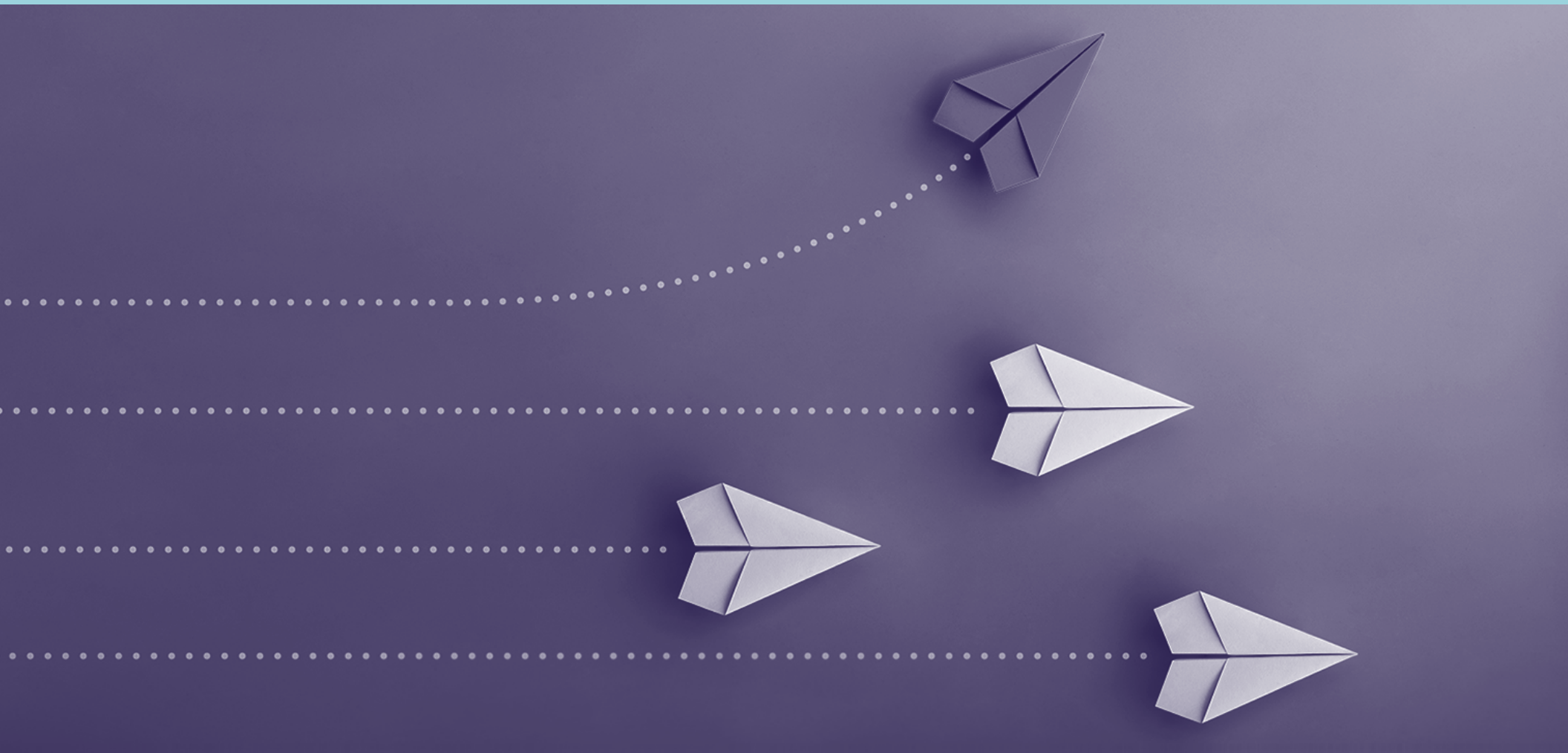
### PROGRAMS REVIEW/REFRESH IN LAST 12 MONTHS BY INDUSTRY:

1. **Healthcare:** 60%
2. **Technology:** 54%
3. **Financial:** 38%
4. **Insurance:** 14%
5. **Government:** 9%

### PROGRAM MATURITY (SELF-RATING) OF "EVOLVING" OR "CAPABLE" BY INDUSTRY:

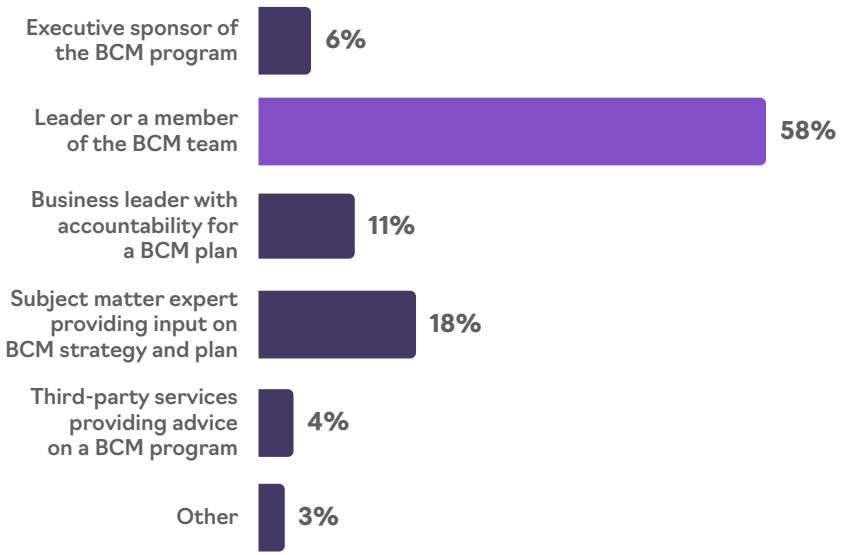
1. **Financial:** 60%
2. **Insurance:** 43%
3. **Healthcare:** 40%
4. **Technology:** 31%
5. **Government:** 27%

# Demographics



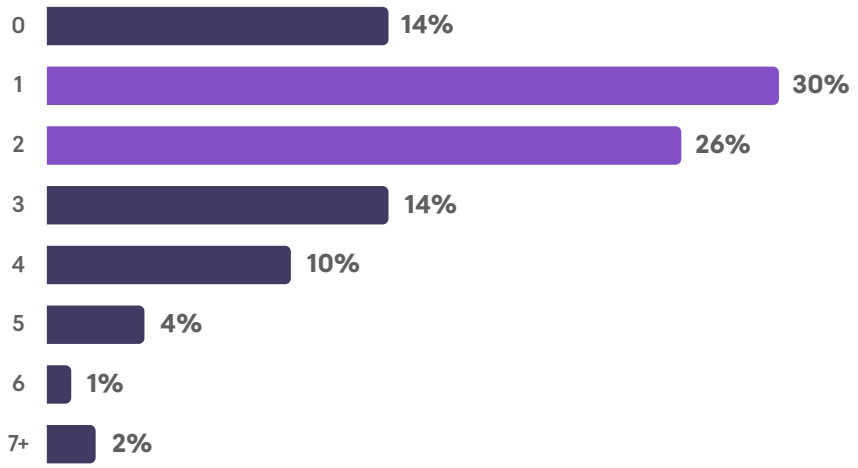
# Percent of Survey Respondents

## Respondents Level of Responsibility

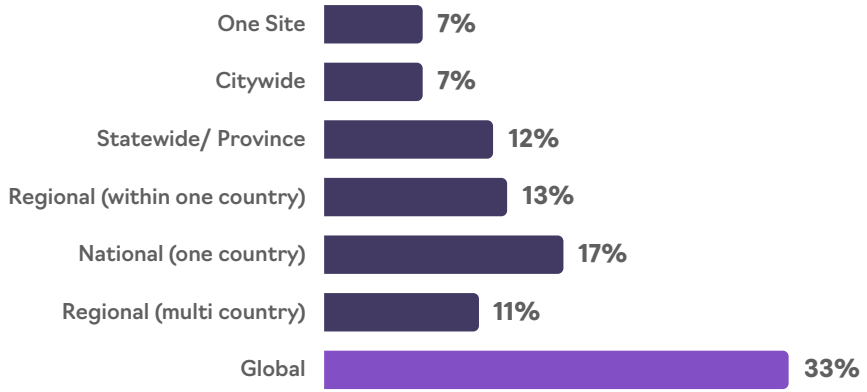



## Level of Separation from Executive Management

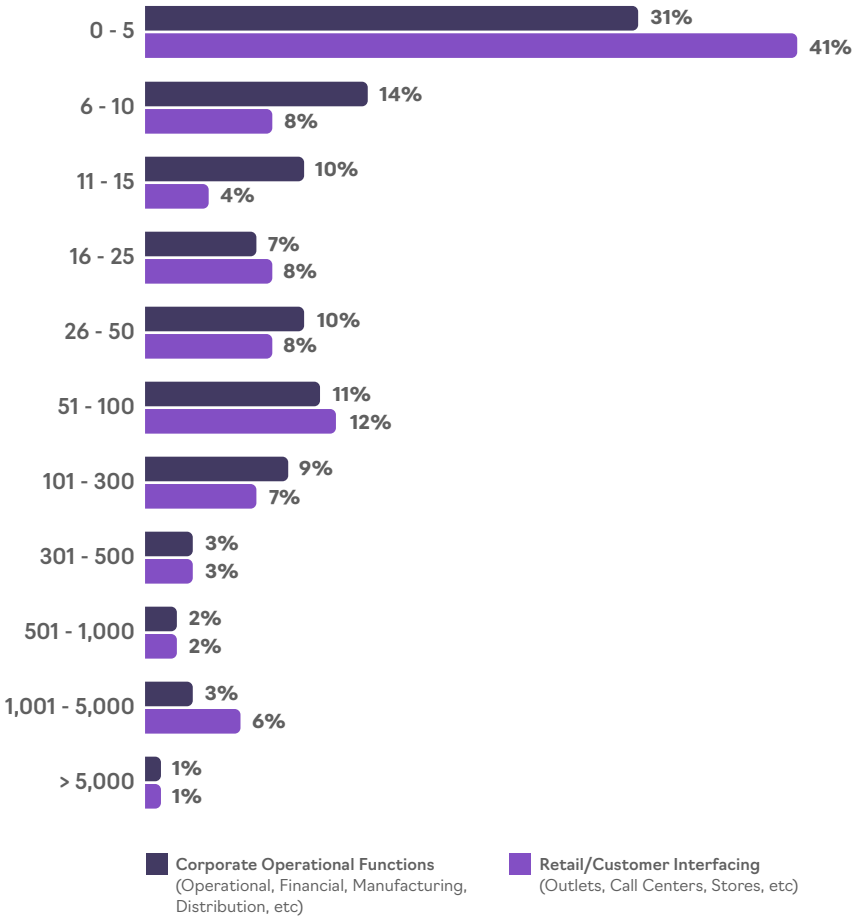
(Number of People between You & Executive Team)



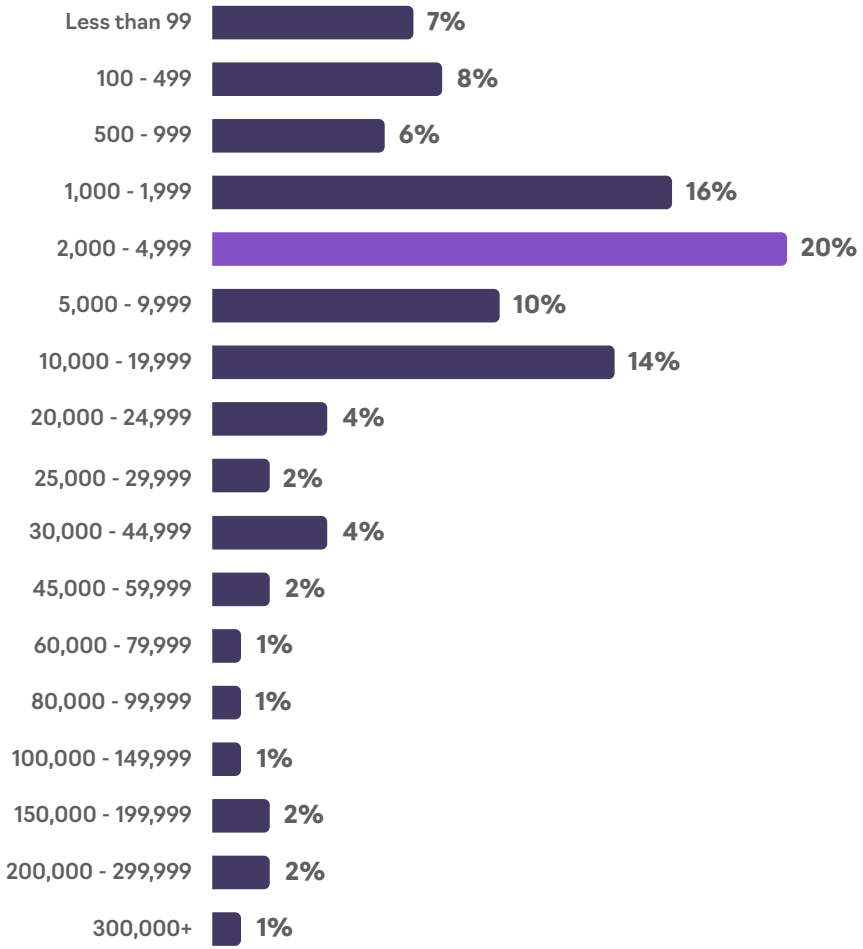

## Percent of Respondents by Organizational Distribution



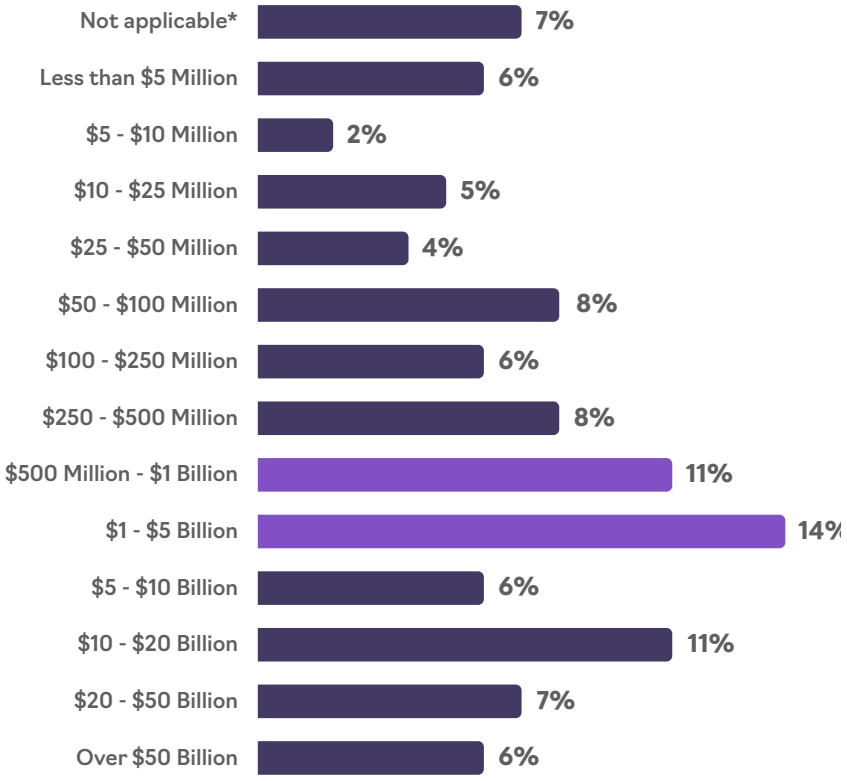
## Percent of Respondents by Number of Organizational Locations




## Percent of Respondents by Number of Employees



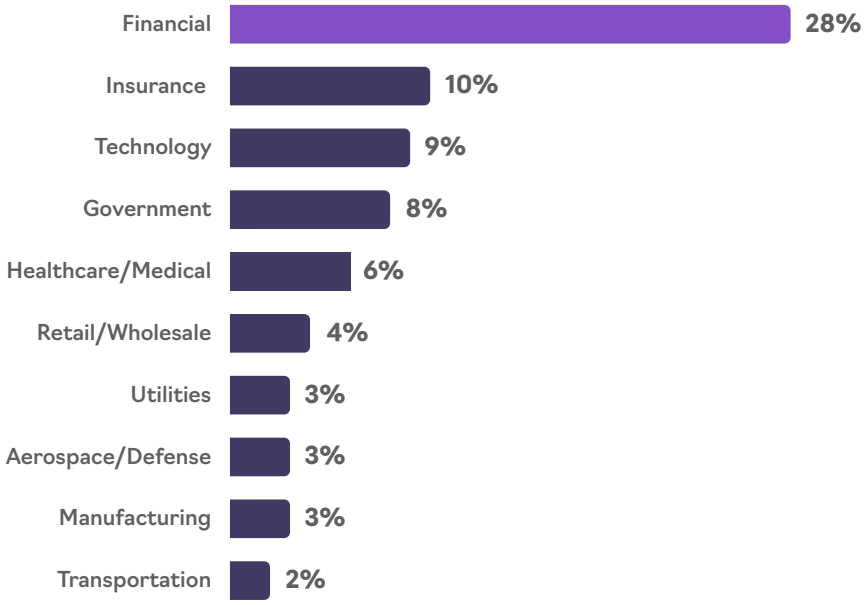
## Percent of Respondents by Organizational Revenues (Annual Gross Revenues – USD)



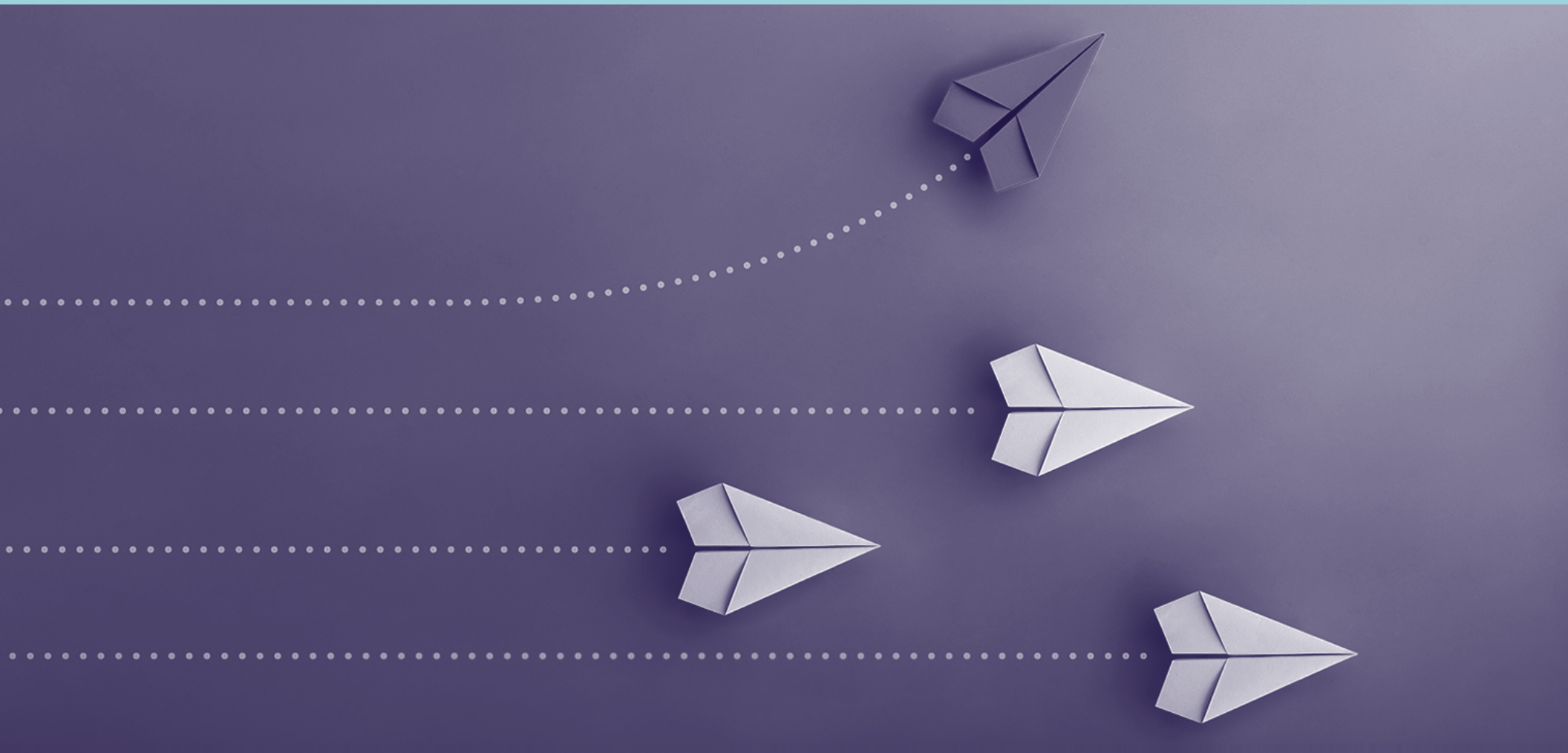

* Government/non-profit

## Percent of Respondents by Industry

### TOP 10 INDUSTRIES



# BCM Research Overview



# BCM Research Overview

## REPORTING HISTORY

Since 2001, BC Management has been gathering data on business continuity management programs and compensations to provide professionals with the information they need to elevate their programs. Each year our organization strives to improve upon the study questions, distribution of the study, and the reporting of the data collected.

## STUDY METHODOLOGY

The on-line study was developed by the BC Management team in conjunction with Castellan Solutions and the BC Management International Research Advisory Board. WorldAPP Key Survey, an independent company from BC Management, maintains the study and assesses the data collected. The study was launched on October 13, 2021 and it will remain open through September 2022. Participants were notified of the study primarily through e-newsletters and notifications from BC Management, Castellan Solutions, Continuity Insights, Disaster Recovery Journal, and from many other industry organizations. All participants are given the option of keeping their identity confidential.

## ASSESSMENT OF DATA & REPORTING

BC Management is continuously reviewing and verifying the data points received in the study. Data points in question are confirmed by contacting the respondent that completed that study. If the respondent did not include their contact information, then their response to the study may be removed. Data findings in many of the figures were rounded to whole numbers, thus the total percent may not equal 100%.

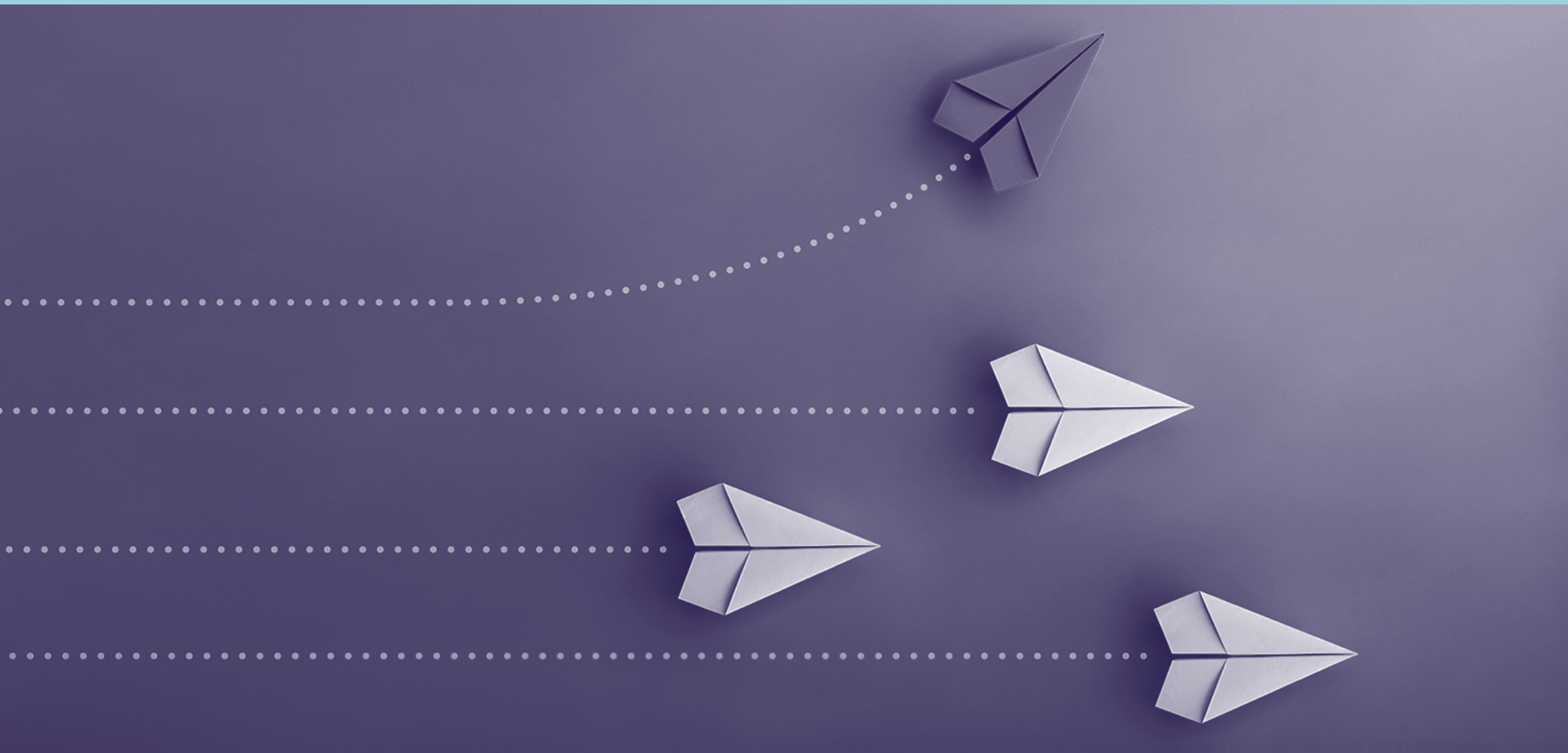
## PARTICIPANT OVERVIEW

**165 professionals** participated in our Evolving Resiliency Strategies Study.

Responses were received from **21 countries.** The most significant responses are bolded and associated with a response.

Antigua and Barbuda, **Australia (3%),** Bahamas, Belgium, **Canada (6%),** Cyprus, India, Japan, Luxembourg, Mexico, New Zealand, Portugal, Saudi Arabia, Singapore, South Africa, Sweden, Turkey, Uganda, United Arab Emirates, **United Kingdom (9%),** and **United States of America (67%).**

# Advisory Board + Distributing Organizations



# Thank you to BC Management's International Research Advisory Board

BC Management's International Research Advisory Board was instrumental in reviewing the study to ensure it focused on the topics that are of the greatest interest to resilience management professionals today. The goal was to develop a credible reporting tool that would add value to organizational resilience management.

## Larry Chase

**CBCP, Comp TIA A+ (USA Focus)**

Larry is the Director of Operational Resiliency Oversight in Citigroup's Operational Risk Management organization. An eight year United States Air Force veteran, Larry is a recognized and an industry leader in Enterprise Risk and Resiliency Management over the course of three decades. Credited with establishing global programs at Pfizer, Motorola, and most recently with Humana – His professional accomplishments include the 2017 BCI Continuity & Resiliency Team of the Year, 2015 DRI Program Leader of the Year, 2010 BCI Asia Group Excellence Award and the 2005 W.E Upjohn Award for Leadership. He spends a good portion of his free time as a professional musician around the Tampa Bay area and serving in different industry leadership roles; he is also credited as the co-founding of DRI Foundation's Veterans Outreach Program, providing scholarships to 700+ of our returning heroes.

## Kevin Cunningham

**MS, CEM, CBCP (USA Focus)**

Kevin is currently the Director of the Business Continuity Program Officer at Equinix Inc. Previously, he had spent 4 years as Vice President and Head of Global Business Continuity, Crisis Management and Emergency Services at NBCUniversal. Until May of 2013, he was Americas Regional Head of Business Continuity, Crisis Management for UBS AG. Prior to his tenure at UBS, Mr. Cunningham worked for the City of New York as a Preparedness Specialist for the New York City Office of Emergency Management.

## Ing. Jorge Escalera

**MBA, RM-31000, MBCP, CCRP, LA 22301 (Mexico)**

Jorge Escalera Alcazar is President of the Organization Resilience Institute (IRO), Practice leader of Enterprise Risk Management, Business Continuity Management Systems, IT Disaster Recovery, Risk Management, and Insurance. More than 25 years of experience. Consultant for private sector multinational corporations and public-sector institutions. Chemical Administrator Engineer from Tec de Monterrey. MBA from EGADE Business School. Master Business Continuity Professional (MBCP) and Instructor by Disaster Recovery Institute International. Certified Risk Management Professional and Trainer (RM-31000) by IRO. Former President of the Mexican Technical Committee ISO/TC262 Risk Management. Coordinator of WG2 Business Continuity of ISO/TC292 Security and Resiliency. Convenor of the Spanish Translation Task Force of ISO TC262/STTF – Risk Management. First President and founder of the RIMS Mexico Chapter.

## Robert Fucito

**(USA Focus)**

Experienced executive with a demonstrated history of working in the financial services industry. Skilled in Crisis Management, Enterprise Risk Management, IT Service Management, and IT Strategy. Strong professional with a Certificate focused in Design Thinking & Problem Solving from Massachusetts Institute of Technology - Sloan School of Management.

## Guy Gryspeerdt

**AMBCI (USA Focus)**

Guy Gryspeerdt BA (Hons), AMBCI, has a strong experience in aligning the risk, business resilience, and crisis management functions to the organization's strategic business goals and managing both the change process and subsequent organizational systems. He is outcome focused and sees a robust resilience program as a key business enabler to deliver a competitive advantage to the organization and value to customers. He has worked internationally across industry sectors, managing risk, business resilience, crisis management, and security in the financial, retail, manufacturing, and government sectors and has managed high level projects in these areas for leading organizations globally. Organizations have included Ernst & Young, Goldman Sachs, Reinsurance Group of America, The Westfield Group, and Bridgewater.

## Gayle Hedgecock

**(UK Focus)**

Gayle has over 20 years of Business Continuity experience in Financial services and less than 6 months in legal services, covering the full continuity lifecycle from completing BIA's through to creating and implementing BC policies and everything in between. Gayle was the chair of the BCI London Forum for 4 years.

## Ashley Helmick

**MBCI (USA Focus)**

Over the past four years, I have worked with a variety of organizations to implement and maintain successful Business Continuity and IT Disaster Recovery Programs. I have helped clients identify and mitigate risk and respond to disruptions. I have also worked to integrate business continuity and IT disaster recovery into organizations' cultures. The industries in which I've worked include healthcare, manufacturing, utilities, technology services/software, legal services, and financial services. I have also worked with several international organizations.

## Evan Hicks

**CBCP (USA Focus)**

Evan began his Business Continuity career in Blacksburg, VA implementing Emergency Notification Systems across the United States for local government agencies. Motivated by the events of the 2007 Virginia Tech shooting, Evan moved to New York City to pursue a Master's Degree in Emergency Management from John Jay College of Criminal Justice. While completing his graduate studies, Evan held positions at Goldman Sachs' Crisis Management Center and NYC OEM's Training & Exercise division. This unique experience in both the public and private sector, led him to Washington, DC where he held multiple roles across Fannie Mae's Corporate Incident Management Team, Business Continuity Office, Risk and Controls, and Credit Portfolio Disaster Relief Team. In 2016, Evan pursued an opportunity in Portland, OR to establish a Business Recovery program for Nike's world headquarters and global business operations. During his tenure with Nike, Evan elevated Business Continuity to the Board of Directors, authored the COVID-19 Return to Work Playbook, and implemented a global continuity planning process inclusive of incident management, third party risk, technology recovery, facility management, enterprise risk management, supply chain, HR, and other enterprise partners. Today, Evan is applying his crisis management expertise to his community in Portland where he's helping local charities address and resolve the social vulnerabilities revealed by COVID-19 and the BLM movement.

## Alberto Jimenez

**CBCP, PMP (USA Focus)**

Alberto is a founder and director with MiaTomi, a provider of business continuity management consulting services. Alberto has over 20 years of cross-industry experience, helping clients meet their business continuity, risk, compliance, and IT transformation needs. Prior to founding MiaTomi, Alberto was a national practice director at Datalink, Senior Manager at SunGard, Associate Director at Protiviti, and technology manager at Accenture.

## Sohail Khimani

**MBA, MBCP, AFBCI, OSSNHS, ISO 22301 LA**
**(Middle East Focus –Based in UAE)**

An award-winning risk and resilience luminary with over 16 years of experience in all facets of risk and resilience. He is considered as an expert in providing and implementing bespoke end-to-end risk solutions and is a qualified and well-versed risk and resilience thought leader assisting organizations survive and thrive in challenging times.

## Nicola Lawrence

**BCom, MBCI (UK Focus)**

Nicola Lawrence a business continuity professional that has worked in the Banking and Finance industry for 18 years, involved all aspects of resilience from planning and implementing BCM program to developing training and awareness opportunities. She is an active member of both The Investing and Saving Alliance (TISA) and Investment Association (IA) Operational Resilience Working Groups with the purpose of developing guidance for its member firms regarding the upcoming regulatory changes to Operational Resilience in the UK.

## Irfan Mirza

**(USA Focus)**

Irfan Mirza leads the enterprise continuity and resilience program across Microsoft. He has over 25 years of experience in the software and technical services industries in roles ranging from policy and compliance leadership in security, privacy, continuity, to software and service development, alongside enterprise, system and business architecture. He lectures frequently on technology topics and about policy design, implementation and measurement, as well as delivering periodic university lectures in political sociology.

## Desmond O'Callahan

**FBCI (Canada Focus)**

Des O'Callaghan, FBCI, is a practitioner with 30 years of experience in building, leading, and assessing business continuity programs in Canada. Much of his career has involved directing in-house programs in the financial sector. He also has over 10 years of wide ranging consulting experience across multiple sectors. Des has been an educator in BCM for over 12 years, teaching at George Brown College in Toronto for 4 years and currently delivering Business Continuity Institute courses across North America. Des became a Fellow of the BCI in 1996 and is presently Vice President and Secretary of the Canadian Chapter, He was appointed as Lead Assessor for the BCI in 2018. Des frequently presents at conferences and has received a national Canadian Award of Excellence in 2009 and a gifted grade Global BCI Achievement Award in 2015.

## Jayaraj Puthanveedu

**CISSP, MBCI, ISO Lead Auditor (UK Focus)**

Jayaraj is a Senior Executive with over 21 years of experience in Cyber Security, Risk Management and Resilience, primarily focused on helping board level and CXO stakeholders in Tier1 Financial Services institutions in shaping their digital strategy to improve their Cyber Security and Resilience posture. In his current role as the Managing Director in BNP Paribas, he is the Global Head for Cyber Fraud, Cyber Resilience, Third Party Tech Risk, Data Breach Management, Business Continuity, IT Resilience, and overall Operational Resilience. Prior to this, he has held various leadership roles in Deutsche Bank, Goldman Sachs, Northern Trust etc. covering Operational Risk, Cyber & Technology Risk, and Resilience areas.

## Malcom B. Reid

**FBCI, CBCP, CPP, CFE (USA Focus)**

Malcolm is a globally recognized, risk and resiliency thought leader. Among his many accomplishments includes the national critical infrastructure assessment of one of the top Liquified Natural Gas (LNG) exporting nations. He has also led enterprise business continuity, security and risk advisory engagements for large global organizations. Malcolm is a graduate of the United States Military Academy at West Point and holds Masters degrees from Norwich University, Webster University and the University of Reading. He is a Fellow of the Business Continuity Institute and is Board Certified in Security Management. Malcolm is a member of a number of industry and community based boards including that of the BCI-USA chapter and the 2020 global board of ASIS International.

## Wong Tew Kiat

**CBCP, FBCI, CITBCM(S), CITPM(S), COMIT(S), Fellow SCS (Asia Pacific Focus – Based in Singapore)**

More than 30 years of experience in IT Infra, Data Centre Infrastructure & Operations, Business Continuity Management, Pandemic Preparedness, Crisis & Incident Response, IT Disaster Recovery, Emergency Management, and Data Centre (DC) Risk & Health Check. Managed a 100,000 sqft Data Centre for the 30 years. Currently appointed as Chairman for the Data Centre Special Interest Group (DC SIG) by Singapore Computer Society (SCS) as a national platform for DC professionals to network and share research & innovative ideas to meet the changing trends of the DC landscapes. A CBCP by DRII(USA) since 1997 and Fellow of BCI-UK since 2005. Also a Certified IT Project Manager, Certified Outsourcing IT Manager, and Certified ITBCM Manager (CITBCM) by SCS. He was the President for the Business Continuity Group, a chapter in SCS from 2005–2008 & 2010–2011. In addition, he chaired the CITBCM Resource Panel to develop the Body of Knowledge and also chairs the Board of Assessors and he is also the authorised training provider for this CITBCM Certification Course.

## Gilberto Tiburcio Freire

**Junior (LATAM Focus)**

More than 45 years of experience with solid business knowledge in Sales of IT Services, with experience in IBM Brazil, IBM United Kingdom, and REGUS. More than 20 years working as People Manager leading Services Organization (Infrastructure Services, Business Resilience Services, Business Continuity, Disaster Recovery, IT Security). He was responsible to implement a Business Recovery Organization in a IBM Brazil, afterwards he was responsible for this Business in all Latin America for more than 10 years. He is currently responsible in REGUS (IWG Parental company) for Workplace Recovery services in Latin America since 2016.

## Sanjiv Tripathy

**(India Focus)**

Sanjiv is a senior Risk leader and has managed Resilience & BCM for a global banks India set up (RBS Technology) comprising of ~15000 headcount size distributed over multiple locations working with Senior management / Silver & Gold global Incident management teams, partnering with businesses such as Banking business, Operations, Financial services, and Risk services for India wide organisation (~25000 team size). Conceptualized & implemented fit for purpose Business Resilience, BC and Disaster Recovery strategies, reviewed them and implemented improvements as part of major incident review and Regulatory review. Fostered strong stakeholder relationships, developed specialised team, managed Resilience & BC critical processes, reviewed BCM program framework and standards, assessed large global critical 3rd party service providers BCM capabilities, assessed organizations effectiveness of BC / Resiliency, and presented BCM preparedness to Internal audit, External auditor and Regulators.

## Thomas Wagner

**CBCP, MBCI (USA Focus)**

Tom is a recognized expert and innovative thought leader in the Business Continuity Management space with over 25 years' experience as a practitioner, management consultant, and technology executive in the financial services industry. Tom is currently the Managing Director for a major trade association and he previously served in senior BCM roles at HSBC, Marsh, Gartner, Booz Allen, and the NYSE. While at Booz Allen, Tom consulted to the President's Commission for Critical Infrastructure Protection (PCCIP), the White House Critical Infrastructure Assurance Office (CIAO / Homeland Security), and Intelligence Communities where he conducted risk assessments and helped develop strategies to protect the financial services industry from terrorism and natural disasters. Tom is also a recognized thought-leader in the IT Controls and Risk Management space having served as a SME with ISACA ITGI for the on-going development of CobiT and the IT Risk and Governance frameworks.

## Kiyoshi Yoshikawa

**(Asia Pacific Focus – Based in Japan)**

Mr. Yoshikawa has been a BCM professional for over 15 years in the financial and manufacturing industries. He started his career as an IT network engineer and build backup data centers and sites. He brings a sound knowledge of the financial regulations of the APAC countries and understands the residual risks in the production lines and supply chain.

# Thank you to those organizations that assisted with this global effort.

**Distributing Organizations:** BC Management also greatly appreciates the efforts of those organizations that assisted in this global effort. Below is a list of participating organizations that assisted in distributing our annual study. The contribution of each individual organization does not indicate an endorsement of the study findings or the activities of BC Management. This is NOT a complete list of distributing organizations.

# About BC Management

BC Management, founded in 2000, is an **executive staffing** and **research firm** solely dedicated to the resilience management, business continuity, disaster recovery, risk management, emergency management, crisis management, and security professions. With decades of industry expertise, our staff has a unique understanding of the challenges professionals face with hiring, benchmarking, and analyzing best practices within these niche fields.

# Why BC Management

### We're "In" Resilience Management!

We have 40 years of dedicated experience. We understand the language and can identify the skills needed to be successful.

### We're Fast

We have a proven process that gets results - quickly. We also communicate frequently - so you always know the status of your search.

### The Hidden 60,000

We have the largest network of passive resilience management candidates in the world! Many won't be found actively looking for a job or on LinkedIn.

### Global Reach

From Detroit to Delhi - We have worked in dozens of countries.

Now you're ready.™

As the global provider of resilience management solutions – spanning consulting, software, managed services, and staffing – Castellan is uniquely positioned to help organizations find the right balance of risk tolerance and resilience to protect their people, reputation, customers, and bottom-line. Leveraging a proprietary proven process for driving organizational readiness and response, Castellan partners with clients to establish a clear vision, drive real results, and provide ongoing support from their community of resilience experts. Castellan helps organizations replace uncertainty with confidence.

**For more information, visit castellanbc.com.**

# BC Management

## CONTACT US


info@bcmanagement.com

bcmanagement.com

+1.714.969.8006