CAPCO

Operational risk & operational resilience

Built on culture, powered for crisis

a wipro company

Effective operational risk and operational resilience management has never been more critical. Bank collapses in the US and the ransomware attack on ICBC and the global IT outage caused by a faulty CrowdStrike update have thrown operational risk and operational resilience to front of mind for firms and regulators.

Organizations have faced cascading shocks that reveal the stark consequences of inadequate preparedness. While risk management as a discipline has matured significantly over the past two decades, driven by regulatory reform, crisis-driven learning, and the formalization of governance structures, operational resilience remains less well understood, less embedded, and far more culturally dependent.

The traditional focus has often been on frameworks, controls, and compliance, rather than on adaptive capacity, human behaviors, or organizational learning. In this article, we explore how culture is at the core of an effective risk and resilience management and proposes guiding principles to help build a strong culture.

A dynamic agenda

In today's complex and volatile environment, the operational risk and operational resilience agenda is rapidly evolving.

Firms are shifting from a primarily risk-based compliance mindset to broader, capability-driven models. While traditional financial and credit risks remain important, global regulators have increasingly elevated non-financial risks, including operational resilience, cybersecurity and third-party risk. These areas are now receiving a level of scrutiny and importance comparable to financial resilience.

In the UK, the Bank of England, PRA and FCA require firms to identify and map important business services, conduct scenario testing to demonstrate recovery within defined impact tolerances, and remediate vulnerabilities across important business services.

On a global level, several macro factors are driving this agenda further up boardroom priorities. These include geopolitical tensions, a rapidly evolving threat landscape, an increased reliance on third parties, and emerging technologies including transformer-driven AI models.

As a result, investment is increasingly focused on:

- enhancing scenario testing rigour
- cyber and ICT resilience
- supply chain management
- cloud adoption as a resilience enabler
- strengthening response and recovery capabilities.

Despite improvements in tooling and governance, many firms still struggle to embed operational resilience culturally and behaviorally, particularly in decentralized or hybrid environments. Leading organizations are therefore beginning to integrate culture, leadership, and decision-making agility into their risk and operational resilience strategies.

A strong organizational culture is the foundation for effective operational risk and resilience management because it shapes behaviors, decision-making, and accountability across all levels.

Weak culture often results in audit findings and control failures. A culture that prioritizes integrity, transparency, and continuous learning ensures that control frameworks are applied consistently and adapted proactively, rather than reactively. In resilience testing, such a culture drives active participation and realistic scenario planning, rather than box-ticking exercises.

For both risk and resilience modeling, a healthy culture promotes the sharing of accurate data, candid reporting of weaknesses, and constructive challenge, enabling models to reflect true operational realities rather than optimistic, unvalidated assumptions.

A refocusing of regulatory priorities

Regulators across the globe are intensifying their focus on firm's operational resilience capabilities as risk events have shown that lack of resilience can threaten the stability of financial institutions and markets

"Operational resilience is more than a regulatory requirement – it's fundamental to competitiveness, customer service, and financial stability. Let's ensure it becomes part of our sector's DNA" – **Suman Ziaullah, Head of Technology, Resilience and Cyber, FCA**[1]

While local approaches vary, a clear pattern is emerging. Supervisory bodies are embedding expectations related to operational resilience, governance, and risk culture into formal guidance. The table below highlights some notable current regulatory imperatives across a number of leading global markets.

Regulatory body	Guidance	Focus areas	Culture emphasis
FCA/PRA (UK)	PS21/3, PRA SS1/21, SYSC 4.1, 15A	Operational resilience framework (IBS, impact tolerances, scenario testing)	Empowered front-line response and decision-making; board-led resilience embedding
ECB (EU)	Guide to internal Governance, Supervisory priorities	Governance and operational resilience integration through internal controls, risk culture, and supervisory oversight	Risk culture treated as a formal governance mechanism; expectations for board tone and cultural transmission
EBA (EU)	EBA Guidelines on ICT and Security Risk Management, Fit and Proper Guidelines (EBA/GL/2021/06)	Incident root cause analysis, governance failings and accountability under ICT and Fit & Proper frameworks	Explicit flagging of cultural deficiencies behind operational lapses; focus on behavioral root causes in failures
MAS (Singapore)	MAS TRM Guidelines (2021)	Cyber resilience enforced via TRM guidelines; operational continuity, cyber hygiene, and access controls	Cultural readiness and employee vigilance as the first line of cyber defense; prevention culture embedded
SEC (US)	Whistle-blower program, Enforcement Releases	Crisis escalation frameworks, governance accountability, and disclosure discipline under whistleblower and enforcement regimes	Escalation culture and accountability norms enforced through legal protections, deterrent penalties, and transparency mandates

Key challenges in a shifting landscape

To navigate today's increasingly complex and uncertain landscape, firms must address several persistent challenges that continue to undermine effective operational risk and operational resilience practices.

In the table below, we look to capture some of these challenges.

Challenge	
Policy–practice gap in risk and resilience	Many firms appear mature on paper but fall short in practice. Although 73.5% of organizations reported greater post-pandemic appreciation for resilience (BCI, 2022), only 37.3% had a dedicated C-suite lead, 40.5% provided formal outage plans for remote workers, and fewer than 30% had implemented power outage or comms resilience for remote-critical roles.[2] Regulators often uncover these gaps during deep dives, highlighting the disconnect between policy and actual implementation.
Deficient speak-up and psychological safety culture	A 2021 Irish Banking Culture Board survey found that 58% of staff felt encouraged to speak up, yet 19% of those with concerns didn't escalate them—citing fear or futility. Only 67% felt safe sharing opinions without negative consequences.[3] In a 2024 Lloyds culture survey, almost a third of respondents did not respond that they felt concerns raised were taken seriously or that they believed their organization responds effectively to feedback.[4] These dynamics hinder early threat detection and timely escalation.
Cultural frictions undermining agility	Cultural blockers like defensiveness and discomfort with challenge, impede adaptive behavior. The Lloyds survey data shows that almost a quarter of respondents do not feel safe to disagree or challenge dominant opinions without fear of negative consequences.[4] These subtle frictions degrade responsiveness and trust under pressure, especially in high-stakes situations.
Assumed rather than demonstrated resilience maturity	Despite 73.5% recognizing resilience as a priority post-COVID, practical readiness remains weak: only 40.5% offer formal outage plans to remote staff, and under 30% have critical resilience measures for remote roles (BCI, 2022).[2] Few firms test behavioral readiness, despite 87.7% of practitioners rating training and exercises as top priorities. Resilience maturity is often assumed, not proven.
Reliance on control frameworks without validating underlying assumptions	Many organizations place confidence in established control frameworks, assuming they remain effective across contexts. However, these frameworks are often built on outdated or untested assumptions about behaviors, environments, and system interactions. Without routine validation through stress testing, behavioral insights or scenario-based challenge, firms risk blind spots where controls may not perform as intended. This over-reliance fosters a compliance mindset rather than adaptive resilience and can undermine agility in dynamic or high-stakes situations.

Building a strong operational risk & resilience culture

Review your operational risk and operational resilience culture health. Building a strong risk and operational resilience culture starts with understanding your current state. Below are five key questions that can serve as a starting point for firms assessing the health of their culture.

	Question	Insight
	Are operational risk and operational resilience embedded in daily decisions and leadership behavior?	Cultural alignment from top to bottom
	Are escalation roles and responsibilities understood?	Role clarity and accountability
	Do staff feel psychologically safe to raise concerns?	Trust and openness
	Do we learn from incidents and improve?	Feedback culture and agility
	Are we prepared and regularly testing disruption response?	Operational readiness and foresight

Key Principles. Firms aiming to build a robust operational risk and operational resilience culture should follow key guiding principles. These principles help embed the right mindset across the organization, making firms more adaptable, proactive, and better equipped to prevent and detect threats and respond to disruptions.

Principle	Key considerations
Tone from the Top	Leadership visibility, consistent messaging, resource allocation, leading by example
Empowered accountability	Clear roles, decision-making autonomy, non-punitive environment, risk ownership
Integrated by design	Embedding in strategy, cross-functional planning, alignment with objectives
Continuous learning	Incident reviews, learning from near-misses, scenario testing, knowledge sharing
Test and validate assumptions	Challenging assumptions through scenario testing, real-world simulations and ongoing validation to ensure controls and decisions remain fit for purpose
Transparency	Transparent reporting, safe challenge, timely escalation, feedback mechanisms

Tone from the Top. Tone from the top is crucial for building a successful culture. Senior leadership must view risk management and resilience as core to business success.

A major firm recently asked Capco to help them develop a third-party risk management capability compliant with DORA. A significant challenge was internal resistance due to a lack of understanding of what was needed and why. The support and buy-in of senior leadership were key to overcoming this gap and driving the necessary changes to create a more forward-thinking and robust risk management environment.

Behavioral science suggests that leadership behaviors serve as powerful social cues.

Leaders who model desired behaviors are proven to inspire others to follow. When leaders normalize discussion of risks, reward speaking up, and visibly engage in scenario planning, these behaviors cascade through the organization.

It is not enough for leaders to advocate for values and policies. The credibility and impact of leadership depend on their ability to model those principles in their daily decisions, behaviors, and priorities. Employees take cues from what leaders do, not just what they say.

Empowered accountability. Clearly defined and well-understood roles and responsibilities are essential. Individuals across all levels must feel trusted and supported to own operational risks and operational resilience within their areas. Empowered accountability fosters a culture of speaking up, intelligent risk-taking, and informed decision-making, without fear of blame.

Encouraging ownership can be reinforced with behavioral nudges such as embedding ownership prompts in workflow tools, or by using storytelling to share positive examples of risk escalation and mitigation. This aligns with the concept of self-efficacy: when people feel capable and responsible, they are more likely to take appropriate action.

Integrated by design. Operational risk and operational resilience must be embedded into core business processes, decision-making, and strategic planning from the outset. Rather than being reactive or siloed, operational risk and operational resilience should be integrated into how the organization operates, plans, and evolves. This enables smarter, more sustainable decisions.

A major financial institution recently asked Capco to deliver a global operational resilience training curriculum. A key component was helping staff recognize how risk and operational resilience are relevant to everyday activities, and how to adopt a mindset that incorporates these elements into all levels of the organization. Post-training data showed that staff had a clear understanding of their responsibilities and were confident in applying operational resilience principles in business processes, decision-making, and change initiatives.

Using behavioral design techniques, like prompts and reminders embedded into standard operating procedures, can help make this integration effortless and automatic.

Continuous learning. A strong culture of operational risk and operational resilience is one where continuous improvement is embedded. Firms should ensure that post-incident reviews, testing analysis, and related activities are treated as opportunities to gain experience and evolve future robustness.

A client engaged Capco to reinvigorate a continuous learning program to strengthen operational resilience and meet FCA/PRA expectations. The resulting program included clear data and KPIs that helped identify common themes and informed targeted capability improvements.

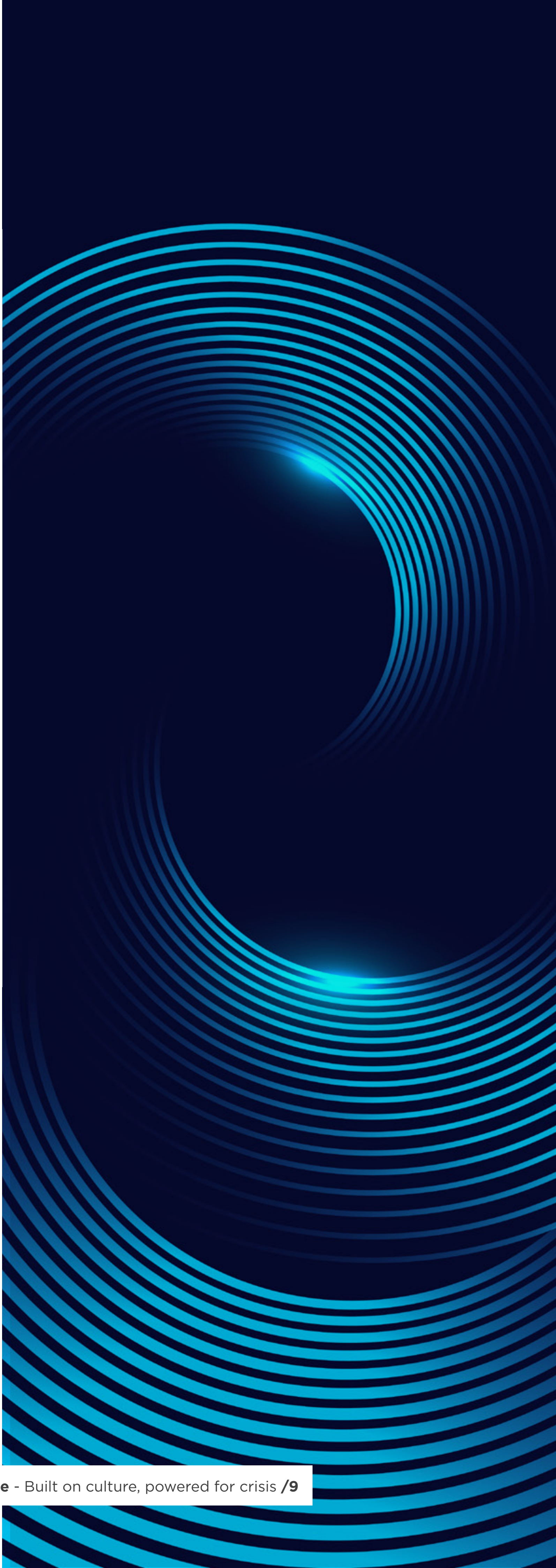
Behavioral science shows that feedback is most effective when it is timely, specific, and linked to future actions. Embedding these feedback loops across teams reinforces learning and helps shape more adaptive behaviors.

Test and validate assumptions. The testing and validation of assumptions are critical to building resilience and avoiding blind spots. Assumptions are often taken forward and not themselves subjected to rigorous validation exercises. This increases the risk that outdated assumptions are used to model future behavior or risks.

Firms must get ahead by building in status quo challenges in which assumptions are properly challenged, discussed, reviewed, and tested. Testing and validation are an ongoing exercise, and firms should move away from viewing these as one-off exercises. This will ensure that controls and frameworks remain fit for purpose in anticipating and responding to emerging threats.

Transparency. A culture of transparency is essential for embedding a strong operational risk and operational resilience mindset. It builds trust, encourages timely reporting, and supports structured debriefs and shared learning. This enables early identification of vulnerabilities across systems, processes, and behaviors. Transparency also improves after-action reviews and institutionalizes lessons learned through incident learning loops. It fosters honesty, accountability, and cross-functional collaboration, enhancing an organization's ability to anticipate and respond to emerging risks. Importantly, it ensures staff understand their roles and feel engaged in initiatives.

Capco observed one large firm where poor collaboration and unclear responsibilities led to inconsistent risk system usage, low trust, and compliance issues. This underscores the importance of a well-communicated, transparent culture. Behavioral science shows that visible actions such as sharing lessons, recognizing contributors, and communicating change, reinforce belief in the system and drives continued engagement.



Strategies for success

To build a strong and sustainable risk and operational resilience culture, firms can adopt a combination of the following strategies.

- **Embed** operational risk and operational resilience in decision-making: use structured frameworks and behavioral nudges to guide risk-aware decisions.
- **Develop** operational risk and operational resilience leadership at all levels: educate leaders to model the right behaviors and create psychologically safe environments.
- **Promote** active learning loops: establish mechanisms that enable feedback, reflection and behavioral reinforcement across teams.
- **Integrate** cultural metrics into operational resilience exercises: assess staff comfort with escalating issues, decision-making confidence under simulated stress and post-exercise feedback quality.
- **Calibrate** appropriate reward and performance management to be commensurate with staff ability to display adaptive behaviors: ensures that flexibility, learning agility and proactive risk ownership are recognized alongside traditional performance metrics.

Using the guiding principles and diagnostic questions outlined above can help determine which strategy or combination is best suited for each firm.

How can we measure?

Regulators are no longer satisfied with theoretical compliance or well-documented frameworks. As firms respond to evolving regulatory expectations, measuring culture effectively is becoming essential.

To effectively evidence culture, firms must evolve from relying solely on traditional compliance metrics to incorporating behavioral and experiential indicators that reflect how risk and operational resilience are truly embedded in day-to-day practice. The table below compares these two approaches across key dimensions.

Area	Traditional metrics	Innovative/behavioral metrics
Policy awareness & adherence	• Policy attestations • Mandatory training completion	• Pulse surveys on policy confidence • Decision logs reflecting policy use in practice
Incident & issue management	• Number of incidents reported • Breach closure timeframes	• Quality of escalation narratives • Staff willingness to self-report or challenge
Third party risk oversight	• Contract review rates • Due diligence checklist completion	• Behavioral reviews of supplier interactions • Evidence of proactive escalation by relationship managers
Cybersecurity resilience	• Phishing simulation pass rates • Control testing frequency	• Observed behaviors during live exercises • Staff response during unplanned cyber events
Scenario testing & BCP	• Completion of test cycles • Documented recovery plans	• Quality of decision-making during tests • Evidence of cross-functional coordination under pressure
Risk & controls	• RCSA completion rates • Control testing scores	• Thematic analysis of control failure responses • Conversations and behaviors in control design meetings
Governance & oversight	• Attendance rates • Paper submissions on time	• Quality of challenge in committee discussions • Track record of early escalation before issues materialize

A role for Behavioral Risk?

Behavioral Risk improves operational risk and operational resilience by addressing the underlying behavioral drivers that influence how people perceive, assess and respond to uncertainty in real settings. It highlights where human judgement deviates from rational models, often due to biases such as normalcy bias (expecting the future to reflect the past), confirmation bias (seeking data that fits preconceptions) or optimism bias (underestimating the likelihood of adverse outcomes).

In risk modeling, behavioral risk insights help firms:

- Identify and challenge hidden assumptions about human behavior, such as how quickly people will detect or report anomalies
- Adjust model inputs to reflect realistic rather than idealized behaviors, particularly under stress or time pressure
- Improve the calibration of loss estimates or control effectiveness by accounting for overconfidence, anchoring or status quo bias in historical data interpretation.

In scenario testing, Behavioral Risk contributes by:

- Designing stress scenarios that are psychologically plausible, not just statistically extreme, and that reflect how people might behave under pressure.
- Testing team responses to disruption in ways that surface cultural barriers to escalation, ownership and cross-silo coordination
- Using structured pre-mortems, red teaming or devil's advocate roles to counter groupthink and drive more critical challenge of 'known' risks
- Supporting better preparation by helping teams rehearse decision-making under uncertainty, build comfort with ambiguity and improve the speed and quality of risk-related communications. It reinforces psychological safety, which enables earlier detection and faster escalation during testing or real events.

To unlock these benefits, firms should embed behavioral capabilities within operational risk and operational resilience teams, incorporate behavioral criteria into model validation and ensure scenario testing exercises simulate not just external shocks but internal human dynamics.

Embracing culture for long-term success

As the risk landscape grows more complex and the expectations of regulators continue to evolve, firms can no longer afford to treat operational risk and operational resilience as technical or compliance-driven exercises alone.

Success in this new environment demands a shift toward culture – toward lived behaviors, empowered ownership, transparent communication and continuous learning.

Frameworks and policies remain essential, but they must be supported by leadership that leads by example, employees who feel accountable and safe to act, and systems that reward learning and adaptation.

The firms that will thrive in the face of disruption are those that embed operational resilience not just into their structures and processes, but into their mindsets, decisions, and daily actions. By anchoring their approach in culture, organizations can move from reactive to proactive, from compliance to confidence – and from fragility to true resilience.

How can Capco help?

Operational risk and operational resilience maturity assessment. We help firms assess the maturity of their risk and resilience models, identify and address gaps to strengthen their capabilities

Integrating operational risk and operational resilience. We help firms transition from a transformation to BAU state ensuring that operational risk and operational resilience programs achieve long lasting improvements, align frameworks and integrate end-to-end operating models across the disruption lifecycle

Regulatory compliance and remediation. We help firms assess compliance with major regulations such as DORA and PRA/FCA requirements and industry practices, and implement sustainable change to improve service operational resilience posture

Target operating model and framework design. Capco is industry leader in target operating model and framework design and implementation supporting firms achieve cost and efficiency gains, enabled through technology and AI.

Behavioral science. We are at the forefront of harnessing the power of behavioral science insights and turning them into tangible actions to effect positive behavior change at firms and support advanced risk modeling and resilience scenario testing.

References

1. Operational resilience: beyond regulatory raincoats | FCA
2. https://www.thebci.org/news/continuity-resilience-report-2022-launch.html
3. IBCB-eist-2021-report-RS-060521_Final_ONLINE.pdf
4. Lloyd’s 2024 Culture Dashboard_scroll_final

Author

Thomas Echlin-Harradine
Consultant

Contacts

Jamilia Parry
Partner, Global Head of Financial Crime, Risk, Reg & Finance (FRRF)
jamilia.parry@capco.com

Marija Devic
Head of Capco UK Operational Resilience & Cyber Practice
marija.devic@capco.com

About Capco

Capco, a Wipro company, is a global management and technology consultancy redefining transformation across the financial services and energy industries. Capco leverages the power of AI and our deep domain expertise to help our clients move faster, make smarter decisions, and drive greater impact. Our award-winning Be Yourself at Work culture and diverse talent drive bold, forward-thinking ideas and lasting change.

To learn more, visit www.capco.com or follow us on LinkedIn, Instagram, Facebook, and YouTube.

Worldwide Offices

APAC
Bengaluru – Electronic City
Bengaluru – Sarjapur Road
Bangkok
Chennai
Gurugram
Hong Kong
Hyderabad
Kuala Lumpur
Mumbai
Pune
Singapore

MIDDLE EAST
Dubai

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
Glasgow
London
Milan
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto

SOUTH AMERICA
Rio de Janeiro
São Paulo

capco.com

CAPCO
a **wipro** company