

Agenda

2026

Aware but unprepared

A snapshot of crisis comms readiness within mission-led organisations



Welcome

03 About this report

06 Executive summary

09 The results

23 Conclusion

Agenda

About this report



Are you ready for a crisis?

For many years, Agenda has helped organisations respond to communications crises. We've dealt with *Daily Mail* exposés, spokespeople tweeting inappropriately, political crises, accusations of misconduct by senior level staff – you name it, we've seen it. Sometimes it's involved keeping stories out of the press, other times it's been about minimising the damage caused by a front-page article.

Trends have emerged from this work that indicate to us that few organisations are ready for a crisis, most think it will never happen to them, and all will struggle in a myriad of ways when it actually does. We wanted to find out if these experiences are seen more widely, so we asked senior comms practitioners from mission-led organisations a simple question: Are you ready for a crisis?

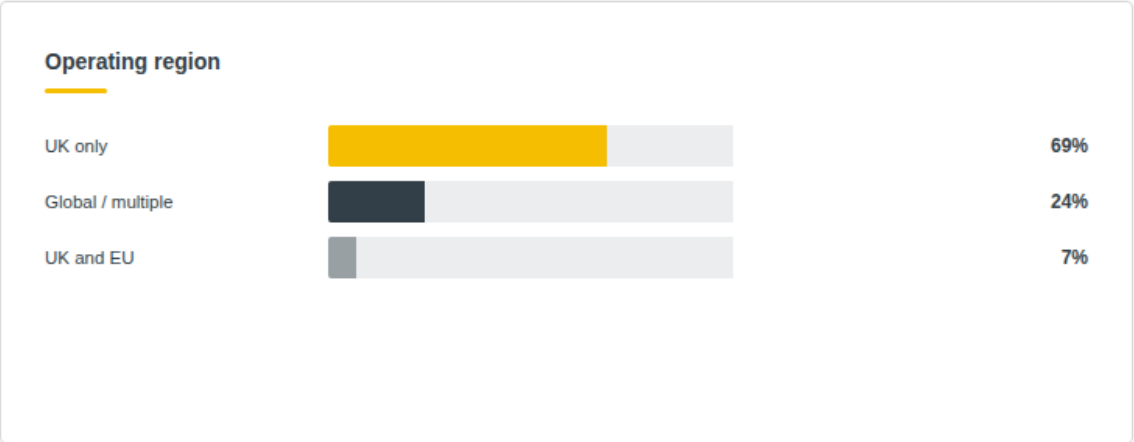
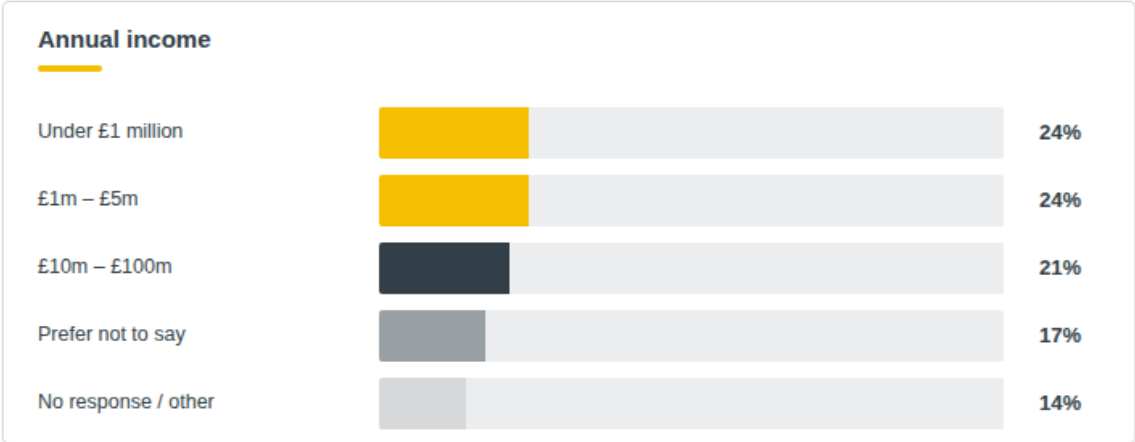
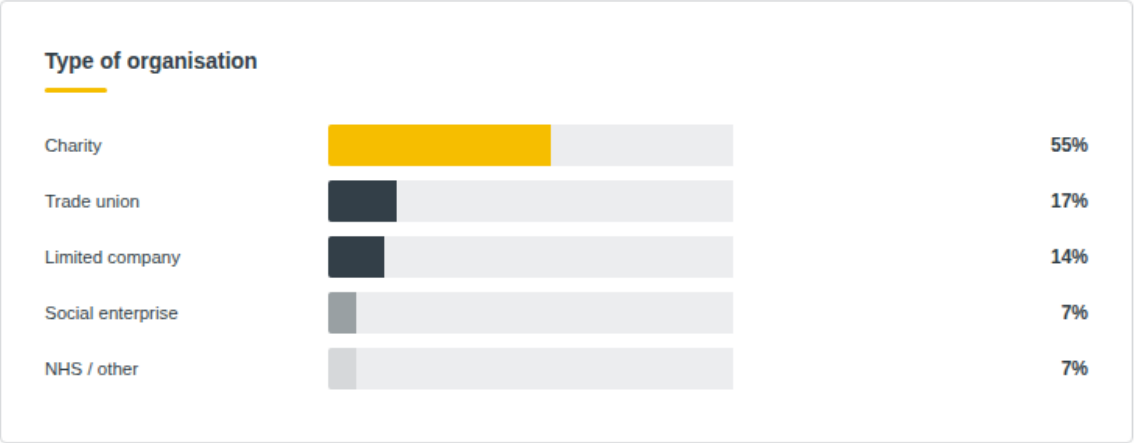
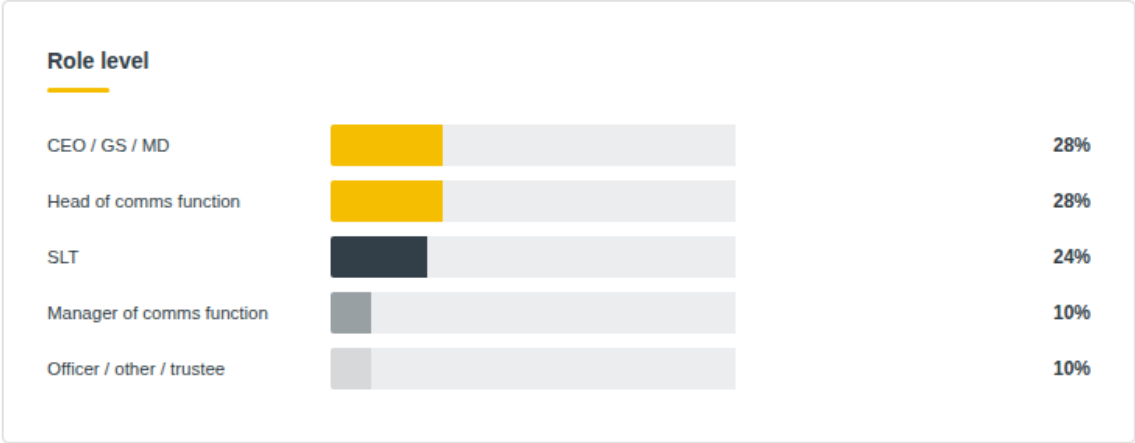
We received 29 responses. Some 80 per cent of respondents are at CEO, senior leadership or head of communications level with good oversight of their organisation and its plans.

While the sample size is modest, the findings strongly align with Agenda's experience of working with organisations across the sector, suggesting these patterns reflect a wider reality.

We will repeat the exercise again next year. To register your interest in taking part, please contact: hello@your-agenda.com



Who is ready for a crisis?



Executive summary



Executive summary: A clear gap between awareness and action

Most organisations believe they could handle a crisis. From what we see, many couldn't - at least not as well as they think.

From online attacks to funding shocks and political pressure, social impact organisations are operating in an increasingly volatile environment. Crises don't unfold slowly or neatly.

They escalate fast, often in public, and the reputational, financial and operational consequences are tightly connected.

Our survey respondents are not blind to these risks, but many are not equipped to manage them.

The findings in this report reflect what we see in our day-to-day work here at Agenda: there is a clear gap between awareness and action. Many organisations understand what could go wrong, but far fewer are set up to respond effectively when it does.

This is because crisis comms plans are missing, out of date or untested; roles in a crisis are unclear; and while there is confidence about responding to a crisis, the capability to do so isn't necessarily present.

Headline findings

- Just seven per cent of respondents consider themselves fully prepared for a comms crisis, with the vast majority (79 per cent) only partially prepared.
- Over half (55 per cent) would face a crisis without a current, reliable communications plan in place.
- While 72 per cent have a risk register, this drops to 41 per cent for incident monitoring and 24 per cent for a crisis comms plan – highlighting a clear gap between identifying risks and being ready to respond.
- Only 17 per cent have tested plans in the last 12 months, limiting their effectiveness in real-world scenarios.
- Planning is weakest in comms and external risks – despite these being the most likely to escalate quickly.
- Confidence is higher than preparedness, suggesting respondents overestimate their ability to respond.

Executive summary: What this means and what to do about it

Put simply, our respondents recognise what could go wrong but aren't always set up to deal with it when it does.

There is a clear gap between what they know to expect and what they are ready for. In a crisis, that gap is what trips people up.

“ Awareness is not being converted into operational capability.

“ Confidence is often not grounded in tested plans or clear processes.

“ Roles and decision-making become clear only when plans are rehearsed, not just written down.

“ This creates a capability gap: organisations know what could go wrong but lack the systems and preparation to respond effectively when it does.

Crisis preparedness isn't just about knowing what might go wrong; it's about being ready to act when it does. The organisations that invest in planning, practice and clarity won't just manage crises better, they'll protect their reputation, maintain trust and make better decisions when the pressure is on.

What to do about it

The good news is these gaps can be filled quite easily. The organisations that handle crises well focus on a small number of practical things and do them consistently:

1. Have a clear, usable crisis communications plan – not a document that sits in a folder, but something people can act on quickly.
2. Test that plan regularly, so that you know where the gaps are before a real crisis hits.
3. Make sure roles and decision-making are clear, especially at senior level.
4. Spend more time preparing for communications risks, such as dis- and misinformation and online attacks, not just operational issues.
5. Sense-check confidence against reality – and build capability where it's needed.

The results



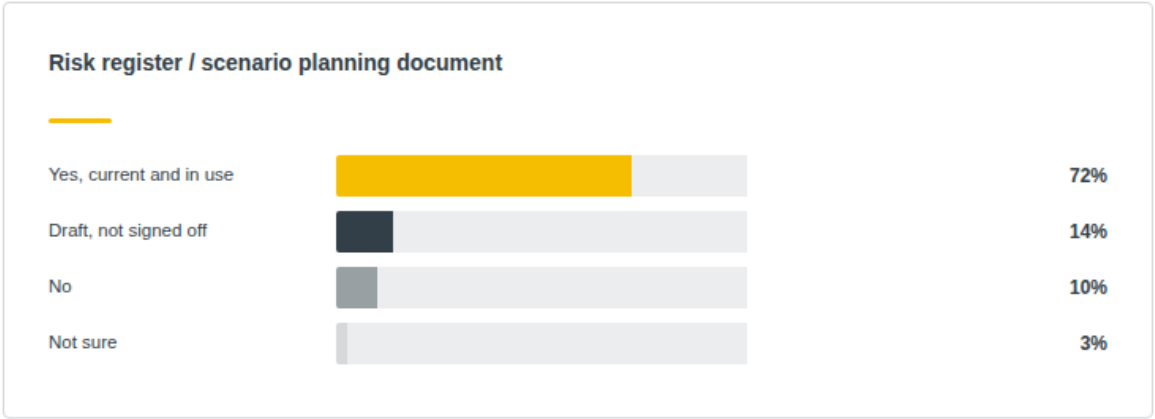
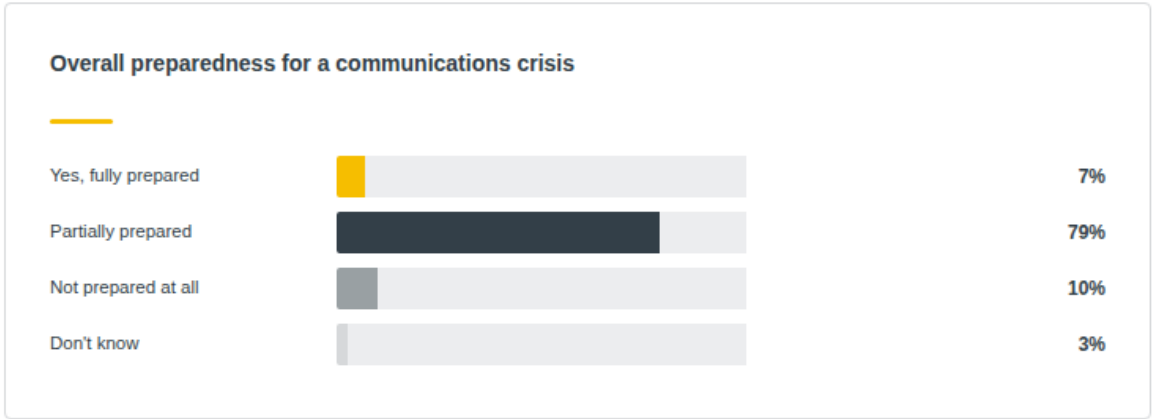
Preparedness: Do you think your organisation is ready for a crisis?

The headline finding is stark. Just seven per cent of respondents consider their organisation fully prepared for a comms crisis. The vast majority – 79 per cent – describe themselves as only partially prepared, while a further 10 per cent say they are not prepared at all.

This is a fairly typical pattern that fits with Agenda's own experience of working with similar organisations. "Partial preparedness" often signals that organisations have some elements in place (perhaps a contact list or a general policy) but lack tested plans, trained spokespeople or clear decision-making protocols under pressure.

To help us dive into this in more detail, we asked if the three foundations of crisis management were in place: a risk register or scenario plan; an incident monitoring process; and/or plan.

The data reveals a clear and concerning pattern of declining readiness as organisations move through the crisis management lifecycle – from risk identification to incident monitoring to active response planning.



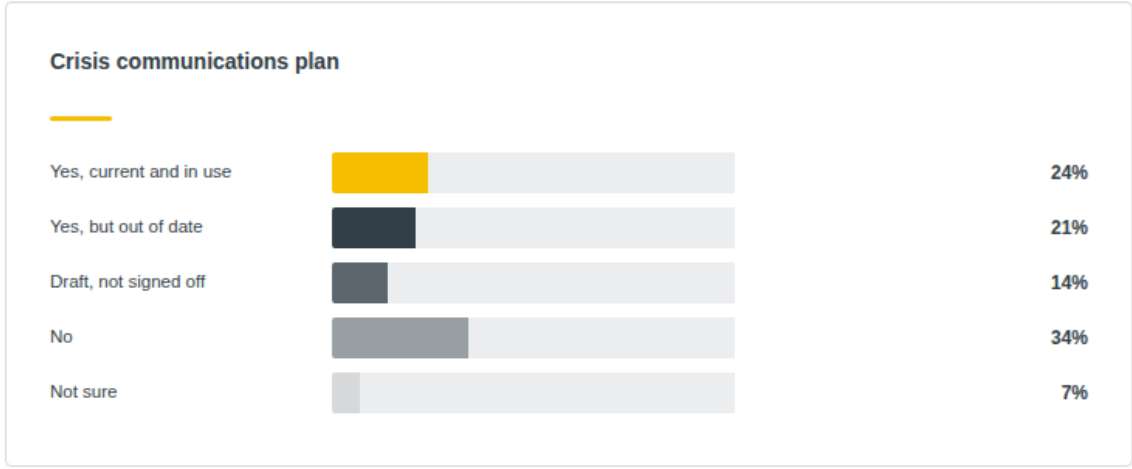
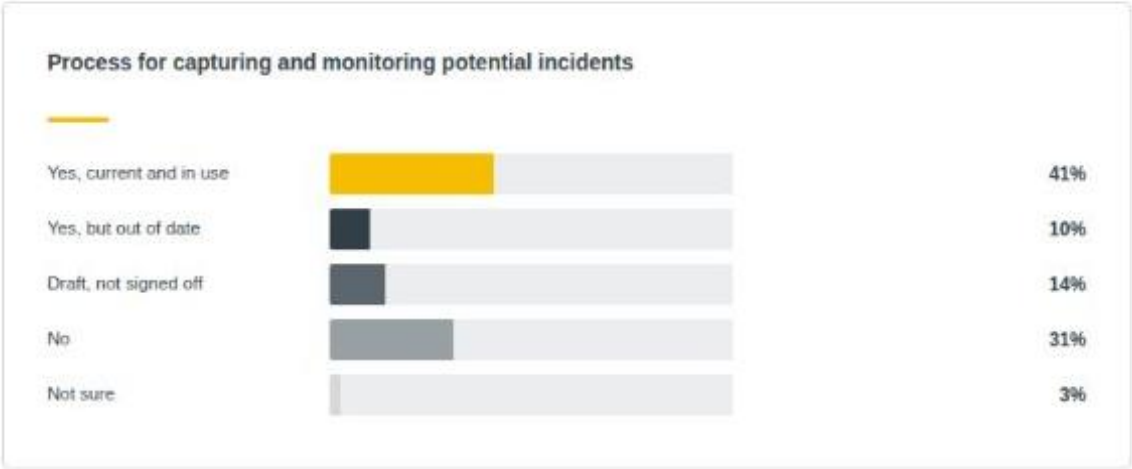
Preparedness: Do you think your organisation is ready for a crisis?

The risk register is the strongest element with 72 per cent saying they have one that is current and in use. This is a relatively strong baseline and what you would hope any organisation would have as part of its strategic plan.

However, as we often find, a list of potential problems and broad mitigations does not translate into the tools or knowledge needed to act on that risk.

Incident monitoring – the early warning system that allows organisations to spot a crisis before it escalates – drops to just 41 per cent for “current and in use”. Nearly a third have no process of collecting and assessing potential issues at all, while 10 per cent are working from one that is not kept up to date. This creates a critical blind spot: organisations may only recognise a crisis once it has already escalated.

The crisis communications plan – the operational document that tells people what to do when a crisis actually hits – is the weakest link. Only 24 per cent have a current, in-use plan. Whereas 34 per cent have no plan at all and 21 per cent are relying on something they know is out of date.



Preparedness: Do you think your organisation is ready for a crisis?

Recommendation #1

Some 55 per cent of organisations face a genuine crisis without a reliable, current plan in place.

The gap between knowing the risks and having a plan to manage them is the defining finding of this survey.

To resolve this, prioritise the development of clear, operational crisis communications plans that move beyond mere risk identification.

Awareness alone is not sufficient – it must translate into practical tools that can be used under pressure.



Roles, responsibilities and testing: Who is responsible for what during a crisis?

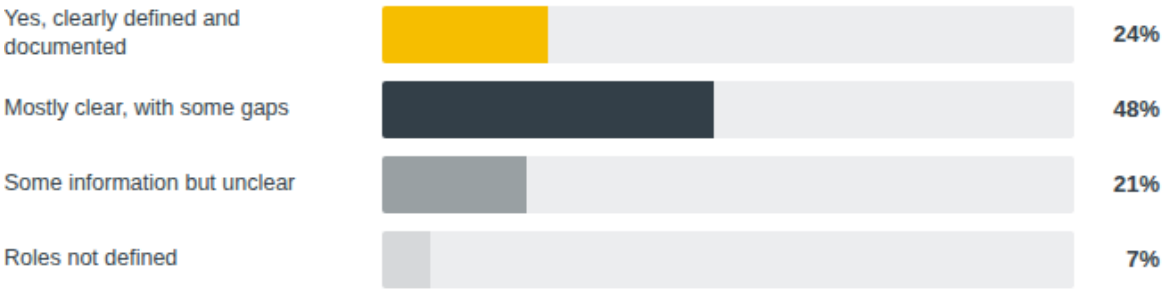
Only 24 per cent have clearly defined roles and responsibilities for a crisis scenario. The largest group (48 per cent) say that roles and responsibilities are mostly clear but with some gaps.

One would assume that it would be the organisations with a comms plan that felt roles and responsibilities were clear. However, it was a mixed bag. Some with a comms plan were still lacking clarity, while others without a plan felt that they knew who was responsible for what in a crisis.

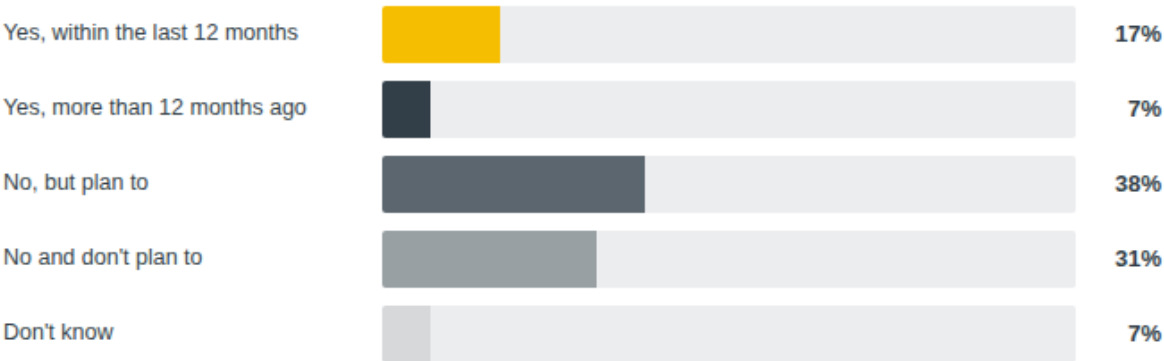
Plan or no plan, our experience shows that when an organisation is under pressure, these gaps tend to become critical: unclear roles and decision-making authority slow response, create confusion and can make a manageable situation much worse.

Testing a crisis comms plan ahead of an actual crisis will help identify any weaknesses in the process. However, 31 per cent of respondents have no plan to test at all, while seven per cent had tested it more than 12 months ago. Only 17 per cent of respondents had tested their plan within the last 12 months.

Clarity of roles and responsibilities in a crisis



Has your organisation ever tested its crisis communications plan?



Preparedness: Do you think your organisation is ready for a crisis?

The lack of testing is particularly worrying because checking plans is not a luxury – it is the mechanism that reveals whether your activities will actually work, whether people know their roles and whether teams can move at the speed a crisis requires.

Not running a testing exercise risks discovering gaps for the first time under real pressure, something that could make or break an effective crisis response.

Recommendation #2

Test your plans regularly.

Plans only become effective when they are rehearsed, with roles clearly understood and decision-making processes tested in practice.

Without this, gaps are likely to emerge at the point of crisis.



How well are you prepared for different types of risk?

Operational

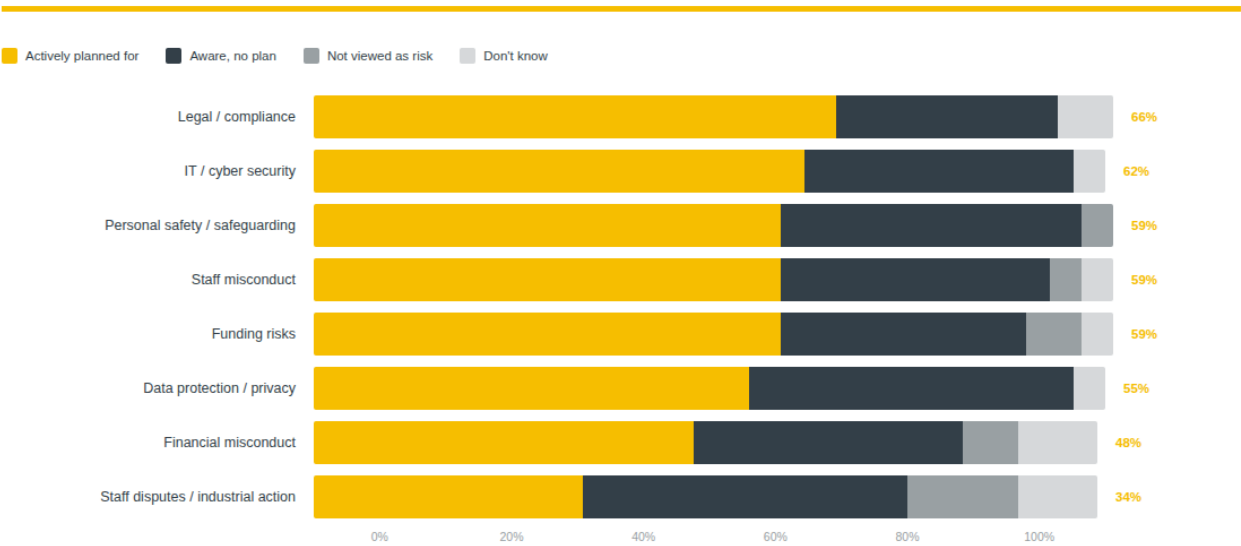
Operational risks – those involving internal systems, people and finances – show the strongest planning rates of the three categories. Legal and compliance issues (66 per cent actively planned) and IT/cyber security (62 per cent) are the best-prepared areas, which may reflect regulatory pressure and the high visibility of cyber incidents in recent years.

Staff disputes/industrial action stand out as the most neglected operational risk area – just 34 per cent actively plan for it, 14 per cent do not view it as a risk at all and 10 per cent simply do not know. Given that internal disputes can quickly become public, reputational issues, this gap in planning represents a material communications risk as well as an operational one.

Communications

Planning for communication-specific risks – such as negative/hostile media coverage or public backlash – is markedly weaker. No category exceeds 52 per cent actively planned and several fall below 25 per cent.

Operational risks — to what extent does your organisation plan for these?



How well are you prepared for different types of risk?

Coordinated attacks and harassment – an increasingly common feature of the online environment – is the least planned-for communications risk, with only 17 per cent actively preparing and 24 per cent not viewing it as a risk at all. Given the speed with which online pile-ons can escalate, the absence of preparation here is a real risk for many organisations.

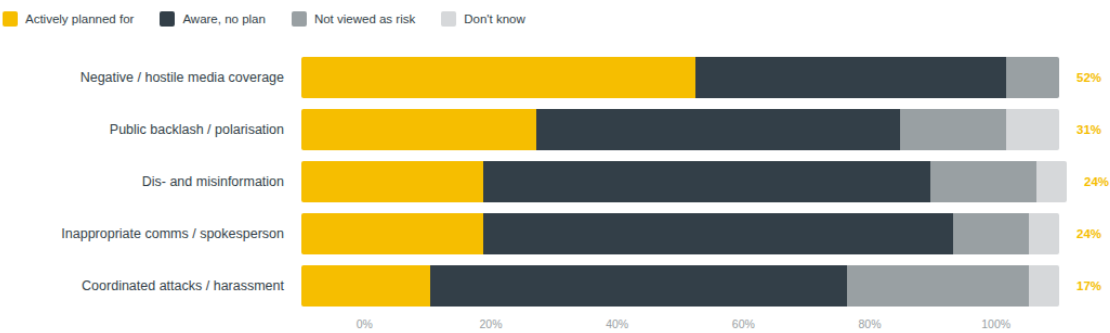
Dis– and misinformation is also notable: despite being one of the defining comms challenges of the current era, 59 per cent are aware of the risk but have no plan to address it.

Social and political

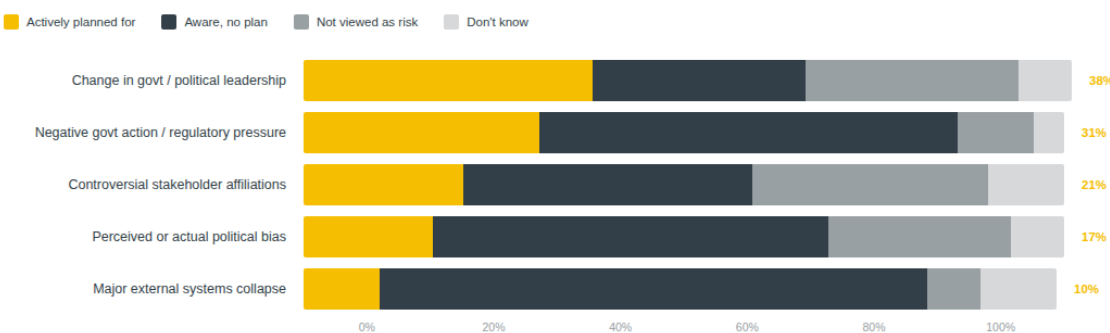
Social and political risks are the least planned-for category overall. The data reveals significant blind spots in areas that many organisations are likely to encounter.

Major external systems collapse – fuel shortages, widespread IT or energy outages – is the single most neglected risk in the entire survey. Only 10 per cent are actively planning for it, 72 per cent are aware but have no plan, and 10 per cent do not know where they stand.

Communications risks — to what extent does your organisation plan for these?



Social and political risks — to what extent does your organisation plan for these?



How well are you prepared for different types of risk?

As dependency on digital infrastructure increases and the geopolitical environment becomes more unstable, this represents a growing and largely unmanaged exposure.

Taken together, despite high potential impact, planning is weakest when it comes to communications and external risks compared to operational risks, which are relatively well covered.

Recommendation #3

Balance planning efforts across all risk areas according to their potential impact.

And while social and political risks are beyond an organisation's control, this shouldn't stop efforts to prepare for how to communicate should a major event of this nature occur.



How confident are you that you can respond to different types of risk?

Operational

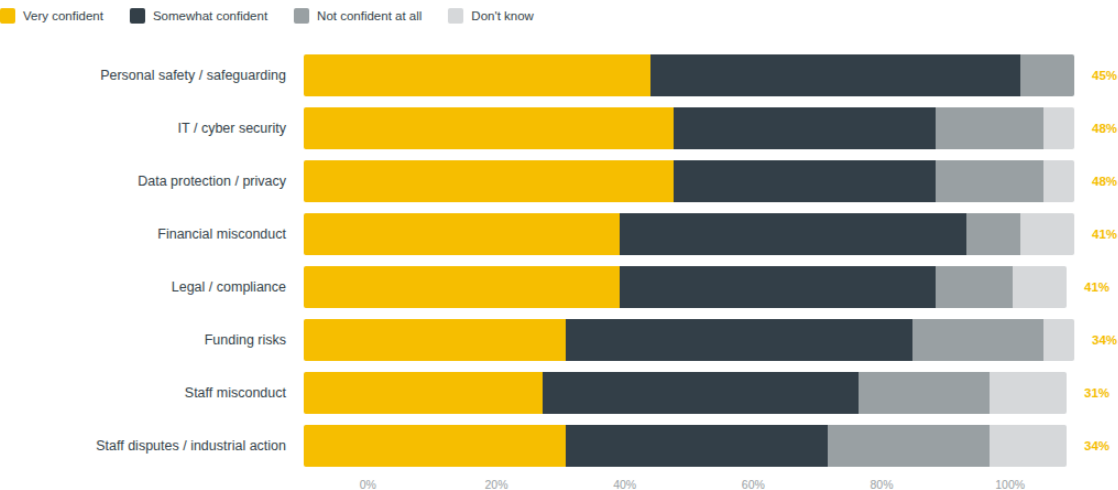
Confidence is highest for operational risks, broadly reflecting the stronger planning rates in this category. Personal safety (45 per cent very confident), IT/cyber (48 per cent) and data protection (48 per cent) sit at the top.

However, confidence figures across the board are higher than planning data would suggest is warranted. For example, 62 per cent actively plan for IT/cyber while 48 per cent feel very confident in their response – a reasonable match. But for data protection, 48 per cent actively plan for these risks, while a significant proportion report having no plan or relying on one that is out of date. What this tells us is that there is a disconnect between perceived and actual preparedness.

More broadly, the data indicates that self-reported confidence does not always align with the presence of robust, up-to-date planning, reinforcing the risk that organisations may feel more prepared than they are in practice.

Staff disputes and misconduct generate the lowest confidence in this category, with 17–21 per cent not confident at all, which is consistent with being the least-planned operational risk.

Operational risks — how confident are you in your organisation's ability to respond?



How confident are you that you can respond to different types of risk?

Communications

Confidence drops notably for communications risks. Across all five communications risk areas, “very confident” responses fall between 14 per cent and 31 per cent – considerably lower than for operational risks.

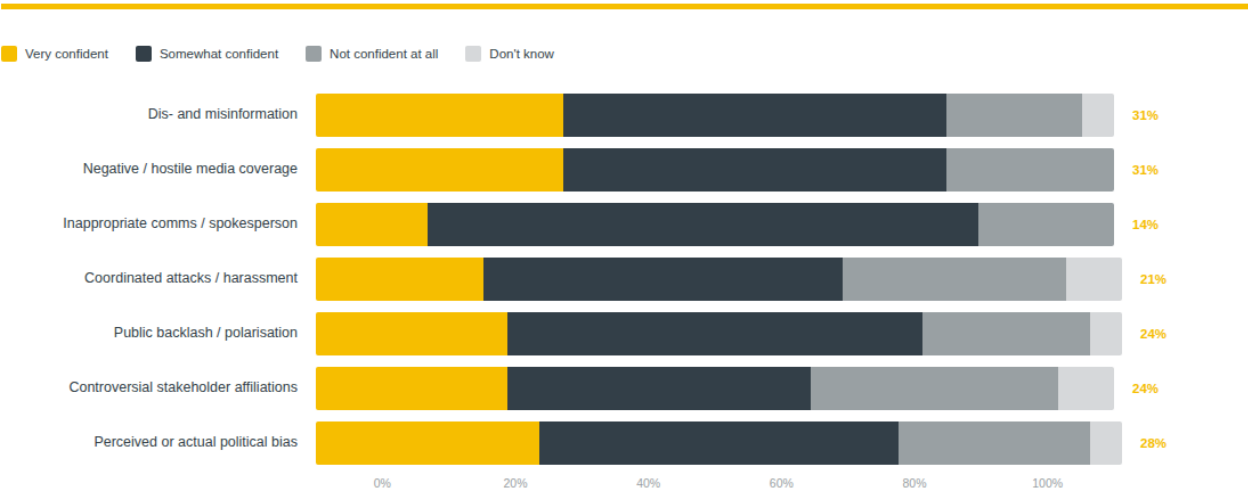
The most striking finding is that only 14 per cent feel very confident about their ability to respond to an inappropriate communications incident or spokesperson error – despite this being one of the most controllable and most preventable risks. Media training, approved spokesperson protocols, and clear sign-off procedures are all established and accessible tools; the gap suggests underinvestment rather than inherent difficulty.

Coordinated attacks and harassment produces the highest “not confident at all” response (28 per cent) in this category, mirroring the low planning rates seen earlier.

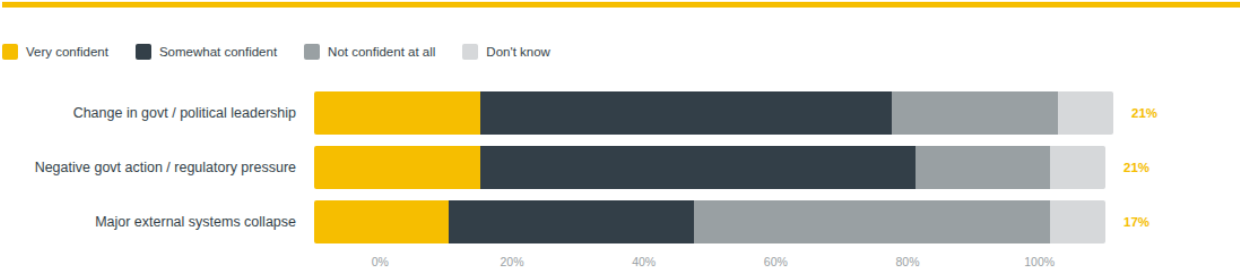
Social and political

Reflecting the planning results, confidence in the social and political risks category is lowest across the board.

Communications and social risks — how confident are you in your organisation's ability to respond?



Social and political risks — how confident are you in your organisation's ability to respond?



How confident are you that you can respond to different types of risk?

Major external systems collapse is the single lowest-confidence risk across the entire survey – 45 per cent are not confident at all, and only 17 per cent feel very confident. This is entirely consistent with having the lowest active planning rate of any risk area.

Government change and negative regulatory action show broadly similar confidence profiles: around 21 per cent very confident and 17–21 per cent not confident at all. These are foreseeable, often anticipated risks, yet confidence remains modest.

Across all three sections, “somewhat confident” is the most common response – suggesting organisations feel capable in principle but may struggle in a genuine high-stakes situation.

Recommendation #4

Focus on aligning perceived readiness with actual capability, ensuring that confidence is grounded in tested plans, defined roles and practical experience.



Biggest fears

We asked respondents to share in their own words what they are most worried about in relation to their ability to respond to a communications crisis. Six clear themes emerged.

1. Resourcing and capacity

The most consistently raised concern is structural: small teams, limited budgets and the absence of out-of-hours arrangements leave organisations exposed. Day-to-day workload means crisis preparedness is perpetually deprioritised.

One respondent captured the anxiety precisely: it is not the ability of the team that they worry about, it is the speed now required before something escalates, particularly in our social media age. The volume of work required to deliver day-to-day communications and the limited resources available mean that no one has the capacity to think about potential risks ahead.

2. Reputational and funding crises as the same event

For many respondents – particularly those in the charitable and third sector – a reputational crisis is inseparable from a funding crisis. Donors, statutory funders and trustees all factor into the calculus of a crisis response in ways that make decision-making more complex and the stakes higher.

3. Decision-making under pressure

A specific worry centres on what happens when the clock is running: risk-averse senior leaders, slow sign-off processes and unclear accountability.

The concern is not just about having a plan, but about being empowered to execute it quickly. One respondent identified the conflict between making timely statements and the caution of senior leadership under pressure.

4. Plans that exist but are not embedded

Several respondents acknowledge that plans have been handled previously, but on an ad hoc basis rather than through documented, rehearsed processes. Getting plans formally approved and signed off – not just drafted – is a recurring frustration. The gap between “we have something” and “we have something that works” is where most organisations sit.

Biggest fears continued

5. Key person dependency

A quiet but significant vulnerability: several respondents identify the risk of their most experienced communicators being unavailable when a crisis hits. In small teams, this is a scenario that is both plausible and largely unplanned for.

6. Sector-specific complexity

Respondents working in politically contested or adversarial environments flag that their communications baseline is already difficult – every response carries added complexity when the organisation's purpose itself is contested. This makes crisis planning harder and the consequences of getting it wrong more acute.

These concerns are not hypothetical – they reflect structural pressures facing many organisations.

Recommendation #5

Invest in planning, resourcing and decision-making processes. Don't rely on informal or reactive approaches.



Conclusion



Conclusion: Connecting preparedness, confidence and capability

Plans vs confidence: confidence outpaces capability

We would expect organisations with a current crisis communications plan to feel more confident in their ability to respond. The data only partially supports this.

Respondents with a current, in-use plan do report higher levels of confidence overall. However, the difference is not as pronounced as might be expected. A notable proportion without a current plan – or with an outdated one – still report moderate to high confidence in their ability to respond.

This reveals a critical disconnect: confidence consistently exceeds demonstrated preparedness. In practical terms, many organisations appear to be relying on experience, judgement or informal ways of working rather than structured, tested plans. While this may work in lower-pressure scenarios, it introduces significant risk in fast-moving or high-stakes crises.

Testing vs clarity: practice makes perfect

A clearer relationship emerges when looking at testing. Organisations that have tested their crisis communications plans within the last 12 months are significantly more likely to report that roles and responsibilities are clearly defined.

In contrast, those who have not tested – or do not have a plan to test – are far more likely to describe roles as only “mostly clear” or “unclear”. This reinforces that clarity is created through practice, not documentation alone.

Testing appears to act as the mechanism that turns theoretical roles into understood, actionable responsibilities. Without it, gaps in accountability and decision-making remain hidden until exposed under pressure.

Risk awareness vs planning: the capability gap

Across multiple risk areas, the data reveals a consistent pattern: awareness of risk is not translating into active plans, particularly when considering comms and external risks:

- Dis- and misinformation: a majority of respondents recognise this as a risk, yet most have no plan in place to address it.
- Coordinated attacks and harassment: awareness is relatively high, but active preparation is among the lowest of all risk areas.
- Major external systems collapse: one of the most widely recognised risks, but the least planned-for.

Conclusion: Connecting preparedness, confidence and capability

This creates what can be described as a capability gap: organisations understand the risks they face but lack the operational tools to respond effectively.

The implications are significant. In each of these areas, crises are likely to escalate quickly, often in public, leaving little time to design a response from first principles. Without pre-existing plans, organisations are forced into reactive decision-making, increasing the likelihood of missteps.

Bringing it together: a system under strain

Taken together, these cross-cutting findings point to a broader structural issue.

- Confidence is often decoupled from actual preparedness.
- Clarity of roles is dependent on testing, not just planning.
- Risk awareness is not being converted into operational capability.

This implies that the sector understands of crisis risk, but is lacking in the systems, processes and investment required to act on that understanding.

There is a need to move from perceived readiness to demonstrated capability – ensuring that confidence is grounded in tested plans, clearly defined roles and practical experience.

This requires a deliberate shift from informal, experience-led approaches to structured, rehearsed crisis response systems that can perform under pressure.

Eight steps to crisis comms success

1. Close the gap between risk and response

Develop practical crisis comms plans that set out what to do, who is responsible and how decisions will be made in real time. Join the dots between potential risks and the clear, actionable plans needed to manage them.

2. Test plans regularly

Run regular simulations or scenario exercises on a regular basis to test crisis comms plans. Testing is the mechanism that reveals gaps, builds confidence and ensures teams can operate at speed.

3. Define and rehearse roles and decision-making

Establish clear roles, responsibilities and lines of authority in advance to support a speedy response – i.e. before a crisis, not during one.

4. Strengthen preparedness for comms risks

Invest in planning and training for misinformation, online attacks and reputational crises. These are increasing in frequency and impact.

5. Build resilience beyond individuals

Distribute capability across teams to reduce dependency on any one person, particularly in smaller organisations.

6. Align confidence with capability

Confidence without capability is a risk. Shift from informal, experience-led approaches to structured, rehearsed crisis response systems.

7. Address structural barriers to readiness

Limited capacity, competing priorities and lack of senior buy-in are persistent challenges. Make crisis comms a core organisational priority, with appropriate resourcing, leadership support and integration into wider planning.

8. Lean on experts

You don't have to face this alone. Agenda can help. From a risk register or scenario plan and incident monitoring process, to a full crisis communications plan and 24/7 crisis response, we can be by your side when it matters most.

Agenda

**Don't wait for the crisis.
Make a plan. Train your team.
Prepare your response.**

**Because reputation is easier
to protect than rebuild.**

Find out how we can help
hello@your-agenda.com

