



BT Response to:

Ofcom's procedural guidance
consultation dated 12 May 2026

4 August 2026

Overall position

BT welcomes the opportunity to respond to this consultation¹ and supports Ofcom's objective of maintaining effective oversight of telecoms security. We agree that the framework should continue to evolve where doing so improves Ofcom's regulatory insight in a proportionate manner.

BT's response focuses on three themes:

- **Clarity** – the reporting framework should be capable of being applied consistently by the operational teams who make reporting decisions, often at pace and while an incident is still unfolding. Several of the current requirements can only be applied by cross-referring between multiple overlapping thresholds, categories and timelines, which makes consistent, real-time decision-making difficult.
- **Proportionality** – new requirements should be operationally workable and their benefits should be weighed against their cost. Responding to Ofcom's information-gathering already carries a material burden: BT estimates that each of the three major TSA s135 notices issued to date has cost at least half a million pounds to respond to.
- **Regulatory value** – reporting obligations should be targeted at the information that delivers the greatest regulatory insight. Where the reporting boundary is drawn too broadly, a higher volume of lower-significance notifications risks diluting Ofcom's visibility of the incidents that matter most.

Any additional reporting or data requirements should be clearly linked to a specific regulatory objective and supported by a proportionate assessment both individually and cumulatively taking all reporting as a whole.

Our principal concern is that the consultation assesses each proposed change in isolation rather than in the round. Taken together, the proposals would require providers to supply more information, more frequently and in greater detail, and the consultation does not yet demonstrate that this would materially improve Ofcom's ability to identify, assess or respond to the incidents presenting the greatest risk.

This is inconsistent with Ofcom's Growth Duty, which recognises that:

*"a disproportionate approach, conversely, goes far beyond what is necessary and can stifle productivity as it ties up business and regulator's time and resources that could be more productively deployed elsewhere."*²

BT therefore encourages Ofcom to test the cumulative impact of the proposals and, where the regulatory benefit is not clearly established, to refine them so that the final framework remains both effective and proportionate. In that spirit, BT has included a practical decision tree at Annex A (based on Ofcom's proposed changes) and a proposed trade-media list at Annex B to help make the regime workable in practice.

The remainder of this document sets out BT's responses to Ofcom's specific questions.

Question 1 – Compliance monitoring

BT supports an active, risk-based approach to supervision and recognises that Ofcom should have the tools needed to focus on areas of greatest risk. In principle, BT welcomes Ofcom's intent behind using assessment notices³, especially where they are a more efficient and effective way to enable Ofcom to gain a better understanding of how CPs have implemented the TSA measures. However, Ofcom's consultation lacks clarity on how these would operate in practice, in particular on how and when Ofcom would expect to use an assessment notice instead of an information notice.

Ofcom's use of assessment notices must fit within a coherent and streamlined framework. Without clear boundaries, there is a risk of duplication and an increase (rather than decrease) in the operational burden on operators, thereby undermining the proportionality Ofcom is seeking to achieve. Responding to s135 information notices already requires significant cross-functional resource and coordination, with a material operational and cost impact. BT estimates that each of the three major TSA s135s issued by Ofcom to date has cost at least half a million pounds to respond to. In that context, BT does not accept Ofcom's suggestion (paragraph 3.14) that assessment notices are inherently less burdensome.

¹ [Consultation on Ofcom's draft general statement of policy under s105Y of the Communications Act 2003 \(Ofcom's procedural guidance\)](#).

² See Driver 5: Efficiency and Productivity in [Growth Duty: Statutory Guidance - Refresh](#), 21 May 2024, Department for Business and Trade

³ See consultation paragraphs 3.13–3.15 and draft guidance paragraphs 3.37–3.39.

To ensure the regime remains targeted and workable, the final guidance should include clear criteria for when assessment notices will be used, how they will be coordinated alongside existing processes, and what safeguards will prevent duplication and unnecessary disruption.

BT also considers that assessment notices, information notices and other formal assurance activities should be followed by timely feedback from Ofcom. Providers invest significant resources in these exercises, yet BT has received little substantive feedback to date. Ofcom's supervision programme would deliver greater regulatory value if it shared clear observations, good practice, areas for improvement and common themes that providers could use to inform further development.

Before issuing the first TSA s135, Ofcom undertook a voluntary time-limited pilot with three Code of Practice measures. BT suggests that a similar exercise might prove helpful to both Ofcom and operators by providing a practical way to test whether the approach delivers the intended benefits and adapt it accordingly before wider implementation.

Question 2 – Testing

BT supports testing as part of the security framework. TBEST is a well-established mechanism which BT has previously participated in and supports its continued use.⁴

Any further testing should be targeted, risk-based and designed around clear gaps in assurance. Where providers already have mature capability in place to carry out internal testing, red-teaming or other assurance activity, Ofcom should take that into account before requiring additional work.

The final guidance should set out what triggers additional testing, how often providers should expect it, and how duplication with existing assurance will be avoided.

Question 3 – Security incident reporting thresholds and criteria

BT agrees that reporting criteria should be clear and consistently applied. Determining whether an incident is reportable, its severity classification and the applicable reporting timeline often requires navigation across multiple overlapping provisions rather than a single end-to-end framework. BT has historically found this challenging to operationalise and, to support consistent decision-making, has developed a decision tree at Annex A to help operational teams rapidly determine if and when an incident should be reported. We would welcome Ofcom's feedback on our understanding of Ofcom's proposed changes to the guidance on incident reporting.

Several proposals introduce additional qualitative factors, examples and reporting triggers alongside the existing threshold framework. We provide details on each of these below.

While these may be reasonable individually, taken together they increase complexity and are likely to increase reporting volumes and regulatory burden. BT is concerned that this may not be matched by a corresponding improvement in regulatory insight, as greater volumes of lower-significance notifications risk diluting the visibility of genuinely significant incidents and reducing the overall effectiveness of the reporting regime. Greater clarity on the reporting boundary, together with a stronger emphasis on objective and operationally workable criteria, would help ensure that the regime remains proportionate and effective.

Additionally, we understand that the clarification at paragraph 3.41, that incidents with a significant effect remain reportable even where they meet no specific threshold, is intended to reflect the underlying duty in section 105K rather than to create a new obligation. Presented as a standalone catch-all in the guidance, however, and without further explanation of what a significant effect outside the specified thresholds might look like, it creates real uncertainty for providers applying the guidance, and it is likely to encourage defensive over-reporting. We ask Ofcom to provide qualitative guidance or worked examples of the kinds of incident it has in mind, so that the standard can be applied consistently.

⁴ See 3.16–3.17 and reflected in draft guidance paragraphs 4.5–4.7.

Question 3(a) – Informing users

Section 105J requires a provider to inform users where there is a “significant risk of a security compromise” that may adversely affect them, and to take steps that are “reasonable and proportionate” to bring relevant information to their attention, including any action users can take to prevent or mitigate the impact.

BT supports this approach. The statutory test is appropriately targeted at situations where users may be adversely affected and where providing information enables them to take action to protect themselves or reduce potential harm.

BT welcomes the guidance in Annex 7 (paragraphs 5.1–5.6)⁵, which explains the factors providers should consider when deciding whether and how to communicate with users. In BT’s view, the guidance should continue to reflect the principle that user notifications are most valuable where they provide clear, actionable information to users who may be affected by a security compromise.

BT therefore supports an approach that focuses notifications on circumstances where there is a genuine risk of adverse impact to users and where communication is likely to assist those users in preventing, mitigating or responding to that risk, consistent with the “reasonable and proportionate” standard set out in section 105J.

Question 3(b) – Cyber security incident reporting

BT supports Ofcom having appropriate visibility of material cyber security incidents and relevant threat trends. However, cyber operations generate a high volume of routine activity — including attempted attacks, scanning, vulnerabilities, indicators of compromise, threat intelligence and early-stage triage — much of which does not result in a security compromise or material impact. If the reporting boundary is drawn too broadly, it risks generating a high volume of low-value notifications and reducing Ofcom’s ability to identify genuinely significant incidents.

BT already goes beyond its formal reporting obligations in this area. It formally notifies Ofcom of P1-severity incidents in the moment, and separately provides Ofcom with regular cyber threat intelligence on a voluntary basis through its monthly cyber threat levels report. That monthly report also shares details of P2 and P3 incidents directly impacting BT Group, alongside relevant vulnerabilities, threat-actor activity and trends affecting the telecoms sector — giving Ofcom visibility of the wider threat landscape over and above formal security compromise reporting under section 105K. BT intends to continue providing this monthly report to Ofcom.

Given that BT already provides this information to Ofcom on a voluntary basis, BT considers that the proposed changes in paragraphs 5.13–5.15 of the guidance — particularly the treatment of pre-positioning attacks — are intended primarily to formalise the provision of information Ofcom already receives through this established route. BT would welcome further engagement with Ofcom to confirm that understanding, and to clarify how pre-positioning is to be defined and distinguished from routine background activity or vulnerabilities under management.

Question 3(c) – Which security compromises to report

BT supports the use of objective thresholds because they provide an operationally workable basis for determining whether an incident should be reported. In practice, however, BT has found the way the guidance is drafted challenging to follow. Providers must cross-refer between multiple overlapping thresholds, severity categories and reporting timelines before they can determine whether an incident is reportable and, if so, when it must be notified.

That complexity matters because reporting decisions are made by operational teams, often at pace and while an incident is still being assessed. BT has therefore developed the decision tree at Annex A, which sets out BT’s understanding of how the reporting framework operates in practice. BT would welcome Ofcom’s confirmation that the flowchart reflects the intended operation of the guidance. This would help ensure that providers and Ofcom are applying the same reporting logic and reduce the risk of inconsistent interpretation.

Separately, BT would welcome clarification on the role of the “significant effect” test in paragraph 5.18 of Annex 7. The draft guidance appears to suggest that an incident may be reportable under section 105K even where it does not meet any published threshold. BT is concerned that this risks creating an open-ended and subjective reporting obligation that undermines the purpose of having clear thresholds. BT does not consider this additional requirement has been justified and believes it should be removed from the final guidance. If retained, Ofcom should provide clear and objective criteria governing when a below-threshold incident is expected to be reported under section 105K.

⁵ See 5.3–5.9 of Annex 7 and the discussion at consultation paragraph 3.19

Question 3(d) – Repeat security compromises and severe weather

Linking dispersed incidents: ⁶BT can report on the overall impact of a widespread event, but only through post-event analysis. During a live incident the operational priority is restoring service, and linking geographically dispersed outages into a single view in real time is not practical. BT therefore asks Ofcom to confirm that aggregated reporting of this kind is expected on a post-event basis, not in real time.

Severe weather: “Severe weather” is used as an example but is not defined, which makes it unclear when the aggregation expectation is triggered. The final guidance should define “severe weather” by reference to objective criteria, such as named storms or recognised Met Office warning categories.

Question 3(e) – Critical reporting of media coverage

BT is not persuaded that media coverage is a reliable proxy for incident severity. Coverage may be influenced by factors unrelated to the scale, duration or customer impact of an incident and can be driven by local interest, timing or wider public attention. BT therefore considers that media coverage is more appropriately treated as contextual information rather than as an independent trigger for critical classification.

Furthermore, the extension of the three-hour reporting trigger to local, national and trade media coverage,⁷ in practice, suggests that providers proactively monitor a broad range of media sources in order to identify reportable incidents within the required timeframe.

BT already operates a national mainstream media monitoring process based on a defined list of publications. This reflects a pragmatic approach agreed with Ofcom set out in BT's 16 March 2018⁸ correspondence. BT therefore considers that Ofcom should maintain an agreed list of outlets for proactive monitoring and would support extending that list to include the suggested telecoms and infrastructure trade publications set out in Annex B.

Local media is fragmented, high-volume and difficult to monitor consistently within a three-hour window. If Ofcom intends to introduce a proactive monitoring obligation, its scope should be clearly defined by way of a pre-determined list of publications. However, BT does not consider proactive monitoring of local media necessary to achieve Ofcom's objective and is not persuaded that it would materially improve Ofcom's understanding of incidents.

Customer and network impact should remain the primary basis for determining whether an incident is critical. Media coverage may provide useful context but should not override objective measures of severity. BT will continue to notify Ofcom of relevant local coverage where it becomes aware of it.

Question 3(f) – MNO numerical thresholds

BT supports Ofcom's objective of improving visibility of outages that disproportionately affect rural communities.

⁹BT's existing reporting already captures significant events, and if Ofcom wished providers to distinguish rural from urban impact within that reporting, BT would support that approach.

A single-site trigger, however, would not reliably identify the incidents Ofcom is seeking to capture. It risks generating a high volume of low-value notifications while doing little to improve visibility of genuinely significant impacts on rural communities. Three features of the proposed threshold illustrate the problem:

- **Classification does not track customer impact.** A site's rural classification depends on the location of the mast rather than the community it serves, creating a risk of both over- and under-reporting.
- **Restoration times reflect operational reality, not resilience failings.** Rural sites are inherently more challenging to restore because of geography, access constraints and longer engineer travel times. An eight-hour threshold may therefore capture outages that reflect the practical realities of operating rural infrastructure rather than any resilience or security failing.
- **Shared sites generate duplicate reports.** Where a shared rural site fails, the same underlying event may be reported separately by multiple operators, inflating volumes without adding insight.

If Ofcom's objective is to identify where rural communities are being disproportionately affected, a measure focused on the scale, duration and community impact of an outage would target that far better than a single-site trigger. BT

⁶ See consultation paragraph 3.46 and draft guidance paragraph 5.22.

⁷ See reportable incident criteria in draft guidance paragraph 5.19 and the critical incident criteria in paragraph 5.28.

⁸ See BT letter to Ofcom dated 16 March 2018, from Alex Quinn to Mike Lee and Ben Willis

⁹ See proposed mobile reporting thresholds described in consultation paragraphs 3.26–3.35 and draft guidance paragraph 5.19 (Table 2).

therefore asks Ofcom to work with the MNOs to develop a more proportionate mechanism that captures genuinely significant rural outages while avoiding unnecessary reporting volume.

BT is also concerned that the proposed site-based thresholds may capture incidents that do not represent genuinely significant service disruption. In particular, a two-hour threshold for multi-site outages may be short relative to common transmission and backhaul faults, many of which are routinely restored within normal operational timescales. BT therefore encourages Ofcom to consider whether the proposed thresholds are appropriately calibrated to differentiate between routine operational incidents and outages that warrant regulatory reporting. In doing so, Ofcom should take account of the operational realities acknowledged in its June 2026 Network and Service Resilience Guidance¹⁰, including the presence of single points of failure in access networks, the cost of building highly resilient rural infrastructure and the limitations of some legacy network technologies. These factors mean that extended site outages may not necessarily indicate a resilience or security failing.

Consistency with Ofcom's updated Network and Service Resilience Guidance (published in June 2026)

BT notes that Ofcom's Network and Service Resilience Guidance, also uses the current reporting thresholds as useful architecture, design and operational targets and cross-refers to the existing section 105Y reporting framework. It is therefore unclear whether the threshold changes proposed in this consultation are intended solely to amend incident notification requirements or whether they are also intended to alter the resilience and network design targets against which providers are expected to operate. If the latter, BT disagrees. Reporting thresholds are designed to identify incidents that warrant regulatory notification and are not necessarily an appropriate proxy for the level of resilience that providers should be expected to engineer into their networks. Any proposal to alter network design expectations should be consulted on explicitly and supported by a separate assessment of costs, benefits and operational feasibility.

Therefore, BT encourages Ofcom to ensure that any changes resulting from this consultation are reflected consistently across its wider resilience and security guidance. In particular, if the reporting thresholds are amended, corresponding updates may be required to the Network and Service Resilience Guidance to avoid uncertainty arising from conflicting reporting and resilience expectations.

Question 4 – Reporting templates

BT supports standardised templates where they improve consistency, comparability and data quality, and has no concern with the existing location reporting requirements. BT's comments are directed at two things: the additional detail proposed for mobile incidents— particularly affected-site information and Global Cell IDs— and, more broadly, the overall level of detail the revised templates would require. These issues arise across both the 72-hour and monthly reporting routes. BT also has some practical points on the usability of the templates and how they should be introduced. Its comments on each follow below.

72-hour reporting: BT welcomes Ofcom's recognition that a report may be submitted before full information is available and updated as more information emerges (Annex 7, 5.41)¹¹, and that a postcode is expected only "where possible" (5.56). This reflects operational reality. For mobile and RAN incidents, accurate affected-site and Global Cell ID information may not always be available within the initial 72-hour reporting window and may only be established through subsequent analysis. BT asks Ofcom to confirm that this flexibility also applies to the new reporting fields, so that an initial report is not considered deficient where information is not yet available.

Monthly reporting: Monthly reporting allows more time for analysis, but the proposed changes still expand what providers must produce¹². BT comments below on the three aspects most likely to create practical challenges (consultation 3.52):

- **Level of detail:** BT notes that the proposed bulk reporting template appears to require a level of detail closer to that expected for higher-priority incident reporting. For moderate or bulk incidents, this could require significant input from IT service, incident management and operational teams without a clear corresponding benefit. BT asks Ofcom to explain why bulk reports need the same or a similar level of detail as 72-hour

¹⁰ See sections 3.3.1 and 4.2.1 in [Network and Service Resilience Guidance for Communications Providers](#), which acknowledge that "it can become costly to create highly resilient access networks" and that this domain "is likely to have single points of failure"; see also footnote 32 (noting that "some traditional 2G and 3G RAN components may not support the type of resilience mechanisms that we expect of 4G and 5G networks").

¹¹ See draft guidance paragraphs 5.41 and 5.56 and the associated changes to the incident reporting templates.

¹² See proposed template changes described in consultation paragraph 3.52.

reports, and to distinguish more clearly between information required for immediate regulatory action and information that is useful for later trend analysis.

- **Global cell IDs:** ¹³BT does not consider a separate monthly RAN cell dataset to be proportionate. Any such dataset would represent a point-in-time snapshot and may not reflect the precise network configuration at the time of an incident. As a more proportionate alternative, BT suggests adding relevant site identifiers and location data to its existing Connected Nations submission and providing that information quarterly rather than twice yearly. This would support Ofcom's analysis while avoiding the burden of maintaining a separate monthly reporting process.
- **Third party details:** BT has historically treated this field as relating to third parties affected by a security compromise and has provided relevant information on that basis where available. ¹⁴ The draft guidance does not appear to change that approach. BT would welcome confirmation that this remains the intended scope of the field.

Template usability and implementation: Given how much the usability of the templates affects the speed and completeness of the information that reaches Ofcom during an incident, BT encourages Ofcom to pilot the revised templates with a small group of provider volunteers before finalising them and allow a reasonable transition period before they take effect.

Question 5 – RAN cell data

BT understands Ofcom's aim of improving geographic insight into mobile incidents. ¹⁵ However, BT has concerns about both the scope and frequency of the proposed requirement. Ofcom's stated intent is to map the geographic impact of incidents using global cell IDs. However, the Cell Data Standard requires 40 data fields, many of which go beyond location information and relate to network configuration and operation. BT considers that the final guidance should explain how each category of information within the Cell Data Standard aids Ofcom's understanding of the geographic impact of incidents.

BT disagrees that this requirement will not create additional burden. BT does not currently provide a dataset of this kind to any third party on a monthly basis. In addition, some elements of the dataset may change over time, meaning a monthly submission would represent only a point-in-time snapshot and may not reflect the network configuration at the time of an incident.

There is also a terminology issue. Ofcom uses "cell sites", "RAN cells" and "global cell IDs" across the consultation, draft guidance and reporting templates. BT welcomes confirmation that the reporting thresholds operate at site level and asks Ofcom to provide greater clarity on the scope of the monthly dataset, supported by a glossary in the final guidance.

As a more proportionate alternative, BT suggests adding the Physical Site ID, Sector IDs and Easting/Northing of each site to its existing Connected Nations submission and providing this quarterly rather than twice yearly. This would provide Ofcom with regularly updated site location information to support geographic analysis while avoiding the burden of a separate monthly RAN dataset.

¹³ See Ofcom's proposal regarding Global Cell IDs and monthly RAN reporting, in consultation paragraph 3.53 and draft guidance paragraphs 5.59 and 5.61.

¹⁴ See proposed reporting template changes described in consultation paragraph 3.52 and the associated draft guidance.

¹⁵ See consultation paragraphs 3.53–3.55 and draft guidance paragraph 5.61.

Annex A – BT internal reporting decision flowchart

This Annex sets out BT's understanding of Ofcom's incident reporting requirements under section 105K in the form of a decision flowchart. Figure 1 reflects BT's interpretation of Ofcom's current guidance, and Figure 2 reflects BT's understanding of the changes Ofcom is proposing in this consultation, with those proposed changes highlighted in yellow.

Figure 1: BT understanding of current 105k Resilience reporting requirements

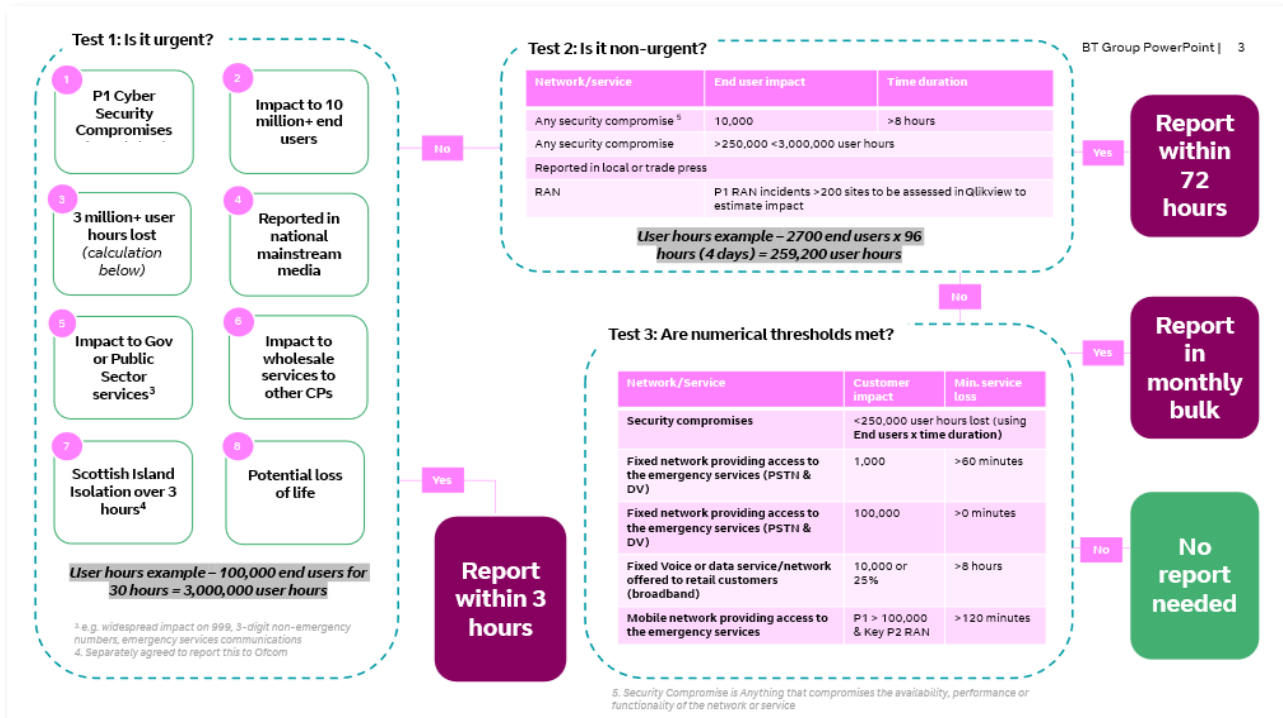
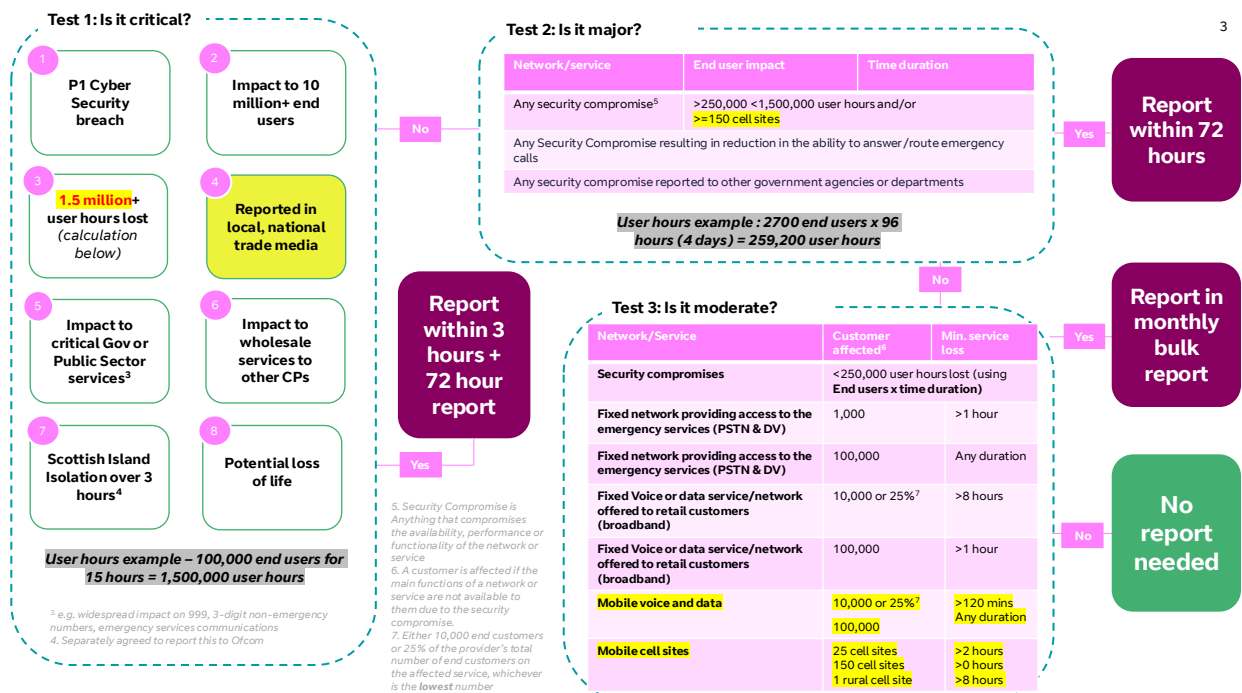


Figure 2: BT understanding of proposed 105k Resilience reporting requirements



Annex B – Media outlet reporting requirements

BT notes the existing list of media outlets covered by our current process:

National media and online outlets

Daily Express	Daily Mail	Daily Star
The Daily Telegraph	Evening Standard	Financial Times
The Guardian	The Daily Mirror	The Sun
The Times	The Mail on Sunday	The Observer
Sunday Express	Sunday Mirror	The People
The Sunday Telegraph	The Sunday Times	The Economist
The New York Times	International New York Times	Metro (London)
Daily Star on Sunday	Sky News (Web)	City AM
i (The paper for today)		

Broadcast media

BBC 1	BBC 2	BBC News
BBC World News	BBC Radio 2	BBC Radio 4
BBC Radio 5	BBC World Service	BBC Radio London
ITV 1	Channel 4	Five
Sky News	CNN	Bloomberg English
LBC 97.3	Capital	talkSport
talkRadio		

Trade publications

As set out in Question 3(e), BT considers that any proactive media-monitoring requirement should be supported by a pre-determined list of relevant publications. This could include telecoms trade publications such as Think Broadband.