

Your response

Question	Your response
Question 1: Do you have any comments on our proposed updates to our guidance on compliance monitoring?	Confidential? – N Overall position Sky supports Ofcom keeping its procedural guidance up to date now that the TSA framework has been operating for several years. However, we have concerns about the cumulative impact of the proposed monitoring programme, particularly where annual TSA section 135 notices continue alongside additional targeted section 135 notices and a potentially wider use of section 105O assessment notices. It is not clear that the proposed measures are consistent with the principle of proportionality. We ask that Ofcom identify what specific objective each measure is designed to achieve, and the analysis that identifies it as the least intrusive way of achieving that objective. Cumulative burden and sequencing of s135 notices Ofcom should recognise that targeted section 135 notices are an additional burden to the annual TSA section 135 process, not a substitute for it. Sky is already seeing significant resource pressure from targeted information requests, including recent requests relating to subsea cables and risks. These draw resource from teams seeking to make security improvements to our networks. We therefore ask that Ofcom sequences supervisory requests wherever possible and avoids concurrent or overlapping section 135 exercises unless there is a clear and urgent regulatory need. This approach would be consistent with the principle of proportionality, to which Ofcom is required to have regard by its statutory duties. Ofcom should also reuse evidence already provided through the annual TSA process and previous requests and identify where it is able to rely on existing evidence before requesting fresh material. The final guidance should include clearer expectations on coordination, forward planning, proportionality and cumulative burden, including how Ofcom will assess the

Question	Your response
	total impact of multiple monitoring activities in any given year. Assessment notices Sky is concerned that Ofcom’s use of assessment notices is moving from an escalation tool of last resort to a more routine supervisory tool. That is a significant shift because assessment notices can involve interviews, testing, site access, inspection of information and potentially provider-funded costs. Ofcom should explain the likely triggers for assessment notices, the criteria it will apply before using them, the notice providers can expect to receive, and the safeguards it will apply to scope, proportionality, confidentiality, operational stability and third-party dependencies. Where Ofcom proposes to use an assessment notice, Sky considers that draft notices should normally be provided for comment before finalisation, except in genuinely urgent circumstances. Ofcom should also explain how assessment notices will interact with voluntary TBEST activity. Where a provider is participating in, or has recently completed, a relevant TBEST or equivalent assurance exercise, Ofcom should take that into account and avoid requiring separate duplicative assessments unless there is a clearly articulated, risk-based reason. Sky also asks Ofcom to clarify how the cost-recovery provisions for assessments and inspection-type activity will operate in practice. In particular, Ofcom should explain what it considers to be “costs reasonably incurred by Ofcom in connection with the assessment”, whether those costs may include third-party assessment or testing vendors, and how providers will be given transparency over scope, estimated cost, procurement approach and cost control before an assessment begins. We ask that where a provider already has independent third parties to perform such testing that those third parties can be re-used. Ofcom should not assume that assessment notices will always be less burdensome than information notices. For live networks, operational systems and security controls,

Question	Your response
	the burden and risk associated with assessment notices can be significant, particularly where testing is involved. Ofcom should take account of provider evidence from existing assurance activity, control monitoring, governance forums, security quality gates and other compliance processes before deciding whether an assessment notice is necessary. Sky asks Ofcom to strengthen the final guidance so that the monitoring approach is clearly risk-based, proportionate, sequenced to avoid overburdening security teams, and supported by transparent scoping and engagement with providers. Ofcom could consider setting out a 'playbook' covering how it will use assessment notices in practice.
Question 2: Do you have any comments on our proposed updates to our guidance on testing?	Confidential? – N Sky broadly supports Ofcom simplifying the testing section and cross-referring to the Code and TBEST handbook where those documents contain the detailed technical guidance. Sky considers that any mandated testing - particularly testing that could risk causing a security compromise or service disruption - must be carefully planned with the provider in advance. Ofcom should provide detail on the objectives, scope, method, timing, safety controls, rollback arrangements and expected operational impact of the testing. This will ensure that the provider can assess risk and ensure the appropriate internal subject matter experts are available. This is especially important where testing is proposed urgently or where it may affect live services, shared infrastructure, customer-facing systems or third-party managed environments. In those cases, Ofcom should ensure that the timing and scope of testing are proportionate to the regulatory need and do not create avoidable operational or customer risk.
Question 3: Do you have any comments about our proposed changes to	Confidential? – N Overall position

Question	Your response
our security incident reporting thresholds and criteria, as described in paragraphs 3.19 to 3.48?	Sky supports clear and consistent incident reporting requirements, but considers that several of the proposed changes need further clarification to avoid over-reporting, duplicated reporting and disproportionate operational burden. Mobile and MVNO thresholds The proposed customer-based mobile thresholds are relevant to Sky Mobile as an MVNO. However, Ofcom should recognise that an MVNO does not have the same network visibility as an MNO, particularly for cell-site level data, point-in-time location impacts and detailed RAN information. Sky may be able to estimate customer impact using available operational data, historic baselines and information received from its host MNO, but it cannot identify and calculate all impacts with the same precision or speed as the MNO that controls the underlying network. MVNO information expectations Ofcom should clarify what information it expects MVNOs to provide, what is considered reasonable where the information is held by the host MNO, and whether 72 hours is realistic where the MVNO must obtain information from a third party. It may be challenging in practice for MVNOs to identify where the 10,000 customer threshold has been met where the provider has an aggregated customer view and does not hold the underlying network or cell-site data required to identify such impacts directly. Third-party dependencies Sky already reports incidents affecting Sky-service end users where a third party is involved in delivering the service. Sky supports reporting where the provider's own end users are affected and the relevant information is reasonably available. However, the final guidance should avoid creating duplicate reporting obligations. Providers should not be required to change our monitoring systems or obtain information that is not reasonably available from a third party. The guidance should be clear that providers may rely on the information available through existing operational channels, including

Question	Your response
	third-party service status information, while providing appropriate estimates where exact information is unavailable. Cyber reporting and pre-positioning Ofcom is proposing to clarify that "pre-positioning attacks" are reportable <i>"even where the provider's existing defences make a successful follow-on attack unlikely, <u>and even where multiple layers of defence remain between the attacker's initial access and the point at which significant harm could be caused</u>"</i>. This appears to go beyond the wording of section 105K(1)(b) of the Communications Act 2003, which requires providers to notify <i>"any security compromise within section 105A(2)(b) that puts any person <u>in a position to be able to</u> bring about a further security compromise that <u>would have</u> a significant effect on the operation of the network or service"</i> [Emphasis added]. Ofcom's proposed wording would place an unnecessary and disproportionate reporting burden on providers, over and above that contemplated under the Act, and so should be removed from the final guidance. Coordination with other cyber reporting routes Where incidents are already reported to the ICO, NCSC, law enforcement or other relevant authorities, Ofcom should explain how it will deconflict its reporting expectations and avoid duplicative reporting. This is particularly important for cyber incidents involving personal data, criminal activity or sensitive threat intelligence. Ofcom should also recognise existing cyber threat-intelligence sharing routes and the need for appropriately secure channels when handling sensitive cyber information. Critical threshold Sky notes the proposal to reduce the critical threshold from 3 million to 1.5 million user-hours. Ofcom should ensure the final guidance is clear on the rationale, particularly whether the appropriate metric is the number of user-hours or the number of users impacted by a compromise. The reference to MVNO subscriber base starting at 1.5 million does not necessarily translate directly to 1.5 million user-hours lost. Ofcom should also recognise that identifying when a user-hour threshold

Question	Your response
	has been crossed can be difficult during a live incident, particularly where a provider depends on third-party network information. Media trigger Sky considers that local or trade media coverage does not automatically make an incident critical regardless of operational thresholds and therefore cannot of itself lead to a security compromise being reportable under section 105K(1). It is therefore outside Ofcom's powers for the guidance to make such incidents reportable automatically. Media coverage may emerge after the event, may be incomplete or inaccurate, and does not always correlate with customer harm or urgency. Sky considers that media coverage would be more appropriately treated as a review or escalation factor, rather than an automatic criticality trigger. Criticality should remain tied to operational impact, customer harm, emergency-service risk, live cyber risk or urgent remedial action to define the circumstances in which security compromise do, or would, have a significant effect on the operation of the network or service in accordance with the governing legislation.
Question 4: Do you have any comments about the proposed changes to our reporting templates?	Confidential? – N Overall position Sky supports the principle of making reporting templates clearer and more consistent. In particular, aligning the 72-hour and bulk templates may help providers understand Ofcom's expectations. However, Sky is concerned that some proposed template changes may create disproportionate burden during live incidents and for lower-severity bulk reporting. Bulk reporting The proposed bulk reporting template appears to require a level of detail closer to 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. Ofcom should explain why bulk reports need the same or similar level of detail as 72-hour reports,

Question	Your response
	and should distinguish more clearly between information required for immediate regulatory action and information useful for later trend analysis. The current approach appears disproportionate. Third-party and cell-site fields Third-party details should only be required where they are known and reasonably available to the provider. Providers should not be required to obtain detailed third-party operational data beyond existing contractual and operational reporting channels. Global cell IDs and RAN-cell information should be explicitly confirmed as relevant to MNO reporting only. MVNOs should not be required to populate fields that depend on infrastructure data they do not control or routinely receive. Practical reporting during incidents Templates should allow staged reporting, with initial best-available information followed by updates where more complete data becomes available. The final templates should be clear, proportionate and operationally usable under incident pressure, rather than designed around information that may only be available after post-incident analysis (which would be provided to Ofcom via post-incident reports where relevant).
Question 5: (for MNOs): Do you have any comments about the requirement to provide us with a list of your RAN cells for purposes of mapping incidents and their impact?	Confidential? – Y / N Not applicable.

Please tell us how you came across this consultation.

- ☒ Email from Ofcom
- ☐ Saw it on social media
- ☐ Found it on Ofcom's website
- ☐ Found it on another website
- ☐ Heard about it on TV or radio
- ☐ Read about it in a newspaper or magazine
- ☐ Heard about it at an event
- ☐ Somebody told me or shared it with me
- ☐ Other (please specify)

Please complete this form in full and return to securityconsultation@ofcom.org.uk.