T-062 Telecoms Security

Response to consultation and final Procedural Guidance (Statement of Policy) and final Resilience Guidance

Document No: JCRA 26/14 Publication date: 9 April 2026

Jersey Competition Regulatory Authority
2nd Floor Salisbury House, 1-9 Union Street, St Helier, Jersey, JE2 3RF
Tel 01534 514990

Web: www.jcra.je

Contents

1 Overview and summary 3

2 Response to consultation..... 7

3 Response to additional consultation 28

4 Consultation outcome and next steps 30

Annex A: steps and timeframe for each compliance monitoring Information Request Notice 31

Annex B: Additional Consultation – changes to be incorporated into final Procedural Guidance 32

1 Overview and summary

Introduction

1.1 This document is a response to a consultation (the **Consultation**) on Draft Procedural Guidance (Statement of Policy) and Draft Resilience Guidance issued by the Jersey Competition Regulatory Authority (the **JCRA**) in August 2025.[1] The purpose of these documents is to explain the JCRA's planned approach to carrying out its operational telecoms security functions under new powers and duties conferred by the amended Telecommunications (Jersey) Law 2002 (the **Law**).[2] The purpose of the consultation was to seek views and comments on this planned approach. After assessing the consultation responses, the JCRA is issuing this document alongside final versions of its Procedural Guidance and Resilience Guidance in preparation for carrying out its new operational telecoms security functions from 1 June 2026.

1.2 This section of the document provides a brief overview of the context and process associated with the development of these two guidance documents (see Consultation on Draft Procedural Guidance (Statement of Policy) and Resilience Guidance for further contextual information[3]) along with information on the outcome of the consultation. It contains the following subsections:

- Background
- Response to consultation
- Additional consultation
- Changes made to accommodate Code of Practice adjustments
- Final guidance documents
- Next steps

Background

1.3 In August 2023, the Government of Jersey (the **Government**) explained its intention to introduce legislation to enhance and maintain the security and resilience of Jersey's communications in a public consultation setting out principles, approach and timescale.[4]

1.4 In September 2024, the States Assembly passed the Telecommunications Law (Jersey) Amending Regulations 2024, which updated the Law with the addition of a new telecoms security framework. Its purpose is to secure the Island's vital telecoms networks and services, ensuring they are

[1] JCRA: T-062 Telecoms Security Draft Procedural Guidance and Draft Resilience Guidance consultation – see here for more information.
[2] States of Jersey: Telecommunications (Jersey) Law 2002 as amended on 1 October 2024 – see here for more information.
[3] JCRA: T-062 Telecoms Security Draft Procedural Guidance and Draft Resilience Guidance consultation – see here for more information.
[4] Government of Jersey: Telecoms Security Framework consultation – see here for more information.

inherently resilient and reliable and protected from cyber threats arising from criminals and other hostile actors.

1.5 The Government subsequently issued further elements of the planned telecoms security framework for consultation:[5]

(a) The Telecommunications (Security Measures) (Jersey) Order 202 containing a list of defined security measures that telecoms providers must implement (the **Security Measures Order**).

(b) Guidance on how telecoms providers can demonstrate compliance with implementing the Security Measures Order (the **Code of Practice**).

1.6 The amended Law provides the JCRA with a range of new powers and duties, which it plans to deliver through new operational telecoms security functions. Once fully commenced[6], these duties include a general duty to seek to ensure that local providers of public electronic communications networks and services (the **Providers**) comply with their security duties under the new telecoms security framework. This remit encompasses working with Providers to monitor and improve the security of their networks and services along with the investigatory and enforcement powers needed to address concerns over potential non-compliance.

1.7 Under the Law, the JCRA created two documents explaining its planned operational telecoms security functions and issued them for consultation. These are:

(a) **Draft Procedural Guidance** explaining the processes operated by the JCRA to deliver its telecoms security functions.

(b) **Draft Resilience Guidance** explaining expectations associated with designing and operating inherently reliable networks and services.

1.8 The purpose of the Consultation was to bring these two draft guidance documents to the attention of interested parties, including Providers with legal obligations to design and operate secure and resilient networks and services, and to seek views and comments before issuing updated final versions.

Consultation outcome

1.9 There were four responses to the Consultation, with non-confidential versions issued on the JCRA's website alongside this document. The respondents were:

- Home Net Limited (**Home Net**)
- JT (Jersey) Limited (**JT**)

[5] Government of Jersey: Draft telecoms security measure – see here for more information.
[6] The States will commence certain parts of the Amending Regulations by Order to bring all elements into force.

- Newtel Limited (**Newtel**)
- Sure (Jersey) Limited (**Sure**)

1.10 The JCRA is grateful for all responses, which have been carefully considered when developing the final versions of the Procedural Guidance and Resilience Guidance issued alongside this document.

Additional consultation

1.11 In January 2026, the JCRA issued an additional consultation (the **Additional Consultation**) following a Government proposal to change the telecoms security framework to make relevant turnover the criteria for determining Providers in scope of the Security Measures Order. The outcome of the Additional Consultation, which proposed potential changes to the Procedural Guidance, is shown in Section 3 of this document.

Changes made to accommodate Code of Practice adjustments

1.12 Following its consultation, the Government has decided to specify a later deadline for completing the first set of Code of Practice measures, deferring this from 2027 to 2028. Minor amendments have been made to the Procedural Guidance to reflect this adjustment, shown in mark-up in the that version of the document published under the case files (T-062 Telecoms Security). The JCRA has also produced a non-statutory Information Note to explain the resulting adjustments to its compliance monitoring framework also published under the case files.

Final guidance documents

1.13 This document contains an analysis of views and comments received through the Consultation and the Additional Consultation, along with the JCRA's analysis and the conclusions it has reached. It explains the amendments incorporated into the final versions of guidance documents, which are shown in mark-up style text. Full marked up versions of the Procedural Guidance and Resilience Guidance along with final versions of both documents are as part of the case files on the JCRA website.

1.14 Note that the final documents include some non-substantive changes to align with recent organisational style updates—such as replacing the term 'the Authority' with 'the JCRA'. These non-substantive changes are not shown in the mark-ups.

Next steps

1.15 The Government intends commencing the Security Measures Order on 1 June 2026 alongside another Order bringing into force the remaining provisions of the amended Law. At this point, the JCRA will begin its operational telecoms security functions as explained in the Procedural Guidance.

2 Response to consultation

2.1 The Consultation described the JCRA's role in the planned telecoms security framework, provided context for the development of its Draft Procedural Guidance and Draft Resilience Guidance, and asked for views and comments on the JCRA's intended approach to carrying out its operational telecoms security functions. This section summarises and analyses responses received and associated JCRA conclusions. It contains the following subsections:

- Consultation Section 2: The planned process and timetable
- Consultation Section 3: Development approach
- Consultation Section 3: About the Draft Procedural Guidance
- Consultation Section 3: About the Draft Resilience Guidance

Consultation Section 2: The planned process and timetable

Consultation question 1: Do you have any comments on the Authority's role in the telecoms security framework and its approach to issuing Procedural Guidance and Resilience Guidance under the Law?

Consultation focus

2.2 The JCRA provided background to the Government's planned new telecoms security framework and the role allotted to the Island's telecoms regulator under the amended Law, and invited general views and comments about the JCRA's plans to fulfil that role.

Summary of responses

2.3 While supporting the overall aims of the telecoms security framework, Home Net and Newtel proposed that responsibility for regulatory oversight should be given to an independent technical authority rather than the JCRA.

2.4 Offering support for the JCRA having a role in the planned telecoms security framework, JT drew attention to the compliance challenges faced in comparison to larger UK providers operating under a similar telecoms security regime.

2.5 Sure supported the JCRA's planned involvement in the telecoms security framework, but cited concerns it had raised with the Government over the approach for deciding which Providers need to demonstrate compliance with the Security Measures Order—specifically, Sure believed the JCRA should have a role in this process.

Analysis and JCRA conclusions

2.6 Addressing Home Net's and Newtel's view on the JCRA's role in the telecoms security framework, the JCRA reminds them that it is the Government's decision that the amended Law confers the

legal responsibility on the JCRA for monitoring compliance and provides the JCRA with new telecoms security powers and duties to carry out this role.

2.7 Considering JT's comments on operational challenges, the JCRA recognises that limited scale, turnover and access to resources have the potential to create compliance challenges for local Providers, when they are compared to Tier 1 providers in the UK[7]. However, the JCRA also notes that smaller Tier 2 providers in the UK equally need to demonstrate compliance—albeit in an extended timeframe compared with Tier 1—and face the same consequences if they do not meet their legal obligations. Moreover, the JCRA fully supports the aims and intentions of the Government's telecoms security framework to protect the Island's vital communications networks and services. This means that the JCRA must carry out its operational telecoms security functions in line with the powers and duties conferred under the Law. In consequence, the JCRA believes that the Draft Procedural Guidance must stand, while identifying and making reasonable adjustments to accommodate local contextual differences from those that may apply in the UK.

2.8 While noting Sure's detailed suggestions on alternative arrangements for deciding which Providers the Security Measures Order and Code of Practice should apply to, the JCRA considers that this is a subject for the Government's consideration and decision on whether to make any changes in approach within the final telecoms security framework. The JCRA will respond to and accommodate any amendments that the Government believes appropriate.[8]

Consultation Section 3: Development approach

Consultation question 2: Do you have any comments on the Authority's approach to developing its Draft Procedural Guidance and Draft Resilience Guidance?

Consultation focus

2.9 The JCRA was seeking views and comments primarily on its intentions to align its approach to equivalent frameworks issued by the UK communications regulator Ofcom, while considering and taking account of local context.

Summary of responses

2.10 JT and Sure broadly support the JCRA's approach.

Analysis and JCRA conclusions

[7] The UK Government divided providers into three categories or tiers based on company turnover, with Tier 1s being the largest.
[8] See Section 3 for relevant Procedural Guidance changes being made to accommodate a recent Government decision on determining the scope of the Security Measures Order.

2.11 The JCRA will continue with its current approach to developing its Procedural Guidance and Resilience Guidance.

Consultation Section 3: About the Draft Procedural Guidance

Consultation question 3: Do you have any comments on the Authority's proposed approach to compliance monitoring?

Consultation focus

2.12 The JCRA explained the background to its proposed approach to compliance monitoring—as explained in Section 3 of the Draft Procedural Guidance—and sought views and comments on the details this contained.

Summary of responses

2.13 JT broadly supported the planned approach, acknowledging the importance of a proactive and structured monitoring regime. However, JT also expressed concern over the potential workload that may be imposed by following the same volume and frequency of information requests employed by Ofcom in the UK. Instead, JT proposed what it considered to be a more proportionate approach, with formal information requests being issued once per year, rather than every nine months.

2.14 Sure likewise broadly agreed with the JCRA's planned approach, while raising several points / queries for consideration / clarification, as identified and summarised below:

(a) **Remedial action**: Sure drew attention to Paragraph 3.11 of the guidance and requested further information on the circumstances in which remedial action via supervision would be adopted and when escalation to enforcement action would be used.

(b) **Code of Practice deadlines**: Sure requested clarification on how and why the JCRA will be assessing compliance against the Code of Practice prior to the first tranche (and subsequent tranches) of Code of Practice security measures coming into force.

(c) **Secure platform:** Sure asked for further information about the planned JCRA system used to securely store confidential information.

(d) **Assessment notices:** Sure requested clarification on the cost implications for Providers should the JCRA use assessment notices as part of compliance monitoring.

(e) **Powers of entry**: Sure requested more information about the JCRA's power to require entry to a Provider's premises.

Analysis and JCRA conclusions

2.15 Considering JT's response, the JCRA appreciates that the telecoms security framework will place considerable additional administrative demands on both itself and Providers—particularly those having to demonstrate compliance with the Code of Practice. However, there is also clear recognition (by both the JCRA and respondents) that this is a necessary change, given the essential nature of Jersey's communication networks and services and the need to protect Islanders and local organisations from a loss in service—as a result of either cyber attacks, resilience issues or both.

2.16 However, the JCRA understands JT's concerns over the potential workload involved in responding to information request notices released every 9-months and accepts JT's suggestion that moving to every 12-months should improve the efficiency and quality of response. Paragraph 3.30 of the Procedural Guidance will be modified to reflect this change, as shown below:

> *3.30 (Extract) The JCRA ~~Authority~~ plans to release subsequent information requests at 12-month ~~nine-month~~ intervals with around ~~six~~ five requests expected to cover all Code measures. The intention behind the multiple requests is to help keep the burden imposed by each manageable.*

2.17 The JCRA further recognises the importance of allowing Providers to plan resourcing around the intended compliance monitoring information gathering programme and is taking the following steps to support this:

(a) Annex A to this document explains the planned steps and timeline associated with each compliance monitoring information request notice; and

(b) The JCRA will engage Providers that must demonstrate compliance under the Security Measures Order in advance of issuing the Information Request Notices to further explain the planned approach and share an example notice.

2.18 In the context of Paragraphs 2.16-2.17 (above), it is important to point out that Paragraph 3.24 of the Procedural Guidance states that the JCRA may also refine the compliance monitoring process based on experience gained through implementation and operation. This may result in subsequent changes to the overall information gathering timeline and structure of its individual requests.

2.19 Turning to Sure's response to this question, the several points and queries for consideration / clarification summarised in Paragraph 2.14 (above) are addressed separately below:

(a) Remedial action

2.20 While respecting Sure's request for more detail / certainty on the circumstances where remedial / enforcement actions may be necessary, the JCRA believes that it is better to avoid being overly-prescriptive at this time. This will allow it to retain flexibility within which to adjust its approach based on operational experience for both the JCRA and Providers. However, the JCRA accepts that

further clarification within the Procedural Guidance section relating to this request would be beneficial at this point and so will amend Section 3 as shown below:

3.15 The telecoms security framework establishes the steps that Providers subject to the Security Measures Order must take to achieve compliance with the Law and the Order. Through its supervisory model, the JCRA will initially use statutory information gathering powers to monitor progress that each Provider is making towards implementing appropriate organisational and technical measures with sufficient pace, as they continue to work towards full compliance.

3.16 Where the JCRA finds areas of concern, it will seek to work with Providers through informal engagement to ensure appropriate and proportionate measures are implemented in accordance with the telecoms security framework. The JCRA expects that this collaborative approach will foster more compliant behaviours, reduce the volume of breaches under the Law, as well as reducing the need for regulatory investigations.

3.17 If the JCRA determines there are reasonable grounds to suspect a Provider is not taking appropriate and proportionate measures to act in accordance with the Code, it may use its powers under 24R of the Law to notify its concerns and give an opportunity for the Provider to explain its position.

3.18 The JCRA will assess information received in response to a notification under 24R of the Law in conjunction with the other information it holds to determine whether to take further steps, which may include issuing an assessment notice which can require the Provider to carry out testing, attend a formal interview, permit onsite observation, etc.

3.19 As necessary, the JCRA will also stand ready to engage its suite of enforcement powers at any relevant time within the supervisory framework, with the approach to enforcement set out in Section 5 of the Procedural Guidance.

(b) Code of Practice deadlines

2.21 Considering Sure's request for clarification about the interplay between Code of Practice deadlines and the compliance monitoring approach, the JCRA draws attention to the following key telecoms security framework principles:

- Once commenced by the Minister, the Security Measures Order establishes a legal requirement for local Providers required to demonstrate compliance to take appropriate and

proportionate measures to be compliant with articles set out in the Order from that point forward.

- Recognising the potential challenges involved for Providers to be fully compliant with the Security Measures Order at the time it comes into force, the Minister has issued the Code of Practice containing guidance on specific measures through which Providers can demonstrate compliance. The Code of Practice also contains recommended timeframes by when Providers would be expected to have implemented the requirements of each measure and stating that all measures should be completed by 31 August 2030.
- The final Procedural Guidance states that the JCRA will carry out five compliance monitoring information gathering rounds, with the first expected to be issued in 2027 and the final one planned for issue in 2031. Each will focus on a range of Code of Practice measures and seek to understand how Providers are compliant with a measure or how they plan to become compliant in line with the recommended Code of Practice timeframes.

2.22 In summary, the JCRA expects Providers to be aware of their legal obligations under the Security Measures Order and expectations to demonstrate compliance established by the Code of Practice measures, which includes explaining and justifying compliance or a plan in place that will lead to compliance.

(c) Secure platform

2.23 The JCRA accepts that it is important to fully explain its planned approach to securely receiving, processing and storing confidential information received from Providers through the compliance monitoring framework or following a risk or occurrence of security compromise. The JCRA is mindful of the importance of reassuring Providers as to its approach for secure information gathering and handling, given the potential sensitivity of the data relating to local communications networks and services.

2.24 Sure's request for further information about the planned JCRA secure information management system is therefore reasonable, and will be addressed through information supplied directly to each Provider required to demonstrate compliance with the Security Measures Order. This will be shared in advance of the JCRA commencing its operational telecoms security functions and will include an opportunity for responding to questions about the system, which in summary will feature:

- Industry grade secure storage capacity.
- Defined internal privileged access controls.
- Secure reporting portal.
- Secure provider log-in and document upload provision.

(d) Assessment notices

2.25 The JCRA acknowledges Sure's comments on the cost implications of having to co-operate with assessments and will always aim to be mindful and consider whether using this power is appropriate and proportionate to the circumstances.

2.26 Considering Sure's suggested alternative approach, the JCRA broadly supports the expressed intentions and will amend Section 3 of the Draft Procedural Guidance to accommodate the principles, as shown below:

3.51 *While the JCRA expects to gather the majority of information through its routine monitoring using Information Request Notices, it may, in some circumstances, decide it is appropriate to use an assessment notice to inform the Authority's assessment of a Provider's compliance with their security duties.*

3.52 ~~*The Authority recognises*~~ *Recognising that complying with an assessment notice may require more substantial effort or additional costs for Providers than responding to receiving Information Request Notices or providing a statement in response to one, the JCRA will normally seek to initially issue a draft assessment notice as part of its compliance monitoring process. This may include the following information:*

- *An explanation of the reasons for planning to issue a formal assessment notice;*
- *The chosen assessment method and reasons for its selection;*
- *The expected requirements on the Providers including timeframe for completing the assessment activity;*
- *The anticipated outcome of the assessment activity and potential next steps;*
- *A request for the Provider to assess and provide the JCRA with its reasonable external costs associated with carrying out the assessment; and*
- *An opportunity for the Provider to propose an alternative assessment approach they consider appropriate for achieving the same outcome.*

3.53 *The JCRA will review any response from a provider to a draft assessment notice and will take information received into account before deciding to proceed with the assessment. However, for the avoidance of doubt, nothing contained in this process limits the JCRA's power to issue assessment notices.*

3.54 *Where appropriate, the JCRA may also use assessment notices to inform its enforcement activity, and reminds that Providers have a duty to cooperate*

with an assessment under the Law and holds the view that this would include not doing anything to disrupt an assessment, such as destroying documents to which access is sought or interfering with testing required by an assessment notice. The JCRA has powers to enforce any breach of this duty of co-operation under Schedule 2, Part 2, 8(3).

(e) Powers of entry

2.27 In response to Sure's request for more information about the power to require entry to a Provider's premises, the JCRA will amend Paragraph 3.57 of the Draft Procedural Guidance to read:

> *3.57 In exercising its powers of entry, and having regard to any relevant legislation or guidance provided in this area, the JCRA expects to use the following framework: ~~to have regard to any relevant legislation or guidance provided in this area~~*
>
> *(a) The option to enter a Provider's premises will be carefully considered before making an evidence-based decision to proceed.*
>
> *(b) Providers will receive reasonable advanced notice of the JCRA's intention to enter its premises (usually not less than 48-hours) including specifying the date and time of arrival.*
>
> *(c) The advanced notice will name the persons or persons who will be entering the premises, and they will carry appropriate verification ID.*
>
> *(d) The advanced notice will explain why the JCRA has chosen to enter the premises, and state the activities that will be carried out once inside and assistance required.*
>
> *(e) The Provider must commit to ensuring suitable representatives are available at the premises to allow entry and remain with the JCRA's representative(s) throughout to provide the required assistance.*
>
> *(f) The JCRA's representative(s) would make a record detailing the circumstances associated with the entry and detail the information obtained.*

Consultation question 4: Do you have any comments on the Authority's proposed approach to reporting security risks or compromises?

Consultation focus

2.28 The Draft Procedural Guidance contains detailed information on increased requirements under the amended Law for Providers to report both the substantial risk and occurrence of security compromise and explains the JCRA's proposed approach to this. The Consultation sought views and comments on these proposals.

Summary of responses

2.29 Offering broad support for the JCRA's approach, JT's response included several relevant suggestions on ways to ensure an effective reporting process, including on minimising the need for multiple reporting requirements and efficiency in any secure reporting system. JT further highlighted the challenges faced by Providers deploying finite resources to resolve an issue and provide ongoing progress updates to the regulator. Providing observations on the Procedural Guidance reporting tables, JT also queried some of the information they contain.

2.30 Sure also offers broad support for the JCRA's planned approach, but requested further information on the 'secure communication methods' referred to in the Procedural Guidance. Sure further questioned the practicality of being able to provide a 'full report' on a security compromise within 72-hours, stating the challenges associated with investigating complex incidents.

Analysis and JCRA conclusions

2.31 The JCRA welcomes JT's constructive comments on ensuring an effective reporting process, which have been taken into account within the development of the intended secure information management system and associated processes. These will be shared with Providers in advance of them having to commence their reporting obligations, and may be adjusted in response to feedback received. This includes the ability to securely upload documents, a form-based approach to reporting, and functionality allowing updates as the incident evolves.

2.32 The JCRA further notes JT's point on resource challenges faced by Providers when dealing with the risk or occurrence of security compromises, and understands that a balance needs to be struck between devoting resources to address the security compromise and to report to the regulator as mandated under the amended Law. In general, the JCRA believes it is for Providers to determine what is the appropriate and proportionate approach to achieving both requirement, based upon an assessment of the situation faced, and to be prepared to justify any prioritisation decision.

2.33 Noting JT's observations on figures in the reporting tables, the JCRA is grateful for the feedback and will correct in the final Procedural Guidance.

2.34 For a response to Sure's request for explicit information on secure communication methods (for reporting incidents), the JCRA refers to paragraphs 2.23 and 2.24 above.

2.35 The JCRA appreciates Sure's position on the potential challenges associated with providing a full report within 72-hours of notifying an urgent security compromise. However, the JCRA also draws attention to its legal obligation to inform others, including the Minister and users, of the occurrence of security compromises with the principle being to ensure the broad interests of

Islanders and local organisations (and potentially national interests) are being prioritised and protected. Fulfilling this requires Providers to inform the JCRA with relevant facts that accurately explain the situation in a timely fashion.

2.36 Addressing Sure's points explicitly, the JCRA offers the following expanded explanation of expectations:

- An initial notification(referred to in Paragraph 4.33 of the Draft Procedural Guidance and required within 24-hours): This should contain as much information about the urgent security compromise as is known at that time, where possible satisfying the 'data required' fields described in paragraphs 4.42-4.62 of the Draft Procedural Guidance.
- The full report (referred to in Paragraph 4.33 in the Draft Procedural Guidance and required within 72-hours): This should contain all the information about a security compromise required to complete the 'data required' fields described in paragraphs 4.42-4.62 of the Draft Procedural Guidance.
- The JCRA accepts that some of the information required to complete the full report may not be fully available after 72-hours—such as the date and time of resolution—but expects Providers to make every effort to complete the report as required, with subsequent updates clarifying or confirming any fields containing previously incomplete, estimated or inaccurate information.

2.37 The JCRA will further amend Section 4 of its Procedural Guidance to clarify expectations for the initial notification and full report, as shown below:

> *4.33 The JCRA expects Providers to make an initial notification in relation to an urgent security compromise as soon as possible and usually within 24-hours of the Provider becoming aware of them. The JCRA expects the primary purpose of this initial notification is ~~simply~~ to acknowledge that the Provider is aware of such security compromise, and give an indication of its nature. Providers are not expected to supply all the information defined in paragraphs 4.42-4.62 (below) but any ~~Any~~ other information that is readily available will be welcomed. Following this initial notification, the JCRA then expects the full report to be provided within 72-hours.*

Consultation question 5: Do you have any comments on the Authority's proposed approach to enforcement?

Consultation focus

2.38 The amended Law gives the JCRA considerably enhanced enforcement powers, which reflect the expanded expectation for increased security and resilience for the Island's communications networks. The Consultation sought views and comments on the intended approach to these.

Summary of responses

2.39 JT acknowledged the requirement for enforcing compliance with legal expectations and Sure had no specific comments.

Analysis and JCRA conclusions

2.40 The JCRA will adopt its planned approach without amendment.

Consultation question 6: Do you have any comments on the Authority's proposed approach to information sharing?

Consultation focus

2.41 Recognising that Jersey's communications networks are integrated with those of UK and global telecoms operators and that the cyber threats faced locally are broadly the same as those faced by other jurisdictions, the amended Law creates formal pathways for sharing information between aligned organisations involved in protecting the Island. The Draft Procedural Guidance explains how the JCRA plans to share information with these organisations and asked for views and comments on proposals.

Summary of responses

2.42 JT supported JCRA's commitment to securely sharing information.

2.43 While not objecting to sharing information with others, Sure drew attention to the risks associated with this practice—i.e. the potential for loss of control over confidential information—and requested further information about the JCRA's planned approach to assure security from third parties.

Analysis and JCRA conclusions

2.44 The JCRA welcomes the broad support received from respondents and confirms that it places the highest possible priority on securely treating any sensitive information received from Providers through its operational telecoms security functions—this commitment is fully extended to any information that might need sharing with others.

2.45 For clarity, the JCRA has defined three categories of information that might be shared with others, and its approach to sharing, as shown in Table 1 (below):

Category	Explanation	Approach to sharing
1. Non-confidential	General telecoms security information that does not specifically relate to any Provider, situation, incident or open case. Generic incident trends, for example, or the general application of processes and procedures.	No specific arrangements – share as a means of developing the JCRA's knowledge and that of organisations involved in telecoms security.
2. Confidential	Specific telecoms security information about a situation, incident or open case that does not identify any Provider. Warning others of the existence of a cyber threat, for example, or explaining a local trend that may assist others involved in telecoms security.	Through appropriately robust ways-of-working arrangements covering inter-organisation communications.
3. Highly Confidential	Specific information that identifies a Provider associated with a security compromise or compliance status. Informing the Minister of a specific risk or occurrence of a security compromise if it is considered appropriate and proportionate for the security of Jersey, for example, or when informing others, including users, under the JCRA's legal powers.	Through a legal information sharing gateway and established MoU or equivalent, or under specific circumstance permitted by the Law.

Table 1: Information sharing categories

2.46 The JCRA's approach to sharing highly sensitive information is explained in Section 6 of the Draft Procedural Guidance, including seeking permission beforehand where appropriate or subsequently notifying that information has been shared.

2.47 The JCRA will further encourage Providers to share information with others involved in telecoms security—the JOIC, for example, or the Government's Emergency Planning team—where either legally required or as best practice, and to inform the JCRA that such sharing has taken place.

2.48 Responding to Sure's specific concerns on seeking security assurances from organisations receiving information, the JCRA confirms that it will only share highly confidential information

through a secure sharing system or under specific circumstance permitted by the Law, with appropriate and demonstrable arrangements and assurances in place to ensure information received will be treated with the same level of sensitivity as that employed by JCRA.

Consultation question 7: Do you have any other comments on the Authority's Draft Procedural Guidance?

Consultation focus

2.49 This question was included to provide a broad opportunity to offer any further views and comments on the approach to and contents of the Draft Procedural Guidance.

Summary of responses

2.50 JT draws attention to a response it has given in feedback to the Government's consultation on the Draft Security Measures Order and Draft Code of Practice, explaining that it is disproportionate for locally proposed timescales contained in the Code to be much stricter than similar ones established in the UK.

2.51 Sure requests clarity on the terms 'bespoke services' and 'publicly available services' (referring to information contained in Paragraph 2.4 of the Draft Procedural Guidance).

Analysis and JCRA conclusions

2.52 While following JT's point on timescales to demonstrate compliance, the JCRA reminds that the Draft Code is the Government's guidance and presumes this feedback will be considered by the Government within its consultation analysis and conclusions. The JCRA also draws attention to adjustments to compliance dates made by the Government in its amended Code of Practice.

2.53 Addressing Sure's request for clarification on public and bespoke services, the JCRA generally believes that the explanation given in the Draft Procedural Guidance provides sufficient information for Providers to consider and judge an arrangement for themselves. However, for further clarity, the JCRA will amend Paragraph 2.4 of the Procedural Guidance[9] to:

> *2.4 For clarity, the JCRA considers that "Public Electronic Communications Service" means any electronic communications service that is generally available for use by any and all members of the public who are both willing to pay for it and to accept the associated terms and conditions. A publicly available service is distinguishable from a bespoke service restricted to a limited group of individual and identifiable customers, and generally tailored to their unique operational, technical or strategic needs.*

[9] And the same paragraph in the Resilience Guidance.

2.54 The JCRA expects that many bespoke services falling under this definition are likely to be provided to customers using public network infrastructure—including physical and virtual components—which it reminds Providers will come within scope of the amended Law once fully commenced.

Consultation Section 3: About the Draft Resilience Guidance

Consultation question 8: Do you have any comments on the Authority's key concepts, drivers and relevant risks contained in Section 3 of the Draft Resilience Guidance?

Consultation focus

2.55 Under the amended Law, the definition of a security compromise includes 'anything that compromises the availability, performance or functionality of the network or service' and 'anything that causes signals conveyed by means of the network or service to be lost.'[10] The JCRA developed the Draft Resilience Guidance for Providers required by the Law to comply with these expectations and responsibilities so that robust and resilient communication networks and services are available for use by Islanders and local organisations. The focus of this Consultation question was to gain views and comments on the first part of the Draft Resilience Guidance, which establishes a broad underpinning framework for the more technical requirements that follow.

Summary of responses

2.56 JT offered support for the key concepts and risk drivers identified in the Draft Resilience Guidance, while drawing attention to potential resource implications and financial challenges faced by smaller Jersey operators compared with UK providers able to benefit from larger-scale operations.

2.57 Sure broadly agreed with the JCRA's position on key concepts, drivers and relevant risks, while challenging one aspect relating to architecture/design vulnerabilities and failings.

Analysis and JCRA conclusions

2.58 The JCRA welcomes JT's support and takes note of the points made on proportionality.

2.59 Addressing Sure's challenge on the wording used to discuss architecture / design vulnerabilities and failings (paragraphs 3.26-3.29 of the Draft Resilience Guidance), the JCRA has carefully considered the points made. To better reflect the expectation that Providers give due regard for the concepts in 3.26 to 3.28 as part of design and implementation, the JCRA has adjusted the wording within 3.29 of its final Resilience Guidance as shown below:

> *3.29* ~~*Poor*~~ *Architecture/design policy that does not effectively consider these concepts and account for them or* ~~*poor*~~ *implementation that does not follow* ~~*of adequate*~~

[10] States of Jersey: Telecommunications Law (Jersey) Amendment Regulations 2024, Article 24K(2) – see here for more information.

architecture/design policy that has considered them can ~~both~~ lead to unexpected significant network and service impacts.

Consultation question 9: Do you have any comments on the Authority's technical guidance for reliability and resilience contained in Sections 4, 5 and 6 of the Draft Resilience Guidance?

Consultation focus

2.60 This consultation question focused on the more technical sections of the Draft Resilience Guidance, covering scope of Provider network and service resilience, network and service implementation resilience guidance and processes, tools and training.

Summary of responses

2.61 JT supported the technical elements of the Draft Resilience Guidance while drawing attention to the potential challenges for Jersey-based Providers having to secure the technical and operational capacity needed to meet the principles expressed and to make the required investments.

2.62 While not objecting to the technical elements, Sure sought clarification or further information on the information contained in several sections, as summarised below:

(a) **Third party facilities:** certain specific scenarios where third party input is required to discharge Sure's security duties.

(b) **Use of shared facilities:** risk assessments and the use of generators.

(c) **Regular reviews**: with suppliers, partners and peers.

(d) **Remote distribution facilities**: clarification in meaning.

(e) **User-hours lost**: appropriateness.

(f) **Spare equipment stores**: additional guidance.

(g) **Testing**: provision for emergency planned works.

Analysis and JCRA conclusions

2.63 The JCRA welcomes JT's support and takes note of the points made on technical and operational capacity.

2.64 Considering Sure's request for clarification or further information on several sections of the Draft Resilience Guidance, the JCRA addresses this individually below.

(a) Third party facilities

2.65 The JCRA notes Sure's concerns and the potential challenges for smaller scale Providers in reaching agreements or terms with third party providers of facilities or services. However,

Paragraphs 4.11 to 4.13 of the Draft Resilience Guidance are intended to make it clear to Providers that they cannot delegate their responsibilities relating to the networks or services that they provide.

2.66 Where a Provider relies on a third party facility or service, the JCRA expects the Provider would take steps to implement appropriate agreements allowing it to meet its network or service resilience requirements (as noted in Paragraph 4.13). Where a Provider is unable to assure itself through agreement with a third party, the JCRA would expect the Provider to give due consideration to the risks associated with such a position and to take what it considers to be appropriate and proportionate steps to manage such risks.

2.67 The JCRA does not consider it necessary or appropriate to adjust the proposed Draft Resilience Guidance on this matter—it is for each Provider to consider their approach to and treatment of any third parties relied upon, which will vary significantly in each case.

(b) Use of shared facilities

2.68 The JCRA notes Sure's request for clarification on its expectations associated with the management of risks relating to the use of shared facilities. However, it considers the approach to risk management to be a matter for each Provider to determine and justify, giving due consideration to the particular circumstances that apply to it and its networks or services.

2.69 The nature of potential risks to a Provider's network or service can only be effectively considered by the Provider through taking into account the likelihood and impact of any identified risk along with treatments and mitigations implemented to help manage it.

2.70 On this basis the JCRA does not intend to provide further information or make amendments to the Draft Resilience Guidance in response to Sure's comments on this matter.

(c) Regular reviews

2.71 Noting Sure's request for further detail on expectations for suitable periodic reviews with suppliers, partners or peers, the JCRA considers this to be a matter for each Provider to determine. Providers should be prepared to justify what they consider to be an appropriate period for such reviews, taking into account the nature of the arrangement and agreement with the involved parties.

2.72 In view of this, the JCRA does not consider it necessary or appropriate to amend the Draft Resilience Guidance in response to Sure's comments.

(d) Remote distribution facilities

2.73 In its equivalent UK guidance, Ofcom refers to 'street cabinets (or larger walk-in cabins)'. Considering the situation in Jersey, the JCRA understands there are few, if any, street cabinets deployed as part of the aggregation / backhaul domain for fixed network services. It has therefore chosen to use the term 'remote distribution facilities' to describe smaller aggregation sites which may be operated to support connections between customer premises and central sites.

2.74 The JCRA understands that JT may operate 'service distribution rooms (**SDRs**)' as part of its Fibre To The Premises (**FTTP**) network, which are remote facilities used to aggregate connections within a limited area and then connect these back to a more central 'exchange', The JCRA expects these SDRs as likely to fall into the scope of remote distribution facilities. However, considering the term 'service distribution room' may be specific to JT and its FTTP network designations locally, the JCRA has chosen to use a generic term that can apply more broadly to the networks and services of other Providers.

2.75 While noting Sure's request for examples to be included in the Resilience Guidance, the JCRA believes the current wording along with the information contained in this consultation response document provides enough clarity.

(e) User-hours lost

2.76 The JCRA welcomes Sure's comments on this point and understands that in a network possessing what might be termed a 'dynamic' or 'nomadic' user base (such as mobile), some assumptions must be made about the number of impacted users when assessing the user-hours lost for a particular location or RAN site, meaning there will likely be a margin for error in any such assessment or calculation.

2.77 The JCRA has chosen to use the concept of user-hours lost because it can apply irrespective of the type of network or service provided. It can therefore apply to Providers whatever their situation, as opposed to outlining a more detailed concept which may not so broadly apply, or a range of concepts. Should a Provider choose to use a different concept within key decision making for particular networks or services, it should be prepared to justify its approach if required.

2.78 Given the explanations in Paragraphs 2.76-2.77 (above), the JCRA does not believe it is necessary to modify its Draft Procedural Guidance and the interrelationship with the Draft Resilience Guidance to further clarify the thresholds for categorising and/or reporting of security compromises.

(f) Spare equipment stores

2.79 The JCRA notes Sure's comments on the previous T-049 case and associated decisions made by the JCRA.[11]

2.80 Considering Sure's overarching question on whether Providers should take a risk-based approach to management of spares, the JCRA considers that this may be an appropriate approach to enable a Provider to meet its service level targets or obligations while equally, considering others that may also be appropriate and proportionate. The JCRA will amend the wording in the final Resilience Guidance to reflect this, as shown below:

[11] Case T-049 – Telecoms Service Incidents – see here for more information

6.15 *Such measures also include, in some cases, determining an appropriate approach—such as risk-based—to pre-emptively build up dedicated spare equipment stores of hardware stock to meet the service level targets or obligations.*

2.81 Turning to Sure's specific query on where to hold spares (as noted in Paragraph 6.15 of the Draft Resilience Guidance), the JCRA believes that Providers should seek to manage spares in the most appropriate way needed to meet their service level targets or obligations. It is therefore a matter for the Provider to determine where spares should be held, taking into account any risks associated with spares being held outside of Jersey.

2.82 Providers are welcome to undertake a broader consideration of a best-practice approach to the holding of spare equipment. However, the JCRA reminds Providers that it is for them individually to evidence and justify that any adopted approach is appropriate and proportionate in relation of the networks or services being operated and the service level targets and obligations associated with these.

(g) Testing

2.83 The JCRA acknowledges Sure's comments on the matter of testing and understands there may be occasions where a Provider's normal approach to testing and validation needs to reflect the situation and circumstances. Nonetheless, the JCRA would expect Providers to have given consideration to when this may be required and what may be acceptable within the Provider's chosen change management approach.

2.84 The Draft Resilience Guidance does not seek to set out what a Provider must do for testing and validation management in all circumstances but rather highlights key considerations in this area. The JCRA would draw attention to the last point under Paragraph 6.25 of the Draft Resilience Guidance and urge Providers to give consideration to how this could apply in the various situations that may occur.

2.85 The JCRA does not propose to amend its Draft Resilience Guidance in response to this comment as it considers it highlights appropriate objectives.

Consultation question 10: Do you have any other comments on the Authority's Draft Resilience Guidance?

Consultation focus

2.86 This question was included to provide a broad opportunity to offer any further views and comments on the proposed approach to and provisional contents of the Draft Resilience Guidance.

Summary of responses

2.87 JT offered several specific comments relating to sections 4 and 5 of the Guidance, which are summarised below:

(a) **Paragraph 4.19**: suggestion to merge terms.

(b) **Paragraph 4.28**: suggestion to clarify wording.

(c) **Paragraph 4.35**: use of term 'quality of service'.

(d) **Paragraph 5.7**: UK EC-RRG guidelines.

(e) **Paragraph 5.10**: impact of climate change.

2.88 Highlighting that Paragraph 2.32 states that the Resilience Guidance shall 'supersede and replace any previous guidance given by the JCRA on general network and services resilience and reliability', Sure requested confirmation of intentions.

Analysis and JCRA conclusions

2.89 The JCRA welcomes JT's request for clarification or further information on several sections of the Draft Resilience Guidance, which are addressed individually below.

(a) Paragraph 4.19 (and subsequent references)

2.90 In relation to the suggestion of merging certain terms within the Draft Resilience Guidance, the JCRA is satisfied that those chosen terms are appropriate. The term 'site' refers to a specific physical location and the term 'domain' is more generally applicable to groups of sites performing a function or interactions with another function.

(b) Paragraph 4.28

2.91 The JCRA refers to the response given in Paragraph 2.90 (above) on the appropriateness of terminology.

(c) Paragraph 4.35

2.92 Considering JT's point on the term 'quality of experience', the JCRA accepts this is a wider measure of customer satisfaction and that service reliability is one aspect. To more clearly make this point, the JCRA has amended the Draft Resilience Guidance as shown below:

> *4.35 Different services and applications used by end-users and devices have differing dependencies on the network functions mentioned above. It is important to note that a Provider's level of quality of experience, ~~(~~service reliability~~)~~ being a key factor influencing this, is heavily dependent on ~~a Provider's~~ its ability to forecast capacity demands on the network and functions in the core domain.*

(d) Paragraph 5.7

2.93 As explained in Paragraph 5.6 of the Draft Resilience Guidance, the JCRA expects Providers to give appropriate consideration to relevant good practice guidance and incorporate recommendations they contain wherever appropriate. In this context, the UK's EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure is a source of good practice approaches.

2.94 The JCRA believes that each Provider should consider such good practice guidance when designing, building and maintaining its networks and services. The JCRA may consider such guidance as the UK's EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure when assessing possible resilience incidents or considering compliance situations.

(e) Paragraph 5.10

2.95 The JCRA confirms that this statement is intentionally broad because the impacts of climate change may vary significantly between Providers depending on the types of networks or services that they operate and where they operate from. Furthermore, the nature of climate change may mean that the associated impacts change over time.

2.96 Within its Resilience Guidance, the JCRA seeks to highlight that Providers should give due consideration to the impacts of climate change when planning and making key decisions in respect to designing, building and maintaining their networks and services. The impact of applicable climate change considerations should be taken into account.

2.97 Considering Sure's request for clarification on the interrelationship between the proposed new guidance and the existing 999 Guidance, the JCRA provides the following explanation:

(a) Following consultation, the JCRA issued Guidance on the Provision of a Public Emergency Call Service in June 2022 (updated in August 2024) (the **999 Guidance**)[12] to establish expectations on how licensed operators should approach compliance with obligations established by telecoms license conditions relating to emergency service calls. The 999 Guidance includes separate sections on 'Operator Network Resilience', on the 'CHA Function'[13] and on 'Service Incidents'.

(b) The Resilience Guidance is intended to supersede the Operator Network Resilience section of the 999 Guidance, while the latter's CHA Function section remains in place and should be considered current along with other sections of the 999 Guidance (see Table 2 below for more details).

(c) Sure's response also refers to incident reporting tables in the 999 Guidance and asks whether they are superseded by those in the Draft Procedural Guidance. The JCRA thanks

[12] JCRA-Updated Guidance on the Provision of a Public Emergency Call Service – see here for more information.
[13] CHA = Call Handling Agent, which is the function that initially answers 999 or 112 calls to the emergency services.

Sure for raising this point and confirms that the tables in the Procedural Guidance align with those shown in the 999 Guidance for fixed or mobile networks providing access to the emergency services.

(d) The JCRA further thanks Sure for its question about notification of service incidents involving calls to the emergency services, which the JCRA confirms should be made via the planned secure reporting portal (see paragraphs 2.23 and 2.24 for more information).

999 Guidance section	Status
Section 3: Overarching Principles	Not superseded—999 Guidance remains current
Section 3: Operator Network Resilience	Superseded by the Resilience Guidance
Section 3: VoIP Considerations	Not superseded—999 Guidance remains current
Section 3: CHA Function	Not superseded—999 Guidance remains current
Section 3: CHA / ES Technology Platform	Not superseded—999 Guidance remains current
Section 3: Service Management and Development	Not superseded—999 Guidance remains current
Section 3: Service Reporting	Not superseded—999 Guidance remains current
Section 3: Service Incidents	Not superseded—incident reporting for fixed or mobile network providing access to the emergency services aligns with Resilience Guidance

Table 2: interrelationship between new guidance and existing 999 Guidance

2.98 The JCRA intends updating its 999 Guidance at the earliest opportunity to fully reflect these changes.

3 Response to additional consultation

3.1 This section contains the outcome of an additional consultation issued by the JCRA in January 2026 in response to the Government proposing changes to its Security Measures Order.[14] It contains the following subsections:

- About the additional consultation
- Consultation responses and outcome
- Next steps

About the additional consultation

3.2 Following consultation, the Government proposed changing the telecoms security framework to make relevant turnover the criterium for determining Providers in scope of the Security Measures Order. The change also proposed giving the JCRA a role in assessing which Providers must therefore demonstrate compliance with the Code of Practice.

3.3 In view of this, the JCRA issued an additional consultation in January 2026, setting out its proposed approach to the proposed new role and changes needed to accommodate it with the Draft Procedural Guidance. The consultation closed on 23 February, with responses received from Sure (Jersey) Limited

3.4 A non-confidential version of the response will be published on the JCRA website alongside this document.

Consultation responses and outcome

Additional Consultation question 1: Do you have any concerns about the JCRA's approach to preparing for the Government's proposed changes to the Security Measures Order? If so, please explain what they are.

Additional Consultation question 2: Do you support the JCRA's approach to potential modifications to its Draft Procedural Guidance? If not, please explain why.

Additional Consultation question 3: Do you have any specific comments on the potential modifications to the Draft Procedural Guidance contained in Annex A of this document?

Consultation focus

[14] Government: Draft Security Measures – see here for more information.

3.5 The JCRA explained the Government's proposed changes to its draft Security Measures Order and the potential modifications to the Draft Procedural Guidance needed to accommodate these changes.

Summary of responses

3.6 Sure had no comments on the specific JCRA approach contained in the additional consultation, but set out its concerns about the Government's intention to use relevant turnover based on relevant activities carried out wholly or partly in Jersey. Sure explained that it believes that this results in Providers operating in Jersey being excluded because of a comparatively small local presence, but which could be providing services essential for critical national infrastructure provision.

Analysis and JCRA conclusions

3.7 The JCRA welcome Sure's response, which offers valuable comments on the development of the telecoms security framework.

3.8 Considering the comments on the Government's approach to the scope of the Draft Security Measures Order, the JCRA understands the points raised. However, these considerations that the Government should have considered and taken into account when finalising any changes.

3.9 Taking into account Sure's position on the potential modification to the Draft Procedural Guidance, and that there are no further consultation responses, the JCRA considers it appropriate to proceed with the potential modification as set out in the consultation.

Next steps

3.10 The Government has confirmed it intends changing the Draft Security Measures Order as proposed in its focused consultation.

3.11 The JCRA will make the changes to Section 4 of its Draft Procedural Guidance proposed in the Additional Consultation. These are shown in Annex B of this document and as mark-up text in the Telecoms Security - Procedural Guidance (Marked-up) document in the case files.

4 Consultation outcome and next steps

4.1 This document summarises the responses received by the Consultation closure date on 17 October 2025 and incorporates further responses received to the Additional Consultation by its closure on 23 February 2026.

4.2 The responses received were broadly positive, while offering further points for consideration by the JCRA or requesting clarification on certain content in the guidance documents. In return, the JCRA has provided supplementary information within this document wherever relevant, and accommodated clarification requests where considered appropriate through amendments to the final versions of the Procedural Guidance and Resilience Guidance.

4.3 Marked-up versions of both documents showing amendments are available alongside this document on the JCRA website – see here for more information.

4.4 The JCRA website will also contain final versions of the Procedural Guidance and the Resilience Guidance, which should be considered final and applicable from 1 June 2026 (the date on which the Government intends to commence the remaining parts of the amended Law). These documents may be updated from time to time, which will be carried out through a structured consultation and amendment process.

Annex A: steps and timeframe for each compliance monitoring Information Request Notice

Note: may be subject to change based on experience gained through implementation and operation.

Month	Activity	
	JCRA	Provider
Commence compliance monitoring information gathering round		
1	Prepare and issue a draft compliance monitoring Information Request Notice to Providers at the start of month 1.	Review Information Request Notice, request clarification information and confirm understanding of requirements to the JCRA by the end of month 1.
2-6	Issue compliance monitoring Information Request Notice to Providers in final at the start of month 2.	Assemble information required in response to Information Request Notice and submit to JCRA by the end of month 6.
7-8	Review information provided received to ensure submission is complete and ready for detailed review of compliance status. Engage Providers as needed to request further information or clarification.	Respond to any JCRA request for further information or clarification.
9-11	Carry out detailed review of information received, engaging Providers as necessary to request further information or clarification.	Respond to any JCRA request for further information or clarification.
Close compliance monitoring information gathering round		

Annex B: Additional Consultation – changes to be incorporated into final Procedural Guidance

Following the Additional Consultation, the relevant sub-sections of Section 3 will be changed as shown in mark-up below.

Compliance monitoring principles

Duty to seek to ensure compliance

3.3 The Amending Regulations significantly enhance the Law to add substantial additions to regulate security in the Island's telecommunications sector. Within this telecoms security framework, Providers have a greatly expanded range of security duties and the JCRA has important new duties and associated powers including seeking to ensure compliance through proactive monitoring and, if necessary, enforcement with legal and regulatory requirements.

3.4 The JCRA expects Providers to ensure that they understand and comply with duties placed on them by the telecoms security framework. This means being fully aware of the Law, associated Orders and relevant guidance given by the Minister in the Code and in regulatory guidance issued by the JCRA, including guidance on the resilience of local communications networks and services.[15]

3.5 Article 24V of the Law places a general duty on the JCRA to seek to ensure that Providers comply with security duties imposed on them by Articles 24K to 24N, 24S and 24T, which means taking a proactive approach to monitoring and ensuring compliance and carrying out positive enforcement activities if necessary.

~~**Approach to monitoring providers**~~

The approach to monitoring Providers within the scope of the Order

3.6 ~~While legal duties contained in the Law apply equally to all public telecoms providers, the Authority's compliance monitoring principles apply only to those Providers the Minister has specified in the Order. The rest of this section explains how the Authority intends to approach this monitoring.~~

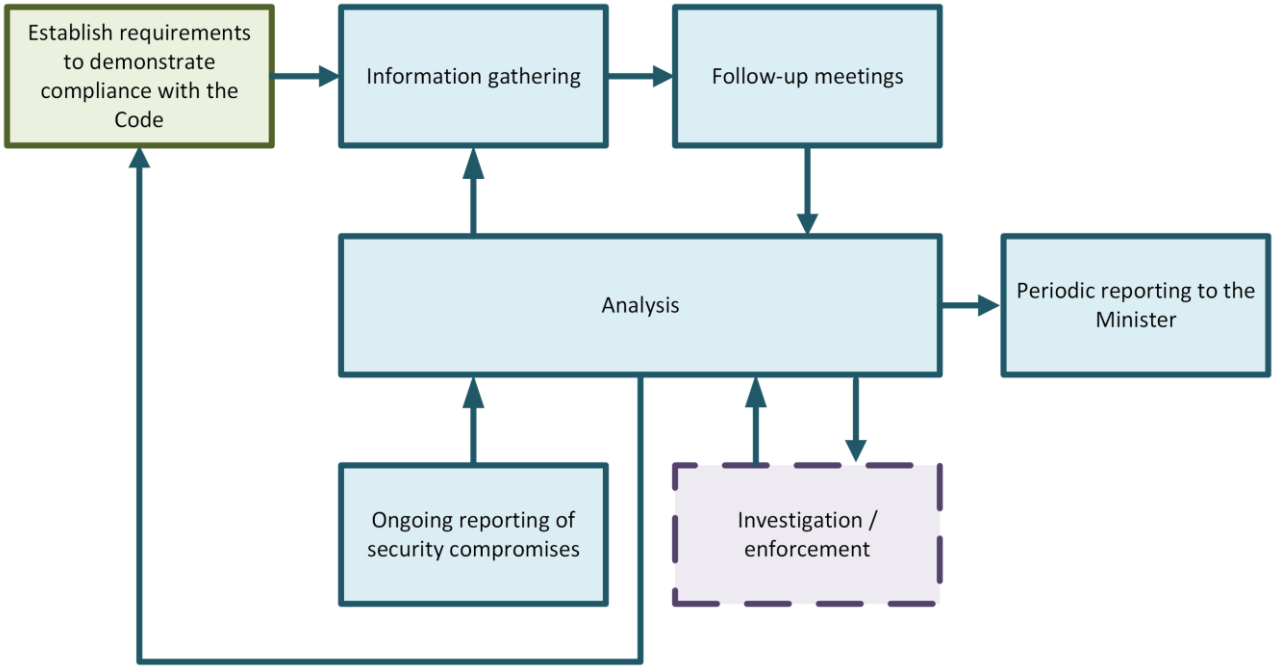
While legal duties contained in the Law apply equally to all public telecoms providers, the Order only applies to those with an annual relevant turnover of £1 million (or equivalent) or above.

[15] JCRA: Resilience Guidance – see here for more information.

Consistent with the scope of the Order, the rest of this section explains how the Authority intends identifying and notifying those Providers and the approach to monitoring their compliance with the Order.

3.7 Due to the nature of the telecoms security framework, the Providers' implementation of telecoms security measures will evolve and the JCRA expects to understand more about their networks, services and compliance approaches over time. For this reason, it sees compliance as an ongoing journey, which will ramp up in line with the phased implementation timeframes set out in the Code. An overview of the JCRA's planned approach for the first few years is summarised in Figure 1 below and explained further in this section of the Procedural Guidance.

Figure 1: Compliance monitoring approach for Providers with scope of the Order



~~3.8 The Authority understands that the Minister may revise the Order and the Code from time-to-time based on ongoing analysis of the threats and risks faced by Jersey and the need to maintain the security and resilience of the Island's public telecoms networks and services. This may include adding or removing Providers from the list of those identified as having to demonstrate compliance with duties under the telecoms security framework.~~

Establish requirements to demonstrate compliance with the Code

3.8 The Order defines relevant turnover as turnover from any relevant activity carried out wholly or partly in Jersey after the deduction of sales tax (GST). Relevant activity means:

- the provision of electronic communications services to third parties;
- the provision of electronic communications networks, electronic communications services and network access to communications providers; or
- the making available of associated facilities to communications providers.

3.9 Consistent with its established approach to assessing turnover for the purpose of calculating annual telecoms licence fees, the JCRA interprets relevant activity as meaning all a Provider's commercial activities except:[16]

- Non-telecoms related business
- Services carried out entirely outside the Bailiwick
- Data centre hosting and services
- Mobile handsets and accessories
- Consultancy
- Sales of CPE and customer wiring
- Managed services
- Call Centre Services

Other deductions for non-qualifying services[17]

3.10 The JCRA already collects data on relevant turnover based on the relevant activity criteria shown above for another purpose. The JCRA will use data it already holds to establish and notify Providers in scope of the Order, which it expects to do so by in April/May 2026. Where a Provider already submits turnover statements to the Authority that demonstrate relevant turnover in excess of £1 million (or equivalent) it should presume that it will be in scope of the order, nonetheless the JCRA will notify them of the outcome of its assessment by the date given previously. Providers that do not receive any notification from the JCRA at this time can assume they are not within scope of the Order and therefore will not be required to demonstrate compliance with the Code.

[16] For the avoidance of doubt, this definition of relevant activity relates solely to the calculation of turnover for the purpose of establishing the scope of the Order and not to the scope of regulatory principles or activities under the Law.
[17] Other services that a Provider can legitimately demonstrate as nor being commercial activities considered relevant activities for the purpose of establishing the scope of the Order.

3.11 From 2026, the JCRA will expand the use of data it collects to include establishing and notifying Providers in scope of the Order, including assessing movement in or out under the Order's qualifying criteria.

3.12 The telecoms security framework established by the Amended Regulations encompasses Providers of electronic communications services that may not require a telecoms licence under the Law. Where the JCRA becomes aware of any Provider in this category, it will use information gathering powers under Article 24ZC of the Law to establish whether they are in scope of the Order and therefore required to demonstrate compliance with the Code.