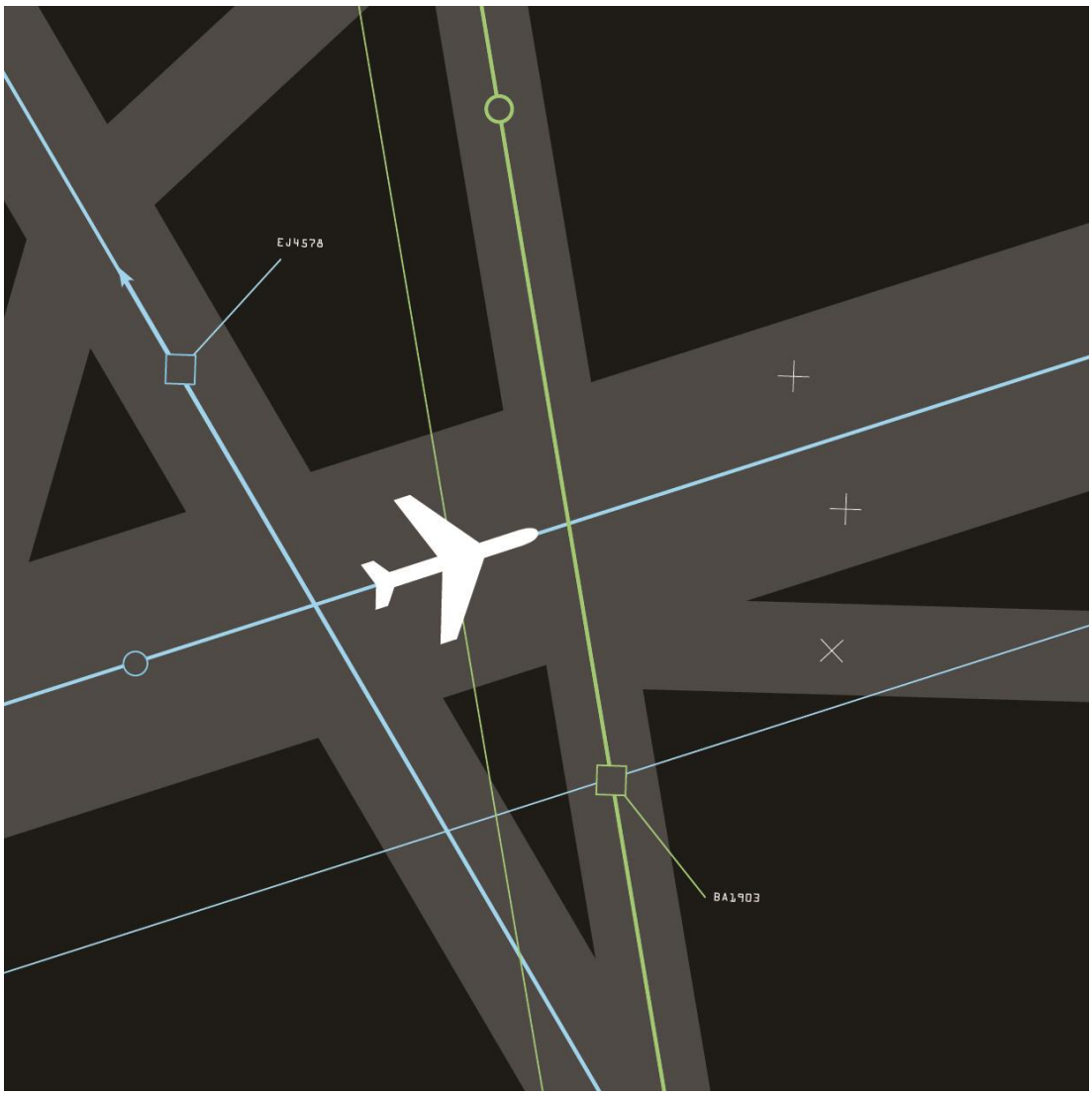
Summary Report
June 2020

# Assessment of NERL's Resilience Plan




Civil Aviation Authority
Our ref: 23531202
Client ref: 2862

steer

Summary Report
June 2020

# Assessment of NERL's Resilience Plan

Prepared by:

Steer
28-32 Upper Ground
London SE1 9PD

+44 20 7910 5000
www.steergroup.com

Prepared for:

Civil Aviation Authority
Westferry House
11 Westferry Circus
London E14 4HD
Client ref: 2862
Our ref: 23531202



steer

# Contents

## Figures



## Tables

# 1 Introduction

## Background

1.1 NATS (En Route) plc (NERL) was required to submit a Resilience Plan to the Civil Aviation Authority (CAA) by 18 March 2019 under the terms of modifications to Condition 2 of its Licence, as set out in the CAA's publication CAP 1682.

1.2 NERL was required to incorporate the guidance issued by the CAA in developing the form, scope and level of detail of the Resilience Plan. The Plan was required to set out the principles, policies and processes which will be employed to ensure that NERL will comply with its service obligations regarding resilience, contingency and business continuity, whilst "*protecting the users of those services against the occurrence and impact of disruption*".

1.3 Steer was appointed by the CAA as an Independent Reviewer to advise on the principles, policies and processes set out in the Resilience Plan in accordance with the CAA's guidance, and to identify any improvements. Steer was supported in this role by Helios, which provided technical advice on NERL's systems and processes.

## Scope of Work

1.4 The overall scope of work for the Assessment of NERL's Resilience Plan was as follows:

- Assess NATS Resilience Management System to provide a view to the CAA as to NERL's ability, through its resilience, planning and management policies and processes, to deliver the requirements of Condition 2 of the NERL Licence;
- Review the Resilience Plan to assess if the Plan, Management System and its outputs allow NERL to manage and continuously improve its service resilience, contingency and business continuity requirements;
- Comment on NERL's resilience and continuity alignment with CAA Guidance and other relevant best practice; and
- Make recommendations for improvements to the Resilience Plans by NERL.

1.5 This Summary Report presents the summarised and redacted findings of the review.

**Out of Scope**

1.6 According to our terms of reference from the Invitation to Provide a Proposal (IPP), the Independent Reviewer is not required to assess the following:

- The actual resilience of NERL's individual Information Technology (IT) systems;
- Compliance with the NIS Regulation[1] cyber security controls framework set out in CAP 1574; and
- NERL's Service and Investment Plan (SIP).

[1] UK regulation implementing EU Directive 2016/1148 on the security of networks and information systems

## Methodology

**Interaction with NERL**

1.7 Early in the project, the Independent Reviewer met with representatives of NERL at NATS' London Office to formalise arrangements for the study and was given an initial overview of the Resilience Plan.

1.8 In addition to the Resilience Plan document itself, the Independent Reviewer requested a number of supplementary documents from NATS to provide a more detailed understanding of the Plan and the resilience management system in which it operates.

1.9 The Independent Reviewer undertook two site visits, one each to the Swanwick and CTC Whiteley centres and spoke to relevant personnel involved in the management of resilience.

**Data Analysis and Review**

1.10 As the Independent Reviewer, Steer and Helios have taken an independent approach to review and analyse information provided by NERL and presented during the two site visits. We have asked follow-up questions and requested additional evidence where we perceived a gap or insufficient detail was originally provided.

1.11 The report reflects our understanding and interpretation of NERL's resilience processes, based on the information presented to the Independent Reviewer. NERL has commented that these are not necessarily consistent with its own understanding of those processes.

1.12 We have reviewed best practice guidance on Business Continuity and consulted Steer's in-house Business Continuity expert to understand the application of Industry Standard ISO 22301 in order to provide benchmarks for our review of NERL's Resilience Plan.

1.13 We have also reviewed the Business Continuity Toolkit information presented on HM Government's website, explaining how business impact analysis is conducted and how resilience thresholds are determined. This facilitates the understanding and assurance of resilience assessment performed by NATS.

## Summary of assessment

**Based on the assessment against the CAA's Guidance set out in Appendix B of CAP 1682 our assessment is that the Resilience Plan is fit for purpose and that it is consistent with the requirements set out in Condition 2 of NERL's Licence. We have identified some areas where the Plan could be improved in future iterations.**

# 2 Resilience framework

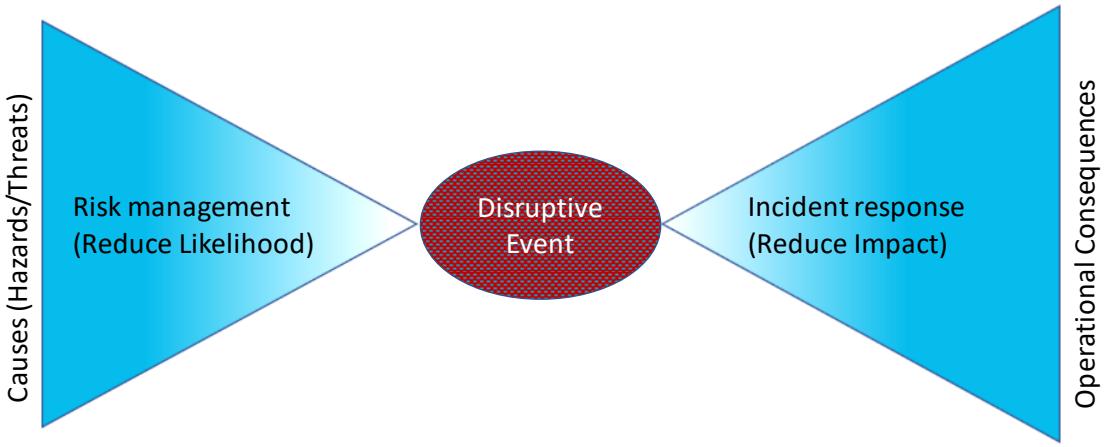
## Introduction

2.1 This chapter describes the framework NERL has adopted for its management of the resilience of its Licensed Services. We explain the core principles of resilience as part of a Business Continuity management system and describe the contents of NERL's Resilience Plan.

## Resilience principles

2.2 The concept of resilience forms part of Business Continuity Management and can be illustrated through a so-called "bow-tie" diagram, as shown in the figure below.

**Figure 2.1: Bow-tie diagram**




Source: Steer

2.3 On the left side of the diagram, management of risks is undertaken to reduce the likelihood of disruption. In NERL's Resilience Plan, this is referred to as "***proactive resilience***". On the right hand side, if a "disruptive event" (e.g. bad weather, system failure, accident) occurs, responses to incidents are made to reduce the impact of the event. In NERL's Resilience Plan, this is referred to as "***reactive resilience***".

## The NERL Resilience Plan

2.4 On 18 March 2019, NERL submitted its 52-page Resilience Plan setting out the principles, policies and processes by which NERL will comply with its obligations under Condition 2 of the NERL Licence. The Plan provides an overview of NERL's approach to business continuity and proactive and reactive resilience management. It contains a certificate from the Chief Executive Officer (CEO) stating that the directors of NERL consider that the Resilience Plan is fit for purpose and complies with its obligations under the Licence.

2.5 The Resilience Plan document is structured as follows:

- Part 1 – Background;

- Part 2 – Principles;
- Part 3 – Proactive resilience;
- Part 4 – Reactive resilience; and
- Part 5 – Maintaining and improving resilience.

2.6 Although the Resilience Plan sets out the principles of resilience management in NERL, it represents only a top-level description of the resilience management system in place in the company. Therefore, in order to assess the Plan, it has been necessary to review a wider range of documents setting out particular aspects of the approach taken. In this context, we note that the Resilience Plan itself does not include references to these other documents. However, NERL has, on request, provided a mapping of how the different elements of the resilience management system map to the different parts of the Plan.

## NERL's Resilience Assessment Framework

2.7 The Resilience Plan states that NERL uses business continuity best practice techniques, as set out in the ISO 22301 and the BCI Best Practice Guidelines 2018. The underlying principle of this approach is to identify the extent to which failures in NERL's assets (hardware such as radars and computers and the software which runs on them), or in its availability of air traffic control officers (ATCOs) or of technical staff, would lead to disruption of its normal (licensed) activities. Where this disruption would trigger the formal intervention thresholds set out in CAP 1682[2], NERL needs to determine whether to:

- strengthen the barriers to disruption occurring (**proactive resilience**);
- strengthen its ability to recover from the disruption more quickly (**reactive resilience**); or
- accept the risk of disruption (for example, because the likelihood of its occurring is sufficiently small, or because the investment required to improve either proactive or reactive resilience is too great compared to the problems which would be caused if the disruption were to occur).

2.8 In establishing the Resilience Plan, NERL undertook an assessment of its level of confidence in the proactive and reactive resilience of each of its major asset and key staff groups. For proactive resilience, in particular of technical assets, the level of confidence relates to the probability of failure of the asset being sufficiently low. This assessment is linked to the safety cases for the assets. These safety cases are themselves validated through NATS' Safety Assurance Process, which is overseen independently by the CAA.

2.9 For reactive resilience, the level of confidence relates to the ability, following a disruptive event, to recover functionality before disruption reaches an unacceptable level. This is assessed through the process of Business Impact Analysis, described below.

## Business Impact Analysis (BIA)

### Overview

2.10 In the development of the Resilience Plan, NERL undertook a Business Impact Analysis (BIA) to assess the level of resilience within the organisation under disruption. BIA is an industry standard approach described in ISO 22301 and the BCI Good Practice Guidelines to assess the impact of disrupting activities, identifying dependencies for service provisions and to evaluate business continuity and recovery priorities.

[2] CAP 1682, Appendix C, Table 1, Levels of performance for CAA intervention and licence enforcement

2.11 For proactive resilience, the BIA involves assessing the likelihood of failure of each key service, capability or resource used by the organisation. For proactive resilience, the BIA process consists of identifying the length of time after any such failure which is likely to lead to an unacceptable level of impact on the operation. A suitable "Recovery Time Objective" to restore the relevant capability is then established to avoid this unacceptable impact. The process used by NERL is consistent with the process outlined on the HM Government's website describing the Business Continuity Management Toolkit[3].

**Resilience by Major Asset**

2.12 The BIA process involved a range of experts within NERL. The level of resilience for each asset was reviewed by the relevant Subject Matter Experts (SMEs) for that asset within NATS, rating the level of confidence in the proactive and reactive barriers as high, medium or low. For proactive resilience this review was based on the Asset Management processes described below. For reactive resilience, the review was based on whether the expected recovery time of the asset was achievable within the Recovery Time Objective (RTO).

2.13 The BIA identified high confidence ratings for resilience across the large majority of NERL's assets but recommended exploring enhancements on a small number.

2.14 Confidence tended to be stronger in relation to proactive resilience than for reactive resilience, reflecting the high reliability of NERL's technical systems but also the high level of disruption which would rapidly occur should they become unavailable. This imbalance is understandable, as the BIA approach focuses on the highly negative impact of a complete failure of an asset, however rarely occurring, rather than on the lesser impact of a potential partial failure (which might be more frequent).

## Summary and assessment

**The Resilience Plan document submitted by NERL captures many existing management policies, procedures and processes relevant to NERL's resilience in a condensed way. However, while some reference is made to management processes, the Plan does not contain any references to the underlying documents detailing the processes described in the Plan. Including such references would represent an improvement.**

**The NATS' resilience framework explained in the Plan is consistent with the standard industry practice for business continuity. It also addresses the objective of the change to Condition 2 of NERL's Licence by developing a framework which takes into account the enforcement triggers set out in the CAP 1682 modifying NERL's licence in respect of resilience requirements.**

**The Business Impact Analysis (BIA) used in developing the Plan is consistent with the approach set out in HM Government's Business Continuity Management Toolkit. There could be additional value in also considering the impacts of partial failures of assets (and the time needed to recover from them) as well as the consideration of complete failures undertaken in the standard BIA approach.**

3 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/137994/Business_Continuity_Managment_Toolkit.pdf

# 3 Risk identification and mitigation

## Introduction

3.1 This chapter describes NERL's processes for risk identification and mitigation. These form a key element of Business Continuity Management and represent the "proactive resilience" part of the bow-tie diagram in Figure 2.1. They are described in Part 3 of the NERL's Resilience Plan (Proactive resilience).

## Proactive resilience links with NATS' Management System (NMS)

3.2 Risk identification and mitigation are key elements of business continuity management and represent the "proactive resilience" part of the process. The processes for supporting proactive resilience set out in the Resilience Plan form part of an eco-system of assurance processes within NERL's Management System (NMS) which are highly interlinked. Indeed, much of the confidence in NERL's proactive resilience stated in the Resilience Plan depends on these other assurance processes, which in organisational terms significantly pre-date the development of the Resilience Plan itself. Therefore, it is important to understand the links between proactive resilience of the technical assets and:

- **Asset Management**, the hardware and software of NERL's core technical systems;
- **Safety Management**, processes to ensure technical systems support safe operations (safety aspects of people-related issues are considered separately); and
- **Risk Management,** NERL's overarching process for managing all risks.

3.3 The section below documents NERL's Asset Management, Safety Management and Risk Management processes.

## Asset, Safety and Risk Management

**Asset management**

3.4 NERL manages assets using a risk-based approach under an ISO55001 certified asset management system, following its defined Asset Management Policy (AMP).

3.5 Technical assets lie at the heart of NERL's capability and their reliability is fundamental to the effectiveness of NERL's operation as well as its overall resilience. There are a number of rigorous processes for managing NERL's technical assets, both hardware and software. Each asset is under the authority of a technical expert, the Asset Design Authority (ADA), who has responsibility for its design and safe and reliable operation. Groups of assets, which together form a functional system (such as Surveillance), are under the authority of a System Design Authority (SDA, a more senior role).

3.6 Each system is analysed to gain an understanding of how it may fail, using formal techniques such as:

- Failure Modes Effects Analysis (FMEA);
- Functional Failure Analysis (FFA); and

- Fault Tree Analysis (FTA).

3.7 FMEA reviews the ways in which an asset can fail. FFA (an extension of FMEA) considers potential focuses on interfaces between systems. FTA provides a quantitative analysis of likely failure rates. In addition to these formal analysis techniques, the Field Service History (i.e. actual performance while in operation) is reviewed to strengthen the understanding of the likelihood and causes of any failures.

**Safety Management**

3.8 Safety lies at the heart of NATS' business and the NATS Safety Management System describes the organisation's commitment to safety and associated procedures and required standards. Safety management and asset management are highly interlinked, and the processes used to assure that NERL's technical systems are managed safely also feed into the assessment of those systems' levels of resilience.

3.9 All the information on safety criteria and approval of system safety cases is recorded in the "safety assurance" documents. The analysis of the system design uses techniques such as FMEA and FFA identifying how a system may fail. Quantitative analysis based on the component parts of the system and known reliability/performance data uses techniques like FTA to verify that the components of the system behave as specified. Safety management thus utilises similar techniques to those forming part of the asset management process.

3.10 NERL has confirmed that safety cases exist for all its major technical assets. These safety cases are subject to independent verification by the CAA. Therefore, safety cases generally underpin the proactive resilience analysis of NERL's technical assets (although the likelihood of safe operation and of resilient operation are not necessarily identical, since some "failsafe" back-up safety solutions may result in an interruption or reduction in the level of service provided).

**Risk Management**

3.11 NERL's Risk Management Policy and Risk Management Guidance outline the approach to be taken for the identification, evaluation and cost-effective control of risks, preventing them from materialising into issues and minimising impacts on business objectives. Risk Management is an overarching process which documents issues identified in the Asset and Safety Management processes (*inter alia*) and links to the Resilience Management process.

3.12 Through the Risk Management Process, documented in the NATS Management System (NMS), decisions are taken either to eliminate risks or to reduce them to a tolerable level. Identified risks are subject to an evaluation whose output is logged onto the risk database. A Risk Owner is assigned to each risk and is accountable for reviewing, monitoring and reporting on the risk. A risk could be treated in four different ways:

- close the risk;
- cancel the risk;
- treat the risk; or
- manage the risk (whereby a risk is accepted and does not receive treatment, but continues to be monitored).

3.13 If the decision is made to manage the risk, the review on the validity of this decision takes place several times per year. The outcomes of these reviews are documented on the risk register and routinely communicated to the Risk Owner. Closing or cancelling a risk only takes place if it is perceived no longer to be applicable. Otherwise, risks must be "treated" or

accepted and “managed”. This approach is applied to NERL’s resilience processes to deal with risks arising in respect of both proactive and reactive resilience.

## Cyber Security

3.14 Cyber security is an important contributor to resilience. In the past, ATM systems were designed and built to only address unintentional hazards and events, whereas cybersecurity addresses intentional threats (i.e. malicious intent). A cyber-incident may be particularly of concern to resilience as it can, in effect, be a common cause failure; i.e. the same security vulnerability may be present in redundant and fall-back systems, so traditional approaches to reliability and resilience do not necessarily readily apply. Cyber-incidents which cannot be contained may spread quickly across ATM infrastructures.

3.15 Therefore, a multitude of controls is applied across people, process and technology, with a focus on defence-in-depth. These include a strong security awareness culture, additional protection on devices, regular security risk assessments and threat intelligence gathering.

3.16 NERL is covered by the NIS regulations. The CAA's approach to cyber-oversight of NERL is centred within its ASSURE programme, which is out of scope of this study. Therefore, this document does not analyse NERL cybersecurity further.

## D-SESAR

3.17 D-SESAR (Deploying SESAR) is the programme within NATS to deploy a next generation operational system, aligned to the European SESAR (Single European Sky ATM Research) initiative. As part of the D-SESAR programme, NATS has established a number of projects to deliver specific aspects of the future systems, and to establish transition arrangements from the current systems to the future systems. The projects under the D-SESAR programme are managed using the formal NATS Project Management processes, while system change is managed using the NMS (NATS Management System) Manage Change process.

The D-SESAR programme aims to refresh every aspect of the NATS Operational environment. While this will deliver clear benefits, the introduction of D-SESAR may present challenges to maintaining resilience, as there will be less scope to rely on service history performance as an indication of reliability, while the need for parallel running of legacy systems and D-SESAR during its introduction will lead to a need for additional effort to ensure resilience during the transition.

## Staff-related resilience measures

3.18 The delivery of the resilience of the Core Services depends on the level of appropriately skilled staff, both ATCO and engineering staff, including both proactive and reactive resilience measures.

3.19 Proactive measures include the planning of both demand and supply of staff. The demand side includes a review of anticipated seasonal airline schedules and more tactical considerations closer to the day of operation. Rostering supply takes into account the sustainability of the operations, whilst supporting the investment programme and various business change projects.

3.20 Agreements between NATS and its staff are in place to facilitate flexible working arrangements, in order to deliver the satisfactory level of service to customers. The Working Practices Agreement (WPA) applies to operational shift working ATCO staff, setting out rostering criteria, additional and contingency arrangements. Additional proactive measures for

individual staff resilience include programmes and mechanisms in place to prevent work-related occupational health issues and vaccines programme for seasonal flu. *Note that this review predated the COVID-19 pandemic, which has therefore not been considered.*

3.21 In the event of disruption, the WPA and other staff arrangements such as the ATCO Voluntary Additional Attendance (VAA) agreement allow for mitigation actions including redeployment of staff, overtime, swapping of shifts, recalling of training and cancellation/sale of leave, providing a measure of reactive resilience.

3.22 For events where the staff shortfalls are widespread or span multiple shifts, such as road conditions due to severe weather, the Silver Team (see Chapter 4) will coordinate the response following Incident Management procedures.

## Summary and assessment

**This chapter has outlined NERL's practice on proactive resilience management of assets in the interlocking system of risk, asset and safety management, which forms the basis of the proactive resilience assessment and drives the rating of the confidence level in their proactive measures.**

**We assess there are detailed and comprehensive asset management processes which ensure assets and systems are regularly monitored, providing assurance that these assets are operating and behaving within expectations. We also assess that NERL has a robust and comprehensive approach to safety management and that the safety cases for its assets underpin the assessment of their proactive resilience. However, care needs to be taken to distinguish between the level of safety assurance and the level of resilience, since not all backup systems and processes designed to facilitate safe operation also allow for unimpaired business continuity.**

**Based on the evidence made available to us, our assessment is that the overall approach to Risk Management at NERL appears reasonable and consistent with best practice.**

**The actual resilience of NERL's individual IT systems and compliance with the NIS Regulation cyber security controls framework are out of scope, however we have summarised the general procedures and incident response of cyber security.**

**The D-SESAR programme is a challenging initiative which aims to refresh every aspect of the NATS Operational environment. The introduction of D-SESAR will present particular challenges to maintaining resilience. Firstly, as a new system, there will be less scope to rely on service history performance as an indication of reliability. Secondly, the parallel running of D-SESAR and legacy systems during its introduction will lead to a need for additional effort to ensure resilience during the transition.**

**NERL depends on the availability of highly skilled operational (ATCO) and technical staff. There are extensive planning procedures in place to define the required staff level from the demand forecasting of traffic and available staff level from supply constraint assumptions. Additional arrangements supplementary to the rosters allow greater flexibility to adjust staff level depending on the day operations.**

# 4 Incident response procedures

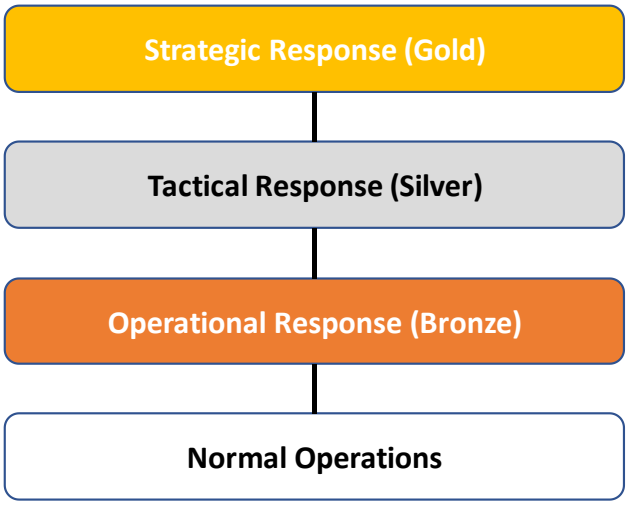
## Introduction

4.1 This chapter describes NERL's approach to responding to disruptive incidents (reactive resilience). The approach, set out in Part 4 of the Resilience Plan, includes a range of different activities which are referred to by the Plan. In most cases these activities already existed when the Plan was drafted. The description of reactive resilience in the Plan is largely extracted from a number of source documents, although these are not explicitly referenced and there is sometimes a lack of clarity over which source documents are definitive.

## Framework for incident response

4.2 The framework for responses to disruptive incidents is set out in a 2019 document, NERL's Core Services Resilience Response Plan. The Resilience Response Plan describes a "response architecture" for NERL's response to disruptive incidents, based on different layers from "normal operations" to the bronze, silver and gold incident response levels used by NERL to describe its "command and control" procedures. This is shown in the figure below.

**Figure 4.1: NATS' Incident response architecture**




Source: NERL's Core Services Resilience Response Plan (adapted)

4.3 The structure illustrated in Figure 4.1 is consistent with the industry standard 'Command and Control' structure described in NATS' incident management framework, comprising a hierarchical structure of Gold, Silver and Bronze Incident Management Teams. This system is used extensively by the UK civil emergency services based on the Civil Contingencies Act 2004 Guidance.

4.4 The strategic response (gold) is at the corporate level, the tactical response (silver) is at the level of NATS' major facilities such as its ATC centres and the operational response (bronze) is at the functional level. In parallel with the arrangements for setting up Gold, Silver and Bronze

incident response teams, suitable dedicated communications facilities are established during significant disruptions to facilitate critical communications to internal and external stakeholders during incidents

## Managing responses to disruption

4.5 This section describes the stages of managing a disruption and the expected responses by the ATC, Engineering and Facilities Management services respectively.

**Disruptions response process stages**

4.6 The Resilience Response Plan applies to disruptive events above a threshold broadly corresponding to "moderate" delay or disruption, as defined in CAP1682 Appendix C, Table 1 ("Levels of performance for CAA intervention and licence enforcement"). As soon as an incident occurs, an Operations Management Team (OMT) is formed, comprising the relevant senior operational staff. An initial assessment is then made as to how to handle the incident, depending on the expected level of delay or disruption.

4.7 Where it is determined that it is not possible to return to business as usual, the OMT will hand over the incident response to a "bronze" team and return to its day-to-day role to ensure that normal procedures continue to be managed. An incident management process will be invoked, involving bronze, and potentially also silver and gold, response teams. During the incident, there will therefore be parallel management processes, with service delivery managed by the OMT and the incident itself being managed by gold/silver/bronze command and control processes. Managing the response may require the ATC service to continue at reduced capacity.

4.8 Once it has been possible to restore the service to an acceptable level, the ATC service can be restored to normal levels of operation. Traffic regeneration processes can be implemented if required to allow flights to return to normal operation. Once this is achieved the incident response can be stood down and normal management procedures are resumed.

**Responses by ATC, Engineering and Facilities functions**

4.9 When a disruptive event that has potential to reduce ATC capacity is detected, the general behaviour and response follow the procedures set out in a "First Actions Checklist", which sets out how to respond. An approach called "Pause for Thought" (P4T) is applied, as shown in Figure 4.2. P4T is a technique to prompt managers to step back and think through emerging issues, ensuring that safety considerations remain the top priority under high pressure situations.

**Figure 4.2: Pause for Thought**


Source: NERL's Core Services Resilience Response Plan

4.10 Regardless of the cause of a disruptive event, there is usually an immediate increase in ATCO staff workload. The actual manageable traffic levels are likely to depend on the particular nature of the incident and will be determined tactically, depending on operational factors such as ATC impact, sector staffing distribution, operating conditions like weather, and time of failure (early morning or evening).

4.11 The Resilience Response Plan also describes in more detail how traffic continuity is provided during the period of the disruption. These can include measures regulating or stopping aircraft departures and rerouting of aircraft.

4.12 A likely cause of reduction in operating capacity is a loss of technical capability. The process for restoring lost capability is set out in NERL's incident management procedures, which we have reviewed. These include measures to resolve the technical problem identified or, if necessary, to escalate to the relevant support team. Analogous to the ATC response, the general response is guided by 'Take-5' for engineering as shown below (Figure 4.3), intended to ensure that a measured and systematic approach is adopted.

**Figure 4.3: Take-5 Engineering Response**


Source: NERL's Core Services Resilience Response Plan

4.13 Facilities Management is tasked with providing a response to issues affecting the operations environment. It has well established procedures responding to different types of incident affecting the physical facilities which support both operational staff and the technical systems.

**Loss of Operations Centre**

4.14 NERL has specific plans for the situation when one of the two Operations Centres, Swanwick or Prestwick, ceased to be available. Clearly this situation would represent a very serious disruption, likely to have been caused by a major incident. The plans include processes for providing a (modified) air traffic service in such circumstances, which have been explained to the Independent Reviewer.

## Stakeholder management

4.15 In parallel with the Gold, Silver and Bronze incident response teams, dedicated communications facilities are established during significant disruptions. NATS' Air Traffic Incident Customer Communications Cell (ATICCC) is a communications facility to update customers on operational issues, set up when Silver command has been invoked. When activated in the event of disruption, ATICCC provides regular updates on the operational impact of the incident, including applicable network management and airspace restrictions.

## Capacity Prioritisation

4.16 In the event of a loss of airspace capacity, NERL's primary operational reaction is to ensure safety is the priority regardless of the cause. This was emphasised during the Independent Reviewer's visits to the Swanwick and CTC centres. While important, the service continuity aspects of resilience are necessarily considered secondary to safety. However, the procedures adopted have consequences for the resilience of the service and in particular how scarce capacity is prioritised following a disruptive event.

4.17 Depending on the nature and the scale of an event, capacity restrictions may initially be applied to reduce the traffic in the airspace, and hence the loading on the systems and staff. These will be set to maintain the maximum throughput consistent with safe operation. The capacity restrictions may be applied either to the entire airspace, or to one or more sectors. Departure restrictions will be applied if needed in order to ensure that aircraft in flight can be handled safely, with all aircraft being treated equally on a first-come-first-served basis.

4.18 In the event of capacity restrictions, NERL will also liaise with neighbouring ANSPs and the Eurocontrol Central Flow Management (CFM) Unit to ensure that the number of flights entering UK airspace is maintained at a manageable level. The neighbouring ANSP may choose to re-route and slow aircraft in flight and hold aircraft on the ground where needed to accommodate this. Regulations are generally communicated to airlines via Eurocontrol.

## Summary and assessment

**NERL has a sophisticated, well thought-through and documented set of procedures to deal with foreseeable causes of disruption. However, these procedures are not well referenced in the Resilience Plan itself and there would be benefit in some streamlining of the documentation.**

**The Gold, Silver and Bronze hierarchy of the Command and Control structure within NATS is consistent with the Civil Contingencies Act 2004 Guidance and is widely used by the UK civil emergency services. Considerations of NATS' reputational risks and critical communications to internal and external stakeholders during incidents are incorporated in the design of the dedicated incident management rooms and communications facilities.**

**There are well-defined procedures for invoking incident management teams while simultaneously maintaining management of the ongoing ATC service. The approaches to managing disruption for each of the ATC service, technical and Facilities Management are well thought through and include techniques to support staff decision-making under pressure.**

**There are specific plans to deal with the situation where an Operations Centre ceases to be available, indicating that NERL has fall-back procedures to cope with even the most extreme circumstances. These appear to be appropriate.**

# 5 Establishing and maintaining resilience processes

## Introduction

5.1 This chapter describes how NERL has established and intends to maintain its resilience processes. The first section describes the processes NERL undertook to establish its resilience management system. The chapter then describes NERL's processes for maintaining and improving its resilience management system, as set out in Part 5 of the Resilience Plan. It then goes on to consider a key element of this maintenance/improvement process, namely the undertaking of exercises to practise NERL's response to disruption and learn lessons from the process.

## Establishing NERL's resilience management system

5.2 To establish its resilience management system, NERL undertook an internal Resilience Assessment, with recommendations for improvements to be made. These were then translated into a "Resilience Direction" document, setting out how these improvements were to be delivered.

5.3 The Resilience Assessment included undertaking a Business Impact Analysis (BIA) in 2018 which was presented to NERL's Business Continuity Steering Group. The BIA identified high confidence ratings for resilience across the large majority of NERL's assets but recommended exploring enhancements on a small number. In addition, areas for improvement were identified in relation to some business processes.

5.4 In advance of the development of the formal Resilience Plan, the resilience enhancement decisions and proposals for implementation were collated into a resilience direction document. Other enhancements were more general and applicable across most businesses within NATS. The Resilience Project Team was asked to lead work across all workstreams, including on:

- the architecture of business processes, ensuring incident management and response aligns with business continuity objectives;
- training to embed capability amongst key resilience staff;
- briefing and supporting the transition to the full time Business Continuity Manager; and
- operationalising the NMS process and embedding the process for assuring resilience.

5.5 All Resilience Leads were required to review, enhance and develop response plans that could provide continuity during disruption and integrate with Incident Management procedures, taking into account the Resilience Thresholds. Specific actions involved reviewing the current arrangements and contracts with critical suppliers or call-out teams and assessing how suppliers meet NATS' resilience and continuity arrangements. Future process and programme should be developed to assess suppliers' resilience and continuity arrangement in complying

NATS' requirements. Enhancements were required on NATS' risk processes and database to align risk and resilience planning.

## NERL's processes for maintaining and improving resilience

5.6 NERL's processes for maintaining and improving resilience are set out in Part 5 of the Resilience Plan. The Plan describes how NERL intends to manage resilience and to continuously improve its resilience processes, based on recognised guidance and standards, including ISO 22301 (Business Continuity), ISO 22316 (Organisational Resilience), ISO 31000 (Risk Management), ISO 22320 (Incident Response), BS11200 (Crisis Management) and the BCI Good Practice Guidelines 2018.

5.7 The Plan sets out NERL's approach to each of the following aspects of the resilience management system:

- **Governance of Improvement.** At the top level, the Board hold the ultimate accountability for the effectiveness of its resilience and will submit an up-to-date Resilience Plan with a certificate to the CAA every two years affirming NERL's effectiveness. The Business Continuity Manager leads operational level resilience and business continuity within NATS. At the operational level, Service Resilience Leads ensure that coherent and effective proactive and reactive resilience arrangements are implemented and understood by wider NATS staff.
- **Continuous Improvement.** Resilience management is integrated into the NATS Management System (NMS) so that it can feed into multiple other NATS processes and reflect the top level NATS Quality Management Policy. Continuous improvement is governed by the BC Steering Group and follows best practice.
- **Assurance.** Assurance of effective resilience is evidence-based within the categories of People, Policies/Processes/Plans and Technology assurance. People aspects involve proactive planning for staffing, ongoing training for disruptive events, incident and crisis management training, and exercising. Policies, process and plans include assessment and assurance of their accessibility, their compliance with policy, regulation, standards, and the adequacy of document control. Technology assurance includes its availability, reliability and security aspects.
- **Resources, Roles and Responsibilities.** Key resilience roles require specific competency and are allocated based on the experience and expertise. These staff attend relevant training, exercises and test as individuals and as formed teams.
- **Capability: competence, tests and exercises.** All teams and individuals with resilience responsibilities are required to take part in individual and collective training for upskilling and develop their experience through tests and exercises (described in more detail in the next section).
- **Awareness and Communications.** An internal communications plan has been developed to raise awareness of the Resilience Plan and its work. This involves engaging key stakeholders across the business and promoting an understanding of the importance of Business Continuity and resilience to wider staff.

## Scenario planning and exercises

5.8 As noted above, all teams and individuals with resilience responsibilities are required to take part in individual and collective training for upskilling and develop their experience through tests and exercises. Staff with resilience responsibility, resilience planning and/or response, receive specific training to ensure that they can fulfil their specified role. Competence is

mapped and training is monitored on an ongoing basis. For ATC operational staff, Training for Disruptive Events is covered within the wide range of ongoing operations training programmes and is tailored according to role.

5.9 The NATS Business Continuity Manager maintains the exercise programme and has oversight of this activity. Service Resilience Leads provide assurance reporting to the Steering Group that this requirement has been fulfilled. Any lessons learned and improvements captured from these exercises are fed into the process for lessons learned and corrective actions/enhancements. The process shall ensure that the root causes are identified and corrective actions are defined to close these out.

## Summary and assessment

**NERL has adopted a thorough approach to establishing its resilience management system. It has followed the initial assessment with a programme for improving its resilience processes, which it appears to be following. Some areas for improvement remain, but NERL has recognised these and we understand is working to address them.**

**NERL has set out a comprehensive strategy for the management and improvement of its resilience management processes. While these appear to be appropriate in principle, NERL will need to demonstrate that this is effective in practice, particularly in the context of the complex interaction between resilience and other NERL Management System (NMS) processes such as Risk, Asset and Safety Management.**

**NERL has comprehensive training programmes and exercises for key operations staff such as ATCO, engineering staff and incident management teams. These programmes and exercises have different formats (desktop or simulator exercises) and are designed to best fit individuals' resilience responsibilities. Exercises involving multiple teams are important in improving the coordination and communications between teams. Based on the evidence provided to the Independent Reviewer, the exercises are appropriate and the lessons learned are fed into the continuous improvement process. The Resilience Plan clearly specifies how frequently these exercises should be undertaken.**

# 6 Assessment and recommendations

6.1 This chapter presents a summary of the Independent Reviewer's assessment of NERL's Resilience Plan in fulfilling the guidance issued by the CAA under the resilience licence condition, drawing together all the documents provided by NATS and discussions during the site visits. We then provide our Recommendations.

## Assessment against CAA Guidance

6.2 The table below lists out the core criteria set out in Appendix B of CAP1682, and our assessment. We have scored the criteria with the standard Red/Amber/Green (RAG) classification, where:

- Green indicates that the Plan is acceptable against the criterion (with possibly minor improvements possible);
- Amber indicates that areas for improvement in the Plan with respect to the criterion have been identified; and
- Red indicates that there are significant concerns with the Plan in respect of the criterion.

6.3 The RAG assessment should not be interpreted as stating whether the particular aspect is compliant with NERL's Licence, which is for the CAA to determine.

**Table 6.1: Assessment of Resilience Plan against CAA Guidance**

| Criteria set out in Appendix D of CAP 1682 | High-level Comments | RAG |
|---|---|---|
| The resilience plans should: | | |
| • Include a clear, high-level overview of NERL business continuity and resilience, both preventative and reactive, covering all aspects of the business, including its assets, personnel and systems that NERL relies on to supply the services required by its Licence. | The Plan does provide this high-level overview of each of these aspects. As noted below, the links to the underlying documents are not fully explicit. | |
| • Draw on existing documentation, policies and plans to show how NERL will minimise the risk of the occurrence of, and minimise the impact of, the loss of key IT systems, infrastructure, personnel and suppliers. | Existing policies and plans are cited in the Resilience Plan covering these elements. However, the Plan does not generally reference directly to existing documentation. | |

| Criteria set out in Appendix D of CAP 1682 | High-level Comments | RAG |
|---|---|---|
| Policies in place to provide Proactive Resilience: | | |
| 1) Risk assessment and management; | Risk assessment is guided by underlying processes within safety, asset and risk management. This is supplemented by the resilience assessment (Business Impact Analysis, BIA), though it is not entirely clear how the BIA integrates into the existing decision-making process. | |
| 2) Asset management; | Asset management is underpinned by quantitative analysis and regular system health checks, and we assess that the asset management in place supports proactive resilience. However, the asset management quantitative analysis is focused principally on safety, rather than resilience, so care needs to be taken when the fall-back option provides a reduced level of service. | |
| 3) Reliability and redundancy measures to enable systems to continue to function despite disruptive events (including errors or loss of data, failure of system components, denial of service attacks, loss of power, etc.). | These measures are built into the design of systems and validated through the quantitative analysis underpinning safety cases for each asset. | |
| 4) Staff planning to ensure as far as practicable that adequate numbers of qualified staff are available to fulfil the service performance regime established for the relevant reference period. | Strategic and tactical planning determine the number of staff required and supply side planning feeds into rostering construction. | |
| Policies in place to assess the value and effectiveness of relevant barriers that will be specified in new systems, architecture and business models. | The approach to managing the resilience of D-SESAR is essentially the same as that used for existing systems. However, it is recognised that the service history evidence currently used will not be available for new systems and the introduction of D-SESAR will present particular challenges to maintaining resilience. | |
| Policies and procedures in place to provide reactive barriers to minimise and mitigate the impact of disruption on services: | | |
| 1) Incorporating measures into systems to allow them to continue to provide a reliable service during an unexpected event. | The in-built redundancy in NERL's systems will provide continuity of service in many situations, underpinned by the analysis undertaken for safety cases. | |

| Criteria set out in Appendix D of CAP 1682 | High-level Comments | RAG |
|---|---|---|
| 2) Plans for service fall-back and recovery, to provide a service where possible without compromising safety, both during and following a disruptive event. | There are extensive fall-back plans for different modes of failure within the air traffic operations and engineering responses involving third party contractors and support. | |
| 3) Plans for short term additional resource requirements whether as part of resilience plans for non-staff disruptive events or for specific staff based disruptive events. | Working Practices Agreement (WPA) and ATCO Voluntary Additional Attendance (VAA) documents provide evidence on the flexible working arrangement to cover short term additional resource requirements by recalling staff and safety is not compromised by operating airspace at manageable level. | |
| 4) Command and control – e.g. clear rules for triggering different command levels; formal training, practice and testing regimes for command level leaders; clear levels of authority (including spending authority); regular testing of facilities and equipment for command and control. | These are clearly set out in NERL's resilience plan documents. | |
| 5) Stakeholder management – processes for keeping stakeholders informed on a regular basis of the situation, the likely size and duration of the impact and alternative arrangements available, such as rerouting. | The processes for communicating with stakeholders during an incident, including the ATICCC facility, are well designed and resourced. | |
| 6) Policies and procedures for capacity reallocation and prioritisation, to the extent available to NERL, during the recovery process, (such policies and procedures having been subject to consultation with stakeholders). | NERL has clear policies on capacity prioritisation. It is working with the rest of the industry to facilitate service recovery, through the Industry Resilience Group. | |
| 7) Exercises – continuous improvement / lessons learned: e.g. regular (to be decided in accordance with risk assessment processes) table top and practical exercises, where relevant in collaboration with stakeholders; reviews of exercises and actual events, including an assessment of the effectiveness of the current plans in light of the findings of those reviews. | NERL has comprehensive training programmes and exercises for key operations staff such as ATCO, engineering staff and incident management teams. The exercises are assessed to do what is required and capture lessons learned which are fed into the continuous improvement process. The Resilience Plan clearly specifies how frequently these exercises should be undertaken. | |
| 8) Options for rerouting services where possible to alternative sectors. | There are procedures in place for rerouting, depending on the nature of the disruption and on-the-day demand. | |

| Criteria set out in Appendix D of CAP 1682 | High-level Comments | RAG |
|---|---|---|
| 9) Contingency arrangements for offering an alternative service from an independent location. | Documentation on Contingency Plan is clear and well-thought, including limitations and risks of the Plan. | |

## Summary of assessment

**Based on the assessment against the CAA's Guidance in Table 6.1, our assessment is that the Resilience Plan is fit for purpose and that it is consistent with the requirements set out in Condition 2 of NERL's Licence.**

**However, we have identified some areas where the Plan could be improved in future iterations, as set out in our recommendations below. These are based on the findings from the main body of the report, as well as this chapter.**

## Recommendations

6.4 Our recommendations for improvements to the Resilience Plan are set out below.

6.5 The top-level Resilience Plan has been created subsequent to most of the constituent plans and procedures which it documents. The Plan does not reference these constituent plans in a robust and consistent manner, making it difficult to trace down the high-level statements in the Plan to the underlying documents. This referencing should be improved in subsequent versions.

- In addition, a mapping of the elements of the Plan to the CAP 1682 Guidance should be provided.

6.6 The Business Impact Analysis process is fundamentally sound. However, for most of the assets, NERL relies heavily on their proactive resilience (in which its experts have "high confidence" in most cases). We recommend the following enhancements:

- NERL should undertake an assessment of a wider range of disruption impacts for each capability, considering not just a situation of total failure (with a very low probability of failure), but also partial failures (with a higher likelihood of occurrence). This analysis would be likely to lead to a more balanced reliance on reactive as well as proactive resilience. We assess such balance to be desirable in principle, avoiding the situation where the reactive resilience criteria are not met for the loss of a large number of capabilities, while recognising that potential cost implications also need to be considered.
- NERL needs to ensure that, where the assessment of proactive resilience is based on existing Safety Cases, the assumptions in the Safety Cases are consistent with continued operation at normal levels of service (rather than just safe operation at lower or zero capacity).

6.7 While in principle, NERL's resilience processes can be applied to the new D-SESAR operational systems, the fact that this is such a large step-change means that it would be appropriate to develop enhanced resilience procedures for D-SESAR, particularly since, unlike with existing systems, it will not be possible to verify their reliability through Service History. An approach to the resilience of D-SESAR is set out in the Resilience Plan, but more detail could usefully be provided.

## Control Information

**Prepared by**

Steer
28-32 Upper Ground
London SE1 9PD
+44 20 7910 5000
www.steergroup.com

**Prepared for**

Civil Aviation Authority
Westferry House
11 Westferry Circus
London E14 4HD

**Steer project/proposal number**

23531202

**Client contract/project number**

2862

**Author/originator**

Peter Wiener

**Reviewer/approver**

Stephen Wainwright

**Other contributors**

Michelle Kwok, Andy Boff

**Distribution**

Client: Steer:

**Version control/issue number**

Summary Report – v07

**Date**

16 June 2020

# Complex questions.
# Powerful answers.

Explore **steergroup.com** or visit one of our 21 offices:

Bogotá, Colombia
Bologna, Italy
Boston, USA
Brussels, Belgium
Leeds, UK
Lima, Peru
London, UK
Los Angeles, USA
Manchester, UK
Mexico City, Mexico
New Delhi, India
New York, USA
Panama City, Panama
Rome, Italy
San Juan, Puerto Rico
Santiago, Chile
São Paulo, Brazil
Toronto, Canada
Vancouver, Canada
Washington DC, USA

steer