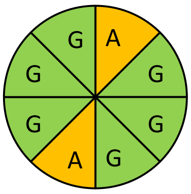
Internal Audit

NHS
Lothian

Business Continuity Planning

June 2016

Report Assessment



This report has been prepared solely for internal use as part of NHS Lothian’s internal audit service. No part of this report should be made available, quoted or copied to any external party without Internal Audit’s prior consent.

Contents

Introduction

This audit reviewed the effectiveness of business continuity management (BCM) arrangements within NHS Lothian. The Board is required to have BCM arrangements in place which are kept up to date and tested to ensure they can assist in the continuity of services in adverse circumstances, and comply with regulations and guidance. Without appropriate BCM arrangements, NHS Lothian would not be considered adequately prepared if operational activities were adversely impacted. The lack of preparedness could mean service areas where resilience is weak are not identified and the opportunity to mitigate risk is lost.

For NHS Lothian, interruption may be defined as any disruptive challenge that threatens the continuity of service provision, for example impacts on personnel, buildings or the operational procedures of the Board and which requires special measures to be taken to restore normal operating functions. The ability, therefore, to be able to anticipate, prevent, mitigate and respond to unexpected events and provide continuity of service is critical to NHS Lothian.

The effectiveness of these BCM plans requires a structured and methodical approach to identifying critical business processes, contingent resources, and optimal management strategies as well as robust maintenance and test processes. The effectiveness of preparations requires the involvement of staff from all areas of the organisation so that departmental and corporate aspects of BCM work well together and staff have the necessary skills and understanding to apply BCM in practice.

Scope

To determine whether business resilience plans and capabilities are up to date, embedded in the organisational culture, adequately communicated and regularly tested. The objectives of our review were based on the international standard ISO22301 (the international business continuity standard) and Scottish Government guidance. This report uses the terms BCM and resilience interchangeably as NHS Lothian considers business continuity to be integrated within its overall resilience work. The audit did not cover emergency resilience arrangements.

Acknowledgements

We would like to thank all staff consulted during this review for their assistance and cooperation.

Executive Summary

Conclusion

Although there is a strategy in place to provide guidance to relevant staff about preparation and testing of Business Continuity Plans (BCPs), which is supported by template documents and staff with clear responsibility for Business Continuity Management (BCM) across NHS Lothian, the control framework used to confirm whether these arrangements are applied consistently and effectively across NHS Lothian requires improvement.

Summary of Findings

The table below summarises our assessment of the adequacy and effectiveness of the controls in place to meet each of the objectives agreed for this audit. Definitions of the ratings applied to each action are set out in Appendix 1.

No.	Control Objective	Control objective assessment	Number of actions by action rating			
			Critical	Significant	Important	Minor
1	A BCM framework, including policy and governance arrangements, has been implemented with roles and responsibilities assigned.	**Amber**			3	
2	A business continuity plan is in place which demonstrates a comprehensive understanding of the organisation, identifies the key services, as well as the critical activities that support them.	**Green**		1		
3	Business continuity strategies have been identified for all activities and resources of the organisation, including consideration of the ‘maximum tolerable period of disruption’ and the consequence of inaction.	**Green**		1		
4	Comprehensive and robust business continuity plans have been developed to manage the initial response to an incident and ensure the continuity of critical activities can be maintained.	**Green**			2	

No.	Control Objective	Control objective assessment	Number of actions by action rating			
			Critical	Significant	Important	Minor
5	Effective processes exist to ensure BCM arrangements are kept up-to-date and plans are regularly exercised and reviewed.	**Amber**		2		
6	BCM is embedded within the culture of the organisation and has strong support from senior management and active participation by local areas and specialties. There is good awareness of BCP issues.	**Green**			1	
7	Local speciality and departmental BCM arrangements are integrated with corresponding corporate arrangements response structures.	**Green**			1	
8	eHealth Disaster Recovery plans and procedures covering the core IT infrastructure and critical business systems are in place and are regularly exercised and reviewed.	**Green**		1		

Control Objective Ratings

Action Ratings	Definition
Red	Fundamental absence or failure of controls requiring immediate attention (60 points and above)
Amber	Control objective not achieved - controls in place are inadequate or ineffective (21 – 59 points)
Green	Control objective achieved – no major weaknesses in controls but may be scope for improvement (20 points or less)

Main findings

A Resilience Strategy and a Resilience Assurance Protocol are in place, which provide guidance on the organisation’s strategic direction for resilience and a methodology for measuring compliance with the strategy. There are three resilience groups in place, namely the Tactical Resilience Group (TRG), the Resilience Committee (RC), and a dedicated Resilience Team. The Resilience Team consists of three members of staff who are charged with providing oversight of the overall resilience work of the organisation and providing expert advice to NHS Lothian staff. The Business Continuity Lead is the newest member of the team, joining in January 2016. This post had been vacant since the previous spring when it was moved from the Strategic Planning directorate. This allowed the organisation to have a greater focus on business continuity work.

The TRG meets quarterly and is a working group designed to improve Board resilience and ensure that resilience work is being performed in line with organisational objectives. The Group has membership from across the organisation, in terms of both location and profession. The RC also meets quarterly and provides strategic leadership and governance oversight of resilience for the organisation, and includes senior staff such as the Chief Executive and the Director of Public Health & Health Policy.

In addition, all of the areas sampled for this audit had a continuity plan in place and had members of staff who attended the TRG. The plans all used the template created by the Resilience Team to allow for a more standardised approach.

We identified five significant issues for improvement during the review:

- The Resilience Team does not as a matter of course review all the local area business continuity plans submitted to them;
- The impact of losing services through disruptions has not been fully quantified, and the prioritisation of services and activities has not been performed in a structured way;
- Effort has been made to determine and document critical services and activities as well as resource requirements at a local departmental level. However, this data has not been amalgamated into a central Board-wide view. As such, there has been no central review, harmonisation, or prioritisation of activities and resources to identify organisation-wide contingencies and interdependencies; and
- Seven of the nine areas sampled did not have tested plans in place, including eHealth. In addition, although the Resilience Team has carried out some exercising of plans on all acute sites, there is not a structured oversight of all lessons learned.

Further details of these points, in addition to seven important points, are set out in the Management Action Plan.

Management Action Plan

Control objective 1: A BCM framework, including policy and governance arrangements, has been implemented with roles and responsibilities assigned.

1.1: NHS Lothian's resilience strategy is not complete	**Important**

Observation and Risk:

NHS Lothian's *Resilience Strategy* sets out the organisation's approach to resilience, and includes the organisation's strategic and tactical incident management plans, to address such issues as mass casualties or a flu pandemic. In addition, there is an *Assurance Protocol* which sets out requirements for departments on how to routinely assess and report on their resilience capabilities. These two documents were created by the Emergency Planning Officer, who was brought into the organisation to improve the effectiveness of resilience work. Also, policy guidance from the Scottish Government is used to ensure that NHS Lothian's approach to business continuity conforms to national standards. Finally, resilience work is overseen by the Resilience Committee, which meets quarterly and provides governance oversight, and the Tactical Resilience Group which is designed to improve resilience within the organisation.

However, many sections of the Resilience Strategy are incomplete, such as the sections on risk management, the Primary & Community Services response plan, and hospital site-specific plans. The Emergency Planning Officer has stated that he will need to have further conversations with relevant departments before they are able to complete these sections of the Strategy. The delay has been due to several factors: the vacancy of the BC Lead post for most of 2015, competing demands in the responsible departments, the introduction of the Integration Joint Boards on 1 April 2016, and the need for the Resilience Strategy to reflect the changes brought about by this organisational change.

If the organisation has not fully stated its strategic approach to resilience there is a risk that the organisation does not have an effective resilience process.

Recommendation:

The Resilience Strategy should be completed and then approved by the Resilience Committee.

Management Response: The current version of the Resilience Strategy has been signed off. Some sections need to be completed by staff outwith the Resilience Team and this has begun. A Risk Management process is in development and has been piloted.

Management Action: Ensure completion of Resilience Strategy by relevant staff.

Responsibility:	**Target date:**
• facilitation by Resilience Team, • writing of missing sections: senior managers in relevant areas	• Acute areas: 31 Jan 2017 • Facilities: 30 Apr 2017 • Health & Social Care: 31 July 2017

1.2: The relationship between the Resilience Committee and the Tactical Resilience Group needs to be clarified	**Important**

Observation and Risk:

Remits have been created for the TRG and the RC which set out their objectives and membership. Both groups meet quarterly and there is good attendance by senior staff from across the organisation.

However, the remits of both groups are very similar and do not focus on the respective responsibilities of each group, i.e. with the TRG having a more tactical responsibility for improving resilience within the organisation, and the RC being charged with providing scrutiny of that work. In addition, TRG minutes are not being provided to the RC.

If the remits of the TRG and RC are not clarified there is a risk that resilience work is not performed effectively across the organisation and that there is ineffective scrutiny of that work.

Recommendation:

The remits of both the Resilience Committee and the Tactical Resilience Group should be reviewed by the Resilience Committee, in order that resilience work is performed across the organisation and that there is effective scrutiny of that work.

Tactical Resilience Group minutes should be supplied in a timely manner to the Resilience Committee.

Management Response: The TRG minutes are available on the Resilience page on the NHSL Intranet.

Management Action:

- Include TRG minutes as a standing item on RC agenda, for noting.
- Review remits of the RC and TRG, noting the audit comments and recommendations.

Responsibility: Resilience Team	**Target date:** 31 Jan 2017

1.3: The Tactical Resilience Group does not assess performance against its remit to determine whether it is working effectively	**Important**

Observation and Risk:

The Tactical Resilience Group (TRG) meets quarterly and is a working group designed to improve Board resilience and ensure that resilience work is being performed in line with organisational objectives. The Group has membership from across the organisation, in terms of both location and profession. However, the TRG does not have an annual workplan setting out work performed during the year, performance against objectives, and work to be performed for the forthcoming year, in order to confirm that it has fulfilled its remit.

In addition, the TRG remit states that the Group should be proactive in ensuring that resilience is effective across the organisation, for example by establishing workstreams and short-life groups. However, the Group does not perform that work.

Finally, the TRG is not being supplied with performance indicators which could be used to determine if resilience work is being effectively performed. Examples of such indicators are the number of resilience plans which are up-to-date, and whether all plans are being tested.

There is a risk that the TRG does not fulfil its remit effectively, leading to increased risk in relation to the management of business continuity and resilience across NHS Lothian.

Recommendation:

The TRG should develop an annual workplan setting out work performed during the year, performance against objectives, and work to be performed for the forthcoming year. Performance against the annual workplan should be set out in an Annual Report.

Performance metrics should be developed for BCM and resilience, for example which show the number of resilience plans which are up-to-date, and whether all plans are being tested. The metrics chosen should be approved by the Resilience Committee, with results being reviewed at each quarterly TRG meeting.

The TRG should be more proactive in ensuring that resilience is effective across the organisation, for example by establishing work-streams and short-life groups.

Management Response: The TRG Work-plan is currently taken to be the implementation of the RC Work-plan. This is a standing agenda item at TRG meetings. Sub-groups have been formed to carry out specific work. While annual aims may be of help the ability to change priorities and continuously review progress is important. We agree that it would be beneficial to revise these approaches taking the actions below.

Management Action:

- Develop and maintain a specific TRG work-plan, based on that of the RC;
- Develop and maintain performance metrics for the TRG;
- TRG should present a paper to RC annually reporting on its activity and utilising performance metrics as appropriate.

Responsibility: - Resilience Team & RC: develop and approve metrics - TRG: work to metrics	**Target date:** - Structures: 31 Jan 2017 - Outputs: 30 October 2017

Control objective 2: A BCM system is in place which demonstrates a comprehensive understanding of the organisation, identifies the key services, as well as the critical activities that support them.

2.1: Critical resilience activities and resource prioritisation have not been determined	**Significant**

Observation and Risk:

Our audit found that currently effort has been made to determine and document critical services and activities as well as resource requirements at a local departmental level. However, this data has not been amalgamated into a central Board-wide view. As such, there has been no central review, harmonisation, or prioritisation of activities and resources to identify organisation-wide contingencies and interdependencies. This is essential as in a live emergency several departments could be impacted at once and recovery and resource assumptions made within local plans may no longer be valid.

If critical business activities are not identified and prioritised there is a risk that recovery orders and resource priorities across the Board, i.e. from area to area, have not been agreed and this may impact, delay or undermine, recovery and continuity efforts following an emergency.

Recommendation:

A prioritised list of critical organisation business activities and resources should be created, and then approved by the Resilience Committee.

Management Response:

The central review of activities and resources has been limited and has not been formalised as a number of very evident resilience challenges have had to be addressed urgently during a period of staff vacancy e.g. managing the risk of Ebola and terrorism.

We agree that there would be benefit in a more structured prioritisation process but we propose to do this by asking specialties to assess *levels* of impact rather than by producing a prioritised list. This is because creating a prioritised list would require considerable effort and diversion of scarce resources and it is expected that most of the benefit could be got from a simpler five-level impact assessment, using agreed criteria.

A short life project is underway to develop a template that local areas can use for this with assessments being signed off by the department head or director. The Resilience Committee will receive a summary of findings and risks. The Resilience Team will sample the work done locally for QA purposes.

All ‘critical’ activities would be expected to have a similar very high impact and preventing any significant disruption to these would be a top priority.

The challenges of responding to live emergencies affecting different departments are addressed by maintaining a flexible, modular response consistent with the ‘all risks’ approach recommended by *Preparing Scotland: Scottish Guidance On Resilience* and *Preparing Scotland: Having and Promoting Business Resilience* (see also response to 4.1 below)

Management Action:

- Continue to develop consistent, structure methods to assess the criticality of activities and increase awareness of these and risks that might affect them.
- Promote and ensure local ownership of resilience risk assessment in conjunction with a reporting mechanism that escalates more serious risks to senior managers and to the Resilience Committee.
- Carry out sampling of local assessment for QA purposes

Responsibility: Methodology: Resilience Team Implementation: RT and local managers	**Target date:** Method: 31 Jan 2017 Implementation 31 July 2017

Control objective 3: Business continuity strategies have been identified for all activities and resources of the organisation, including consideration of the ‘maximum tolerable period of disruption’ and the consequence of inaction.

3.1: The impact of losing services through disruptions has not been fully quantified, and there has been ineffective prioritisation of services and activities	**Significant**

Observation and Risk:

Having identified their critical activities, organisations should perform a Business Impact Analysis (BIA) to determine what the impact would be if these services were disrupted or lost. The BIA should take into account the time sensitivity of each business function and process, and how urgently it should be restored based on the consequences for the organisation.

However, the resilience plan template which the Resilience Team has asked individual resilience plan holders to complete does not require them to state the impact of losing their services locally, the impact of a service loss to the organisation as a whole, and the maximum period of time each service could be impaired for before seriously affecting the continuity of services. None of the nine resilience plans sampled for the audit contained this information.

Also, none of the nine areas sampled for the audit have stated the impact on the organisation of any disruption of their key activities and resources, with the analysis also not including specific mention of the impact on key areas such as statutory duties and legal obligations, resources required to remedy the situation, and the impact of the disruption on partners.

Finally, for seven of the nine plans sampled, the services or activities provided had not been prioritised, so that the plans did not provide clear guidance on what services to restore first after a disruption.

BIA is the foundation of effective BCM planning. There is a risk that the organisation is not fully prepared for all disruptive events if a comprehensive BIA has not been performed.

Recommendation:

A comprehensive business impact analysis should be performed which includes an analysis of the impact of the loss of key services, the cost of restoring them, and the maximum tolerable period of disruption.

Business plan holders should be instructed to ensure that their plans include a prioritised list of their key activities and services.

Management Response:

We agree that business impacts should be assessed and that outage times may affect the criticality of services. The assessment of loss of services is included in the resilience risk assessment process (see Assurance Protocol) but we recognise that this should be extended, made more comprehensive and consider timing and legal aspects more fully.

We do not feel that a *fully quantified* BIA and *calculation of the cost* of restoring key services leading to a *prioritised list* of key activities and services would be the best use of resources, but we would be happy to work towards an assessment of *levels* of impact. This is because

- There are significant methodological difficulties in a quantified assessment, e.g. quantifying health impacts of different patient groups, comparing these with financial and non-health impacts, ensuring consistency in assessments of different services, incorporating uncertainty in assessments;
- The resources required would be very substantial and detailed knowledge of many specialities areas would be needed;
- Levels of impact are likely to provide sufficient information to achieve the same resilience benefit, including identifying priorities and directing effort;
- This is consistent with other risk methodologies used by the organisation;
- Applying resources to other recommendations in this audit and other scheduled work would be more likely to benefit patients' health and organisational resilience.

We intend to record information of this sort separately from the Resilience Plans so that plans remain focused on response, making them easier to use in an incident.

Management Action:

- Continue to develop an assessment of levels of impacts based on established risk assessment criteria: these group impacts in five bands and include costs, health impacts, enforcement / prosecution, etc.
- Consider more detailed quantification of impacts if additional resources become available.

Responsibility:	**Target date:**
Process: Resilience Team	Process: 31 Jan 2017
Assessment: Service Managers with QA by RT	Implementation: 31 July 2017

Control objective 4: Comprehensive and robust business continuity plans have been developed to manage the initial response to an incident and ensure the continuity of critical activities can be maintained.

4.1: Not all plans contain a list of detailed tasks and actions	**Important**

Observation and Risk:

Business continuity plans should include an incident response structure to provide detailed guidance on how to deal with specific disruptions, e.g. a loss of power or premises, acute staff shortages, and an interruption to IT. This information allows managers to deal with problems in a quick and effective manner, and allows for plans to be more effectively reviewed by responsible senior managers and directors.

Seven of the nine business continuity plans we reviewed did not include a list of detailed tasks and actions to take in the event of disruptions. The plan holders stated that it is the responsibility of managers dealing with incidents to determine what to do in response to individual incidents.

There is a risk that staff charged with dealing with disruptions will not have sufficiently detailed information in order to help them deal with disruptions.

Recommendation:

Business plan holders should be instructed to ensure that their plans include detailed tasks and actions to take in the event of disruptions.

Management Response: Preparing Scotland Scottish Guidance On Resilience recommends an ‘all risk’ approach focussing on ‘Consequences not Causes’ (p.15) that uses ‘a process of generic planning which can be adapted readily to fit to a wide range of issues’. It sees adaptability as a ‘crucial quality’ and warns against ‘rigidly following a plan to the detriment of the response.’ (p.16).

Preparing Scotland: Having and Promoting Business Resilience warns that: ‘It is impossible to anticipate all the circumstances of a disruption and to plan for these in detail. Trying to do so will consume resources without necessarily increasing Business Resilience.’ It recommends flexibility and ‘allowing for the lead responder’s use of judgement … and, where necessary, to improvise alternative solutions ...’ (p.19)

We agree that there are some circumstances where check-lists and options developed in advance may be of help and that planners should consider this. However, having more than a small number of pre-scripted responses has been shown to create problems, including:

- Making plans:
  - Too bulky to use - people just do not have the time to read much more than an action card in many situations;
  - Too thick to find what is needed (or to find that this particular situation was not anticipated)
  - awkward to carry so not available quickly when needed, e.g. when on-call;
- Creating the mistaken expectation that there can be a pre-prepared response to most incidents and trying to make the incident fit the plan when the expectation should be that ‘I

will need to be flexible and keep revising what I do based on changing circumstances'

- Greatly increasing the work of keeping plans up to date at the expense of other more productive resilience preparations;
- Making resilience appear to be more about paper plans than human skills

Preparing Scotland recommends that 'wherever possible, plans should be simple and should offer flexibility and adaptability' (p.13). This approach addresses the difficulty of planning for the almost endless permutations of incidents by combining:

- The skills, experience and local knowledge of front-line staff (most of whom will be doing something close to their normal work, although volumes, priorities, locations etc. may differ)
- flexible generic plans
- Incident-specific prioritisation and decision making by tactical level staff. based on
- situational awareness of the evolving incident/response

This is often referred to as 'planning for *anything* rather than planning for *everything'* (see Principles section of NHSL Resilience website)

Management Action:

- Continue to recommend the inclusion of action cards in local plans
- Consider whether there are circumstances where lists of response options etc. would be of benefit.

Responsibility: Resilience Team	**Target date:** 31 Jan 2017

4.2: Business continuity plans are not always easily accessible, and action plans are not always available or complete	**Important**

Observation and Risk:

BCM documentation, particularly business continuity plans and supporting procedures should be easily available to all relevant staff in the event of a disruption.

Our audit found that for seven of the nine areas sampled, plan holders and relevant staff did not maintain an offsite copy of BCM documentation. Instead the plan holders stated that relevant staff could access their respective share drives from home or from any NHS Lothian site. However, if there is a disruption to NHS Lothian's internal network or to the external internet connection to the network this approach would leave staff without access to their plan.

There is a risk that plans are not available to staff when required.

Recommendation:

All business continuity plans should be held at a secure central point so that stakeholders are clear about where they can find the information in an emergency. This could be with another NHS Scotland board or be cloud-based.

Management Response:

We agree with this recommendation except that we feel there are practical and security difficulties in the use of other NHS Boards or Cloud based systems.

Management Action:

- Assess the risks, benefits and practicalities of different document storage options in light of other NHS Lothian policies;
- Consider loss of access to IT systems on plan storage;
- Specify where resilience plans and information should be held so that relevant staff could access them during incidents;

One option might be to require having:

- an 'original' document held electronically plus an electronic back-up and
- at least two 'hard copies' at different locations

Responsibility: Resilience Team	**Target date:** 30 November 2016

Control objective 5: Effective processes exist to ensure BCM arrangements are kept up-to-date and plans are regularly exercised and reviewed.	
5.1: Business continuity plans are not routinely submitted for review, and are not always complete	**Significant**
Observation and Risk: Resilience plans are created by local managers for their areas using a proforma provided by the Resilience Team. Managers can ask the Resilience Team for advice on completing the proforma as required. Once the plan has been completed the manager provides it to a senior manager or director from their area for approval, with the approval then being communicated to the Resilience Team. However, although some managers provide their plans to the Resilience Team for review and feedback, that does not happen as a matter of course. There is no list of resilience plans maintained by the Resilience Team. As such, although the nominated senior managers and directors provide assurance to the Resilience Team that all plans for their respective areas have been created or updated, the Resilience Team cannot independently verify this information. Six of the nine resilience plans we sampled for the audit were not complete. The managers responsible for these plans stated that they either thought that they were complete or, in two cases, they were waiting for further information from colleagues before completing them. Of these six incomplete plans, three had been approved by the responsible director or senior manager. There is a risk that resilience plans are not of sufficient quality to enable the effective continuity and recovery of critical services following an emergency, and not all areas of the organisation are covered by plans.	
Recommendation: All business continuity plans should be submitted to the Resilience Team for review. The Resilience Team should maintain a list of all plans within the organisation, and use it to determine if all areas of the organisation are covered, and that all plans are being kept up-to-date. Directors and senior managers with responsibility for approval of plans should ensure that plans are complete and will allow for the effective management of business processes.	
Management Response: The Resilience Team request that plans are submitted along with signed assurance reports but we agree that a listing of resilience plans should be maintained by the Resilience Team. We agree that Directors and senior managers with responsibility for approval of plans should ensure that plans are complete and will allow for the effective management of business processes. Without in depth knowledge of each and every service the Resilience Team would not be in a position to fully assess the resilience plans in each service area but non-specialist comment could be provided as part of a rolling programme of plan reviews.	

Management Action:	
- Notify managers if they have signed-off incomplete plans - Keep a list of Resilience plans. - Establish a rolling programme of plan reviews aimed at covering all areas of NHS Lothian in a specified period (possibly 3 or 4 years)	
Responsibility: Resilience Team	**Target date:** to establish processes 31 Jan 2017

5.2: Not all business continuity plans are being effectively tested	Significant

Observation and Risk:

Business continuity plans should be tested to confirm that they will be effective in the event of a disruption. Test plans can be developed to cover potential disruptions, and to state the frequency with which exercises are performed. They should be challenging, realistic, and have clearly stated aims and objectives.

Seven of the nine areas sampled did not have testing plans in place. Instead, the plan holders stated that they would know what to do in the event of a disruption due to their experience and expertise. However, business continuity planning and testing should consider the possibility that experienced staff would not be available to manage disruptions.

In addition, although the Resilience Team has carried out some testing of plans on acute sites, there is no structured oversight of lessons learned. If there is no testing of business continuity plans then there is a risk that the plans will not be effective in the event of a disruption.

Recommendation:

All business continuity plans should be subject to testing to allow plan holders to gain assurance over the effectiveness of continuity and recovery arrangements. There are a number of different types of testing that can be undertaken. These range from basic plan walkthroughs to full-blown continuity tests. In order to achieve a cost-benefit balance, most organisations will typically opt for scenario-based desktop testing with key stakeholders and business continuity representatives.

The TRG, RC, and the Resilience Team should develop guidance to assist local plan holders in determining the appropriate level of testing for each area. The exercises undertaken by local areas and the lessons learned should be reviewed by the Resilience Team to ensure that testing is effectively covering the risks for each area, and that lessons learned are being used to adjust plans, making them more effective.

Management Response: The Resilience Assurance Protocol requests information about the testing of plans and recommends that plans consider lessons learned from exercises and incidents. However we agree there is benefit in strengthening this and monitoring compliance more closely.

Management Action:

- Review and strengthen processes giving direction on the exercising of plans and their addressing of lessons learned

Responsibility: Resilience Team	**Target date:** Commence implementation of processes - 31 Jan 2017

Control objective 6: BCM is embedded within the culture of the organisation and has strong support from senior management and active participation by local areas and specialties. There is good awareness of BCM issues.

6.1: There is insufficient resilience training provided to key staff	**Important**

Observation and Risk:

The Scottish Government's document *Preparing Scotland – Having and Promoting Business Resilience* states that key staff should receive training so that business resilience becomes part of the normal operation of the organisation and thinking of staff. Training for key staff allows them to create more effective business continuity plans.

However, none of the nine resilience plan holders sampled had received any specific business continuity training. We were informed that the plan holders gain knowledge of business continuity planning from attending resilience exercises, and from completing learnPro modules.

There is a risk that stakeholders do not have sufficient awareness of continuity or resilience procedures, and will not be familiar with plans when invoked and so recovery and continuity processes will fail.

Recommendation:

TRG members should decide if resilience plan holders should receive comprehensive business continuity training to allow them to effectively manage business continuity in their respective areas. In addition, as plan holders conduct more exercises within their own areas (see Issue 5.2) they will also gain additional practical understanding of business continuity.

Management Response: 'Business continuity' is one aspect of resilience and best practice recommends that resilience is considered as a whole. The Assurance Protocol contains procedures to ensure that managers consider the resilience training needs of their staff.

Over the last 18 months regular training and exercising has focussed on tactical level staff in control rooms as more junior staff will often be carrying out their normal duties and more senior, strategic level staff, would be called on less often. These sessions have occurred every 2-4 weeks. Staff have also taken part in multi-agency exercise with Police and others, and in several national level exercises. However these have often had a response focus.

The Resilience Committee has been asked to decide whether additional training for senior staff was required but it felt that individual Executive Directors should attend Control Room Exercises and assess their own training needs.

Some specific groups might benefit from specific training e.g. potential STAC chairs.

Management Action:

- Continue to implement the training assessment aspects of the Assurance Protocol
- Ask TRG to consider resilience training needs

Responsibility: Resilience Team & TRG	**Target date:** 31 Jan 2017

Control objective 7: Local speciality and departmental BCM arrangements are integrated with corresponding corporate arrangements response structures.

7.1: Not all departments have confirmed that they can rely on the aid from other departments stated in their business continuity plans — **Important**

Observation and Risk:

Business continuity plans should state how disruptions will be dealt with by individual areas and also what reliance will be placed on other departments to aid the recovery. Stating these interdependencies is important as it provides greater assurance that all key players in recovery efforts are known.

However, two of the nine areas sampled had not confirmed with colleagues in other areas that they were ready to provide relevant support as stated in the plan.

There is a risk that departments who are relied on to aid recovery efforts will not be able to provide the required assistance.

Recommendation:

All business continuity plan holders should confirm that staff external to their departments who are listed in the plan are able to provide the assistance required to deal with disruptions.

Management Response: We agree with this recommendation

Management Action: specify this requirement when reviewing plans

Responsibility: Resilience Team and plan owners	**Target date:** process: 30 November 2016 Implementation: 31 Jan 2017

Control objective 8: eHealth Disaster Recovery plans and procedures covering the core IT infrastructure and critical business systems are in place and are regularly exercised and reviewed.

8.1: eHealth business continuity and disaster recovery plans have not been tested	**Significant**

Observation and Risk:

As stated at Issue 5.2, business continuity plans should be tested to confirm that they will be effective in the event of a disruption, as should disaster recovery plans.

However, the eHealth business continuity plan does not include testing plans, due to the large number of potential scenarios in which systems could face continuity problems. Instead, it is expected that plan holders will know what to do in the event of a disruption due to their experience and expertise. In addition, staff members have experience of dealing with disruptions through the management of any unplanned system failures. There is limited testing of disaster recovery plans, although there is quarterly restore testing of a sample of Windows-based systems. In addition, the eHealth team is asked to recover files on a daily basis, giving further assurance that back-up and restore processes work.

Where there is limited testing of business continuity plans then there is a risk that the plans will not be effective in the event of a disruption. Without testing of plans, there is also an increased risk that disruption to an IT system will have unanticipated consequences to provision of clinical or other services.

Recommendation:

eHealth business continuity plans should be subject to testing to allow plan holders to gain assurance over the effectiveness of continuity and recovery arrangements. The eHealth team should consult with Resilience and clinical / managerial staff when designing testing, to ensure that the tests can capture and assess the potential impact on clinical and other services.

Management Response: We agree with this recommendation but wish to include clinical and managerial stakeholders in this testing and in setting its scope because eHealth failures can have a significant impact on NHSL by disrupting service delivery. Challenges to implementation of a testing programme include the financial cost of such testing, as well as identification of times when it is possible to shut down key systems as part of the testing. It is therefore important that decisions about testing of eHealth BCP / disaster recovery plans are made in consultation with the Resilience Committee.

Management Action:

eHealth will provide the Resilience Committee with a proposed testing programme for eHealth systems. The programme will list all key systems, and state their importance to the organisation, the financial cost of testing each system, and expected system downtime. Once the Resilience Committee has identified key systems that require testing, eHealth will work with the Resilience Team and appropriate clinical and managerial staff to design the testing

in order to maximise the lessons learned from the tests.	
Responsibility: eHealth	**Target date:** Paper to Resilience Committee – 31 Jan 2017 Testing – 31 July 2017

Appendix 1 - Definition of Ratings

Management Action Ratings

Action Ratings	Definition
Critical	The issue has a material effect upon the wider organisation – 60 points
Significant	The issue is material for the subject under review – 20 points
Important	The issue is relevant for the subject under review – 10 points
Minor	This issue is a housekeeping point for the subject under review – 5 points

Control Objective Ratings

Action Ratings	Definition
Red	Fundamental absence or failure of controls requiring immediate attention (60 points and above)
Amber	Control objective not achieved - controls in place are inadequate or ineffective (21 – 59 points)
Green	Control objective achieved – no major weaknesses in controls but may be scope for improvement (20 points or less)