

For Publication

Bedfordshire Fire and Rescue Authority
Corporate Services Policy and Challenge Group
13 September 2018
Item No. 13

REPORT AUTHOR: HEAD OF SERVICE DEVELOPMENT AND ASSURANCE

SUBJECT: CORPORATE RISK REGISTER

For further information on this Report contact: Strategic Operational Commander Andy Peckham
Head of Service Development and Assurance
Tel No: 01234 84 5129

Background Papers: None

Implications (tick ✓):

LEGAL			FINANCIAL	
HUMAN RESOURCES			EQUALITY IMPACT	
ENVIRONMENTAL			POLICY	
CORPORATE RISK	Known	✓	OTHER (please specify)	
	New			

Any implications affecting this report are noted at the end of the report.

PURPOSE:

To consider the Service's Corporate Risk Register in relation to Corporate Services.

RECOMMENDATION:

That Members note and approve the review by the Service of the Corporate Risk Register in relation to Corporate Services.

1. Introduction

- 1.1 Members have requested a standing item to be placed on the Agenda of the Policy and Challenge Groups for the consideration of risks relating to the remit of each Group. In addition, the Fire and Rescue Authority's (FRA) Audit and Standards Committee receives regular reports on the full Corporate Risk Register.
- 1.2 An extract of the Corporate Risk Register showing the risks appropriate to the Corporate Services Policy and Challenge Group will be provided to the meeting. Explanatory notes regarding the risk ratings applied is appended to this report.

2. Current Revisions

- 2.1 The register is reviewed on a monthly basis during the Service's Corporate Management Team (CMT) meetings and by CMT members between these meetings if required. A copy of the risks relevant to the Corporate Services Policy and Challenge Group are attached for your information and approval.
- 2.2 Changes to individual risk ratings in the Corporate Risk Register:
There are no changes to the Corporate Risk Register individual risk ratings.
- 2.3 Updates to individual risks in the Corporate Risk Register:

CRR00029: If we do not communicate well, both internal and external to the Service, then we will suffer from poor staff morale, miss the opportunity to promote ourselves and the excellent work that we do and potentially impact upon our ability to deliver a full range of services.

The new website was launched on the 21st May 2018, this is continually being monitored to ensure all links and platforms function correctly. Analytics are being measured to monitor hits on the website and to ensure customer engagement is maintained.

CRR00043: If the Service suffers a terrorist attack then there is the potential for elements of the Critical National Infrastructure (CNI) to be compromised, our ability to respond to emergency incidents could be significantly affected, we would be unable to fulfil our duties under the Civil Contingencies Act and our reputation could be adversely affected.

The Service has initiated the delivery of "Project Griffin" awareness training, provided under license by Met. Police and supports advice from our CTSA. This is being delivered by Service NIOs following central trainer input. This training enhances an appreciation of the risk and potential threat to our organisation and staff.

CRR00016: If there is an unforeseen change of direction for the FRS (e.g. government request to do something which does not currently fall under the remit of the UK FRS), or there are changes in Government or EU policy on fire and rescue matters or other policy directly affecting the FRS then this may have an impact on our ability to deliver a full range of services due to the need to resource such changes.

The Service welcomed the HMICFRS in July 2018 who will be considering the organisational performance against their core areas of Effectiveness, Efficiency and People. This process commenced in May 2018 and will conclude in December 2018 when we expect to receive a written report. Outcomes will be used to identify areas of strength and any areas for improvement. This process will provide both independent scrutiny and assurance of our awareness and application and inform direction.

CRR00048: There is a risk that the Service may be subjected to a fine from the ICO due to not implementing GDPR resulting in poor data security and process.

A review of progress on the GDPR action plan has taken place. Due to staff changes following a restructure progress has not maintained alignment with proposed completion dates. Resourcing is being reviewed to enable this to be addressed. The action completion date has been extended to reflect this. HSDA has reviewed the risk and it remains unchanged at Inherent at 12 and Residual at 6.

**STRATEGIC OPERATIONAL COMMANDER ANDY PECKHAM
HEAD OF SERVICE DEVELOPMENT AND ASSURANCE**

Explanatory tables in regard to the risk impact scores, the risk rating and the risk strategy.

Risk Rating/Colour	Risk Rating Considerations / Action
Very High	<p>High risks which require urgent management attention and action. Where appropriate, practical and proportionate to do so, new risk controls must be implemented as soon as possible, to reduce the risk rating. New controls aim to:</p> <ul style="list-style-type: none"> • reduce the likelihood of a disruption • shorten the period of a disruption if it occurs • limit the impact of a disruption if it occurs <p>These risks are monitored by CMT risk owner on a regular basis and reviewed quarterly and annually by CMT.</p>
High	<p>These are high risks which require management attention and action. Where practical and proportionate to do so, new risk controls <i>should</i> be implemented to reduce the risk rating as the aim above. These risks are monitored by CMT risk owner on a regular basis and reviewed quarterly and annually by CMT.</p>
Moderate	<p>These are moderate risks. New risk controls should be considered and scoped. Where practical and proportionate, selected controls should be prioritised for implementation. These risks are monitored and reviewed by CMT.</p>
Low	<p>These risks are unlikely to occur and are not significant in their impact. They are managed within CMT management framework and reviewed by CMT.</p>

Risk Strategy	Description
Treat	<p>Implement and monitor the effectiveness of new controls to reduce the risk rating. This may involve significant resource to achieve (IT infrastructure for data replication/storage, cross-training of specialist staff, providing standby-premises etc) or may comprise a number of low cost, or cost neutral, mitigating measures which cumulatively reduce the risk rating (a validated Business Continuity plan, documented and regularly rehearsed building evacuation procedures etc)</p>
Tolerate	<p>A risk may be acceptable without any further action being taken depending on the risk appetite of the organisation. Also, while there may clearly be additional new controls which could be implemented to 'treat' a risk, if the cost of treating the risk is greater than the anticipated impact and loss should the risk occur, then it may be decided to tolerate the risk maintaining existing risk controls only</p>
Transfer	<p>It may be possible to transfer the risk to a third party (conventional insurance or service provision (outsourcing)), however it is not possible to transfer the responsibility for the risk which remains with BLFRS</p>
Terminate	<p>In some circumstances it may be appropriate or possible to terminate or remove the risk altogether by changing policy, process, procedure or function</p>