For Publication

Bedfordshire Fire and Rescue Authority
Corporate Services Policy and Challenge Group
9 June 2016
Item No. 13

REPORT AUTHOR: **HEAD OF SAFETY AND STRATEGIC PROJECTS**

SUBJECT: **CORPORATE RISK REGISTER**

For further information on this Report contact: Service Operational Commander Tony Rogers
Head of Safety and Strategic Projects
Tel No: 01234 845163

Background Papers: None

Implications (tick ✓):

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

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 available at 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:

- **CRR23: The Service IT infrastructure is unable to handle secure e-mails from external partners:** The service has provided an alternative access to secure email through the Criminal Justice Secure email system, managed by the Business Information Manager. This gives access to all government secure email networks including the Police National Network (PNN). Nominated users have access to this which is available via webmail. Service users also have access to secure emails sent by partner public sector organisations using their own internal Egress system or equivalent. This action is closed with the risk mitigated. Future plans to refine and optimise secure email provision include the potential to establish Egress internally once the demand and requirements are identified. This is closely linked to the developments in the emergency services network as part of the ESMCP. Therefore, following a review of the risk and the control measures in place the Inherent Likelihood has been reduced from 3 to 1 and the Inherent Impact has been reduced from 4 to 3 reducing the overall Inherent Risk rating to 3 aligning with the Residual Risk and will now be transferred as a Tolerable Risk.

- **CRR29: Poor communications both internal and external to the Service:** Following a review of the risk controls and action plan aligned to CRR29 that included the external communications audit outcome providing substantial assurance to the Service, and the appointment of the *Communications and Engagement Manager* Role that undertakes a broader aspect of public relations and internal/external communications, the Inherent Risk rating has been revised. The outcome of the review has reduced the Inherent Likelihood from 3 to 2 with an overall reduced Inherent Risk rating from 9 to 6.

- **CRR39: If we have inadequate data management due to poor implementation, inappropriate specification of requirements or poor quality control measures then we are at risk of using the wrong information throughout the organisation and thus potentially affecting the delivery of our services:** The project aligning Service information activities to ISO27001 Information Security Framework is now being embedded with residual risks being monitored through the Abriska Risk Management System. This process is now being refined by the Head of Safety and Strategic Projects ahead of handover to business As usual. Following a review of the risk and the actions taken so far the Inherent Likelihood has been reduced from 4 to 3 resulting in an overall reduction in the Inherent Risk Rating from 12 to 9.

2.3 Updates to individual risks in the Corporate Risk Register:

- **CRR05: If we are unable to provide adequate asset management and tracking facilities then we may cause serious injuries to our staff due to a lack of safety testing. We may also incur unnecessary significant costs and be in breach of health and safety legislation:** CRR05 has a number of control measures in place to assist in mitigating the risk to the Service which includes the introduction of an Asset Tracking system. Following on from the previous update to Members the Technical Equipment Manager has reviewed a number of asset tracking systems and is now in the process of writing the technical specification to enable a tendering process to begin. The tender will take into consideration the needs of the Service and will be procured using allocated funding.

  The procurement of a new software based solution will significantly improve the automated recording of assets and provide a system that will enable an in-depth audit of our resources, maintenance and testing of equipment, however the current system in place continues to provide assurance that appropriate maintenance and testing regimes are secured.

3. Business Continuity

3.1 As part of the Service's Business Continuity (BC) arrangements a programme of testing is now being developed that will cover all of the Service's BC plans on a cyclical process. The thorough testing of these plans will ensure that in the event of functional or service wide business interruption the Service is still able to deliver vital services to the communities.

SERVICE OPERATIONAL COMMANDER TONY ROGERS
HEAD OF SAFETY AND STRATEGIC PROJECTS

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

Risk Rating

Risk Rating/Colour	Risk Rating Considerations / Action
Very High	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: • reduce the likelihood of a disruption • shorten the period of a disruption if it occurs • limit the impact of a disruption if it occurs These risks are monitored by CMT risk owner on a regular basis and reviewed quarterly and annually by CMT.
High	These are high risks which require management attention and action. Where practical and proportionate to do so, new risk controls *should* 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.
Moderate	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.
Low	These risks are unlikely to occur and are not significant in their impact. They are managed within CMT management framework and reviewed by CMT.

Risk Strategy

Risk Strategy	Description
Treat	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)
Tolerate	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
Transfer	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
Terminate	In some circumstances it may be appropriate or possible to terminate or remove the risk altogether by changing policy, process, procedure or function