REPORT AUTHOR: **HEAD OF PROJECTS, SAFETY AND BUSINESS SUPPORT**

SUBJECT: **Corporate Services Risk Register**

For further information
on this Report contact:

Group Commander Darren Cook
Head of Projects, Safety and Business Support
Tel No: 01234 845163

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. <u>Introduction</u>

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 together with explanatory notes regarding the risk ratings applied is appended to this report.

2. <u>Current Revisions</u>

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:

- **CRR00039: 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:** Following a review of the risk, including the associated controls and the action plan has resulted in the Inherent Impact increasing from 3 to 4. Whilst this has increased the overall Inherent score from 9 to 12 the Residual risk remains the same and is being managed within the Head of the department.

- **CRR00038: If we suffer virus / hacking damage to business critical or vital computer systems then this will significantly affect our ability to deliver risk critical services such as emergency response:** Following a review of the risk, including the associated controls and the action plan has resulted in the Inherent Likelihood increasing from 1 to 4 raising the Inherent rating from 4 to 16. However the overall Residual Risk rating remains low and is being managed by the Head of the department

2.3 Updates to individual risks in the Corporate Risk Register:

- **CRR00005: 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:** Following discussion with members of CMT a decision was agreed to place this project on hold pending a full feasibility study due to complete in autumn 2017. In the interim a manual system is in place and embedded which will remain active and continue to sample audit to demonstrate compliance against current testing and maintenance schedules until an alternative system is procured.

- **CRR00015: If we do not properly manage the work issues that can potentially be caused by collaboration or shared services including: 1. Redundancy 2. Relocation 3. Cost of work for the convergence of procedures 4. Use of inexperienced staff familiar with FRS operations 5. Increase in staff numbers and associated cost; then there will be a negative cultural impact upon the service and the projects may fail:** The RMS project went live operationally for *voice mobilisation* in November 2016 with over 12,000 incidents being efficiently managed by Bedfordshire and Essex since then.

  The RMS project for data mobilisation is scheduled to go live shortly using MDT's on appliances. This is awaiting accreditation for the code of connection from the Home Office. The on-going management of the contract for the project will be managed by a shared services agreement between Essex and Bedfordshire FRS.

- **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 Threat Level from international terrorism changed on the 23rd May 2017 from 'Severe' to 'Critical' following the Manchester Arena bombing incident.
  In addition communications with relevant partner agencies have been maintained to ensure that the Service is able to respond quickly to any changes in the threat and risk that the current level of security presents. Staff have had regular and

timely communication and reminded to be vigilant and remain aware of their personal and premises security. For Operational Personnel, there will be further information provided on essential safety critical learning that will be required to be revisited in order to inform and prepare for potential incidents.

GROUP COMMANDER DARREN COOK
HEAD OF PROJECTS, SAFETY AND BUSINESS SUPPORT

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