

For Publication

Bedfordshire Fire and Rescue Authority
Corporate Services Policy and Challenge Group
14 March 2017
Item No. 10

REPORT AUTHOR: HEAD OF SAFETY AND STRATEGIC PROJECTS

SUBJECT: CORPORATE SERVICES RISK REGISTER

For further information on this Report contact: Group Commander Darren Cook
Safety and Special Projects
Tel No: 01234 845 163

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 together with 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: None. All risks that are reported the Corporate Services Policy and challenge Group have been reviewed and there are no risk rating changes to report to Members.
- 2.3 Updates to individual risks 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.**

The new HR/Payroll system is live and is the principal source of people-related information. Integrations are in development to synchronise this information with other systems. The collaboration with Devon and Somerset FRS in the development of workbench is continuing.

- **CRR00045: Exchanges of information such as email, web browsing, removable media, social media, exposes the Service to malicious code and content (malware). There is a risk that malware could seriously damage the confidentiality, integrity and availability of our Service's information and ICT resulting in disruption to the delivery of our Services, unauthorised export of sensitive information, material financial loss and legal or regulatory sanctions.**

A briefing on Cyber Security was delivered at the Management Briefing day (24 November 2016), as part of the on-going awareness programme for Managers. Penetration testing continues regularly and the outcomes of which inform action plans for all impacted departments.

- 2.4 Corporate Services Policy and Challenge Group have nine risks (listed at Appendix A) reporting directly to members that are categorised as 'treat', four of these risks have been reported to Members. These treated risks have had preventative actions put in place to reduce the possibility of an impact occurring.
- 2.5 All corporate risks are reviewed monthly and recorded by their owners for audit and scrutiny purposes.

**GROUP COMMANDER DARREN COOK
SAFETY AND SPECIAL PROJECTS**

Corporate Services Policy and Challenge Group '*Treated Risks*'

CRR00004	If there are a large number of staff absent from the workplace then our ability to deliver services to our communities is severely compromised and our reputation will be adversely affected. Maintaining our staff numbers.
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. Ensure the Service's arrangements are effective in the event of a terrorist attack.
CRR00045	Exchanges of information such as email, web browsing, removable media, social media, exposes the Service to malicious code and content (malware). There is a risk that malware could seriously damage the confidentiality, integrity and availability of our Service's information and ICT resulting in disruption to the delivery of our Services, unauthorised export of sensitive information, material financial loss and legal or regulatory sanctions. Malicious code within information exchange.
CRR00027	If we receive a poor budget settlement from government and the Local Authorities covering both revenue and capital funds and we have an adverse response from our Council Tax Precept consultation processes, then our ability to deliver a full range of services could be significantly affected. Managing our finances to ensure delivery of service.
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. Ensure that our data management arrangements are robust.
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. Managing external partnership and collaborative relationships.
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. Ensuring our assets are tracked and maintained.
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. Maintain effective communication with our staff, partners and communities.
CRR00008	If we do not monitor our key external suppliers of goods and services, particularly in regard to business continuity, then we may suffer a significant and detrimental impact on our ability to deliver our full range of services including emergency response. Ensure key external suppliers can maintain delivery at all times.

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: <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 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 <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.
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.