REPORT REFERENCE NO.	APRC/17/4
MEETING	AUDIT & PERFORMANCE REVIEW COMMITTEE
DATE OF MEETING	18 JANUARY 2017
SUBJECT OF REPORT	CORPORATE RISK REGISTER
LEAD OFFICER	HEAD OF ORGANISATIONAL ASSURANCE
RECOMMENDATIONS	*That the report be noted.*
EXECUTIVE SUMMARY	Managing risks of all kinds, both operational and strategic, is an important part of ensuring that the resources of Devon and Somerset Fire and Rescue Service are used to best advantage. Risk is inherent in most things that we do and much of the Service's activity is already assessed and managed through the application of the operational risk management procedures and good common sense. The Corporate Risk Register details risks and mitigation to ensure risk is managed appropriately and proportionately.
RESOURCE IMPLICATIONS	There are no direct financial implications. However, many of the risks identified relate to financial issues.
EQUALITY RISKS AND BENEFITS ASSESSMENT (ERBA)	Not applicable.
APPENDICES	Nil.
LIST OF BACKGROUND PAPERS	Report APRC/16/7 submitted to the Committee on 11 April 2016 (Minute APRC/31 refers). Report APRC/16/18 submitted to the Committee on 12 September 2016 (Minute APRC/13 refers). Minute DSFRA/36 - 24 February 2014 Minute DSFRA/13/21 - 19 December 2013

1. **INTRODUCTION**

1.1   The aims of Devon & Somerset Fire & Rescue Service's (the Service) Risk Management processes are to:

- Protect the assets of the Service;
- Ensure service continuity; and
- Facilitate innovation and opportunity.

1.2   Risk management does not mean risk avoidance. It is about encouraging officers and managers to identify, understand and control risk and to learn how to accept the right level of risk.

2. **BACKGROUND**

2.1   The Service's corporate risk register captures and describes the Authority's most significant risks, with a focus on cross cutting risks and major projects. It is formally reviewed and refreshed on a regular cycle. The final stage of the process, once the risks have been reviewed by risk owners and directors, is for the Committee to consider and comment on the register.

3. **CORPORATE RISKS FOR CONSIDERATION**

3.1   The Service's risk profile has changed over the last six months. Six risks have been added to the register and three risks downgraded to operational groups and departments. No risks have increased in severity.   As is normal, there have been minor changes to control measures across the risk profile. Risk owners are assigned to each issue and active mitigation in place.   The more substantive changes to the corporate risk register since the previous report to the Committee in September 2016 are set out in section 4 of this report below.

4. **NEW RISKS**

4.1   Risk CR029:

Issue added May 2016 – there has been an escalation in the number of safety events and near misses related to Breathing Apparatus reported in the last 12 months. This has resulted in a Service report being sent to the Health and Safety Executive (HSE), which is the normal process once pre-set triggers are reached. The breathing apparatus management across the Service currently lacks coordination. A working group has been established and now coordinates breathing apparatus activity across the Service. A number of changes have already been implemented, including provision of more training. Safety event levels are being monitored regularly.

4.2   Risk CR030:

Issue added April 2016 – A lack of fixed term or longer term contracts has resulted in a number of project managers leaving the Service.   The Programme Board is managing the risk and 1 x Full Time Equivalent (FTE) project manager has joined the Service in November 2016, which leaves one vacant post.

4.3   Risk CR035:

Issue added June 2016 – Performance information not available from the Vision DS system - due to difficulty extracting information from the mobilising system and the existing performance management system being unsupported, there is a risk of inability to react to performance trends.   The resulting consequence is that data is not available to support the Service's Corporate Plan, existing systems unreliable and inability to report performance to FRA and associated committees. Ongoing activities being managed by project board and fire control.

4.4   Risk CR036:

Issue added June 2016 – lack of integrated asset tracking system. This issue also features in the Annual Statement of Assurance. The Estates Department has a standalone asset management system and the Fleet Department is working collaboratively with other fire and rescue services in pursuit of a suitable system.   There is a corporate project to address this in the change and improvement plan.

4.5   Risk CR037:

Issue added July 2016 - The UK threat level is at severe, Northern Ireland is at substantial and there is an increasing number of cyber-attacks on public sector organisations. The Service's systems have not been compromised and active monitoring has identified the following data:

- Virus attacks – minimum of six per day, all bounced off firewall protection with no adverse impact on the Service's systems;

- Phishing attacks – staff reported 69 events which had breached firewall protection. As a result, the Service's systems were not compromised;

- Half of all email is classified as 'spam'.

The Service is vulnerable to systems and data being lost or corrupted for an unspecified period. There would also be uncertainty as to the subsequent financial impact of system and data recovery, potential fines or public censure for security breach together with adverse media reports adversely impacting on the Service's reputation.

This vulnerability may increase the likelihood of the Service experiencing a safety event. This is based on the number of terrorist attacks experienced across Europe, cyber-attacks targeted at public sector (in last 12 months, 2 other fire and rescues services lost system access for 5 days). The vulnerabilities include the disparate number of systems within the Service requiring password which may be weakening information security as staff keep separate unsecure records, the escalating number of information security events and breaches being reported (Data Protection and ICT systems) and Internal and external Information and Communications Technology (ICT) health check reports identifying outstanding 'patching'.

As a result of the growing threat a full time Information Technology Security Officer (ITSO) role is in place and a wider team managing information assurance since December 2016.

4.6   Risk CR038:

Issue added - Issues with the stability: spikes on the mobilising system servers, with Gartan interface and links to the Basic Input Output System (BIOS).

Because of the current performance issues of the mobilising system, the risk of system unavailability increases. This would impact on the Service's ability to mobilise efficiently, which could result in a breach of statutory duty.

Capita has invested considerably in improving the stability of the mobilising system. The Partnership has engaged with Capita, with a review of the hardware and infrastructure to further reduce the risk of a system failure.   Early 2017, further improvements to the system with more secure physical links between the interface of the partnership.

5.   **AMENDED RISKS**

5.1   No risks have been amended.

6.   **RISKS REMOVED**

6.1   No risks have been removed.

7.   **LEGAL IMPLICATIONS**

7.1   There are no direct legal implications arising from this report. Existing control measures in place are operating effectively to help the Service meet its legal requirements, and other risks also refer to controls that will reduce the risk of legal challenge.

8.   **NEXT STEPS**

8.1   The next formal review of the corporate risk register will take place after the financial year end. The Register may well therefore need to be refreshed.

8.2   The Committee is asked to note this report.

        NICK MANNING
        Head of Organisational Assurance