Finance and Contractual Services

RISK AND AUDIT

RISK MANAGEMENT POLICY

Author/Role	David Johnston, Risk & Audit Manager
Date of Risk Assessment (if applicable)	N/A
Date of Equality Impact Assessment	3 September 2018
Date of Impact Assessment (commenced)	21 August 2018
Date of Impact Assessment (concluded)	3 September 2018
Quality Control (name)	John Thomson, Head of Finance and Procurement
Authorised (name and date)	Sarah O'Donnell, Director of Finance and Contractual Services
Last reviewed (name and date)	21 August 2018
Date for Next Review	21 August 2020

FINANCE AND CONTRACTUAL SERVICES

RISK AND AUDIT

RISK MANAGEMENT POLICY

1.   POLICY STATEMENT

1.1   The Scottish Fire and Rescue Service (SFRS) provides a diverse range of services to the communities of Scotland and is committed to improving community safety, response and resilience, whilst addressing inequalities and enhancing safety and wellbeing.

1.2   The provision of these critical services is undertaken within an ever-changing and challenging environment that presents risks that have to be effectively managed. SFRS is fully committed to the development, implementation and ongoing monitoring and review of an integrated risk management framework, identifying, managing and monitoring those risks which may impact upon the successful achievement of the key priorities of the SFRS.

1.3   The aim of the SFRS is to be risk aware, allowing innovation and aspiration, whilst actively managing risk through a range of measures to ensure key priorities are met. The framework will follow the principles of the International Standard in Risk Management ISO 31000 establishing a consistent and effective framework integrated within the Governance and Assurance arrangements of the Service.

1.4   The Service recognises that it cannot entirely eliminate the risk of disruption to its service delivery and that a residual level of risk will always remain. However, the risk management framework has been developed in order to minimise the likelihood and impact of a risk causing disruption to daily activities. The implementation of the framework will ensure:

- Provision of assurance regarding the effective management of significant risk;
- Improved governance and confidence;
- Improved organisational resilience;

- Improved allocation and use of resources;
- Improved decision making capability;
- Improved likelihood of achieving key priorities.

2. OBJECTIVES

2.1 The main purpose of the policy is to provide an effective framework for the management of risk. This framework will, therefore, contribute towards ensuring an agreed, consistent and standardised approach is taken across all SFRS Directorates.

In implementing the policy and associated framework, the Service will:

- Promote awareness and ownership of service risks and embed the framework throughout the organisation;
- Improve service planning and prioritisation of resources;
- Promote Enterprise Risk Management and effective Governance arrangements;
- Preserve and protect the Service's assets, reputation and staff;
- Demonstrate that appropriate mitigating actions are identified and subject to effective scrutiny and control.

3. SCOPE

3.1 The policy will extend to cover the management of Strategic and Directorate risks that may impact upon the achievement of the strategic aims and objectives of the Service. The policy does not cover the risk management processes used on the incident ground or for general Health, Safety and Wellbeing in the workplace, where SFRS already has systems of control in place.

4. RESPONSIBILITIES

4.1 Chief Officer

The Chief Officer, as the Accountable Officer, is responsible for maintaining a sound system of internal control, risk management and corporate governance that supports the achievement of the SFRS policies, strategic aims and objectives. The Chief Officer will champion the importance of risk management in supporting the wider governance arrangements of the Service.

4.2 The SFRS Board

The Board provides strategic direction, support and guidance to the SFRS ensuring that it operates effectively. It is responsible for the scrutiny of risk, financial management and performance confirming that the principles of risk management are demonstrated within the overall performance management systems of the Service, whilst seeking assurance that the Strategic aims and priorities of the Service are being met. The Board will receive an annual report on the risk management framework and will have responsibility for the Service's risk profile and appetite and for the identification of strategic risk, particularly outward facing risk.

4.3 Audit and Risk Assurance Committee (ARAC)

The Audit and Risk Assurance Committee will advise the Board and Accountable Officer (Chief Officer) on the effectiveness of the application of the strategic processes for risk, control and governance. This will include a quarterly review of the Service's Strategic Risk Register and associated action plans.

4.4   SFRS Committee Structure

Individual Committees retain a scrutiny role, providing assurance to the Board on matters falling within their scope. All SFRS Committees will scrutinise risks pertinent to the business of the Committee.

4.5   Strategic Leadership Team (SLT)

The identification and management of strategic risks will be the primary responsibility of the SLT. The SLT will undertake to monitor and review strategic risks regularly and take appropriate action to control risks. The SLT will champion the importance of risk management in supporting the achievement of the SFRS strategic aims and objectives. The SLT will be responsible for maintaining and reviewing strategic risk, on a quarterly basis, through the Strategic Risk Dashboard - see Appendix C.

4.6   Executive Boards

All Executive Boards will provide a monitoring and scrutiny role for risks falling within their scope and will provide assurance to SFRS Committees and the SLT that risk is being effectively managed. Executive Boards will champion the importance of managing risk as part of an integrated governance framework, ensuring that awareness and ownership of risk is embedded throughout the organisation.

4.7   Heads of Functions / Deputy Assistant Chief Officers (DACOs)

The identification and management of corporate risks will be the responsibility of Heads of Function/DACOs. They will undertake to monitor and review Corporate and Directorate risks regularly and to take appropriate action to control risk. Heads of Function/DACOs will champion the importance of risk

management in supporting the achievement of the Service's strategic aims and objectives.

4.8 Risk and Audit Manager

The Risk and Audit Manager will develop the policy and framework for managing risk, building a risk aware culture, coordinating Service-wide risk management activities and regularly reviewing, managing and reporting risk within the Service.

4.9 Internal Audit

Internal Audit will audit the effectiveness of the Service's risk management process, as appropriate, provide assurance on the management of risk to the Board of the SFRS and help support the risk management process and coordination of risk reporting.

4.10 All Other SFRS Staff

The SFRS's approach to risk management seeks to ensure that risk management is fully integrated throughout the Service with ownership and responsibility retained through the Board and Committee Structure, Senior Management and cascaded through to Directorates, Service Delivery Areas and all other SFRS staff.

Effective risk management depends on the commitment and cooperation of all managers and employees. Individual managers and employees are each charged with the effective management of the risks associated with their particular roles and duties, which may impact upon the delivery of the service's aims and objectives. Consequently, all managers and employees are responsible for adherence to the principles outlined in this policy.

5.   DEFINITIONS

5.1   Strategic Plan

The Strategic Plan has been developed in response to the Fire and Rescue Framework for Scotland 2016 and sets out the Service's outcomes, values and priorities.

5.2   Risk

A risk for SFRS is defined as something with the potential to impact upon the achievement of key service priorities. For SFRS, risk is split into three categories:

- Strategic Risk Themes identified by the SFRS Board and Strategic Leadership Team summarising the overarching risks to the Service;
- Corporate Risks which, if managed, will help mitigate the overarching themes and have an impact across all Directorates; and
- Directorate Risks which relate to a specific Directorate but can be linked back to an overarching Strategic theme.

5.3   Risk Management

Risk management can be defined as the identification, evaluation and control of risks with the potential to impact upon the operation of the Service and its ability to achieve its priorities.

5.4   Risk Appetite

Risk Appetite can be defined as the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time (The Orange Book, HM Treasury).

5.5   Risk Register

The risk register is the means by which the Service captures risks and demonstrates that they are being managed appropriately.

- The Strategic Risk Register captures the key risk themes of the organisation and the corporate risks which, if managed appropriately, will contribute towards the overall control of the key risk themes;
- Directorate Risk Registers capture relevant corporate risks and those additional risks identified by Directorates where they impact only upon that area.

5.6   Risk Action Plan

The risk action plan identifies those additional controls necessary to manage risk down to an acceptable level and provides the focus for ongoing monitoring and review.

5.7   Annual Governance Statement

The Annual Governance Statement outlines the arrangements that are in place for internal control, risk management and corporate governance and how effective these arrangements have been during the period under review.

5.8   Enterprise Risk Management

Enterprise risk management is the term used to bring together linked but individual systems of control and builds upon the risk management and assurance framework allowing information to be shared and communicated effectively across the Service.

5.9   Responsible Officers

Within the risk register template, each risk will be owned by a responsible officer. This officer is responsible for the management of the risk and for the update of any required information. The responsible officer will identify a relevant action plan to manage the risk and will liaise with other officers/directorates, where relevant, to ensure all elements of risk are managed.

6.   THE RISK MANAGEMENT FRAMEWORK

6.1   The SFRS Risk Management Framework will follow the principles of BS ISO 31000, the International Organisation for Standardisation. The risk management standard provides a framework and a process for managing risk, outlining general guidelines on risk management which, if followed, will increase the likelihood of achieving objectives.

6.2   The overarching goal is to develop a risk management culture where employees and stakeholders are aware of the importance of managing risk.
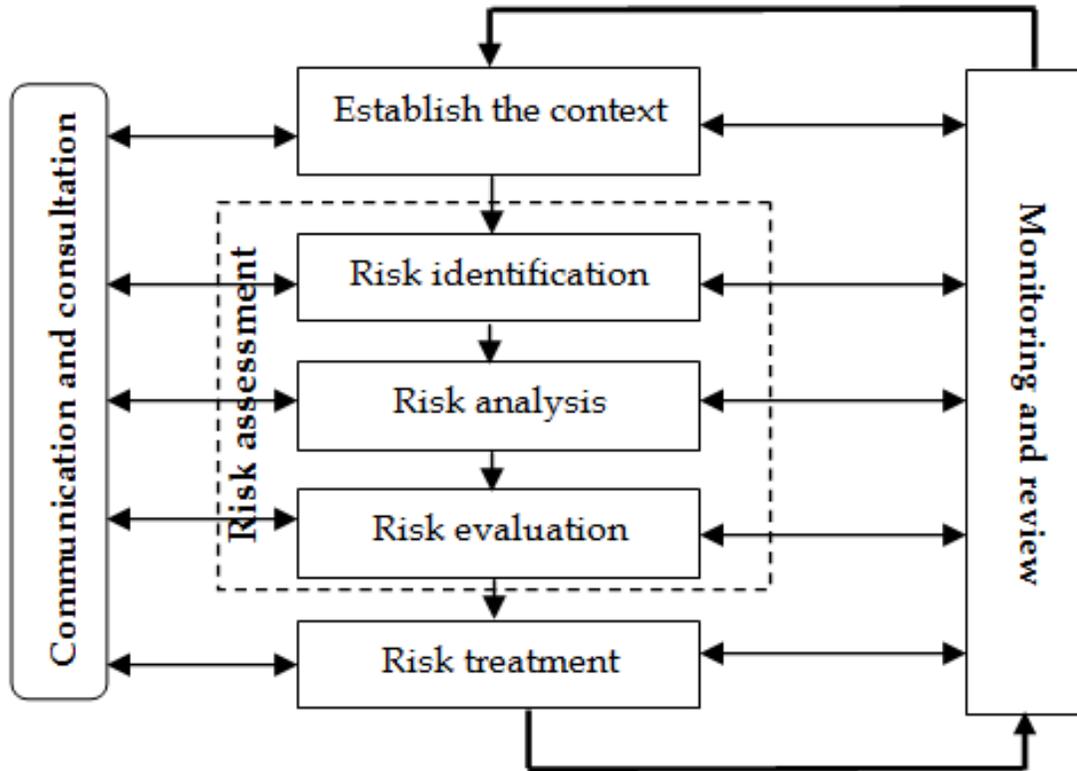
Table 1

6.3   The above framework establishes a simple structure for ensuring that the right information is used to inform decision making and is subject to effective scrutiny and control. Used correctly, it will ensure that risk is managed effectively.

7.   MANAGING RISK

7.1   Risk management can be defined as the identification, evaluation and control of risks with the potential to impact upon the operation of the Service and its ability to achieve its Strategic Priorities.

7.2   In order to manage risk, the framework, outlined in Table 1, is used to ensure that the risk information is available to allow managers to make informed judgements and assessments in relation to risk.

7.3   The framework will follow the principles of the International Standard in Risk Management ISO 31000 and consists of a number of stages:

- Communication and Consultation;
- Identifying Risk;
- Assessing and Evaluating Risk;
- Managing and Treating Risk;
- Monitoring and Reviewing Risk;
- Improve Framework.

7.4   Communication and Consultation

7.4.1   The risk management framework relies upon awareness and ownership of risk being retained across all levels of the organisation. We need to talk about risk and understand how priorities contained within the Fire Framework, the Strategic Plan and other plans expose the organisation to risk.

7.4.2   Risk cannot be managed in isolation to other core business processes if it is to inform decision making. Consulting with and talking to Directorates and individuals, both internally and externally, will ensure that the right inputs are available for us to manage risk effectively.

7.4.3   Risk will continue to be reported quarterly to the Audit & Risk Assurance Committee with a SLT reported prepared in advance of this. The addition of quarterly reporting to all other Committees and the use of the risk register as part of the Executive Board agendas will enhance ownership and awareness of risk across the organisation.

7.4.4   The SFRS Board will receive an annual report on the risk management framework including revisions to its risk appetite, with the Risk Management

Policy updated to reflect any revision.

7.4.5   Quarterly meetings and discussions will be held with Directorates involved in the preparation of updated registers, with any additional adhoc meetings/workshops to be arranged as necessary.

7.4.6   Alignment between Directorate business planning and risk registers will continue allowing Directorates to work smarter by using similar information more widely across the organisation.

7.5   Identifying Risk

7.5.1   The identification of risk should be undertaken in a methodical manner to ensure all risks are accurately identified.

7.5.2   The identification process should be based around the actions and priorities set through the Strategic Plan or relevant Directorate or Functional Plans. Existing documents/areas may already have identified a number of risk areas:

- Business Planning;
- Performance Data;
- Project Boards;
- HMFSI Reports;
- External Audits;
- Internal Audits;
- General Audit Reviews;
- De-briefings / lessons learned;
- Existing Risk Information.

7.6   Assessing and Evaluating Risk

7.6.1   Once the corporate and/or directorate risks have been identified, they need to be assessed in terms of their probability or occurrence and their potential impact upon the delivery of priorities or objectives. It is, therefore, important to use an agreed and standardised process that measures impact and probability consistently across the organisation.

7.6.2   Without this standardised and consistent approach, the comparison and allocation of resources to manage risk becomes more complex to measure. The adoption of the risk assessment and evaluation matrix, outlined in Appendix A, will enable this standardised and consistent approach throughout the SFRS.

7.7   Managing and Treating Risk

7.7.1   As part of an effective governance framework, the Service must be able to demonstrate that risk is being managed in an open and transparent manner and consistently across the Service.

7.7.2   The Risk Register, Appendix B, is the means by which the Service captures risks and demonstrates that it is being effectively managed. The Risk Register forms the core of all risk activity.

7.7.3   A single risk register template has been agreed by the Service to ensure a standardised approach across all areas of service activity, with two primary register types required by the Service:

- Strategic Risk Register (outlining the Service's Strategic Risk Themes and Corporate Risks);
- Directorate Risk Registers (containing both Corporate and Directorate risks).

7.7.4   The Strategic Risk Register identifies a number of key risk themes which are identified by the SFRS Board and the SLT. The SLT is responsible for monitoring these themes collectively through a Strategic Risk Dashboard on a quarterly basis - Appendix C.

7.7.5   Supporting each of these key themes are a number of corporate risks, each allocated to a responsible DACO or Head of Function. These corporate risks will form the basis of Directorate registers which will then be expanded through the identification of risks specific to each separate Directorate.

7.7.6   Both the Strategic and Directorate registers must use the corporate template. Where Project or other Section registers are developed, the corporate template should be used to provide a standardised and consistent approach.

7.7.7   The risk register requires the responsible officer to identify links to the Annual Operating Plan or Directorate Plans where common actions may already have been identified. Section 7.5.2 above identifies additional areas where existing actions may already have been identified and are already subject to monitoring and review. Directorates need to maximise their use of existing information when managing risk, only developing additional actions when no other actions exist.

7.7.8   Having identified existing actions and their effectiveness, directorates will consider any additional actions still required to manage risk to a tolerable level. These risk action plans, Appendix D, will be subject to monitoring and review through the risk framework. However, as the Service's governance arrangements mature, the number of separate action plans should reduce, with core planning documentation containing most relevant management actions. In broad terms, any action taken to manage risk to an acceptable level can fall into four categories:

- **Terminate** - involves deciding to eliminate the risk by ceasing the activity or the pursuance of the objective or priority that presents the risk;

- **Transfer** - involves deciding to pass the risk or costs of the impact outside the Service, i.e. contract out the risk or take out insurance to cover the costs of the impact;

- **Treat** - involves implementing control measures to reduce the risk, thereby lessening the impact. This can involve improved procedures, training or investing in new equipment;

- **Tolerate** - involves accepting the risk and its impact or agreeing to self-insure any associated financial costs, whilst ensuring best value can be demonstrated.

7.8   Risk Escalation / De-escalation

7.8.1   The responsibility to identify and manage risk rests with individual Directorates and the relevant Director. Where the Director has identified a risk, it is for the Director to escalate that risk, via a report to the Strategic Leadership Team and ARAC, to the Strategic Risk Register. This may relate to a risk where the impact has a wider effect on the whole Service rather than specific elements of a single Directorate's work.

7.8.2   For risks already held within the Strategic Risk Register, the SLT and ARAC will agree for risks to be moved from the Strategic Register to the Directorate Register where the overall level of risk has been reduced to a level whereby further action or monitoring will be undertaken by a single Directorate and where the risk no longer significantly impacts upon the whole Service.

7.9   Monitoring and Reviewing Risk

7.9.1   Monitoring of risk will be undertaken through the Executive Boards and Committees of the Service, following the principles of the "three lines of defence model", attached in Appendix E. The model ensures that the right information is used to inform decision making within an overall framework, clearly indicating the separation of scrutiny roles across the organisation.

7.9.2   Where risks are subject to monitoring and review, recommendations may be made to escalate a Directorate Risk to the Strategic Risk Register or to reduce a risk from the Strategic Risk Register to a Directorate Register. The decision on whether to accept this recommendation will rest with the relevant Director, with the decision reported to the SLT and the Audit and Risk Assurance Committee as the central governance reporting route.

7.10   Improving the Framework

7.10.1   To ensure the risk framework continues to remain fit for purpose, it will be continually reviewed in line with the Fire Framework, the Strategic Plan and the overall governance framework. New initiatives and practices identified within partner organisations, or through agreed Scottish Public Finance Manual (SPFM) guidance, will be considered and, where appropriate, incorporated within the framework.

7.10.2   Annual reviews of both risk information and the risk framework will be undertaken in discussion with Directorates, the Strategic Leadership Team and the SFRS Board and relevant Committees.

7.10.3   The SFRS governance framework is subject to internal and external audit review and recommendations arising from audit activity, as impacting upon the risk

management framework, will be considered and implemented to ensure best practice can be demonstrated.

8. RISK APPETITE

8.1   The purpose of the risk register and the wider risk management framework is to encourage debate and discussion, informing our decision making processes. SFRS recognises that it cannot entirely eliminate risk from Service provision and that a residual level of risk will always remain that has to be managed.

8.2   Risk Appetite is part of this overall framework and relates to the scrutiny and assurance requirements developed by the Service to ensure risk is understood and suitably controlled.

8.3   Risk Appetite can be defined as the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time (The Orange Book, HM Treasury).

8.4   The Service's risk appetite is set annually by the SLT and the SFRS Board. Appendix F identifies an example of the tolerance levels set for each of the 5 impact criteria which have been integrated within the risk register to reflect an additional layer of control.

8.5   Risk Appetite is split into 5 classifications:

Averse: Avoidance of risk and uncertainty is a key organisational objective

Minimalist: Preference for ultra-safe business delivery options that have a low degree of inherent risk and only a potential for limited reward

Cautious: Preference for safe delivery options that have a low degree of inherent risk and may only have a limited potential for reward

Open: Willing to consider all options and choose the one that is most likely to result in success, whilst also providing an acceptable level of reward

Risk Seeking: Eager to be innovative and to choose options offering potentially higher rewards despite greater inherent risks

8.6   Each of these classifications is considered against areas of impact agreed by the Service:

- Political;
- Operational;
- Financial;
- Legal/Regulatory;
- Reputational/Stakeholder confidence.

8.7   The outcome of the process will then map risk appetite against the initial impact assessment made for each risk. If the initial impact assessment is greater than the risk appetite impact assessment, the risk is outwith the Service's appetite and will be subject to additional scrutiny.

9.   LINK TO THE ANNUAL GOVERNANCE FRAMEWORK

9.1   The Chief Officer, as the Accountable Officer, has overall responsibility for maintaining sound systems of internal control, risk management and corporate governance that support the achievement of the organisation's policies, aims and objectives.

9.2   The Annual Governance Statement incorporates an evaluation of how well the Service's internal control, risk management and corporate governance arrangements have operated in practice, based upon robust internal assessment processes. Where Improvement Actions are identified from within the framework, the responsible officer must create an Improvement Action Plan, highlighting any link to the Strategic Risk Register.

9.3   The SFRS risk management framework is fully embedded within this process and is an integral element of assurance provided by senior management.

10.   ENTERPRISE RISK MANAGEMENT

10.1   Enterprise Risk Management (ERM) is the term used to bring together linked but individual systems of control and builds upon the Service's established risk management and assurance frameworks, allowing information to be shared and communicated effectively across the Service.

10.2   ERM is an ongoing process flowing through the organisation, impacting across each level of the Service and overlapping individual areas of risk adding to decision-making and awareness. Whilst the risk management framework provides a systematic process, ERM is designed to look across the Service at the interdependencies and how we share experiences and information.

10.3   ERM systems work on a three line of defence principle, as outlined in Appendix E. In broad terms, this means that the first line of defence to risks are the front line operational staff and management who encounter them. The second line is made up of support functions that are responsible for the frameworks and tools the first line uses to manage risk. The third line of defence is the independent or external assurance providers, such as internal/external audit or Her Majesty's.

10.4   No single system can identify and manage all aspects of risk to which the Service is exposed and no single element of control can exist in isolation if best value is to be achieved. It is only when we bring together all core elements of an effective governance system that the Service will be able to ensure that its key aims and objectives can be fully achieved.

11.   ASSOCIATED DOCUMENTS / REFERENCES

Annual Governance Statement Policy
Strategic Plan 2016-2019

APPENDIX A – ASSESSING AND EVALUATING RISK

Likelihood/Probability

Each risk will be initially assessed based on the likelihood of it occurring within the organisation.

Criteria for Evaluating Risk			
Probability	**Description**	**Numerical Value**	**Plain English**
1	Very Low – Where an occurrence is improbable or very unlikely	1 in 20,000	Never happened and doubt it will
2	Low – Where an occurrence is possible but the balance of probability is against	1 in 2,000	Has happened before but unlikely
3	Medium – Where it is likely or probable that an incident will occur	1 in 200	Will probably happen at some point in the future
4	High – Where it is highly probable that an incident will occur	1 in 20	Has happened in recent past and will probably happen again
5	Very High – Where it is certain that an event will occur	1 in 2	It's already happening and will continue to do so

Severity of Impact

Each risk will also be considered in terms of the impact it may have on the achievement of key service priorities.

Many risks may have a number of different impacts upon the organisation but it is the highest impact area that will be chosen in relation to the impact assessment.

Impact	Political	Operational	Financial	Legal& Regulatory Compliance	Reputational/Stakeholder Confidence
RISK ASSESSMENT					
1	Effective Strategic Decision making, full engagement by Board and SLT and meeting in full the expectation of Scottish Government and Local Communities	No negative impact on our ability to deliver the service.	no impact on our ability to deliver a balanced budget	no adverse reputational damage to the service	Rumours, with potential for local public/political concern
2	Minor reduction in Board engagement, minimal impact upon achievement of strategic objectives and no adverse comment from SG	There will be a very minimal impact on our ability to deliver the service.	our ability to deliver a balanced budget will be realised with minimal adjustments	Potential unexpected external scrutiny of our activities due to non compliance. Some adverse media attention received.	Some negative Local press interest or Local public/political concern.
3	Question raised over effectiveness of strategic decision making, noticeable impact upon service delivery, critisim by external bodies, partners and sG	There will be a reduction in the ability for us to deliver our services and there may be minor service disruption.	action required to ensure delivery of a balanced budget. Potential adverse impact on service delivery.	Prolonged adverse media attention. Critcism of our service as a result of srutiny by external bodies. Potential legal action.	Limited damage to reputation. Extended negative local press interest. Some regional public/political concern.
4	Ineffective Board engagement, challenge over strategic decision making of SFRS, failure to delvier against agreed priorities and SG critisim and threat of intervention	Service disruption for an extended period. Major consequences.	insufficient finances available to support service delivery	Inneffective governance arrangements identified resulting in Government intervention in the management of the service.	Loss of credibility and confidence in the service. National negative press interest. Significant public/political concern.
5	Failure to deliver against SG prorities, failure of Board and SLT to engage, intervention by SG and external monitoring bodies	Failure to deliver our services	failure to live within our means	failure of the service	Full Public Inquiry. International negative press interest. Major public/political concern.

The Risk Matrix

The outcome of the likelihood and impact assessment will then be used to determine the overall risk assessment and prioritisation of the risk.

Using the table below, each score will be mapped on the matrix and an overall assessment identified by multiplying the likelihood score against the impact score.

Probability	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
Risk Matrix		1	2	3	4	5
		Impact				

APPENDIX B – THE RISK REGISTER

Scottish Fire and Rescue Service
Strategic Risk Register
Year/Month

Risk Ref. No.	Link to Core Business Planning Documents		Actions Required	Date Identified	Last Reviewed Date	Risk Appetite Category	Risk Description	Consequence of Risk	Control Measures In Place
	Annual Operating Plan	Directorate Plan							
Strategic Risk Theme									
Corporate Risk									
Corporate Risk									
Corporate Risk									

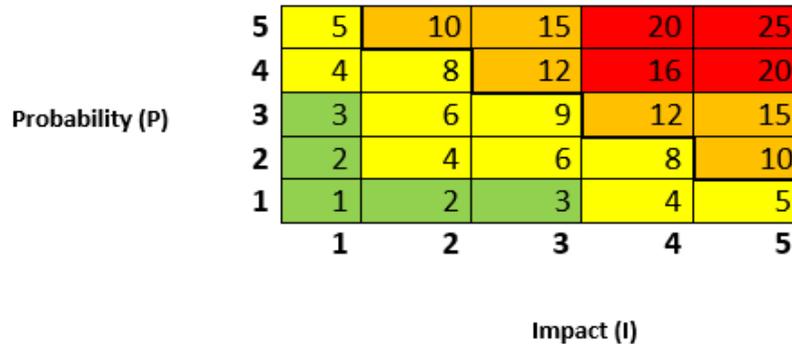| Governance and Scrutiny Arrangements		Current Risk Assessment			Previous Risk Rating	Risk Appetite	Risk Movement	Responsible Officer
Committee Level	Executive Board Level	Probability	Impact	Risk Rating		Impact Assessment		
							➡	**SLT**
							➡	
							➡	
							➡	

APPENDIX C – STRATEGIC RISK DASHBOARD

Strategic Risk Dashboard

Example

SLT Comments
The strategic overview assessment undertaken by the SLT considers the overall cumulative risk to the organisation, based upon information available to the SLT at the time. Individual corporate risk assessments, undertaken by responsible officers, are permitted to be higher or lower than the overall strategic assessment.

	P	I	Risk Rating	Risk Movement
1 - Failure to minimise Communities' exposure to risk and harm	3	4	12	⟹
2 - Failure to Protect the Health, Safety and Wellbeing of Firefighters and other employees	3	4	12	⟹
3 - Failure to deliver Service Transformation	3	4	12	⟹
4 - Failure to ensure Financial Sustainability	3	4	12	⬆
5 - Failure to ensure Legal Compliance is maintained	3	4	12	⟹
6 - Failure to have in place a suitably skilled, engaged and flexible workforce, ensuring capacity, to deliver service priorities	3	4	12	⟹
7 - Failure to maintain effective systems of control	3	4	12	⟹
8 - Failure to maintain confidence in the Service	2	3	6	⟹

	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
Probability (P) **3**	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Impact (I)

APPENDIX D – RISK ACTION PLANS

Risk Action Plans

The following table will highlight the main Directorate actions required to manage risk down to a more tolerable level, providing assurance to scrutiny bodies that effective and efficient systems of control are in place.

As the action plan may become a public document through reporting to a Committee, all personal data should be anonymised. The risk owner will be identified as the Head of Function or DACO, as will the responsible officer.

Strategic Risk				Risk Rating	Assessment from risk register (colour code)	
Risk Ref		Risk Owner		Risk Appetite	Assessment from risk register (colour code)	
Risk Description						
Agreed Management Action(s) (in additional to actions outlined within the AOP or Directorate Plans)			Target / Completion Date	Action Summary		Responsible Officer

It is through the completion and monitoring of these plans that risk will be effectively managed and the integration of these plans within the wider business and performance management systems is critical to the Service's overall management of risk.

APPENDIX E – THE THREE LINES OF DEFENCE MODEL

To ensure the right information is used to inform decision making and the framework is subject to effective scrutiny, additional governance arrangements have been adopted.

The three lines of defence model provides a simple and effective method to clearly identify the roles and responsibilities within the Service in relation to scrutiny and control and, when applied, will allow enhanced dialogue and analysis of risk.

The model distinguishes amongst three groups (or lines) involved in effective risk management:

		Risk Governance	
Assurance Providers	3rd Line of Defence	**RISK PROCESS AND CONTENT Monitoring** • Liaise with senior management and/or board • Renationalise and systematise risk assessment and governance reporting • Provide oversight on risk management content/processes, followed by second line defence (as practical)	Assurance Providers
Standard Setters	2nd Line of Defence	**RISK PROCESS Accountability** • Establish policy and process for risk management • Strategic link for the enterprise in terms of risk • Provide guidance and constituencies • Identify enterprise trends, synergies, and opportunities for change • Initiate change, integration of new events • Liaison between third line of defence and first line of defence • Oversight over certain risk areas and in terms of certain enterprise objectives (e.g. compliance with regulation)	Standard Setters
Business Owners	1st Line of Defence	**RISK CONTENT Accountability** • Manage risks/implement actions to manage and treat risk • Comply with risk management process • Implement risk management processes where applicable • Execute risk assessments and identify emerging risk	Business Owners

Functions that own and manage risk

1st line – Day to day risk management and control. Functions that own and manage risks directly. Responsible for corrective actions to address process and control deficiencies

Functions that oversee risks

2nd line – Functions that oversee risk. Functions that develop and maintain risk management policies and methodologies, identify and monitor new and emerging risks and enforce the enterprise risk management model. Liaison between 1st line and 3rd line of defence.

Functions that provide independent assurance

3rd line – Independent assurance. Functions that provide independent assurance that risk management is working effectively. Greater independence with reports to governing body.

APPENDIX F – RISK APPETITE

Risk Appetite is a management tool to achieve effective governance, ensuring our systems of controls are effective and informs our decision making processes. It sets parameters within which the Service wishes people to operate. Where these parameters are exceeded, the Service/function will not be stopped but rather additional levels of monitoring and scrutiny will be developed to better understand and mitigate the impact upon the organisation.

Simply put, the initial impact assessment, within the risk register, is used to determine whether the risk is in or out of the Service's risk appetite. If the impact assessment is 4 and it relates to a financial risk, it would be red and outwith the Service's appetite and additional scrutiny will be applied:

RISK APPETITE				
Impact	Political	Operational	Financial	Legal & Regulatory Compliance	Reputational/Stakeholder Confidence
Averse (1)	Minimal tolerance for taking any decisions or actions that could result in increased parliamentary scrutiny or criticism of the Service	Defensive approach - aim to maintain or protect existing ways of working, rather than to create or innovate. Priority for tight management controls and oversight with limited devolved decision making authority. Resources withdrawn for all non-essential activities. General avoidance of system/technology developments	The key objective is to operate in line with the agreed budget profile. Only willing to accept the low cost option	Avoid anything which could be challenged, even unsuccessfully	Minimal tolerance for any decisions that could lead to increased scrutiny or criticism of the Service
Minimalist (2)	Only tolerant of making decisions that contradict or challenge national or local governments where there is no chance of significant repercussions for the Service	Innovations are always avoided unless essential. Decision making authority held by the SLT. Resources allocated to core business. Only essential systems/technology developments	Only prepared to accept the potential for very limited variance in budget lines. Minimising cost is the primary concern	Want to be very sure the Service would win any challenge	Only tolerant of risk taking where there is no chance of significant repercussions for the Service
Cautious (3)	Only tolerant of making statements or taking decisions that impact on the political arena where the Service has the support of key political stakeholders	Tendency to stick to the status quo. Innovations generally avoided unless necessary. Decision making authority generally held by SLT. Resources are generally allocated to core business. Systems/technology developments limited to those which are essential, unless low risk	Prepared to accept the potential for some variance in budget lines and the potential for some minor underspend/overspend. Value for money is the primary concern, with an emphasis on quality as well as price	Limited tolerance for sticking our neck out. Want to be reasonably sure the Service would win any challenge.	Only tolerant of risk taking where there is limited chance of significant repercussions for the Service
Open (4)	Appetite to take decisions which may expose the Service to additional parliamentary or political scrutiny, but only where appripriate steps have been taken to minimise any exposure	Innovation supported as long as there is a commensurate improvement in management control. Responsibility for non-critical decisions may be devolved. Resources are allocated to capitalise on potential opportunities, not just to deliver our current practises. Systems/techology developments considered where these will enable delivery.	Prepared to take some financial risk by investing in new projects or activities (recognising that this could result in overspend / underspend) as long as appropriate controls are in place. In assessing value for money, quality considerations are weighted more than price	Challenge will be problematic but the Service is likely to win it. The gain will outweigh the adverse consequences.	Appetite to take any decisions which may expose the Service to additional scrutiny, but only where appropriate steps have been taken to minimise any exposure
Risk Seeking (5)	Appetite to take decisions which are likely to expose the Service to additional political, media and parliamentary scrutiny where the potential benefits to the Service outweigh the risks	Innovation pursued, desire to break the mould and challenge working practices. High levels of devolved authority, management by trust rather than tight control. Resources are allocated to areas of work where there are guarantes of success - investment capital type approach. New technologies viewed as a key enabler of operational delivery.	Prepared to take financial risks by investing for the best possible reward, accepting that this brings the possibility of underspend/overspend.	Chances of losing are high and consequences serious. But a win would be seen as a great coup.	Appetite to take decisions which are likely to expose the Service to additional scrutiny, if the potential benefits outweigh the risks