



FINANCE AND PROCUREMENT

RISK MANAGEMENT POLICY AND FRAMEWORK

Author/Role	David Johnston, Risk and Audit Manager
Date of Risk Assessment (if applicable)	N/A
Date of Equality Impact Assessment	Revised 9 September 2021
Date of Impact Assessment (commenced)	Revised 9 September 2021
Date of Impact Assessment (concluded)	9 September 2021
Quality Control (name)	Lynne McGeough, Acting Head of Finance and Procurement
Authorised (name and date)	John Thomson, Acting Director of Finance and Procurement – October 2021
Date for Next Review	October 2024

VERSION HISTORY

Version	Change	Who	When
1.0	First version issued as Risk Management Policy	GM Roy Dunsire	28/02/2014
2.0	Reviewed and updated	David Johnston	21/08/2018
3.0	Reviewed and updated as Risk Management Policy and Framework	David Johnston	18/11/2021



SCOTTISH
FIRE AND RESCUE SERVICE

Working together for a safer Scotland

FINANCE AND CONTRACTUAL SERVICES

FINANCE AND PROCUREMENT

RISK MANAGEMENT POLICY AND FRAMEWORK

1. [POLICY STATEMENT](#)
2. [RISK MANAGEMENT OBJECTIVES](#)
3. [RISK MANAGEMENT CULTURE](#)
4. [SCOPE](#)
5. [ROLES AND RESPONSIBILITIES](#)
6. [RISK MANAGEMENT PROCESS](#)
 - 6.1 [Risk Identification](#)
 - 6.2 [Risk Analysis and Assessment](#)
 - 6.3 [Responding to and Managing Risk](#)
 - 6.4 [Risk Monitoring and Reporting](#)
 - 6.5 [Risk Registers](#)
 - 6.6 [Risk Escalation](#)
 - 6.7 [Risk Review – Improving the Framework](#)
7. [RISK MANAGEMENT MATURITY MODEL](#)
8. [RISK APPETITE](#)
9. [PROJECT RISK](#)

10. [COMMUNICATION AND ENGAGEMENT](#)

11. [EQUALITIES](#)

12. [ASSOCIATED DOCUMENTS / REFERENCES](#)

[APPENDIX A – ROLES AND RESPONSIBILITIES](#)

[APPENDIX B – RISK ASSESSMENT GUIDANCE](#)

[APPENDIX C – SMART CHARACTERISTICS](#)

[APPENDIX D – RISK SPOTLIGHT BRIEFING NOTE TEMPLATE](#)

[APPENDIX E1 – IIA RISK MATURITY SCALE ASSESSMENT DEFINITIONS](#)

[APPENDIX E2 – RISK MATURITY ASSESSMENT OF SFRS](#)

[APPENDIX F – DEFINITIONS](#)

1. POLICY STATEMENT

The Scottish Fire and Rescue Service (SFRS) provides a diverse range of critical services to the Communities of Scotland. The provision of these services is undertaken within an ever changing and challenging environment that presents risks that must be effectively managed.

SFRS is committed to the development and implementation of an integrated risk management framework, identifying, managing and monitoring those risks which may impact upon the successful achievement of the key outcomes and objectives of the Service.

The aim of SFRS is to be risk managed, allowing innovation and aspiration, whilst actively managing risk through a range of measures to ensure key outcomes are met. Establishing a consistent and effective framework, integrated within Governance and Assurance arrangements, will strengthen our control framework and help further embed an effective risk culture within the Service.

The Service recognises that it cannot entirely eliminate the risk of disruption and that a residual level of risk will always remain. However, the Risk Management Framework has been developed in order to minimise the probability and impact of a risk causing disruption.

The management of risk is fully embedded throughout the Service, forming an integral element of all Committees and Executive Boards. Engagement with the Board, Strategic Leadership Team (SLT) and Directorates will ensure the framework is effectively used to inform decision making, allowing the Service to present a fair and reasonable reflection of the most significant risks impacting upon its operations.

Maturing the risk framework, allowing the Service to effectively consider and manage emerging risks will further strengthen our governance process. SFRS recognises that risk, as well as presenting a threat, also present opportunities for continuous improvement, developing new and innovative ways of working enhancing the delivery of services to our Communities.

2. RISK MANAGEMENT OBJECTIVES

To assist in the management of organisational risk, the following objectives have been identified and form the basis of our Risk Management Framework. We aim to:

- Promote awareness of business risk and embed the approach to its management throughout the organisation;
- Seek to provide assurance that a system of control is in place to identify, assess, control and report on business risk;
- Align the management of risk to our business objectives and processes.

3. RISK MANAGEMENT CULTURE

We recognise the value of an effective risk management culture. Systems and processes are dependent upon people adhering to and supporting them and the environment within which they operate.

Our approach to risk management will therefore:

- integrate risk management with planning at strategic and operational levels;
- implement and monitor risk management arrangements across the organisation;
- independently review our arrangements for the management of risk;
- devolve responsibility for risk ownership and management as appropriate;
- ensure that designated individuals receive the necessary training, ongoing support and advice about risk management;
- ensure that all colleagues understand our approach to, and their role in, the management of risk;
- review the risk register within Committees and Executive Boards to enhance assurance and scrutiny processes.

4. SCOPE

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.

5. ROLES AND RESPONSIBILITIES

The SFRS Board is responsible for the Risk Management Policy, with the Audit and Risk Assurance Committee (ARAC) supporting the Board and Accountable Officer by providing assurance that appropriate risk management systems are in place and operating effectively.

The Chief Officer, as the Accountable Officer for SFRS, is responsible for maintaining a sound system of internal control, with delegated responsibility to members of the SLT for ensuring that adequate systems for internal control and risk management, both financial and otherwise, are in place and are monitored and reviewed regularly.

Internal Audit will audit the effectiveness of the Service's risk management processes, providing independent assurance on the management of risk and contribute to the continuous improvement of governance, risk management and internal control processes.

[Appendix A](#) provides further information on roles and Responsibilities.

6. RISK MANAGEMENT PROCESS

The SFRS Risk Management Framework provides a structure and process for managing risk, outlining general guidelines on risk management which, if followed, will increase the likelihood of objectives being achieved.

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

Key elements of the risk management process:



6.1 Risk Identification

Risk identification is an ongoing activity, with individual risks and the impact and/or likelihood of risk subject to change. The process of risk identification helps SFRS to identify any threats and/or opportunities to the achievement of outcomes and objectives.

The identification process will be based around the business processes of the Service, considering actions and priorities set through the Strategic Plan or relevant Directorate or Functional Plans.

Risks can be identified from a number of sources including:

- Strategic Planning;
- Monitoring of performance reports;

- HMFSI Reports;
- External Audits;
- Internal Audits;
- De-briefings / lessons learned (non-operational);
- Existing forums (Board, Committees, Executive Boards, Project Boards, management meetings);
- Directorates and individuals as part of their normal management roles and responsibilities.

6.2 Risk Analysis and Assessment

Once identified, risks need to be assessed in terms of their probability of occurrence and their potential impact upon the delivery of outcomes or objectives. It is important to use an agreed and standardised process that measures impact and probability consistently across the organisation.

Probability will be categorised and assessed on a scale of 1 to 5, with 1 being Rare and 5 being Almost Certain. Impact will be assessed on a scale of 1 to 5, with 1 being Negligible and 5 being Very High.

[Appendix B](#) provides further guidance on assessments undertaken.

Probability	Almost Certain (5)	5	10	15	20	25
	Likely (4)	4	8	12	16	20
	Possible (3)	3	6	9	12	15
	Unlikely (2)	2	4	6	8	10
	Rare (1)	1	2	3	4	5
Risk Matrix		Negligible (1)	Low (2)	Medium (3)	High (4)	Very High (5)
		Impact				

6.3 Responding to and Managing Risk

The risk management framework will identify that risk is being managed in an open and transparent manner and consistently applied across the Service.

Actions put in place, following [SMART \(Appendix C\)](#) principles of being Specific, Measurable, Achievable, Relevant and Time Bound, will reduce the probability of the risk occurring or minimise the impact if the risk does occur. In broad terms, any action taken to manage risk to an acceptable level can fall into four categories:

- **Terminate** – in this situation, the risk is terminated by deciding not to proceed with an activity. For example, if a particular project is very high risk and the risk cannot be mitigated, it might be decided to cancel the project. Alternatively, the decision may be made to carry out the activity in a different way;
- **Transfer** – in this scenario, another party bears or shares all or part of the risk. For example, this could include transferring out an area of work or by using insurance;
- **Treat** – this involves identifying mitigating actions or controls to reduce risk. These controls should be monitored on a regular basis to ensure that they remain effective;
- **Tolerate** – in this case, it may not always be necessary (or appropriate) to take action to treat risks, for example, where the cost of treating the risk is considered to outweigh the potential benefits.

6.4 Risk Monitoring and Reporting

The management of risk is an ongoing process that needs to be embedded throughout the organisation. The process must be reviewed regularly to remain effective and it is the responsibility of risk owners to review risks on a regular basis to determine whether any revisions are required.

Monitoring of risk will be undertaken through Committees and Executive Boards of the Service. The provision of assurance through a standardised reporting template will ensure the right information is used to inform decision making and enable effective scrutiny of risk.

Within SFRS the following monitoring and review processes will be undertaken:

- Quarterly reporting of Directorate risk registers to the Strategic Leadership Team;
- Quarterly reporting of the risk register to ARAC and other Committees aligned to their terms of reference, utilising [Risk Spotlights \(Appendix D\)](#) to provide additional assurance;
- Regular reporting on risk to Executive Boards aligned to their terms of reference, utilising Risk Spotlights to provide additional assurance;
- Review of Directorate risk registers by management teams as appropriate;
- Project register will be reviewed in accordance with agreed governance arrangements.

It is essential to good governance that the management of risk is integrated within our Committees, Executive Boards, Management Teams and Projects and used as a management tool to inform our decision-making processes.

6.5 Risk Registers

Risk Registers will be used as a management tool to record and report on business risks impacting upon the organisation. The primary purpose of risk registers is to provoke discussion, encourage scrutiny and agree further actions.

The SFRS Strategic Risk Register (SRR) reflects the strategic risk themes identified by the SLT that individually, or collectively, have the potential to prevent the Service from delivering its key priorities outlined within the Strategic Plan.

The SRR is supported by aligned Directorate registers which identify specific risks associated with the delivery of Directorate objectives. These risks are agreed by the responsible Director and will be managed and reviewed through appropriate management teams. An Example Risk Register can be found within iHub.

Functional and Project risk registers are maintained as appropriate to cover risks identified through core activities or areas of work. These registers will be assessed to determine whether any risk should be escalated to a relevant Directorate register for additional monitoring.

Risks will be reported in a consistent manner using a standard risk template. The register includes key information to ensure assurance and scrutiny processes of the Service are undertaken and includes:

Risk Description	Clearly defined utilising a standardised approach. There is a risk of ... because of ... resulting in ...
Risk Owner	Each Directorate risk is owned by the relevant director with the responsible officer identified at a head of function level for ensuring that the register is fully populated and monitoring systems developed to update the information
Aligned Governance Reporting	To ensure levels of assurance and scrutiny are maintained, a Committee and Executive board will be identified for each risk
Risk Assessment	An initial assessment is made at the time of identification with a current assessment of risk undertaken on a quarterly basis. A Target Assessment, or tolerable level of risk taking, acceptable to achieve a specific objective or manage a specific risk, is also undertaken which the risk should be managed towards
Alignment to Strategic Plan	Each risk is assessed against the SFRS Strategic Plan identifying the relevant outcome and objective.

Control actions required	Details of additional actions required will be identified as appropriate. In some circumstances, existing controls may be assessed as adequate and monitoring of their effectiveness is required.
Performance & % complete	Aligned to assurance and scrutiny processes, responsible officers will report on the RAG status of each risk and progress made against identified controls
Comment by Responsible Officer	To ensure that continued monitoring is undertaken the responsible officer will outline

6.6 Risk Escalation

The movement between registers is based upon the assessment of risk and a judgement on the wider impact upon business objectives. It is the responsibility of individual risk owners to escalate risks that they believe require further consideration and action at a more senior level.

A risk assessed as very high to a project or function does not necessarily mean a very high risk being identified within the relevant Directorate register, although the identification of recurring risk themes across a number of projects or functions would require further evaluation to consider its wider impact.

Where risks are assessed as being appropriately managed and, where in the judgement of the responsible owner, the risk rating now enables the removal of a risk from a Directorate register, it can be removed from that register and managed within a relevant functional register. Equally, where the assessment identifies that the risk is now appropriately managed a judgement can be made as to whether ongoing monitoring is undertaken through business as usual processes.

The removal or escalation of a risk within a Directorate rests with the responsible Director, with the risk register providing justification for the decision taken.

The risk assessment undertaken will result in a risk score being identified and will assist Risk Owners in making a judgement in relation to escalating a risk and additional controls that may require to be identified.

Risk Level	Risk Score	Risk Description
Very High	16 – 25	Unacceptable level of risk with additional measures required to terminate, transfer or treat the risk to a more tolerable level. Risk will be subject to risk spotlights by Committee and Executive Boards.
High	10 – 15	May be tolerable where assurance is provided that controls measures are in place, operating effectively and subject to regular monitoring. Risk will be subject to risk spotlights by Committee and Executive Boards.
Medium	4 – 9	Tolerable level of risk where controls measures in place are subject to monitoring by Directorate. Risks will be subject to risk spotlights where appropriate.
Low	1 – 3	Acceptable level of risk monitored at a functional level and considered for inclusion within directorate risk registers.

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 will enable this standardised and consistent approach throughout the SFRS.

6.7 Risk Review – Improving the Framework

To ensure the risk framework continues to remain fit for purpose, it will be continually reviewed in line with the Fire and Rescue Framework, the Strategic Plan and the Service’s 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.

Regular 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.

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.

7. RISK MANAGEMENT MATURITY MODEL

A key aspect of the risk management framework is the establishment of a [Risk Maturity Model \(Appendix E1\)](#) and associated [independent assessment \(Appendix E2\)](#), undertaken periodically by our Internal Audit provider.

The model and assessment provides evidence of where SFRS sits within a defined risk maturity scale and provides senior management with a snapshot of current risk activity and areas where further improvements are required.

The Internal Audit of Risk Management undertaken within the 2020/21 audit plan assessed SFRS as Risk Defined within the maturity scale. Aligned to the Risk Maturity Model additional work will be undertaken to develop and enhance the risk framework moving towards a Risk Managed level of assessment.

8. RISK APPETITE

The purpose of the Risk Management Framework is to encourage debate and discussion on risk and inform our decision-making processes in a manner that helps the organisation. Risk Appetite is part of this overall framework and can be considered as the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time.

The benefits of adopting a formal approach to risk appetite include:

- Supporting informed decision making;
- Reducing uncertainty;
- Improving consistency across governance processes and decision making;
- Supporting performance improvement;
- Focusing discussion on priority areas;
- Informing resource prioritisation.

For SFRS, risk appetite will be based upon a number of underlying principles:

- It will be aligned to the risk maturity of the Service;
- It will be aligned to our capacity and the resources available;
- It will add value to and be supported by the Risk Management Framework;
- It will be measurable by and meaningful to service users.

Defining Risk Appetite

SFRS will evaluate its risk appetite using the following categories / levels:

Risk Appetite Level	Risk Appetite Description
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

The organisation's appetite for risk will be defined and applied across a range of risk categories and can include:

- Political;
- Operational (Service Delivery);
- Financial (Financial Sustainability);
- Legal / Regulatory (Compliance);
- Reputational / Stakeholder Confidence.

A formal Risk Appetite statement for SFRS will be developed by the SFRS Board and SLT and will be appended to the Framework once complete.

9. PROJECT RISK

The Portfolio Office has been established to facilitate improved governance of projects and to build a strong, simple but effective project management methodology that fits the needs of the Service.

The reporting of risk within Projects will adhere to the Risk Management Framework, utilising the risk register and associated reporting processes to manage and report on risk, providing required levels of assurance for scrutiny purposes.

Escalation of risk within the context of Projects will depend upon the risk identified and the judgement of the Project Manager and Programme Office. Project Managers should highlight any significant project risk that will impact wider service delivery and ensure effective communication and engagement with Directorates and Risk Owners on any relevant risks for inclusion or escalation within specific Directorate registers.

The Change Committee provides scrutiny and challenge of the Change Portfolio agreeing an acceptable risk profile and thresholds for the Change Portfolio.

Amendments to the Portfolio Office Framework will be reflected within the Risk Management Policy as required.

10. COMMUNICATION AND ENGAGEMENT

The Risk Management Framework relies upon awareness and ownership of risk being retained across all levels of the organisation. Risk cannot be managed in isolation to other core business processes if it is to inform decision making.

Awareness and ownership will be managed through existing governance reporting but will be enhanced, for identified staff, through a specific e-learning risk management module provided through the Learning Content Management System (LCMS). Guidance on this module will be provided through the Risk and Audit Section who can be contacted for further information.

Consulting with and talking to Directorates, individuals and other stakeholders, both internally and externally, will ensure that the right inputs are available for risk to be managed effectively.

11. EQUALITIES

The SFRS commitment to mainstreaming Equality and Diversity throughout our work means that it is a consideration in our risk management process. Risk management and effective controls will ensure we are able to manage areas where equality and diversity issues may exist.

Where the risk framework identifies revisions within policy or procedures, that have the potential to impact upon Equalities or our wider governance arrangements, responsible owners will review and update existing assessments as appropriate.

12. ASSOCIATED DOCUMENTS / REFERENCES

Example Risk Register

Fire and Rescue Framework for Scotland 2016

Risk Spotlight Briefing Note Template

Strategic Plan 2019-2022

APPENDIX A – ROLES AND RESPONSIBILITIES

Role	Responsibilities
The SFRS Board	The SFRS Board is responsible for ensuring effective arrangements are in place to provide assurance on risk management, governance and internal control. The Board will approve any amendments to the Risk Management Policy and will set the risk appetite for the Service.
Audit and Risk Assurance Committee (ARAC)	ARAC 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.
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 through identified risk spotlights.
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.
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 and will ensure that adequate systems for internal control and risk management are in place.

<p>Executive Boards</p>	<p>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.</p>
<p>Risk Owner</p>	<p>Each Directorate risk is owned by the relevant director with the responsible officer identified at a head of function level for ensuring that the register is fully populated and monitoring systems developed to update the information.</p>
<p>Internal Audit</p>	<p>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 and help support the risk management process and coordination of risk reporting.</p>

APPENDIX B – RISK ASSESSMENT GUIDANCE

Tables below provide a guide to assist in assessments undertaken:

Probability Criteria		
Probability Rating	Description	Plain English
1 Rare	Very Low – Where an occurrence is improbable or very unlikely	Never happened and doubt it will
2 Unlikely	Low – Where an occurrence is possible but the balance of probability is against	Has happened before but unlikely
3 Possible	Medium – Where it is likely or probable that an incident will occur	Will probably happen at some point in the future
4 Likely	High – Where it is highly probable that an incident will occur	Has happened in recent past and will probably happen again
5 Almost Certain	Very High – Where it is certain that an event will occur	It's already happening and will continue to do so

Impact Criteria					
Impact	Political	Operational	Financial	Legal / Regulatory compliance	Reputational / Stakeholder confidence
1 Negligible	Effective Strategic decision making, full engagement by Board and SLT	No negative impact upon ability to deliver services	No impact on our ability to deliver a balanced budget	No impact on our ability to achieve compliance with relevant legislation	No adverse reputational damage to the Service
2 Low	Minor reduction in Board engagement, minimal impact upon achievement of strategic objectives	Minimal impact on ability to deliver service	Ability to achieve a balanced budget with minimal adjustments	Acts or omissions resulting in minor legal or regulatory breach causing minimal loss	Some negative local press or public interest/concern

<p>3 Medium</p>	<p>Questions raised over effectiveness of strategic decision making, noticeable impact upon service provision, criticism by external bodies</p>	<p>Reduction in ability to deliver services and minor disruption to services</p>	<p>Action required to ensure delivery of balanced budget and potential impact upon service delivery options</p>	<p>As above causing moderate loss</p>	<p>Limited damage to reputation, extended negative local press, Regional press coverage</p>
<p>4 High</p>	<p>Ineffective Board engagement, challenge over strategic decision making, failure to deliver against agreed outcomes and objectives</p>	<p>Service disruption for extended periods</p>	<p>Insufficient finance available to support service provision</p>	<p>As above causing major loss</p>	<p>Loss of credibility and confidence in the Service, national negative press coverage, significant public concern</p>
<p>5 Very High</p>	<p>Failure to deliver against Fire Framework, Failure of Board and SLT to engage and intervention by Scottish governance and scrutiny bodies</p>	<p>Failure to deliver service</p>	<p>Failure to demonstrate effective use of public funds</p>	<p>As above causing catastrophic loss resulting in legal or regulatory supervision</p>	<p>Public enquiries into actions of Service, prolonged negative national press coverage</p>

APPENDIX C – SMART CHARACTERISTICS

Characteristic of SMART Actions
<ul style="list-style-type: none">• SPECIFIC: the performance measure indicates exactly what result is expected so that performance can be judged accurately
<ul style="list-style-type: none">• MEASURABLE: data are available or can be collected relatively easily
<ul style="list-style-type: none">• ACHIEVABLE: they are realistic, not based on aspirations
<ul style="list-style-type: none">• RELEVANT: they matter to the intended audience and clearly relate to the service being measured
<ul style="list-style-type: none">• TIMELY and have information available frequently enough to have value in making decisions

APPENDIX D – RISK SPOTLIGHT BRIEFING NOTE TEMPLATE



Agenda
Item:

Meeting – Date

Title

Risk:

Submitted by:

Background: What would cause the risk to materialise / what is the effect likely to be?

-

Controls and mitigating actions (stating what actions are being taken if the residual/current risk assessment is operating above or below risk appetite).

-

External or other factors which might impact on the current risk assessment.

-

APPENDIX E1 – IIA RISK MATURITY SCALE ASSESSMENT DEFINITIONS

Risk Maturity	Definition
Risk Naïve	Risks must be identified through discussion with Senior Managers / Board Members and existing knowledge of the Client/external environment. An annual audit of the risk management framework or provision of consultancy is recommended.
Risk Aware	Risk should be confirmed through discussion with Senior Managers / Board Members and supported by existing knowledge of the Client/external environment. An annual audit of the risk management framework or provision of consultancy is desirable.
Risk Defined	Risks can be relied on; however, due to possible inconsistencies across the organisation, supporting conversations with Senior Managers, particularly for those business areas without any identified risks, is advised. An annual audit of the risk management framework is desirable; however, due to the time to embed cultural changes, a review every two years may be more appropriate.
Risk Managed	The risk register and risk framework can be relied on; however, for those business areas where management are not providing assurance over the risks / risk framework a short discussion with the relevant Senior Manager may be helpful. A review of the risk management framework every 3-5 years would be appropriate.
Risk Enabled	The risk register and risk framework can be relied on. As the risk management framework assurance is being provided directly by management, an audit of this area should be considered on a cyclical basis in line with the audit prioritisation process.

APPENDIX E2 – RISK MATURITY ASSESSMENT OF SFRS

SFRS Internal Audit Providers, AZETS, used the Chartered Institute of Internal Auditors (IIA) Risk Maturity Scale to assess the risk maturity of the Scottish Fire and Rescue Service (SFRS).

	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk Enabled
Key Characteristics	No formal approach developed for risk management	Scattered silo-based approach to risk management	Strategy and policies in place and communicated and risk appetite defined	Enterprise approach to risk management developed and communicated	Risk management and internal controls fully embedded into the operations
Process					
The organisation's objectives are defined	Possibly	Yes - but may be no consistent approach	Yes	Yes	Yes
Management have been trained to understand what risks are and their responsibility for them	No	Some limited training	Yes – responsible officers are trained in corporate processes. No wider training in core fundamentals of risk management.	Yes	Yes

	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk Enabled
A scoring system for assessing risks has been defined	No	Unlikely, with no consistent approach defined	Yes	Yes	Yes
The risk appetite for the organisation has been defined in terms of the scoring system	No	No <i>*currently being developed</i>	Yes	Yes	Yes
Processes have been defined to determine risks, and these have been followed	No	Unlikely	Yes, but may not apply to the whole organisation	Yes	Yes
All risks have been collected into one list. Risks have been allocated to specific job titles	No	Some incomplete lists may exist	Yes, but may not apply to the whole organisation	Yes	Yes
All risks have been assessed in accordance with the defined scoring system	No	Some incomplete lists may exist	Yes, but may not apply to the whole organisation	Yes	Yes
Responses to the risks have been selected and implemented	No	Some responses identified	Yes, but may not apply to the whole organisation	Yes	Yes
Management have set up methods to monitor the proper operation of key processes, responses and action plans ('monitoring controls')	No	Some monitoring controls	Yes, but may not apply to the whole organisation	Yes	Yes

	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk Enabled
Risks are regularly reviewed by the organisation	No	Some risks were reviewed, but infrequently	Regularly reviewed, probably annually	Regularly reviewed, probably quarterly	Regular reviews, probably quarterly
Management report risks to directors where responses have not managed the risks to a level acceptable to the board	No	No	Yes	Yes	Yes
All significant new projects are routinely assessed for risk	No	No	Most projects	All projects	All projects
Responsibility for the determination, assessment, and management of risks is included in job descriptions	No	No	Limited	Most job descriptions	Yes
Management provide assurance on the effectiveness of their risk management	No	No	No	Some managers	Yes
Managers are assessed on their risk management performance	No	No	No	Some managers	Yes

APPENDIX F – DEFINITIONS

Definitions	
Strategic Plan	The Strategic Plan has been developed in response to the Fire and Rescue Framework for Scotland 2016 and sets out the Services outcomes, values and priorities.
Risk	A risk for SFRS is defined as something with the potential to impact upon the achievement of key service priorities.
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.
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).
Risk Tolerance	A Target Assessment, or tolerable level of risk taking, acceptable to achieve a specific objective or manage a specific risk.
Risk Register	The risk register is the means by which the Service captures risks and demonstrates that they are being managed appropriately. The risk register will enable effective assurance and scrutiny processes.
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.
Risk Owner	Within the risk register template each risk will be owned by a risk owner. 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.