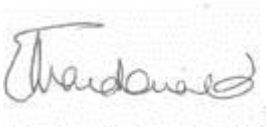
FOOD STANDARDS SCOTLAND

RISK MANAGEMENT POLICY

Date of Issue:		July 2016
Revision Date:		September 2017
Version Number:		3
Document Location:		A15185820
Number of Pages:		18
AUTHOR	**Name:**	GARRY MOURNIAN
	Position/Role:	HEAD OF CORPORATE SERVICES
	Signature:	
APPROVER	**Name:**	ELSPETH MACDONALD
	Position/Role:	DEPUTY CHIEF EXECUTIVE
	Signature:	

VERSION HISTORY

Version no.	Description of Changes
1	Creation of FSS risk management policy and guidance.
2	Updated with revised Saltire links to SG risk guidance and principles.
3	Minor updates to narrative.

TABLE OF CONTENTS

1.0 INTRODUCTION

The aim of this policy is to detail how and why Food Standards Scotland carries out risk management, to lay out the roles and responsibilities across the organisation and to establish the process and techniques FSS utilise to support risk management.

2.0 CORPORATE STATEMENT ON RISK

FSS's primary concern is consumer protection through making sure food is safe to eat, ensuring consumers know what they are eating and improving nutrition. With that in mind, our vision is to deliver a food and drink environment in Scotland that benefits, protects and is trusted by consumers. By undertaking effective risk management we will better manage the successful delivery of our objectives by:

- Reducing the possibility our objectives are jeopardised by unforeseen events by constraining threats to an acceptable level;
- Increasing confidence in achieving our desired outcomes
- Recognising and taking informed decisions to manage and exploit opportunities that may offer an improved way of achieving objectives;
- Providing reasonable assurance to the FSS Board that we are managing risks as part of our internal controls.

Within FSS we shall operate three tiers of risk register in order to manage our risks accordingly:

- **Level 1** – the strategic risk register which outlines strategic risks to the organisation. This will be jointly owned by the Senior Management Team (Executive) and the Board (non-executive). The Senior Management team will be responsible for managing risks identified on the Strategic Risk Register on behalf of the organisation.
- **Level 2** – Senior Management Team Risk Register – covers the tactical and operational risks faced at a Senior Management Team level that will impact the delivery of the Corporate Plan.
- **Level 3** – Directorate risk registers covering the tactical and operational risks faced at a Branch and Project level. The management of these risk registers is delegated to the relevant FSS Directors.

In addition to the three tiers of risk register, programme risk registers may also be developed, and should be established to monitor risks to the delivery of specific key programmes or projects that seek to deliver the strategic outcomes and corporate plan objectives of FSS.

3.0 RISK APPETITE IN FSS

Our risk appetite reflects our overall Strategy, Corporate Plan and stakeholder expectations and as part of FSS governance the Board has considered its risk appetite with regards to the successful delivery of the FSS strategy.

With regards to public health the Board has generally a low appetite for risk. This is because consumer protection and public health are at the core of what we do. Ensuring food is safe is our primary, non-negotiable, function and forms the basis of the trust consumers have in FSS. On public finance the Board has a low tolerance and would expect the accounting officer to apply the principles of sound financial management, managing within budget.

Clearly any organisation needs to think about its reputation and how an organisation is perceived is important. Perceptions will vary between different stakeholders but the trust of consumers is paramount. In this regard the Board's appetite for risk is medium tolerance. Obviously, it is important that we work collaboratively and effectively but it is possible given the breadth of our remit that there are opportunities for disagreement. As our organisation is non-ministerial, it is important that we retain and use that independence from Government wisely taking account of, but not being wholly influenced by the views of others.

Given the current landscape and the challenges the organisation faces, the Board has a high tolerance for innovation and for taking well managed and thought-through risks in areas such as piloting of new ideas, delivery models etc.

4.0 FSS RISK FRAMEWORK

FSS have adopted the principles of the Scottish Government risk framework. The methodology is straightforward and aims to assist the organisation manage risk effectively, following 5 distinct phases.

- **Clarifying Objectives:** This may be established through Directorate, Branch or Programme/Project planning. There should be a direct link between what

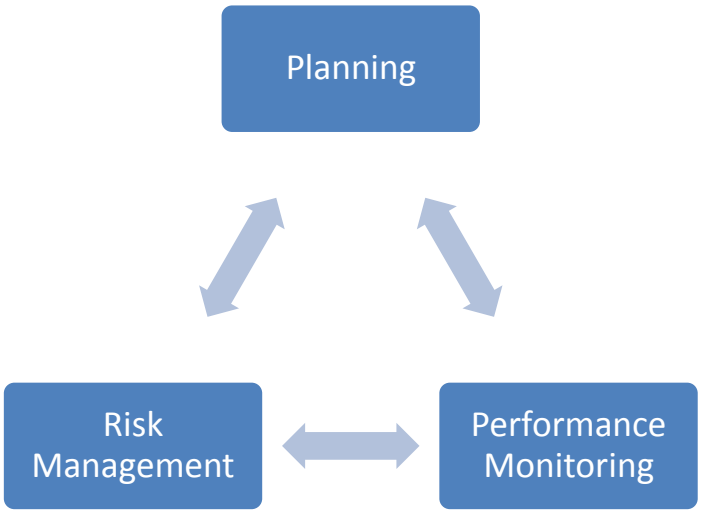
you want to achieve and the risks you are managing to make the risk environment meaningful.

- **Identifying Risks** – In order to manage risks, you need to know what risks are faced and to undertake an evaluation – this is the first step in building a risk profile – an overview of the short, medium and long term risks that may affect the achievement of objectives.
- **Assessing Risks:** This enables the effective prioritisation of risks in relation to objectives and ensures attention is focussed on the key risks and resources are concentrated where they are most required.
- **Addressing Risks:** This is the stage where actions are agreed in order to control or mitigate the risks that have been identified.
- **Reviewing and Reporting Risks:** This ensures that new opportunities and threats or changes to existing risks are managed. Reporting changes helps to raise awareness and coordinate responses to key risks.

5.0 CLARIFYING OBJECTIVES

The first phase of the risk management framework is to understand the objectives that you are trying to achieve. This could be at an FSS, Directorate, Branch, Programme or Project level.

This will then be the focus of any risk management information – a risk is anything that can impede or enhance your ability to meet current or future objectives. Through this process, FSS are aiming to improve our performance through better informed decision making and planning. Risk identification needs to be undertaken with a clear strategy and clarity of purpose and is an important part of managing priorities effectively.



The aim here is to ensure a direct link between risk management and the aims and objectives – whether it be organisational or at an individual project level. It allows focus to be achieved on relevant risks that may present an opportunity or threat to the states goals or deliverables.

At an organisational level, this should be consistent with the FSS business planning process:

- **Delivery Objectives** ("What") – contribution to the FSS statutory responsibilities and Strategy
- **Business Objectives** ("How") – proposals within the FSS Corporate Plan that will deliver the business Strategy
- **Risk Management** ("What If") – the approach to managing risk within FSS as outlined in this policy guidance.

6.0 RISK IDENTIFICATION

In order to manage risk, FSS needs to know what risks it faces, and to evaluate them. Identifying risks is the first step in building the FSS risk profile. There is no single right way to record the FSS risk profile, but maintaining a record is critical to effective risk management. The identification of risk can be separated into two distinct phases:

- **Initial risk identification** – perhaps a new project or activity undertaken by FSS
- **Continuous risk identification** – new risks which previously did not arise or changes in existing risks.

In either case risks should always be related to the delivery of objectives. Risks can only be assessed and prioritised in relation to objectives (and can be done at any level – personal to organisational). Care should be taken to avoid confusion between the impacts that may arise and the risks themselves, and to avoid stating risks that do not impact on objectives; equally care should be taken to avoid defining risks as simply the converse of the objectives. A statement on risk should encompass both the possible cause and the impact to the objective which might arise.

In FSS, risks should be described using the following formula where possible:

EVENT – *there is a risk that*

CAUSE – *as a result of*

EFFECT – *which may result in*

Strategic risks will be identified by the Senior Management Team/FSS Board or will be adopted following escalation from Directorate or Programme/Project risk registers.

It is useful to have a systematic process in place to help identify risk and give assurances that a complete risk profile is articulated. Within FSS, two simple techniques are recommended that provide a wide scan of areas that may affective objectives.

PESTLES

Category	Examples
Political	Changes in SG policy, Stakeholder relationships, Ministerial changes, wider political changes – EU referendum and UK position.
Economic	Budget constraints, effect on economy on food and consumer behaviours, sustainability.
Social	Demographic influence on FSS policy, Trust of consumers, Staff implications, Changes in consumer engagement methods.
Technological	Cost and efficiency of IT solutions, Change in technology and obsolescence, Technical competence of organisation,
Legal	EU requirements, Procurement processes around Official Controls and other key contracts, Accounting rules, legal challenge on FSS policies/proposals.
Environmental	Changing environmental standards, Changes to consumer shopping habits, Staff changes and loss of expertise, change in official control delivery methods.
Security	Physical assets, Information Security and data protection.

SWOT

SWOT analysis allows can also be applied to risk identification and specific pieces of work, focussing on:

Strengths: internal attributes that are helpful to achieving an objective.

Weaknesses: internal attributes that are harmful to achieving an objective.

Opportunities: external conditions that are helpful to achieving an objective.

Threats: external conditions that are harmful to achieving an objective.

Examples:

STRENGTHS	Staff experience, Management support
WEAKNESSES	Communications channels, timescales
OPPORTUNITIES	Stakeholder relationships, IT developments
THREATS	Geographic spread, Current culture

7.0 RISK ASSESSMENT

It is important to clearly establish a structured process in which both likelihood and impact are considered for each risk and that the assessment of risk is recorded in a way that facilitates monitoring and prioritisation. As risk in FSS is assessed on the combination of the consequences of an event (impact) and the probability (likelihood), the table below provides a guide to risk levels and how they should be recorded in the FSS Risk Register template.

Impact – The estimated effect of the risk on the objective or strategic outcome in question. This is focussed on scale, scope and resource implications, as well as the risk appetite of FSS.

Impact	Criteria
Very High – 5	Destructive and unacceptable impact on corporate plan objectives or strategic outcomes that would result in a major change to overall approach. Potentially large resource consequences (>£100K) that outweigh current operational circumstances.
High – 4	Significant and unacceptable impact on corporate plan objectives or strategic outcomes that would require a material change to critical approach/procedure/process. Resource implications would be challenging to absorb (£50-100K) within current operational circumstances.
Medium – 3	Moderate impact on corporate plan objectives or strategic outcomes that may require multiple changes in approach/procedure/process. Acceptable level of resource consequences (£10-50K).
Low – 2	Minor impact on corporate plan objectives or strategic outcomes, requires little overall change in approach. Few resource consequences (£1-10K).
Negligible – 1	No real impact on achieving corporate plan objectives or strategic outcomes. Financial impact <£1K.

Likelihood – This is the estimated chance of the risk occurring and is focussed on probability.

Likelihood	Criteria
Very High – 5	>75% chance of occurring – almost certain to occur.
High – 4	51-75% chance of occurring – more likely to occur than not.
Medium – 3	26-50% chance of occurring – fairly likely to occur.
Low – 2	6-25% chance of occurring – unlikely to occur.
Negligible – 1	1-5% chance of occurring – extremely unlikely to occur.

Most risks are time based and are not constant and estimating the timing of when a risk may occur is sometimes called 'proximity'. Considering this should inform a judgement on the impact or likelihood of a risk and the timing of any response.

The tables below provide a guide, in line with the SG risk management methodology, to the overall risk level based on multiplying the assessment of the impact and likelihood of a risk. This then informs the risk scores recorded on the FSS risk register template.

Assessing the impact and likelihood of a risk (5x5 matrix):

Impact	**Multiplier**					
Very High	5	5	10	15	20	25
High	4	4	8	12	16	20
Medium	3	3	6	9	12	15
Low	2	2	4	6	8	10
Negligible	1	1	2	3	4	5
	Multiplier	1	2	3	4	5
Likelihood		Rare	Low	Medium	High	Very High

Assessing the overall risk level:

RISK LEVEL	SCORE	RISK LEVEL DESCRIPTION
VERY HIGH	20-25	**Rating**: Unacceptable level of risk exposure that requires immediate mitigating action. **Reporting**: report the risk to SENIOR MANAGEMENT TEAM/Audit Committee/BOARD.
HIGH	10-16	**Rating**: Unacceptable level of risk which requires controls to be put in place to reduce exposure. **Reporting**: A decision should be taken as to whether risks recorded as high should be escalated. Scores between 10 and 14 would not usually be escalated where scores are 15 and 16 should be given careful consideration.
MEDIUM	4-9	**Rating** – Acceptable level of risk exposure subject to regular active monitoring. **Reporting**: At Directorate level.
LOW	1-3	**Rating**: Acceptable level of risk subject to regular passive monitoring. **Reporting**: At Directorate level. Consideration should be given as to whether risks recorded as low are still extant.

As outlined above, once risks have been assessed, the risk priorities for FSS will emerge. The less acceptable the exposure in respect or a risk, the higher the priority which should be given to addressing it. The highest priority risks (e.g. key risks) should be given regular attention at the highest level of the organisation.

8.0 ADDRESSING RISK

Once risks have been identified and assessed, the next stage is to decide what action needs to be taken to address the highlighted risks. The purpose of addressing risks is to turn uncertainty to FSS's benefit by constraining threats and taking advantage of opportunities. There are 5 key aspects of addressing risk, depending on the kind of challenge they present according how likely they are to occur, and the impact if they did occur.

- **Tolerate**: for unavoidable risks – the exposure may be tolerable without any further action being taken – or so remote as to take mitigating action may be disproportionate to the potential benefit gained.

- **Treat**: for risks that can be reduced or eliminated by prevention or other control action (new systems, revision of processes etc.). By far the greatest number of risks will be treated in this way.
- **Transfer**: where another party can take on some or all of the risk more economically or more effectively (e.g. sharing risk with a contractor). Some risks are not fully transferable – in particular it is generally not possible to transfer reputational risk even through the delivery of a service is contracted out.
- **Terminate**: for risks no longer deemed tolerable and where exit is possible (e.g. elements of first class travel arrangements). This option is severely limited in government but can be particularly important in project management if it becomes clear that the projected cost/benefit is in jeopardy.
- **Take the Opportunity**: This option should be considered whenever tolerating, treating or transferring a risk and focusses on managed risk taking. This is a considering of how much one is prepared to actively put at risk in order to obtain the benefits of the opportunity. It is about comparing the value (financial or otherwise) of potential benefits with the loses which might be incurred. Judgement should be taken on the level of exposure which is considered tolerable should it be realised.

When considering the option of 'treat' in addressing risk – the following approach should be undertaken when designing control mechanisms to mitigate the risk:

- **Preventative Controls**: designed to limit the possibility of an undesirable outcome being realised. The more important an undesirable outcome should not arise, the more important it becomes to implement appropriate preventative controls. For example – separation of duty or limitation of action to authorised persons.
- **Corrective Controls**: designed to correct undesirable outcomes which have been realised. They provide a route to achieve some recovery against loss or damage. For example – design of contract terms to recover an overpayment or contingency planning as this allows an organisation to plan for business continuity or recovery after events which they could not control.
- **Directive Controls**: designed to ensure that a particular outcome is achieved. They are particularly important when it is critical an undesirable event is

avoided. For example – a requirement for protective clothing to be worn during the performance of dangerous duties, or that staff be trained with required skills before being allowed to work unsupervised.

- **Detective Controls**: designed to identify occasions of undesirable outcomes having been realised. Their effect is, by definition, after the event so they are only appropriate when it is possible to accept the loss or damage. For example – stock or asset checks which detect removal without permission, post implementation reviews which detect lessons learnt and monitoring activities which detect changes that should be responded to.

In designing controls, it is important that the control put in place is proportional to the risk. Apart from the most extreme undesirable outcome (such as loss of human life) it is normally sufficient to design controls to give a reasonable assurance of confining likely loss within the risk appetite of FSS. Generally speaking the purpose of control is to constrain risk rather than to eliminate it.

9.0 REVIEWING AND REPORTING RISKS

The management of risk should be reviewed regularly to monitor whether or not the risk profile of FSS is changing, to gain assurance that risk management is effective, and to identify when further action is necessary.

Within FSS, the following will be undertaken as a minimum:

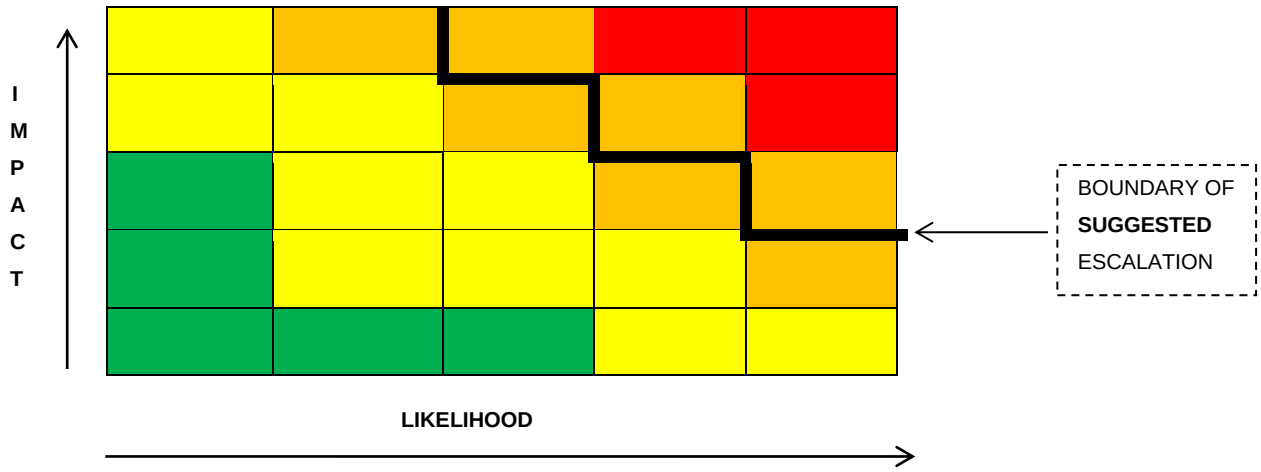
- Level 1, 2 and 3 risk registers will be reviewed on a monthly basis at Senior Management Team meetings and Director led meetings as required. All risks rated High or Very High will be reviewed in detail and action taken to mitigate risks further, as required. Cross Directorate challenge is welcomed at level 3 should it be appropriate.
- The Strategic risk register will also be reviewed by the Board annually or by exception, through escalation by SMT and the Audit and Risk Committee, as required.
- The Strategic risk register will be reviewed quarterly by the FSS Audit and Risk Committee. This will form the basis of a report that will comprise of a summary of all risks rated Very High and a copy of the latest version of the Strategic risk register. Any Red risks on the Level 2 SMT risk register shall also be reported to the Committee.

- Programme risk registers will be reviewed in accordance with the individual reporting arrangements agreed by the relevant Programme Board.

10.0 RISK ESCALATION

When a risk reaches a level whereby the manager can implement no further controls or solutions, the risk must be escalated. The escalation can occur within the risk register either by the project manager, Branch Head, Director or member of the Senior Management Team.

The boundary for suggested escalation within FSS it outlined below, however if the risk owner/Director deems the risk to be of corporate significance, or beyond their delegated tolerance, they can escalate a risk to the Senior Management Team if they are deemed critical of effect FSS as a whole. They will then be considered as corporate risks and will be under SMT management and control.



The FSS policy for risk escalation is that all risks rated VERY HIGH or RED should be escalated to the next level in the risk management chain. Risks that are not rated VERY HIGH or RED should be considered for escalation as above. The FSS risk escalation hierarchy is outlined below and is designed to provide effective support and challenge in managing FSS risks.

11.0 ROLES AND RESPONSIBILITIES

Role	Responsibility
FSS Board	Overall responsibility for the FSS system of internal control and ensuring that an effective risk management system is in place.
Audit and Risk Committee	Advise and provide assurance to the Board on FSS's arrangements for risk management, through constructive challenge and review.
Accountable Officer	Responsible for ensuring and implementing effective risk management processes within FSS and programmes of activity. To ensure there is comprehensive risk reporting arrangements for their area of accountability.
Senior Management Team	Review Level 1 Risks and individual escalated risks. Take appropriate action to mitigate risks. Review Level 1 Risks and new high level risks monthly and advise as to whether contingency plan is required.
Directors	Manage high level risks within their Directorate (Level 2 Risk Register) that are beyond tolerance of Branch Heads. Escalate corporate and Very High rated risks (beyond their own tolerance) to the Senior Management Team (Level 1 Risk Register).
Senior Responsible Owners	Monitor risks to the delivery of programme or project objectives Review and manage high level programme/project risks and escalate to Senior Management Team (Level 1 Risk Register) as necessary.
Head of Corporate Services	Develop, operate, monitor and report on FSS Risk Management System Embed risk aware culture within FSS through appropriate learning and development activities Provide guidance and support to Branch, Project, Programme, Directorate and Senior Management on risk management methodology within FSS.
Branch Heads	Identify, evaluate and manage risks to the delivery of Branch or Corporate Plan objectives.
Project Managers	Identify, evaluate and manage risks to the delivery of individual projects. Escalate risks to Branch Head as necessary.
All Staff	Take ownership of individual Branch and Project risks where appropriate. Be responsible for managing risks as an integral part of the Branch

12.0 REVIEW OF RISK MANAGEMENT POLICY

To ensure it remains fit for purpose, this policy and associated documents will be reviewed, as a minimum, on an annual basis.

13.0 FURTHER GUIDANCE

Further guidance on the FSS risk management policy can be sought from the Head of Corporate Services on 01224 28147 or garry.mournian@fss.scot. Additional information and supporting documentation on risk management within Government can be found:

HM Treasury Orange Book - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

Scottish Government Risk Management –

http://saltire/my-workplace/finance/Pages/Risk-management.aspx

Scottish Public Finance Manual –

http://www.gov.scot/topics/government/finance/spfm/risk