Agri-Food and Biosciences Institute ®

RISK MANAGEMENT STRATEGY

STRATEGY STATEMENT OF THE AGRI-FOOD AND BIOSCIENCES INSTITUTE (AFBI)

www.afbini.gov.uk

AGRI-FOOD AND BIOSCIENCES INSTITUTE

RISK MANAGEMENT

STRATEGY &

OPERATIONAL PROCEDURES

Version Control

Version Number	Date of Issue	Reason	Issued by
1.0	05/11/15	To replace previous AFBI RM Strategy with revised Strategy incorporating Operational Procedures	Head of Governance and Performance
1.1	02/02/17	Annual Review of RM Strategy and Risk Appetite	Head of Governance and Performance
1.2	10/04/18	Annual Review of RM Strategy and Risk Appetite	Head of Governance and Performance
1.3	14/03/19	To include procedures for project level risk management	Head of Governance and Performance

CONTENTS

1. Introduction To Risk Management 4
2. Purpose 4
3. AFBI Risk Management Process & Procedures 5
4. Roles and Responsibilities 12
5. AFBI Risk Appetite 14
6. Accountability 17
7. AFBI Compliance with Relevant Guidance 17
8. Annual Review 18

Appendices

Appendix 1: AFBI's Risk Appetite

Appendix 2: Risk Identification - Categories of Risk to Consider

Appendix 3: Template Risk Register and Guidance

Appendix 4: Branch Business Planning & Performance Management Guidance (Branch Level)

Appendix 5: AFBI Risk Assurance Framework

1 INTRODUCTION TO RISK MANAGEMENT

1.1 Good governance leads to good management, good performance, good stewardship of public money, good public engagement and, ultimately, good outcomes for the public and service users. Good governance enables AFBI to pursue its vision effectively and underpins that vision with mechanisms for control and management of risk.

1.2 An essential aspect of good governance is the way AFBI manages the risks it faces.

1.3 Risk management is an essential business tool that encourages innovation and enterprise rather than risk aversion.

> **Risk Management is defined as: "the process of identifying risks, evaluating their potential consequences and determining the most effective methods of controlling them and or responding to them".**

1.4 When risks are managed effectively, objectives are more likely to be achieved. Conversely, when risk management fails the consequences can be significant and high profile and can threaten the achievement of both the business and corporate objectives and ultimately have an impact on the level of service delivery for our customers.

2 PURPOSE OF THIS DOCUMENT

2.1 This risk management strategy and procedures describes the processes that AFBI has put in place to manage risks and provides guidance to ensure that a consistent approach is applied across the organisation and which facilitates compliance with the current governance requirements.

2.2 The strategy highlights its consistency with HM Treasury's Audit and Risk Assurance Committee Handbook March 2016.

2.3 The strategy defines the key roles and responsibilities in managing risk within AFBI and the working processes that are to be used.

2.4 This document also sets out AFBI's approach to defining risk appetite and describes how risk appetite is to be used in the management of risk.

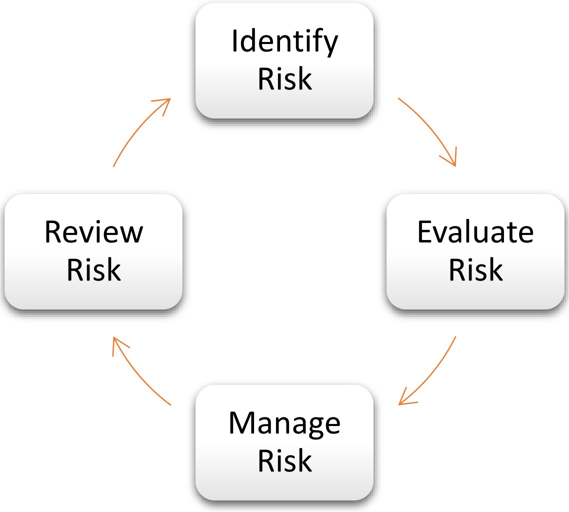
2.5 Section 3 sets out the procedures for the treatment of risk at a Corporate, Division and Branch (operational) level through 4 key steps:

1. Risk Identification
2. Risk Evaluation
3. Risk Management
4. Monitoring & Review

3.0 AFBI's RISK MANAGEMENT PROCESS & PROCEDURES

3.1 The diagram below illustrates the four key steps of the risk management process within AFBI. Each stage of the process is discussed below and equally applicable at the Corporate, Divisional, Branch or Project Level.

Diagram 1: Risk Management Process - 4 Key Steps



STEP 1 - Initial Risk Identification and Scoring of Risks

3.2 Risk management within AFBI starts with the initial identification of risks to the organisation, particularly in relation to the achievement of AFBI's Strategic Outcomes and Business Plan targets.

3.3 This should be carried out as part of the Business planning process **at all levels** of AFBI i.e. when Corporate, Divisional and Branch Objectives are being set, the risks to achieving these should be identified. (See AFBI's Divisional and Branch Business Planning & Performance Management Guidance Appendix 4)

3.4 The Head of Governance & Performance can provide further guidance to staff on how to they can identify risks through meetings, group discussions or facilitated workshops.

3.5 In considering risks, external factors, operational risks and change risks should be considered. **Appendix 2** of this document sets out more detail on the type of risks that should be considered and is adapted from the NIAO publication "Good Practice in Risk Management".

3.6 Once risks have been identified, an appropriate named individual will be nominated as the **risk owner**. The risk owner will take responsibility for monitoring and reporting on the risk as well as taking responsibility for assessing the effectiveness of existing controls and progress toward the implementation of new controls.

3.7 Risks identified at a Corporate and Divisional level should be recorded in an AFBI standard format Risk Register. An example extract is provided at

Appendix 3, which also provides an explanation as to the key details which need to be recorded within the register.

Branch/Operational level

3.8 At a Branch level, operational risks will be identified and recorded as part of the Business planning process as set out in AFBI's Divisional and Branch Business Planning & Performance Management Guidance. **(See Appendix 4)**

Project Level – Project Governance and Risk

3.9 AFBI undertakes a wide range of non DAERA funded activities, mainly with regard to research contracts but increasingly so projects also represent new initiatives which support research. The level of funding and contractual obligations can vary greatly across this portfolio of work.

3.10 While the AFBI Board has ultimate governance responsibility of AFBI, it is the responsibility of all AFBI staff undertaking contractual arrangements which AFBI are bound to, to adopt and deliver an appropriate and proportionate level of governance on all associated activities. As such governance oversight could be adopted at either board, executive/ divisional or branch level, depending on the scale, complexity and novelty of the project.

Governance at Board level:

3.11 The AFBI Board established a Sub Committee to be known as the Oversight & Governance Committee (O&GC). The objective of the Sub Committee, as set out in the Terms of Reference, is to provide a high level oversight for significant, novel or complex projects in terms of governance, expenditure, claims, risk and contract management. It should be noted that EMT retains accountability for the operational management, reporting, accounting and monitoring of Projects.

Determining Projects subject to O&GC oversight – Risk Assessment

3.12 Normal AFBI business involves the completion of a wide range of projects for public and private sector customers. In the majority of cases as these represent 'business as usual' they would not require the additional oversight afforded by the O&GC. However, to ensure consistency it is important that AFBI establishes a mechanism by which projects will be directed through the O&GC.

3.13 AFBI has an existing governance structure in place to ensure that projects are assessed and approved before work can commence. A key stage in this process is the approval stage which will involve the submission of a PAF and subsequently an FCP within the non AWP system. It is proposed that at this stage a risk assessment will be carried out.

3.14 A number of criteria will be used to assess the level of risk associated with a project and whether it needs to be subject to the additional scrutiny by O&GC.

The key criteria to assess the overall level of risk involved will include:

- Value of the Project to AFBI (Whole Life Value) >£1million;
- Any projects which require Department of Finance (DoF) approvals;
- If the project is not ‘normal course of business’
- Is AFBI the lead partner in a consortium (increased reputational risk for non-delivery);
- Is it a significant or strategic partnership / alliance?

3.15 If the project meets any of the criteria outlined above and EMT deem appropriate, an EMT lead governance structure, commensurate to the nature of the activity, will be put in place and reports on these projects will be provided to EMT and then on to the O&GC. Below this level AFBI will ensure that appropriate EMT led project Boards or Head of Branch led project governance and oversight arrangements are in place.

3.16 However, in some instances AFBI may be involved in work/projects which do not fit within the non-AWP process. In such cases staff should seek immediate advice from EMT and the governance team as to how effective oversight will be delivered.

Head of Branch governance

3.17 Where AFBI’s role has the potential to have a major impact or represents major funding to AFBI (Whole life value £100-999K projects) the Head of Branch should specifically ensure such projects are being managed by Project Leaders (PL’s) appropriately.

3.18 Branch heads are expected to review all projects within their branch quarterly to ensure appropriate delivery. Any issues should be flagged through quarterly assurance statements to HoD’s and major issues should be flagged when the HoB becomes aware.

The finance of all projects should be reviewed monthly through the Star Chamber exercises.

Project Leader responsibility

3.19 It is the project leader’s (PL) responsibility to deliver the project as per agreed proposals and contractual arrangements. This will involve both science and financial aspects and it is the PL’s responsibility to monitor and manage budgets, supported by and making requests to finance as required. The PL also should make the HoB aware as soon as possible if problems occur with project delivery. It is also their responsibility to review the contractual arrangements and discuss these with AFBI legal to ensure appropriate delivery.

Use of ‘RAID’ Analysis to identify assess and manage risks in projects

3.20 At a project level AFBI has adopted project governance arrangements based on best practice guidance including the use of a standardised ‘RAID’ template for Project Management.

3.21 RAID analysis is a project planning technique for identifying key project Risks (R), Assumptions (A), Issues (I), and Dependencies (D). Project teams should complete an initial analysis at the beginning of the project and then monitor the issues via a RAID Log. (Appendix x)

3.22 RAID analysis focuses on four key areas:

- Risks – events that can have an adverse impact if they occur.
- Assumptions – things you assume are in place which contribute to the success of the project.
- Issues – current matters that need to be considered and addressed by the group.
- Dependencies – other projects or triggers that your project depends on, or are a beneficiary of your project outcomes.

Why do a RAID analysis?

3.23 A RAID analysis is a best practice for effective project management and is one of the easiest and most practical tools to apply. It is used to:

- Perform a broad environmental scan during the initial planning phase
- Inform regular reviews and keep the project organized and on track
- Involve the whole team in identifying critical issues that may affect the project
- Collate all the relevant matters affecting the project in one place
- Proactively assess changing project conditions
- Focus project efforts and resources
- Assure stakeholders that the project is under control
- Engage with management when you need their input or support

3.24 This will ensure consistency in terms of how a project is assessed and will aid the Executive in determining if a project needs to be brought to the attention of the Committee.

STEP 2 – Evaluating the Risk

3.25 The Risk Owner is responsible for evaluating each risk and assigning a score in terms of both Likelihood and Impact:

Likelihood: The chance of the risk materialising after considering the control measures in place

Impact: The effect of the risk should it materialise. Areas of impact include AFBI assets (including staff), income, expenditure, performance, timing and schedule of activities, environment, intangibles (such as reputation) and organisational behaviour.

3.26 The product of these numbers provides the overall risk score as indicated in the matrix below and applies equally at all levels of the Organisation i.e. at Corporate, Divisional and Branch level.

Risk Evaluation Matrix

Impact	Critical	5	5	10	15	20	25
	Major	4	4	8	12	16	20
	Significant	3	3	6	9	12	15
	Moderate	2	2	4	6	8	10
	Minor	1	1	2	3	4	5
			Remote (<20%)	Unlikely (20-40%)	Possible (40-60%)	Probable (60-80%)	Almost Certain (80%+)
			1	2	3	4	5
	Likelihood						

3.27 Risks of 16 or more will be scored as overall **high** significance, those of 6 or more, but less than 16 will be considered as **medium** significance and those of less than 6 of **low** significance.

3.28 Risks will be scored for inherent risk, residual risk and target level of risk. Each is defined below.

- **Inherent Risk** is that risk which exists before any management controls are applied. This enables decisions to be made about resources and the level of priority given to managing a risk.

- **Residual Risk** is determined as the level of risk that remains after existing controls have been actioned. The residual risk gives an indication of how effectively a risk is being managed by existing controls.

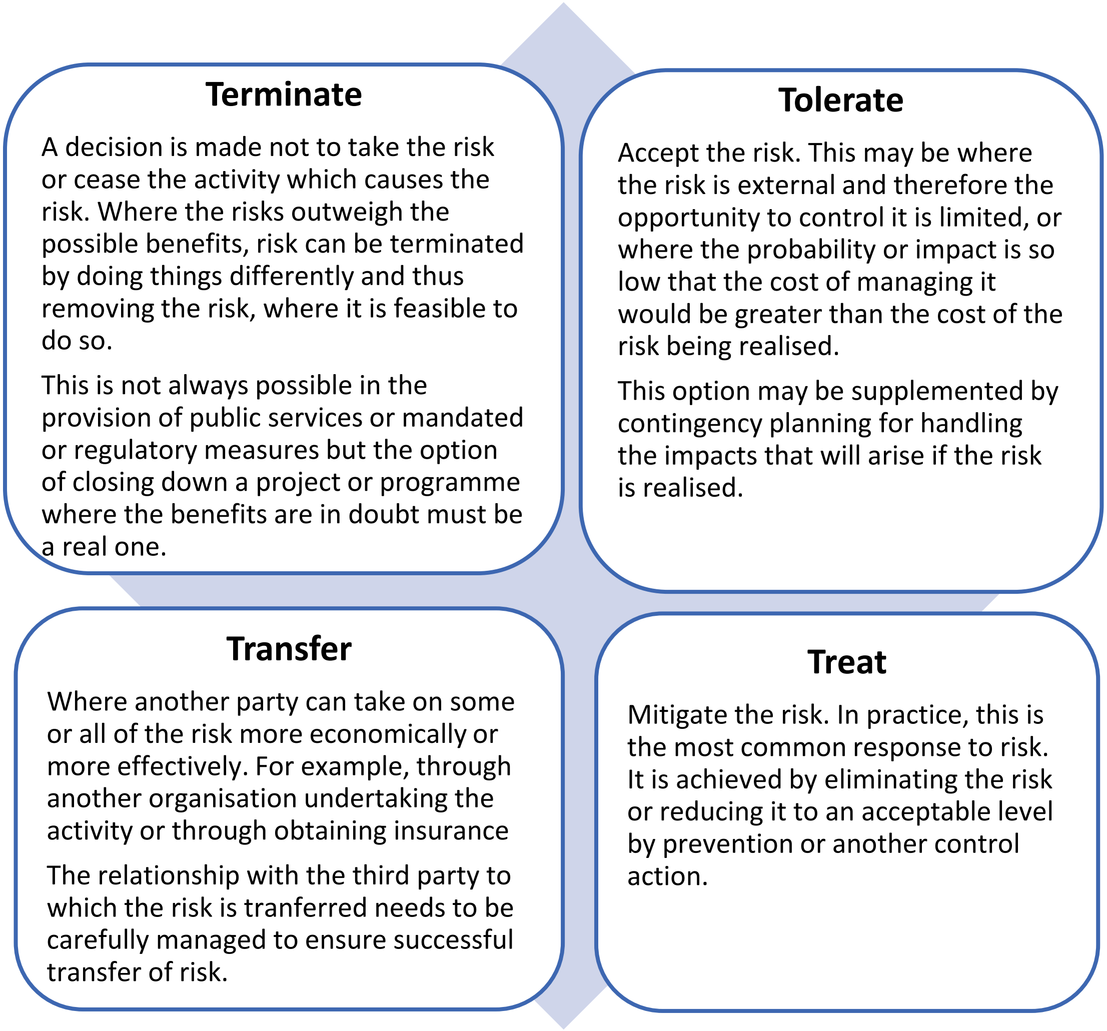
- **Target Level of Risk** is the level of risk that management has set as its target level of risk. This should take account of AFBI's 'Risk Appetite' as outlined in section 5 of this strategy.

3.29 Where the residual risk is higher than the target level of risk, additional controls will be identified to reduce the likelihood and impact of the risk.

STEP 3 - Managing Risk

3.30 Once risks have been identified, management must respond to the risk. There are a number of valid responses to risk. For each risk, the Risk Owner should select one or a combination of the responses set out below:[1]

[1] . It is important to note that some risks are not (fully) transferable - in particular it is generally not possible to transfer reputational risk even if the delivery of the service is contracted out.



Terminate

A decision is made not to take the risk or cease the activity which causes the risk. Where the risks outweigh the possible benefits, risk can be terminated by doing things differently and thus removing the risk, where it is feasible to do so.

This is not always possible in the provision of public services or mandated or regulatory measures but the option of closing down a project or programme where the benefits are in doubt must be a real one.

Tolerate

Accept the risk. This may be where the risk is external and therefore the opportunity to control it is limited, or where the probability or impact is so low that the cost of managing it would be greater than the cost of the risk being realised.

This option may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised.

Transfer

Where another party can take on some or all of the risk more economically or more effectively. For example, through another organisation undertaking the activity or through obtaining insurance

The relationship with the third party to which the risk is tranferred needs to be carefully managed to ensure successful transfer of risk.

Treat

Mitigate the risk. In practice, this is the most common response to risk. It is achieved by eliminating the risk or reducing it to an acceptable level by prevention or another control action.

3.31 In the vast majority of instances AFBI will manage risk through the application of controls. Before determining whether any additional controls are required to be applied to the risk, the current controls which are in place must be considered.

“Control” is any action, procedure or operation which is undertaken by management to increase the likelihood that activities and procedures achieve their objectives. Internal control is therefore a response to risk.

3.32 The purpose of controls is not to eliminate risk altogether but to provide **reasonable assurance** of confining the likely loss or other damage from the realisation of key risks to within the risk appetite of the organisation.

3.33 The option to ‘Treat’ risk through the application of controls can be further analysed into four different types of controls as follows:

Preventative controls -

are designed to limit the possibility of an undesirable outcome being realised. The majority of controls implemented belong to this category.

Examples include password access to computers, supervisory checks and independent authorisations on payments made to suppliers.

Directive controls -

are designed to ensure that a particular outcome is achieved.

Examples include a requirement that protective clothing be worn during the performance of dangerous duties, or that staff are trained before being allowed to work unsupervised.

Corrective controls - (reversibility)

are designed to correct undesirable outcomes which have been realised. Applied after the event, these may consist of contractual remedies to recover overpayments or obtain damages or a detailed contingency plan that will be triggered by an event (e.g. disaster recovery or business contingency plans).

Detective controls -

are designed to identify occasions of undesirable outcomes having been realised. By definition these are after the event, so they are only appropriate when it is possible to accept the loss or damage incurred.

Examples of detective controls include stock or asset checks, reconciliations, post implementation reviews.

3.34 Any controls which are put in place must be properly documented and also be regularly reviewed to ensure that they remain effective and that they continue to offer the best value for money response to the risk.

3.35 The effectiveness of the current controls must be assessed. If the current controls do not reduce the net risk score and therefore the exposure to the risk to within the risk appetite of the organisation, a further response will be required.

3.36 Once initial risks have been identified, evaluated and a response is put in place, the process of risk management will be a continual process to:

- monitor the implementation of controls,
- monitor and change the assessment of risks;
- identify and evaluate any new or emerging risks, in particular considering the achievement of Strategic outcomes and business plan targets; and
- removing risks from the risk register that are no longer relevant.

The Controls should be documented within the Corporate or Divisional Risk Registers. At a Branch/Operational level these will be documented within the Branch Plan (See appendix 4)

STEP 4 – Risk Monitoring & Review

3.37 The fourth stage of the process involves risk monitoring and review to allow management and the Board to gain assurance that risk management is effective and identify when further action is necessary.

3.38 For risk monitoring and review to be effective it is essential that the Risk Registers and Planned Actions are kept up to date in respect of new risks, redundant risks, action taken and revised risk evaluations.

3.39 As Risk Management is intrinsically linked to the Business Planning and Performance Management Process in AFBI, the Risk Management and Business Planning Group will be the main forum for the detailed discussion of Corporate Risks.

3.40 Membership of the Risk Management and Business Planning Group shall comprise AFBI's Executive Management Team, Divisional Business Managers and Risk Owners.

3.41 The Corporate Risk Register will be considered and updated as appropriate to reflect any new or emerging risks to the delivery of Strategic outcomes and targets.

3.42 Divisional Heads will report any new or emerging risks from their areas that are considered as having a potentially significant cross-divisional impact upon AFBI.

3.43 To ensure consistency and to join up key governance processes a copy of the CEO's quarterly Assurance Statement will be forwarded to the Head of Governance and Performance.

Divisional Level

3.44 At a Divisional level the Divisional Management Teams will meet to review the DRR on at least a quarterly basis. Risks from divisions that are considered to impact on the achievement of Strategic outcomes should also be reported by Division Heads and considered for inclusion on the corporate risk register. Once reviewed the Divisional Risk Registers should be forwarded to the Head of Governance and Performance to ensure effective oversight of the process.

3.45 Again, to ensure consistency and to join up key governance processes a copy of the Director's quarterly Assurance Statement will be forwarded to the Head of Governance and Performance.

Branch/Operational Level

3.46 At a Branch level, Branch Management teams must consider risk on a quarterly basis. Branch Heads will report any new or emerging risks from their areas that are considered as having a potentially significant impact upon the achievement of AFBI's Divisional or Corporate Objectives.

3.47The key actions in continually monitoring and assessing risk can be summarised in the table below:

Who	What	When
AFBI Staff	• Bring any significant new risks to the attention of Branch Heads and Senior Management	Continual
Branch Heads	• Bring any significant new risks to the attention of Senior Management	Continual
Risk Owners	• Monitor individual risks and report any significant changes to senior management • Monitor the operation of existing controls and oversee implementation of additional controls	Continual
AFBI Executive Management Team	• Consider new risks and where considered significant, add to the Corporate Risk Register, assign a risk owner and bring to attention of the AFBI Board	Monthly EMT and Board meetings
AFBI Board	• Consider new risks by exception • Consider AFBI's Corporate Risk Register • Consider and agree AFBI's risk appetite	Monthly Approx Quarterly Annually
Risk Management and Business Planning Group	• Consider the Risk Management Strategy and update as appropriate • Identify any new or emerging risks to meeting Strategic outcomes and consider amending risk register as appropriate • Consider and update CRR • Remove any risks that are no longer relevant	Quarterly
Audit & Risk Assurance Committee	• Monitor the process of risk management and report on adequacy to the AFBI Board	Quarterly

4. ROLES AND RESPONSIBILITIES

4.1 In order to ensure that AFBI's Risk Management activities are consistent and effective, and are reported efficiently, a structured framework is required. The main roles and responsibilities in regard to risk management within AFBI are summarised below.

4.1 **Board**

- Oversees and approves the risk management strategy and risk appetite
- Ensures appropriate management monitoring of significant risks
- Challenges risk management to ensure all risks are identified
- Ensures an appropriate response if risks are realised

4.2 **Audit & Risk Assurance Committee (ARAC)**

- Takes responsibility for overseeing and reporting to the Board on the adequacy of the risk management process.
- Reviews risk registers to provide challenge and advice.
- Provides an Annual Report to support the preparation of the Governance Statement.

4.3 **Accounting Officer**

- Retains overall responsibility for ensuring that an effective system of risk management is in place and is regularly reviewed.
- Promotes and embeds a culture of risk identification and management within AFBI, across divisions and branches.
- Reports on risk management to the ARAC and Board and the DAERA through the Assurance Statement process.

4.4 **Executive Management Team**

- Implements risk management policies and procedures.
- Monitors the identification and management of significant risks and reports changes in risks to the Accounting Officer and Board by exception.
- Provides assurance to the Accounting Officer in regard to risk management processes within divisions through the Assurance Statement process

4.5 **Risk Management and Business Planning Group (RM&BPG)**

- Consider the Risk Management Strategy and update as appropriate
- Annually reviews AFBI's approach to risk management and approves changes and improvements to the risk management process.
- Consider new or emerging risks from divisions for inclusion in the Corporate Risk Register.
- Taking account of AFBI's risk appetite, review risk scoring and set an appropriate level of target risk.

- Review the risk register quarterly and ensure that risks are appropriately recorded and that controls are being implemented.
- Agree changes to the risk register under direction of risk owners and supported by the Head of Governance and Performance and the Secretariat and Coordination Unit.

4.6 Risk owners

- Review and update individual risk records regularly and propose changes to how the risk is scored and controlled as appropriate.
- Decide whether a risk is sufficiently serious to be escalated to the next level of the organisation.
- Where there are significant changes in the likelihood or impact of a risk, this will be reported to senior management.

4.7 Divisional Management Teams

- Develop and maintain Divisional Risk Registers (DRR's) identifying key risks to Divisional objectives cascaded from Corporate Objectives.
- Decide whether emerging Divisional Risks should be escalated via the RM&BPG.
- Review DRR's on at least a quarterly basis to ensure risks are being effectively addressed or emerging issues are identified

4.8 Branch Heads and Line Management

- Identifying key risks to Branch objectives including those cascaded from Divisional and Corporate Objectives and documented as part of the Branch business planning process.
- Maintain an awareness of risk within branches and create a culture wherein staff are encouraged to identify risks and bring these to the attention of management.
- Report significant risks, risks of a cross-cutting nature and corporate risks to senior management for consideration for escalation to the Divisional or Corporate Risk Registers.

4.9 AFBI Staff

- Implement risk controls as required by line management and risk owners.
- Maintain an awareness of risk and identify new and emerging risks to line management.

4.10 Internal Audit

- Take AFBI's corporate risks into account and plan audit strategy based on a risk based approach.

- Provide independent opinion to the Accounting Officer and Audit Committee, as to the overall adequacy of AFBI's framework of governance, risk management and internal control.

5.0 RISK APPETITE

5.1 Risk is unavoidable and as such AFBI must take action to manage risk in a way which it can justify to a level which is tolerable. The amount of risk which is judged to be tolerable and justifiable is defined by "risk appetite".

5.2 Within AFBI, the Board is responsible for agreeing and setting the organisations appetite for risk.

5.3 The concept of risk appetite may be looked at in different ways depending on whether the risk (the uncertainty) being considered is a threat or an opportunity:

- When considering **threats** the concept of risk appetite embraces the level of exposure which is considered tolerable and justifiable should the risk be realised. In this sense it is about comparing the cost (financial or otherwise) of constraining the risk with the cost of the exposure should the risk become a reality and finding an acceptable balance;

- When considering **opportunities** the concept embraces consideration of how much one is prepared to actively put at risk in order to obtain the benefits of the opportunity. In this sense it is about comparing the value (financial or otherwise) of potential benefits with the losses which might be incurred (some losses may be incurred with or without realising the benefits).

5.4 The significance of a risk will be an important factor in determining risk appetite. The appetite will also be influenced by the nature of the risk. In the HM Treasury publication on "Managing your Risk Appetite", five levels of appetite are defined:

Risk Appetite

Classification	**Description**
1. Averse	Avoidance of risk and uncertainty is a key organisational objective
2. Minimalist	Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have a potential for limited reward
3. Cautious	Preference for safe delivery options that have a low degree of residual risk and may only have limited potential for reward
4. Open	Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward (and value for money etc.)

5. Hungry	Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk

5.5 HM Treasury uses four broad categories of risk to illustrate the types of behaviour that might be associated with each of the risk appetite levels.

The categories are:

(i) reputation and credibility;
(ii) operational and policy delivery;
(iii) financial/VFM; and
(iv) compliance-legal/regulatory.

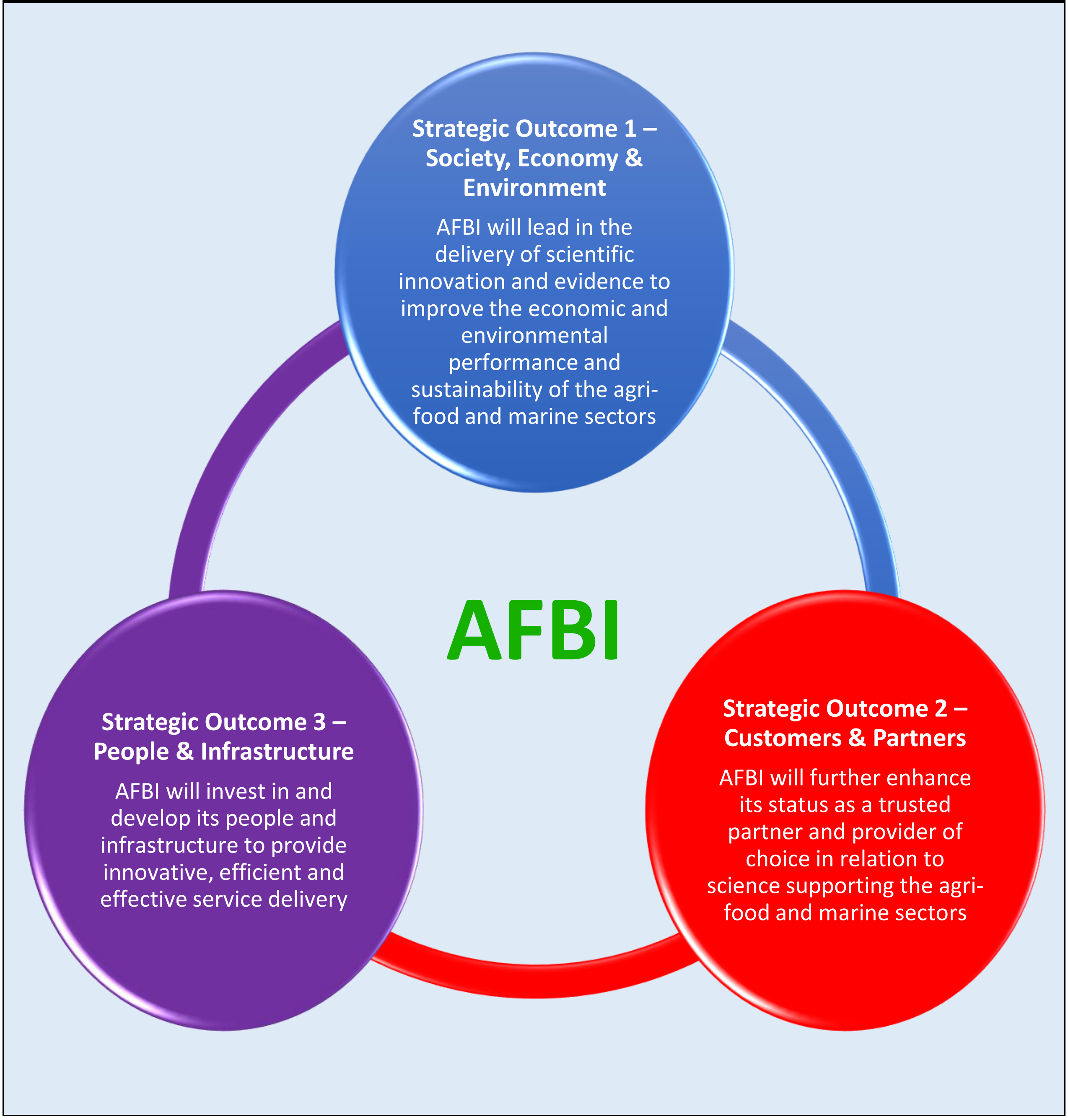
5.6 In defining AFBI's risk appetite, these same categories are adopted, these have however been adapted where appropriate to emphasise key elements of AFBI's corporate strategy.

5.7 The classifications of risk appetite given above can be used to provide qualitative guidance on risk appetite. It must be stressed however that these are generalised appetite levels given for broad guidance only and specific risks in any of the categories may warrant lower or higher tolerance. It is also important to note that business risks do not always fall neatly into single categories.

5.8 In setting target levels of risk, AFBI will consider the levels of risk appetite for the 4 key risk categories as shown in **Appendix 1**. These levels of risk appetite will be set and agreed by the AFBI Board and reviewed annually.

5.9 When considering AFBI's risk appetite against the four broad categories of risk AFBI also takes into account its strategic outcomes for 2018-22 set out overleaf.

AFBI Strategic Outcomes 2018-2022



Strategic Outcome 1 – Society, Economy & Environment

AFBI will lead in the delivery of scientific innovation and evidence to improve the economic and environmental performance and sustainability of the agri-food and marine sectors

AFBI

Strategic Outcome 3 – People & Infrastructure

AFBI will invest in and develop its people and infrastructure to provide innovative, efficient and effective service delivery

Strategic Outcome 2 – Customers & Partners

AFBI will further enhance its status as a trusted partner and provider of choice in relation to science supporting the agri-food and marine sectors

6.0 ACCOUNTABILITY

6.1 All AFBI staff will be alerted to the existence and purpose of this strategy and guidance. The strategy will be included within the induction programme for all new staff and it will be made available via the AFBI Intranet. Changes to the strategy will be brought to the attention of all staff.

6.2 All staff have a duty to report new and emerging risks to line management, who in turn have a responsibility to consider these risks and escalate where risks are significant, have a corporate impact or have a cross cutting nature. Where risks are serious, these should be escalated to the senior management team promptly for consideration.

6.3 Managing risk to the achievement of AFBI objectives is intrinsically linked to the business planning and performance management process. Risk management responsibilities should therefore be embedded within individual Personal Performance Agreements. Where training is required, this should be reflected within individual Personal Development Plans and if formal training is required this should be requested via AFBI's Learning and Development Unit.

6.4 Risk management is an important part of AFBI's system of internal controls. **Appendix 5** outlines the framework for providing assurances to the Accounting Officer and Board in regard to the appropriateness of AFBI's risk management processes.

7 AFBI COMPLIANCE WITH RELEVANT GUIDANCE

7.1 The Department of Finance and Personnel (DFP) issued an "Audit and Risk Assurance Committee Handbook NI[2]" dated April 2014 (the Handbook) draws on the DFP guidance "Corporate Governance in Central Government Departments: Code of good practice NI 2013[3]" (the Code). This provided clear guidance on governance and in particular how public sector organisations should approach the management of risk. AFBI considers it best practice to comply with this guidance.

7.2 The Handbook highlights that following revisions to the Code, Boards are now more clearly tasked with setting the organisation's risk appetite and ensuring that controls are in place to manage risk within this. It also states that the Audit and Risk Assurance Committee is a crucial mechanism for supporting the Board in meeting these obligations.

7.3 The Handbook refers to Principle 5.1 of the Code which provides that the Board should ensure that there are effective arrangements for governance, risk management and internal control and that advice about scrutiny of key risks is a matter for the Board, not a committee. It states that the Board should be supported by:

- An Audit and Risk Assurance Committee (ARAC) chaired by a suitably experienced non- executive board member;

[2] Dear Accounting Officer Letter 06/13

[3] Dear Accounting Officer Letter 05/14

- An internal audit service operating to Public Sector Internal Audit Standards; and

- Sponsor teams of the department's key arm's length bodies.

AFBI is in compliance with each of these requirements.

7.4 On ARAC's, this principle is supported by six supporting provisions in the Code:

- The Board and Accounting Officer should be supported by an ARAC;
- Advising on key risk is a role for the Board. The ARAC should support the Board in this role;
- An ARAC should not have any executive responsibilities or be charged with making or endorsing any decision;
- The Board should ensure that there is adequate support for the ARAC;
- The ARAC should lead the assessment of the annual Governance Statement for the Board; and
- The terms of reference of the ARAC should be made available publically.

AFBI is in compliance with each of these requirements.

8.0 ANNUAL REVIEW

8.1 AFBI's Risk Appetite will be reviewed and agreed on an annual basis by the AFBI Board.

8.2 This strategy and procedure will be reviewed on an annual basis by the Executive. Any changes will be brought to the attention of the AFBI Audit Committee and the AFBI Board.

Appendix 1 – AFBI's Risk Appetite

Risk Category/Type	Risk Appetite Classification	Comment
Reputation and credibility *scientific*	1 Averse	AFBI's vision is "Advancing the local and global agri-food sectors through Scientific excellence". The avoidance of risk to our scientific reputation is crucial. Strategic outcomes *1, 2, and 3relate.*
Reputation and credibility *general*	2 Minimalist	AFBI's ability to secure work from DAERA, public bodies and commercial customers is based upon having a sound reputation. These goals in turn impact on the strength of AFBI's commercial base. Tolerance for risk taking is therefore limited to those events where there is no chance of any significant impediment to the achievement of this objective. Strategic outcomes *1, 2, and 3 relate.*
Operational and policy delivery *general*	4 Open	AFBI is an innovative organisation facing a period of significant change. It will be necessary to consider all potential delivery options and choose the one that is most likely to result in successful delivery while providing an acceptable level of reward. Strategic outcomes *1, 2, and 3 relate.*
Operational and policy delivery *emergency response and statutory testing*	2 Minimalist	AFBI recognises its responsibility to maintain the highest standards of statutory testing and an emergency response capability as agreed with DAERA and other public bodies. Strategic outcomes *1 and 2 relate.*
Financial/VFM *general*	3 Cautious	AFBI will be appropriately cautious in the management of public money. Strategic outcomes *1, 2 and 3 relate*.

Financial/VFM *new business development*	4 Open	AFBI has challenging business development targets which will require an “investment capital” type approach and a willingness to invest for the best possible reward and accept the possibility of financial loss. (Tight controls with close scrutiny, regular review and rigorous evaluation of outputs will be maintained.) Strategic outcomes *1 and 2 relate.*
Compliance – Legal/regulatory	2 Minimalist	AFBI will seek at all times to act within the relevant legal and regulatory constraints. (In the management of Health and Safety the risk appetite will be 1 (averse) and the conformance standard applied will be “as far as is reasonably practicable”.) Strategic outcome *3 relates.*

Factors to Consider when Identifying Risks

The following adapted from the NIAO's Good Practice in Risk Management Guide provides a summary of the most common risk categories which can serve as a useful checklist during risk identification. However, it should be noted that the categories are neither prescriptive nor exhaustive:

External – arising from the external environment	
Category	**Example / Explanation**
Political	Change of government, cross cutting policy decisions, machinery of government changes (e.g. devolution)
Economic	Ability to attract and retain staff in the labour market, exchange rates affect costs of international transactions; effects of global economy on NI economy
Social	Demographic change affects demand for services, stakeholder expectations change
Technological	Obsolescence of current systems, cost of procuring best technology available; opportunity arising from technological development
Legislative	Legal/regulatory EU requirements/laws which impose requirements (such as health and safety or employment legislation)
Environmental	Buildings need to comply with changing standards, disposal of waste and surplus equipment needs to comply with changing standards

Operational – relating to AFBI's existing operations – both current delivery and building and maintaining capacity and capability	
Category	**Example / Explanation**
Service failure	Fail to deliver the service to the user within agreed terms
Project Delivery	Fail to deliver on time / budget / specification
Resources	Financial (insufficient funding / poor budget management / fraud) HR (staff capacity / skills / recruitment and retention) Information (adequacy for decision making / protection of privacy) Physical assets (loss / damage / theft)
Relationships	Delivery partners (commitment to relationship / clarity of roles) Customers / service users (satisfaction with delivery) Accountability (particularly to the Assembly)
Operations	Overall capacity and capability to deliver

Appendix 2: Risk Identification - Factors to Consider

Reputation	Confidence and trust which stakeholders have in the organisation
Governance	Governance Regularity and propriety/compliance with relevant requirements/ethical considerations
Scanning	Failure to identify threats and opportunities
Resilience	Capacity of systems / accommodation / IT to withstand adverse impacts and crises. Disaster recovery / contingency planning
Security	Of physical assets and information

Change – risks created by decisions to pursue new work areas beyond current capability	
Changing Sponsor Department Requirements / Programme for Government Targets	New or changing sponsor department requirements or Programme for Government challenge organisation's capacity to deliver / ability to equip the organisation to deliver
Change Programme	Programmes for organisational or cultural change threaten current capacity to deliver as well as providing opportunity to enhance capacity
New projects	Making optimal investment decisions/prioritising between projects which are competing for resources
New policies	Policy decisions create expectations where the organisation has uncertainty about delivery

Risk Register – Content Required

As set out in paragraph 6.7, the identified Risks should be recorded within a Risk Register (Corporate or Divisional).[4] The Register should capture risk information in 3 sections (an example follows on the following page):

Section A: Records the following information:

Risk Information	**Explanation of information**
Risk Title:	Definition of the Risk
Risk Owner:	The assigned owner for the risk
Corporate Goal Alignment:	The Corporate or Business Plan goals the risk could impact upon and conversely which risks are relevant when considering strategic goals during strategic and business planning.
Risk Scoring:	The scoring for the risk based on impact and likelihood (summarised in the Risk Assessment Matrix para 6.9) for each of the 3 criteria, defined as: **Inherent Risk Score** - that risk which exists before any management controls are applied. This enables decisions to be made about resources and the level of priority given to managing a risk. **Residual Risk Score -** the level of risk that remains after existing controls (section B) have been actioned. The residual risk gives an indication of how effectively a risk is being managed by existing controls. **Target Level of Risk** - the level of risk that management has set as its target level of risk.

Section B: Provides a summary of controls already in place to manage the risk along with details on the person responsible for the control, how often and how it is evidenced.

Section C: provides a summary of additional controls that will be put in place to manage the risk including the date for implementation, the person responsible for the control, how often and how it is evidenced. **Critically** in terms of the risk review process the risk owner will provide at least quarterly updates on the current position as to progress towards implementation.

[4] At a Branch/Operational level these should be recorded within the relevant section of the branch business plan as part of the business planning process.

A	**Risk Definition:** **CR1 -** If AFBI fails to deliver key priority areas of DAERA's Assigned Work Programme (AWP) it may negatively impact its reputational standing with DAERA.	**Risk owner:** Sinclair Mayne/Stanley McDowell

Corporate / Divisional Goal Alignment: **Goal 1 -** To successfully deliver the assigned work programme to DAERA and in doing so support DAERA in protecting the integrity and improving the competitiveness of the NI agri-food sector and rural economy.	***Score Key (Likelihood x Impact = Total Score)** **Impact:** 1. Minor 2. Moderate 3. Significant 4. Major 5. Critical **Likelihood of Occurrence**: 1. Remote (<20%) 2. Unlikely (20-40%) 3. Possible (40-60%) 4. Probable (60-80%) 5. Almost Certain (80%+)

	Inherent Risk Scoring			**Residual Risk Scoring**			**Target Risk Scoring**		
	Impact **5**	Likelihood **4**	**Total Score** **20**	Impact **5**	Likelihood **2**	**Total Score** **10**	Impact **5**	Likelihood **2**	**Total Score** **10**

B	**Controls that are in place to manage the risk**	**Is it performed?**			**Who performs It?**	**How often?**	**How is it evidenced?**
		N/A	**Yes**	**No**			
1	MoU for the delivery of the Assigned Work Programme agreed between DAERA and AFBI		✓		AFBI CEO/DAERA Senior Sponsor	In Place	Signed MoU in place
2	Mid-year and Year-end review of AFBI's delivery of the Assigned Work Programme as required by the MoU		✓		Head of Innovations	Bi-annually	Report to AFBI Board signifying that both DAERA and AFBI are content with delivery of AWP

NB - Risk Information to be recorded in the non-shaded areas of the register

C	Additional actions that will be taken to manage the risk	Proposed implementation date	Who will perform it?	How often?	How will it be evidenced?	Position at XX/XX/2015
1.	Change Control Process being agreed with DAERA.	xx/xx/19	HOB & project Leaders	As required	Forms submitted to DAERA	*Risk Owner provides commentary on the latest position in relation to progress on the planned action*

Extract from AFBI's Divisional and Branch Business Planning & Performance Management Guidance

Risk Management

In setting the Branch / Divisional Objectives and taking account of AFBI's Risk Management Strategy the following were identified as key risks to the achievement of these objectives. All material / key risks have been reflected within the relevant Divisional risk register. ***(This forms an Appendix to the Branch / Divisional Plan***)

Ref	Branch Objective	Key Risk	Risk Owner	Mitigating Actions
1	*Insert –* *e.g. - At least 95% of the DAERA diagnostic and analytical tests stipulated in the Assigned Work Programme delivered to agreed time and quality standards*	*Insert-* *e.g. Unable to deliver programme due to loss of key skills following VES exercise*	*Insert –* *Head of Branch / Division*	*Insert –* *Skills matrix in place to ensure relevant skills retained to deliver service*

Appendix 4 – RAID template

RAID Log

This document should be used by AFBI Project Managers to track Risks, Assumptions, Issues and Dependencies (RAID)

Risks

Assumptions

Issues

Dependencies

Prepared by:

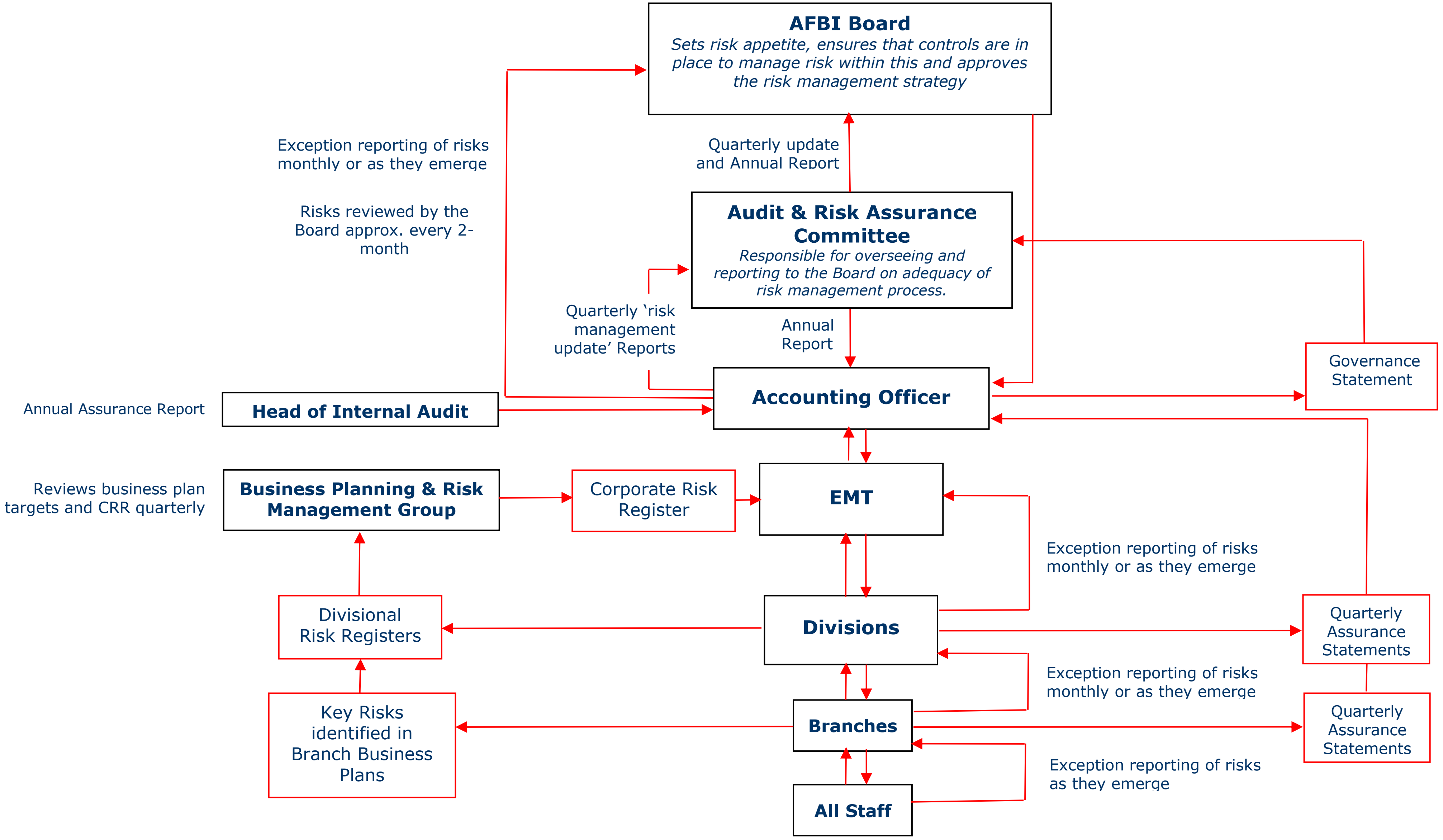
Project Name:

Risk Register

Last Reviewed: {insert date}

DEFINITION: Events that will have a negative impact on the project if they occur. Risk refers to the combined likelihood the event will occur and the impact on the project if it does occur. If the likelihood of the event happening and impact to the project are both high, you identify the event as a serious risk. The log should include a description of each risk, analysis and a plan to manage it.

ID	Date Raised	Risk Description	Likelihood	Impact	Severity	Mitigation Plan	Owner	Status	Date Closed
1					0				
2					0				
3					0				
4					0				
5					0				
6					0				
7					0				
8					0				
9					0				
10					0				


AFBI Board
Sets risk appetite, ensures that controls are in place to manage risk within this and approves the risk management strategy
Exception reporting of risks monthly or as they emerge
Quarterly update and Annual Report
Risks reviewed by the Board approx. every 2-month
Audit & Risk Assurance Committee
Responsible for overseeing and reporting to the Board on adequacy of risk management process.
Quarterly 'risk management update' Reports
Annual Report
Governance Statement
Annual Assurance Report
Head of Internal Audit
Accounting Officer
Reviews business plan targets and CRR quarterly
Business Planning & Risk Management Group
Corporate Risk Register
EMT
Exception reporting of risks monthly or as they emerge
Divisional Risk Registers
Divisions
Quarterly Assurance Statements
Exception reporting of risks monthly or as they emerge
Key Risks identified in Branch Business Plans
Branches
Quarterly Assurance Statements
Exception reporting of risks as they emerge
All Staff