FOOD STANDARDS AGENCY: INFORMATION RELEASED UNDER THE FREEDOM OF INFORMATION ACT

DATE RELEASED: 4 MARCH 2020

Request

1. Does your organisation have a formal policy regarding the production of information and or cyber security risk assessments?
a. If yes, please can you provide a copy of the above policy?
2. Does your organisation hold a register of Information and/or cyber security risk (outside that of the corporate risk register), and if yes:
a. Please can you list the top ten Information and/or Cyber Security Risks?
b. How many risks are there in total on the register?
c. Please state how many risks would be categorised as the highest risk level (i.e. Critical)?
d. Please state how many risks would be categorised as the second highest risk level (i.e. Critical)?
e. Please state how many risks would be categorised as the third highest risk level (i.e. Critical)?
f. How many risk levels do you have in total (i.e. 5)?
3. Do any of the identified information and or cyber security risks also exist on the corporate risk register?
a. If yes, what are those risks?
4. When undertaking an information / cyber security risk assessment, does the authority follow a structured risk assessment process?
a. If so, what is that process?
5. Does your orgnisation follow ISO31000 when undertaking an information / cyber security risk assessment?
6. Does your orgnisation hold ISO27000 accreditation ?
7. Does your organisation have a policy of adhering to any information security standard or framework (i.e. ISO27000, NIST etc)?
a. If yes, please provide a copy of the above policy?
8. Does the authority have the following roles within the origination:
a. Chief Security Officer (CSO),
i. If yes, which role does the CSO report into?

b. Chief Information Security Officer (CISO)
i. If yes, which role does the CISO report into?
c. Head of Information Security (Hd InfoSec)
i. If yes, which role does the Hd InfoSec report into?
9. Who within your organisation who is accountable for undertaking information / cyber security risk assessments (i.e. Chief Information Security Officer, Head of Information Security, Head of Information Technology) ?
10. Who within the authority is responsible for undertaking information / cyber security risk assessments (i.e. Chief Information Security Officer, Head of Information Security, Head of Information Technology) ?
11. How many people within the organisation are responsible for undertaking information / cyber security risk assessments?
12. Does the person(s) responsible for undertaking information / cyber security risk assessment:
a. Have any formal training in this regard?
i. If so, what was it?
b. Have any industry qualifications/certification in this regard?
i. If so, what are they?
13. How many people (permanent and contractors) currently work for the authority?
14. How many people (permanent and contractors) currently work for the authority in information technology roles?
15. How many people (permanent and contractors) currently work for the authority in information / cyber security roles?

Response

1. Does your organisation have a formal policy regarding the production of information and or cyber security risk assessments?
Yes, although this is not specifically for the production of information and cyber security risk assessments.
a. If yes, please can you provide a copy of the above policy? FSA Risk Management Policy is attached.

We also use the Risk Management guidance published by the National Cyber Security Centre:
https://www.ncsc.gov.uk/collection/risk-management-collection
2. Does your organisation hold a register of Information and/or cyber security risk (outside that of the corporate risk register), and if yes: Yes
a. Please can you list the top ten Information and/or Cyber Security Risks? Withheld (Section31(3))
b. How many risks are there in total on the register? Withheld (Section31(3))
c. Please state how many risks would be categorised as the highest risk level (i.e. Critical)? Withheld (Section31(3))
d. Please state how many risks would be categorised as the second highest risk level (i.e. Critical)? Withheld (Section31(3))
e. Please state how many risks would be categorised as the third highest risk level (i.e. Critical)? Withheld (Section31(3))
f. How many risk levels do you have in total (i.e. 5)? 4
For questions 2a to 2e the FSA can neither confirm nor deny that we hold this information, by virtue of the exemptions under Sections 31(3) (prevention and detection of crime) of the Freedom of Information Act 2000 (the FOIA). This is because to confirm or deny whether this information is held would be likely to both prejudice law enforcement and increase the vulnerability of our organisation, which could ultimately aid potential attackers.
The FSA recognises that there is a public interest in the disclosure of information which facilitates the accountability and transparency of public bodies for decisions taken by them and demonstrates that public authorities that hold sensitive information have robust security measures in place. However, there is also a public interest in the security of information held by the FSA which is put to the wider public interest.
Having undertaken the balancing exercise, the FSA has concluded that the public interest in maintaining the exemption significantly outweighs the public interest in confirming or denying whether the requested information is held having regard to the effect that this would not be in the public interest. Particular weight has been placed on the severity of the prejudice which may be caused were the FSA to confirm or deny whether this information is held.
Given that the definition of ‘public’ under the Act is considered to be the public at large, rather than just the individual applicant or a small group of people and that ‘public interest’ is not necessarily the same as what interests the public, it is considered that to confirm or deny whether this information is held is likely to result in prejudice to the security systems of government organisations including the FSA which is not outweighed by the wider public interest for disclosure.
The Information Commissioner’s Office (ICO) has confirmed that they consider that the safeguarding of national security also includes protecting potential targets even if there is no evidence that an attack is imminent. Considering the recent security threats and incidents faced by government organisations and also because of other factors mentioned above we can neither confirm nor deny whether the requested

information is held and hence exempting this information under Section 31(3) of the FOI Act.
3. Do any of the identified information and or cyber security risks also exist on the corporate risk register? No
a. If yes, what are those risks? N/A
4. When undertaking an information / cyber security risk assessment, does the authority follow a structured risk assessment process? Yes
a. If so, what is that process? Process is detailed in our Risk Management Policy
5. Does your orgnisation follow ISO31000 when undertaking an information / cyber security risk assessment? No
6. Does your orgnisation hold ISO27000 accreditation? No
7. Does your organisation have a policy of adhering to any information security standard or framework (i.e. ISO27000, NIST etc)? We follow the HMG Government Security Standards.
a. If yes, please provide a copy of the above policy?
https://www.gov.uk/government/publications/the-minimum-cyber-security-standard
8. Does the authority have the following roles within the origination:
a. Chief Security Officer (CSO), No
i. If yes, which role does the CSO report into?
b. Chief Information Security Officer (CISO) No
i. If yes, which role does the CISO report into?
c. Head of Information Security (Hd InfoSec) Yes (Head of Knowledge Information Management and Security)
i. If yes, which role does the Hd InfoSec report into? Chief Information Officer
9. Who within your organisation who is accountable for undertaking information / cyber security risk assessments (i.e. Chief Information Security Officer, Head of Information Security, Head of Information Technology) ? Head of Knowledge Information Management and Security
10. Who within the authority is responsible for undertaking information / cyber security risk assessments (i.e. Chief Information Security Officer, Head of Information Security, Head of Information Technology) ? Head of Knowledge Information Management and Security, Security Architect
11. How many people within the organisation are responsible for undertaking information / cyber security risk assessments? 2
12. Does the person(s) responsible for undertaking information / cyber security risk assessment:
a. Have any formal training in this regard? Yes
i. If so, what was it?

Management of Risk Foundation
BCS Practitioner Certificate in Information Risk Management
ISO27001 Certified Practitioner
b. Have any industry qualifications/certification in this regard?
i. If so, what are they? See Q12
13. How many people (permanent and contractors) currently work for the authority? 1,251
14. How many people (permanent and contractors) currently work for the authority in information technology roles? 52 (Digital, Data & Technology Profession)
15. How many people (permanent and contractors) currently work for the authority in information / cyber security roles? <5

FSA Risk Management Policy

March 2016

FSA Risk Management Policy

1. Introduction

1.1 This policy sets out the FSA's approach to managing risk and forms part of the internal control and governance arrangements for the organisation.

1.2 Based on the HM Treasury's publication 'Management of Risk'[1] the principles and concepts provided are adopted to provide reasonable assurance to the Executive Management Team and the FSA Board that risk is managed appropriately in the Agency. The criteria to assess the *maturity* of risk management in the organisation is detailed in the HM Treasury's further publication 'Risk Management Assessment Framework'[2]

1.3 Interpretation and implementation of this policy is provided through additional guidance and risk management documentation.

1.4 For the purposes of this policy, the terms 'risk' and 'risk management' are defined as follows:

Risk – a future event / uncertainty that may threaten (or enhance) the FSA's ability to achieve current or future business objectives. Not to be confused with an issue that, by definition, is a present problem or concern. A risk can become an issue, but an issue is not a risk – it has already happened.

Risk management - all the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress.

1.5 The resources available for managing risk are finite and so the aim is to achieve an optimum response to risk, prioritised in accordance with an evaluation of the risks. Risk is unavoidable, and every effort needs to be taken 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 the "risk appetite".

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf
[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/191516/Risk_management_assessment_framework.pdf

2. Our risk appetite

2.1 In order for the FSA to deliver “food we can trust”, whilst managing our reducing resources and external uncertainty, we will need to take risks and exploit opportunities.

2.2 Our aim is to further embed integrated risk management within the FSA and raise the maturity of the organisation in order to deliver better outcomes for consumers. The priority is to reduce risks that impact on consumer protection and consumers’ interests - where the risk/s outweighs the benefits.

2.3 We have a higher appetite for opportunities associated with innovation in how we deliver our functions. We recognise that there are risks associated with the status quo as well as with change, and so we will be open-minded about change and about the potential for change to help us reduce risk.

2.4 This may not be the case in all areas and therefore to encourage considered risk taking and innovation, risks are aligned to themes and for each theme an appetite tolerance is described. This is used by the risk owners to aid with their responsibilities in managing risk and understanding of the parameters to operate.

2.5 The themes are:

- Food we can trust
- Operational / Policy delivery
- Compliance / Legal / Regulation
- Reputation / Credibility
- Finance / VFM

3. The FSA's approach to risk management

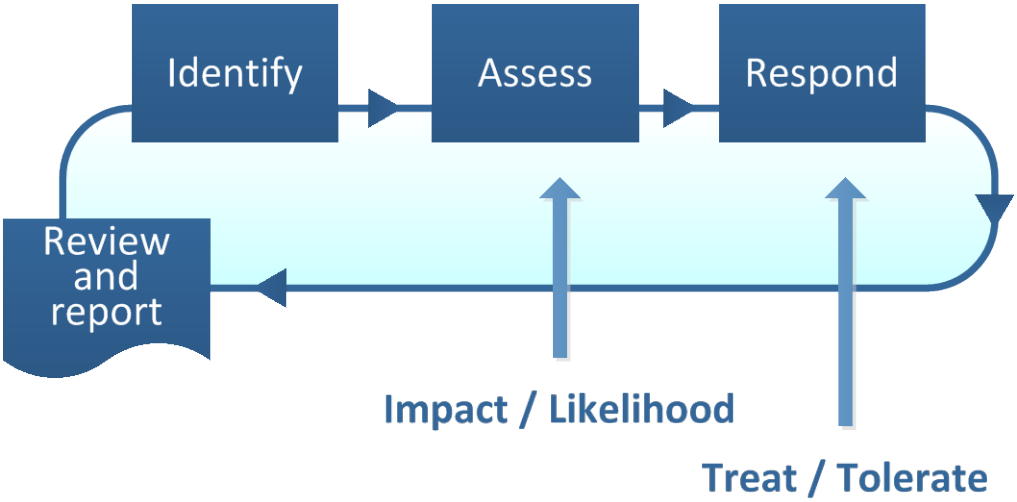
3.1 Our approach is underpinned by a risk management process and clarity of the roles and responsibilities that each of us has in managing risk. The risk management process is an integral part of our approach to business planning, performance management and reporting and programme and project management.

a) Process

3.2 It is our policy to manage risks at the appropriate level across the FSA and maintained monthly by exception, with a detailed review on a quarterly basis ensuring the right risks have been identified, mitigating actions are being progressed, or where no specific action is required/possible contingencies are in place. The quarterly review is used to raise, for consideration, any required movement between higher and lower level risk registers or transfers to other Directorates.

3.3 This is supplemented by an annual refresh as part of the corporate business planning process, typically in the autumn at a Directorate level and culminating with the FSA Board and Executive Management Team annual workshop in spring in preparation for the coming financial year.

3.4 To support the appropriate analysis, treatment and monitoring our policy is to use risk registers (a number of which are mandatory) as part of our management approaches. Where appropriate, risk registers will be used to record the escalation or de-escalation, transfer or aggregation of risks to ensure that they are managed at the most appropriate level within the FSA and that is by those best placed to take decisions as to how best to handle them.



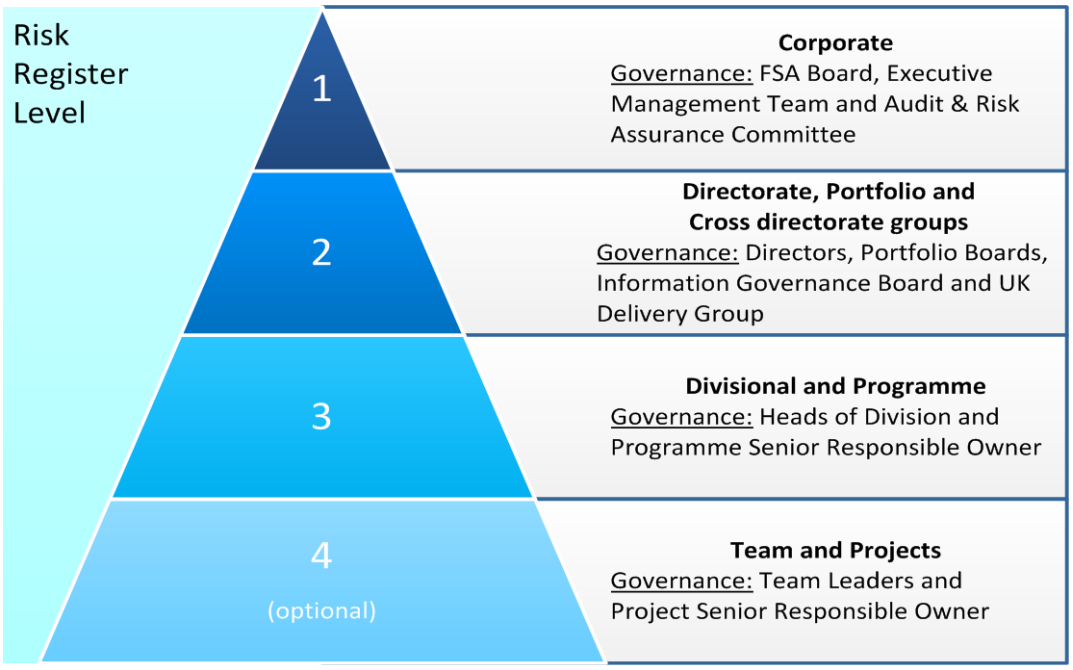
3.5 Part of risk analysis is to assess the likelihood of the risk occurring and the impact that it would have if it did occur. The two aspects are linked and by assessing one against the other using a matric a scale can be determined. This scale (Green, Green/Amber, Amber/red or Red) indicating the seriousness of the risk and is there to aid the determination of mitigation in accordance with the risk appetite.

3.6 The management of risk movement between levels follows standard FSA governance routes i.e. Line Manager – Head of Division / Team – Director / Governance Board chair – Executive. The approach may vary depending on urgency.

- Urgent: using management chain and discussed by EMT at the earliest opportunity (not restricted by meeting schedule)
- Non urgent – using management chain appropriate Manager / Director will table a paper (or AOB item) for the relevant governance meeting i.e. EMT, Portfolio Board, etc to discuss and provide direction.

3.7 At this point it may be that the risk needs escalating or transferring to a new owner but equally once direction is given the risk may effectively be managed at the originating level / owner.

3.8 When introducing a new risk, either as a result of escalation, de-escalation or transfer, consideration needs first to given over aggregation. It may be that the new points only need to be incorporated into an existing risk but with additional context and new mitigations stated. The risk score should always be re-assessed.



3.9 Two forms of risk register are used, Strategic and Functional. The Level 1 Corporate Risk Register which is focussed at strategic risks contains a risk description, owner, context, situation status, the controls already in place and the key mitigating actions management are targeting their focus.

3.10 Functional registers are used at levels 2 through to 4 and these follow a standard template containing the some core information held in the strategic register. Additional scoring criteria (impact and likelihood) are also used to aid consistency of approach across the organisation. These include scores assigned before and after controls have been applied and a target score management are aiming to achieve through managing the risk.

3.11 This policy integrates portfolio, programme and project risk management into the corporate risk management approach. Portfolio-level risks are in level 2, programme risks in level 3 and project risks in level 4. At each level risks that cannot be effectively managed to the target level are escalated to the next level up. For example, a project would escalate to its programme, programmes and standalone projects escalate to level 2 and portfolio risk is escalated to level 1.

3.12 Where delivery is undertaken through partners the FSAs policy is to follow the HM Treasury guidance 'Managing risks with delivery partners - A guide for those working together to deliver better public services'. Effective partnership working is an important aspect and there are two approaches a manager needs to consider:

- 'arms length' – an approach to avoid confusing responsibilities between customer and contractor, to maintain a level playing field for competitors and to reduce the risk of impropriety
- 'partnering' – collaborative working between partners to achieve a common goal, with common risks with a greater degree of openness, communication, mutual trust and sharing information.

3.13 Risk management is an on-going process and risk registers maintained and updated as necessary (monthly by exception with quarterly reviews and annually refreshed). The Corporate Risk Register is controlled by the Executive Management Team and is scrutinised by the Audit and Risk Assurance Committee. Functional risk registers are controlled as part of Directorate, Divisional and local management practice supplemented by a number of governance and programme/project boards.

3.17 All FSA staff are to have an awareness of the FSA's approach to risk management, with the senior management and team leaders having a practical understanding of how this needs to be applied. Knowledge is gained through available Civil Service Learning, FSA policy and guidance and supported through a group of nominated risk specialists representing each Directorate and Governance Board. This enables staff at the appropriate level to play their part in the identification, management and communication of risks in relation to their respective areas of work.

3.18 Risk Owners have an additional responsibility to ensure that assigned risks are effectively managed in line with this policy and supporting FSA risk management guidance.

c) Roles

3.19 FSA Board – risk is considered in all decisions taken by the Board. The Board has delegated oversight of the FSA's approach to risk management to the Audit and Risk Assurance Committee (ARAC) however the Board and Executive Management Team (EMT) have specific responsibility in determining the risk appetite for the FSA.

3.20 Audit and Risk Assurance Committee – a committee of the FSA Board responsible for providing assurance to the Board that all aspects of the FSA's risk management policies are effective and appropriate. ARAC is chaired by a Board member, who reports at least annually to the Board; the membership of the committee is drawn from the Board and FSA senior management.

3.21 Chief Executive – The Chief Executive is the owner of the Corporate Risk Register. As accounting officer for the FSA, the Chief Executive is responsible for the production of the annual governance statement that appears in the FSA's Annual Report & Accounts. This reports on the effectiveness of the FSA's risk management arrangements.

3.22 Directors – are responsible for ensuring that there are effective risk management and monitoring arrangements in place at the right levels within their Directorate, and that these arrangements are compliant with this policy. The Director for Finance and Performance is responsible for championing effective risk awareness and risk management across the organisation.

3.23 Portfolio Board – is responsible for the management of portfolio-level risks and ensuring that programmes and projects within the FSA manage risk in line with this policy.

3.24 Risk Advisors – a nominated representative in each FSA Directorate or Governance Board who holds responsible for:

- Disseminating a risk aware culture across their business area and facilitate an approach to risk management in agreement with the corporate governance,
- Custodian of the risk registers in their business area, challenging and supporting colleagues to ensure that risks to delivery are properly identified, recorded and owned, and
- Contributing to the continued improvement of risk management across the wider FSA by promoting it as an integral part of business management and through sharing of best practice.

4. Support

4.1 Central support on FSA risk management is provided by the Planning,

Performance and Change Team who also facilitate the management of risk at a corporate level. Directorate and Governance Board support is provided by the group nominated Risk Advisors.

4.2 Supporting guidance and information on implementing the FSA risk management policy is available on Foodweb along with contact details for the group of the Risk Advisors.

END