Governance of Risk

National Occupational Standards

January 2013

Skills CFA
6 Graphite Square, Vauxhall Walk,
London SE11 5EE
T: 0207 0919620
F: 0207 0917340
Info@skillscfa.org www.skillscfa.org

Contents

CFAGOR1
Determine the organisation's approach to risk

Overview
This Standard is about the governing body's responsibility for risk and risk management and how it discharges that responsibility. It is about determining the nature and extent of the risks involved in the organisation, formulating and approving the organisation's approach to them.

CFAGOR1
Determine the organisation's approach to risk

You must be able to:

P1 determine the governing body's strategic responsibility for risk taking

P2 formulate the organisation's attitude and policy to risk

P3 identify the key risks the organisation may face

P4 agree the organisation's risk appetite and tolerance for key individual risks

P5 articulate the types of key risks that are acceptable and those that are not

P6 evaluate the risks for their potential positive and negative impact

P7 establish how the organisation overall is exposed to risk

P8 identify appropriate scoring systems showing that effective risk measurements are in place and how these link to the organisation's strategy

P9 define the organisation's exposure to key risks and how this might change as a result of changes to strategy and the operating environment

P10 determine the organisation's ability to reduce the impact of the key risks on the business that materialise

P11 demonstrate an understanding of how different risks interact

CFAGOR1
Determine the organisation's approach to risk

Knowledge and understanding

You need to know and understand:

K1 the concepts of risk, risk appetite, risk tolerance and capacity

K2 the nature and extent of the risks that face the organisation and its component parts internally and externally

K3 how to assess the relationship between risk strategy and the operating environment of the organisation, customers and markets

K4 how to assess the extent and categories of risk and the degree of exposure faced by the organisation

K5 how to assess the likelihood between different key risks concerned materialising

K6 the organisation's risk management capability and ability to reduce the impact of the key risks on the business that do materialise

K7 the principles of identifying, analysing, evaluating, measuring, transferring, modifying, monitoring and reducing relevant risks and defining consistent terminology

K8 the governing body's strategic responsibilities for risk-taking by agreeing the organisation's risk appetite and tolerance, risk exposures and risks that have the potential to undermine the organisation's strategy.

K9 the current regulatory framework that applies to your organisation and the concept of strategic responsibility as it relates to risk

K10 how risk management operates and relates to internal control systems

K11 the different approaches to risk management

K12 how the organisation's key performance drivers are impacted by risk and how key risk indicators and key control indicators operate within the organisation

K13 how to assess the accuracy of the risk data presented to the governing body and how to obtain assurances on data accuracy

K14 how risk tolerance is integrated within the control culture of the organisation

K15 if the organisation has sufficient and appropriate resources and systems in place to achieve the organisation's approach to risk

CFAGOR1

Determine the organisation's approach to risk

Links to other NOS   Refer to core Governance NOS (2011) suite.

CFAGOR1

Determine the organisation's approach to risk

Developed by	Skills CFA
Version number	1.0
Date approved	January 2013
Indicative review date	January 2016
Validity	Current
Status	Original
Originating organisation	Skills CFA
Original URN	CFAGOR1
Relevant occupations	1000 Managers and Senior Officials 1112 Directors and chief executives of major organisations, 1114 Senior officials of special interest organisations 1131 Finance Managers and Chartered Secretaries 1135 Personnel, training and industrial relations managers 2000 Professional Occupations 2421 Chartered and certified accountants 2422 Management accountants 4000 Administrative and Secretarial Occupations 4214 Company Secretaries
Suite	Governance of Risk (2013)
Key words	Governing Body, Governance structure, Governing Body decision making, Governing Body meetings, Governing Body committees, Governance strategy, Governance and Leadership, Governing Body stakeholders, Governing Body role and responsibility, collective leadership, related party transactions

Overview

This Standard is about the governing body's role in establishing an appropriate culture within the organisation to manage risk effectively. It is about effective decision making, promoting transparency, integrity and ethical behaviour and ensuring clear lines of accountability.

CFAGOR2

Set and instil the right culture throughout the organisation

Performance criteria

You must be able to:

P1   formulate and set the organisation's risk culture

P2   promote transparency and clear lines of accountability throughout the organisation to encourage effective risk management

P3   ensure that risk management is integrated into the governing body's own decision making processes

P4   promote a culture which emphasises integrity and ethical behaviour

P5   embed risk management and internal control systems in all aspects of the organisation's activities

P6   ensure that incentives are fully aligned with the strategy and risk appetite or tolerance to reinforce the organisation's risk culture

P7   define the structures and frameworks that are appropriate for the organisation

P8   define the approach to disclosure and transparency

CFAGOR2

Set and instil the right culture throughout the organisation

Knowledge and understanding

You need to know and understand:

K1   the definition and meaning of risk culture including which types of risks are consistent with the culture and those that are not

K2   the organisation's attitude to risk appetite and tolerance

K3   how the governing body's own decision making processes take risk considerations and wider stakeholder issues into account

K4   how to embed and integrate transparent behaviours into risk management and internal control processes throughout the organisation, including whistleblowing

K5   the importance of clear lines of accountability

K6   the importance of diverse perspectives and when the use of specialist input is appropriate

K7   how to promote a culture which emphasises integrity and ethical behaviour and ensuring effective leadership by clear and consistent communications and leading by example

K8   how the behavioural aspects of incentives operate on the organisation's risk management and internal control framework and that risk decisions are taken with full consideration of the impact of incentives

K9   how to create appropriate structures and frameworks and delegated authorities to reinforce the organisation's approach to risk

K10 that managers making decisions understand the degree to which they can expose the organisation to risk

K11 that the organisation has sufficient and appropriate resources, systems and competences are allocated to risk across the organisation

K12 that risk management is distinct from risk oversight

K13 that risk events and 'near misses' should be dealt with openly and consistently in alignment with the agreed culture providing disclosure in the event of bad news

CFAGOR2

Set and instil the right culture throughout the organisation

CFAGOR2

Set and instil the right culture throughout the organisation

Developed by	Skills CFA
Version number	1.0
Date approved	January 2013
Indicative review date	January 2016
Validity	Current
Status	Original
Originating organisation	Skills CFA
Original URN	CFAGOR2
Relevant occupations	1000 Managers and Senior Officials 1112 Directors and chief executives of major organisations, 1114 Senior officials of special interest organisations 1131 Finance Managers and Chartered Secretaries 1135 Personnel, training and industrial relations managers 2000 Professional Occupations 2421 Chartered and certified accountants 2422 Management accountants 4000 Administrative and Secretarial Occupations 4214 Company Secretaries
Suite	Governance of Risk (2013)
Key words	Governing Body, Governance structure

CFAGOR3
Establish and maintain transparent and formal structures and policies in relation to risk and internal controls

Overview   This Standard is about the governing body's role in setting a formal framework for risk management and internal control systems. It is about formulating, reviewing and updating the documents which set out the authorities delegated to various structures and managers. It is about clearly defining roles and responsibilities and having clear lines of delegation. It is about ensuring that managers making decisions understand the degree to which they can expose the organisation to risk.

CFAGOR3

Establish and maintain transparent and formal structures and policies in relation to risk and internal controls

Performance criteria

You must be able to:

P1 oversee and define the organisation's risk appetite, risk management and internal control structures and processes

P2 adopt the most appropriate schedule of matters reserved to the governing body and the scheme of delegation of governing body responsibilities to its structures and individuals

P3 define the roles of its structures and individuals regarding the risk acceptance and oversight of the risk and management processes

P4 delegate or retain the responsibilities for reviewing internal controls and the process of risk management

P5 ensure clarity exists between the roles and responsibility between the audit and the risk structures

P6 ensure that the governing body's attitude to risk is reflected and applied in the structure of the organisation

P7 oversee the organisation's procedures and practices to ensure that they support the governing body's formal structures and policies

P8 review and monitor formal structures and policies from time to time and on a regular basis and ensure that any breaches of risk management are reviewed on a timely basis

CFAGOR3

Establish and maintain transparent and formal structures and policies in relation to risk and internal controls

Knowledge and understanding

You need to know and understand:

K1 how risk management and internal control structures operate both within the organisation and externally

K2 how to build a culture within the organisation that respects risk

K3 how to assess the range of options and choices of risk management frameworks that are available, including the respective roles of line management, risk management and audit ('three lines of defence')

K4 how to assess when the use of specialist input is appropriate

K5 how to assess the capabilities and competences existing within the organisation

K6 how to assess when additional resources are required

K7 how the allocation of authority to structures and individuals will operate and how they are evidenced

K8 how the feedback is received by way of management information and reports from executive management

K9 how to allocate responsibility to structures and individuals and evidence that delegation of authority

K10 how to formulate appropriate terms of reference for individuals and structures of the governing body and to evidence that delegation of authority and clearly communicate it throughout the organisation

K11 how to revise and monitor the formal structures and policies on a regular basis and how to measure performance of the formal structures and policies

K12 how to learn from any breaches in risk management and whistleblowing policies and to update policies and procedures accordingly

K13 how to identify clear objectives for structures and individuals and to demonstrate how those objectives have been satisfied

K14 how risk management is distinct from risk oversight and that risk management is the responsibility of the organisation's management team which should be clearly articulated in the organisation's governance framework

CFAGOR3

Establish and maintain transparent and formal structures and policies in relation to risk and internal controls

Links to other NOS   Refer to core Governance NOS (2011) suite.

CFAGOR3

Establish and maintain transparent and formal structures and policies in relation to risk and internal controls

Developed by	Skills CFA
Version number	1.0
Date approved	January 2013
Indicative review date	January 2016
Validity	Current
Status	Original
Originating organisation	Skills CFA
Original URN	CFAGOR3
Relevant occupations	1000 Managers and Senior Officials 1112 Directors and chief executives of major organisations, 1114 Senior officials of special interest organisations 1131 Finance Managers and Chartered Secretaries 1135 Personnel, training and industrial relations managers 2000 Professional Occupations 2421 Chartered and certified accountants 2422 Management accountants 4000 Administrative and Secretarial Occupations 4214 Company Secretaries
Suite	Governance of Risk (2013)
Key words	Governing Body, Governance structure

CFAGOR4
Identify and assess the risks inherent in the organisation's business model

Overview

This Standard is about 'horizon scanning' and the governing body's role in ensuring that there is an on-going process for identifying, evaluating and managing the significant risks faced by the organisation. It is about identifying and assessing the key risks that are capable of undermining the long term viability of the organisation.

CFAGOR4
Identify and assess the risks inherent in the organisation's business model

Performance criteria

You must be able to:

P1   identify the organisation's key material individual internal and external risks

P2   quantify, where possible, the range of internal and external risks and explore the possibility of mitigation

P3   identify the key risks that are capable of undermining the strategy or long-term viability of the organisation or damaging its reputation

P4   assess the probability and impact of individual risks and how they might combine in undermining the strategy or long-term viability of the organisation or damaging its reputation

P5   demonstrate awareness of new and changing risks in the operational context

P6   regularly review and assess the organisation's key material risks [to ensure the governing body is monitoring the right risks]

CFAGOR4

Identify and assess the risks inherent in the organisation's business model

Knowledge and understanding

You need to know and understand:

K1   the principles of how to measure, manage, evaluate and mitigate key risks both external and internal

K2   how to review and assure the effectiveness of risk management processes within the governing body's areas of responsibility

K3   the principles of identifying, analysing, evaluating, transferring, modifying and reducing risks, including low probability, high impact events ('black swans'), and interacting and correlating risks

K4   when and how to challenge strategic proposals, key risk policies and major operational issues

K5   when the use of specialist input is appropriate

K6   how to ensure effective oversight of the key risks with the potential to undermine the strategy and long term viability of the organisation

K7   the importance of determining when assurance and verification of compliance is necessary within the organisation's risk management strategy

K8   when and how to review breaches of risk management and the importance of timely intervention

K9   how the organisation's performance drivers are impacted by risk

K10   how key risk indicators and key control indicators relate to the overall success to the organisation

K11   the concept of horizon scanning to ensure all current risks are captured such as political, economic, sociological, technological, legal and environmental

CFAGOR4

Identify and assess the risks inherent in the organisation's business model

Links to other NOS   Refer to core Governance NOS (2011) suite.

CFAGOR4

Identify and assess the risks inherent in the organisation's business model

Developed by	Skills CFA
Version number	1.0
Date approved	January 2013
Indicative review date	January 2016
Validity	Current
Status	Original
Originating organisation	Skills CFA
Original URN	CFAGOR4
Relevant occupations	1000 Managers and Senior Officials 1112 Directors and chief executives of major organisations, 1114 Senior officials of special interest organisations 1131 Finance Managers and Chartered Secretaries 1135 Personnel, training and industrial relations managers 2000 Professional Occupations 2421 Chartered and certified accountants 2422 Management accountants 4000 Administrative and Secretarial Occupations 4214 Company Secretaries
Suite	Governance of Risk (2013)
Key words	Governing Body, Governance structure

Monitor the organisation's exposure to risk and the key risks that could undermine its strategy, reputation or long-term viability

---

Overview

This Standard is about the governing body's oversight role in relation to risk. It is about the processes that the governing body use to ensure that the strategy and business model are robust. It is about ensuring that emerging risks are fully considered and reflected in the organisation's risk management systems.

CFAGOR5 Monitor the organisation's exposure to risk and the key risks that could undermine its strategy, reputation or long-term viability

21

CFAGOR5

Monitor the organisation's exposure to risk and the key risks that could undermine its strategy, reputation or long-term viability

Performance criteria

You must be able to:

P1 receive reports on a timely and regular basis from those charged with managing key risks

P2 evaluate the quality and sufficiency of reports on the impact of key risks

P3 review risk management reports and take appropriate action

P4 review the business model at all times to ensure the key risks and emerging risks remain within the organisation's risk tolerance

CFAGOR5 Monitor the organisation's exposure to risk and the key risks that could undermine its strategy, reputation or long-term viability

22

CFAGOR5

Monitor the organisation's exposure to risk and the key risks that could undermine its strategy, reputation or long-term viability

Knowledge and understanding

You need to know and understand:

K1 the importance of clear lines of accountability that exist within the organisation

K2 how to interpret reports and analyse the data received

K3 how to question and challenge management reports when necessary

K4 how to identify when, and what action, needs to be taken on risk management reports

K5 the extent and frequency of the communication and information flows to the governing body gathered in the course of monitoring

K6 what assurance and verification processes have been applied to reports and the basis of such assurance and verification if any

K7 the impact of any emerging risks on the business model

K8 how any emerging risks impact the organisation's risk appetite

K9 the political, economic, social, technological, legal and environmental (PESTLE) climate within which the organisation operates

K10 how the organisation interrelates with any supervisory or governmental authorities who may have systemic risk oversight

K11 when the use of specialist input is appropriate

K12 that management is responsible for ensuring appropriate disciplines are in place over risk management data and risk management information

K13 how to ensure that there is data accuracy in reports and assurance over supporting data governance

K14 the need for flexibility as risk management may need to be reviewed outside of the normal cycle of governing body meetings

CFAGOR5

Monitor the organisation's exposure to risk and the key risks that could undermine its strategy, reputation or long-term viability

---

Links to other NOS   Refer to core Governance NOS (2011) suite.

CFAGOR5

Monitor the organisation's exposure to risk and the key risks that could undermine its strategy, reputation or long-term viability

Developed by	Skills CFA
Version number	1.0
Date approved	January 2013
Indicative review date	January 2016
Validity	Current
Status	Original
Originating organisation	Skills CFA
Original URN	CFAGOR5
Relevant occupations	1000 Managers and Senior Officials 1112 Directors and chief executives of major organisations, 1114 Senior officials of special interest organisations 1131 Finance Managers and Chartered Secretaries 1135 Personnel, training and industrial relations managers 2000 Professional Occupations 2421 Chartered and certified accountants 2422 Management accountants 4000 Administrative and Secretarial Occupations 4214 Company Secretaries
Suite	Governance of Risk (2013)
Key words	Governing Body, Governance structure

CFAGOR5 Monitor the organisation's exposure to risk and the key risks that could undermine its strategy, reputation or long-term viability

25

CFAGOR6
Oversee the effectiveness of management's internal controls and mitigation processes and monitor organisational compliance

Overview
This Standard is about the governing body's responsibility for ensuring that rigorous and robust processes are in place to monitor organisational compliance with agreed strategy. It is about effective communication and training within the organisation and ensuring a culture of continuous risk awareness is maintained throughout the organisation.

CFAGOR6

Oversee the effectiveness of management's internal controls and mitigation processes and monitor organisational compliance

Performance criteria

You must be able to:

P1   ensure that rigorous and robust processes are in place to monitor organisational compliance with agreed strategy and risk appetite

P2   ensure that communication and training is implemented across the organisation at all levels to highlight risk management processes and responsibilities

P3   ensure appropriate assurance processes are in place on effective management controls

P4   ensure regular opportunities to evaluate the processes in place and implement improvements where necessary

P5   ensure a culture of continuous improvement (to include learning lessons from failures or weaknesses in the risk management system)

CFAGOR6

Oversee the effectiveness of management's internal controls and mitigation processes and monitor organisational compliance

Knowledge and understanding

You need to know and understand:

K1   how the management's internal control and mitigation processes operate

K2   the techniques of assessing the effectiveness of the management's internal control and mitigation processes

K3   how to identify and follow up potential weaknesses or failures within the existing internal control and mitigation processes

K4   how to identify the causes of control weakness and effectiveness and the management's role in on-going processes for designing, operating and monitoring the system of internal control

K5   how to assess any potential weaknesses that have occurred within the management's internal control and mitigation processes and the extent to which they have had a material impact on the organisation

K6   the importance and timeliness of escalation processes

K7   how to communicate and embed identified changes to internal control and management processes

K8   the importance in acknowledging when specialist input is appropriate and initiate such specialist input as and when it is necessary

K9   the cost of operating particular controls relative to the benefits to be obtained

K10   the techniques and methods available for providing assurance to, and testing of, existing controls and mitigation processes

K11   how to ensure that training requirements in risk management systems are assessed throughout the organisation and identify and target areas that require improvement

K12   how to ensure that reports are received from independently validated sources are not subject to conflicts of interests

K13   how to ensure data integrity and accuracy of risk management data

CFAGOR6

Oversee the effectiveness of management's internal controls and mitigation processes and monitor organisational compliance

Links to other NOS   Refer to core Governance NOS (2011) suite.

CFAGOR6

Oversee the effectiveness of management's internal controls and mitigation processes and monitor organisational compliance

Developed by	Skills CFA
Version number	1.0
Date approved	January 2013
Indicative review date	January 2016
Validity	Current
Status	Original
Originating organisation	Skills CFA
Original URN	CFAGOR6
Relevant occupations	1000 Managers and Senior Officials 1112 Directors and chief executives of major organisations, 1114 Senior officials of special interest organisations 1131 Finance Managers and Chartered Secretaries 1135 Personnel, training and industrial relations managers 2000 Professional Occupations 2421 Chartered and certified accountants 2422 Management accountants 4000 Administrative and Secretarial Occupations 4214 Company Secretaries
Suite	Governance of Risk (2013)
Key words	Governing Body, Governance structure

CFAGOR6 Oversee the effectiveness of management's internal controls and mitigation processes and monitor organisational compliance

30

CFAGOR7
Ensure the organisation has effective business continuity and crisis management systems

Overview

This Standard is about the governing body's role in formulating, establishing and overseeing appropriate business continuity and crisis management systems within the organisation. It is about ensuring that adequate independent third party assurance and testing of Business Continuity and crisis management plans take place on a regular basis.

CFAGOR7

Ensure the organisation has effective business continuity and crisis management systems

---

You must be able to:

P1 determine the organisation's approach to business continuity and crisis management

P2 set up systems for improvements in techniques and processes to ensure effective business continuity and crisis management

P3 ensure that responsibility for managing specific risks is clearly allocated to individuals at all levels throughout the organisation and their performance is measured and reflected, where appropriate, in the organisational awards (remuneration) system

P4 monitor and reviewing the levels of risks and setting robust business continuity and crisis management plans

P5 ensure that appropriate assurance and testing of the business continuity and crisis management plans take place on a regular basis

P6 ensure that adequate assurance of the business continuity and crisis management systems take place on a regular basis

P7 ensure a detailed review of learning follows a crisis event

CFAGOR7
Ensure the organisation has effective business continuity and crisis management systems

---

Knowledge and understanding

You need to know and understand:

K1   the benefits to the organisation of effective business continuity and crisis management systems [e.g. reputational and other damage]

K2   the resources, techniques and attitudes that are needed to formulate effective business continuity and crisis management systems

K3   when external input is appropriate

K4   how to embed business continuity and crisis management plans throughout the whole organisation

K5   that mechanisms are in place, and are tested frequently, including early warning processes to ensure the robustness of the business continuity and crisis management plans

K6   when to follow up on any potential identified weaknesses

K7   the importance in obtaining independent and unconflicted third party assurance as appropriate to ensure that business continuity and crisis management plans are effective

K8   how to promote a culture that emphasises the importance of effective business continuity and crisis management plans

K9   the resources that are required to deliver effective business continuity and crisis management plans

K10   the risk escalation processes that are in place and the mechanisms by which management have the responsibility to notify the governing body when the risk exposure approaches the maximum level that the organisation is willing to tolerate

CFAGOR7

Ensure the organisation has effective business continuity and crisis management systems

---

Links to other NOS   Refer to core Governance NOS (2011) suite.

CFAGOR7

Ensure the organisation has effective business continuity and crisis management systems

Developed by	Skills CFA
Version number	1.0
Date approved	January 2013
Indicative review date	January 2016
Validity	Current
Status	Original
Originating organisation	Skills CFA
Original URN	CFAGOR7
Relevant occupations	1000 Managers and Senior Officials 1112 Directors and chief executives of major organisations, 1114 Senior officials of special interest organisations 1131 Finance Managers and Chartered Secretaries 1135 Personnel, training and industrial relations managers 2000 Professional Occupations 2421 Chartered and certified accountants 2422 Management accountants 4000 Administrative and Secretarial Occupations 4214 Company Secretaries
Suite	Governance of Risk (2013)
Key words	Governing Body, Governance structure

CFAGOR8
Reporting to stakeholders on risk, the mitigation of risk
and internal control

Overview

This Standard is about the governing body's role in communicating to the relevant stakeholders that there is an on-going process for identifying, evaluating and managing the risks faced by the organisation. It is about the disclosure of the key risks that the organisation face and the mitigation put in place to address those key risks. It is about communicating to stakeholders what the governing body's role is and what the governing body has done throughout the reporting period.

CFAGOR8

Reporting to stakeholders on risk, the mitigation of risk and internal control

Performance criteria

You must be able to:

P1 report on the organisation's key risks by addressing any changes to the organisational strategy and future developments and the implications for exposure to risk

P2 disclose how you have monitored the robustness of contingency and resilience planning for risk threats and opportunities

P3 report on how the organisation has reviewed, challenged and approved management's information on risk management

P4 report on strategically significant risks and on organisational risk oversight by linking risk reporting to discussion of the business model

P5 disclose any risk oversight challenges that have emerged over any reporting period and explain actions taken or planned to be taken to address them

P6 articulate how the organisation ensures that broader economic risks and systemic risks that could affect the organisation are taken into account

P7 have consideration for the impact of the disclosure of commercially sensitive risks to stakeholders

CFAGOR8

Reporting to stakeholders on risk, the mitigation of risk and internal control

Knowledge and understanding

You need to know and understand:

K1   how to communicate effectively to stakeholders on the significant risks as they relate to the business model

K2   how to embed reporting on risk into narrative reporting

K3   how risk updates are presented to the board for assurance

K4   how to highlight to stakeholders changes to organisational strategy following a risk event

K5   how to clearly demonstrate to stakeholders the levels of assurance obtained by way of independent and third party verification

K6   the current regulatory framework of disclosure and stakeholder engagement

K7   the potential impact of the disclosure of commercially sensitive risk information

CFAGOR8

Reporting to stakeholders on risk, the mitigation of risk and internal control

Links to other NOS Refer to core Governance NOS (2011) suite.

CFAGOR8

Reporting to stakeholders on risk, the mitigation of risk and internal control

Developed by	Skills CFA
Version number	1.0
Date approved	January 2013
Indicative review date	January 2016
Validity	Current
Status	Original
Originating organisation	Skills CFA
Original URN	CFAGOR8
Relevant occupations	1000 Managers and Senior Officials 1112 Directors and chief executives of major organisations, 1114 Senior officials of special interest organisations 1131 Finance Managers and Chartered Secretaries 1135 Personnel, training and industrial relations managers 2000 Professional Occupations 2421 Chartered and certified accountants 2422 Management accountants 4000 Administrative and Secretarial Occupations 4214 Company Secretaries
Suite	Governance of Risk (2013)
Key words	Governing Body, Governance structure