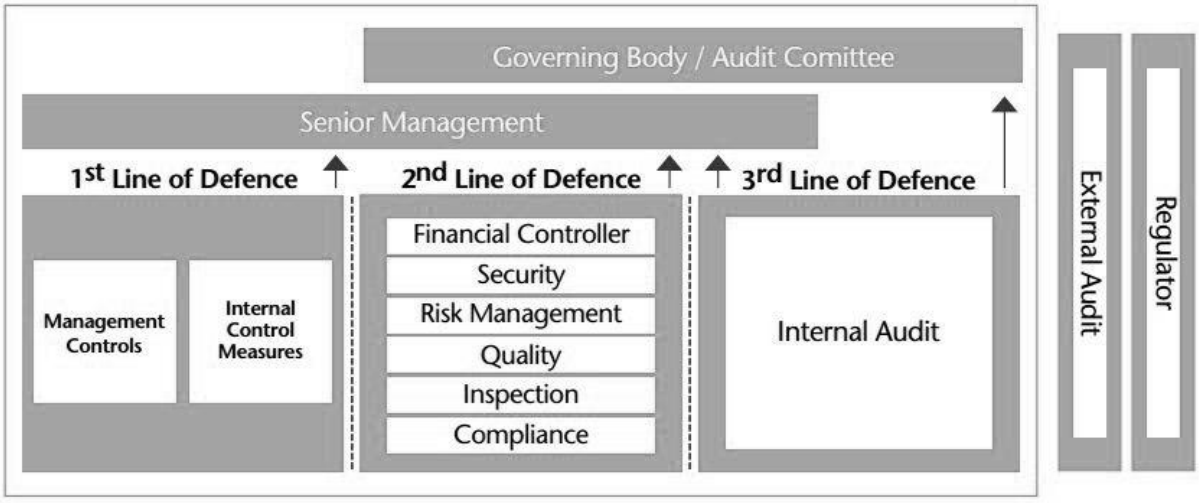
icsa
The Chartered
Governance
Institute

## ICSA Qualifying Programme

# Risk Management

**Sample mark scheme 2019**

# Section A

| Question number | Indicative content |
|---|---|
| 1(a)<br>14 marks | As the questions specifically mentions the 'three lines of defence' model it is expected that answers will show an understanding of this framework as a method of risk control within the governance framework of an organisation. If an alternative structure or framework is mentioned, then marks can be awarded as long as the argument around such structure or frame work shows a robust understanding of how and why it could be applied in the control of risk.Students must ensure that they align their comments with the case study.<br><br>**Answers could include the following content:**<br><br>Many organisations have now adopted, or at least claim to have adopted and implemented, a modular approach to control of risk, referred to as the *'three lines of defence*'. The starting point for this is the model itself, which illustrates the segregation of duties between:<br>• The operational ownership and management of risk within the organisation.<br>• The professional oversight of risk within the organisation.<br>• The objective consideration of risk from an independent, if sometimes internal, perspective.<br><br>*NB – the model illustrated in this indicative answer is an expanded version of the classic 'three lines of defence' model for illustrative purposes.*<br>  <br><br><br>The model recognises the same need as the FRC (Guidance to Audit Committees, and Guidance on Board Effectiveness) for a holistic approach to the control of risk, with a significant action between operation and governance.<br><br>The case study scenario suggest that Chocs has no holistic approach to assessing risk across its different sites. A framework such as the 'three lines of defence' would enable the Chocs directors to take an appropriate view of top-down governance and control of risk within Choc, and to decide how, when and where further intervention might be required.<br><br>Although the governing body are not perceived as one of the core '3 lines', they are depicted as the ultimate internal organisational recipient of assurance from the individual defence mechanisms. Note that the regulator and the external audit function, although included in the model, are both viewed as being outside the control structure, and perhaps are seen as both having some external observational role, but with minimal real influence over effective control. |

| | |
|---|---|
| | The first line includes control measures that have been built into the internal processes and the direct management oversight and control of risk within the organisation. These controls are accountable to the senior management, who in turn are accountable to those empowered with governance, often through a direct interaction with the audit or risk committee.<br><br>At Chocs this would seem to happen at the different sites, but with each site having developed its own approach to satisfy the particular regulatory requirements within its particular jurisdiction. There is insufficient detail within the case study, but we could assume that each site has developed its own management controls and internal control measures. The big gap for Chocs would appear to be the lack of senior management oversight as required by the model, and therefore a further gap when this moves to the top of the model and the governing body oversight.<br><br>The second line includes a range of professional control functions, each empowered with the scrutiny, oversight and control off the direct risks of the organisation. These people are likewise accountable to the senior management, who in turn are accountable to those empowered with governance, under these professionals will frequently have a direct interaction and reporting line (straight or dotted) to the audit or risk committee.<br><br>The case study suggests that individual Chocs sites have a high level of autonomy for their own risk oversight and control. We could therefore assume that the particular roles identified in the 2nd line of defence are carried out at a local level. As with the comment above on the 1st line of defence, the gap would then appear to be the summation of risk information by the team in Ireland, resulting in only overview charts ever reaching the directors of Chocs.<br><br>The third line is the internal audit function within an organisation. This is depicted as having a dual reporting structure, to both senior management and those empowered with governance. The link between the internal audit function and the audit and/or risk committee is often perceived as a firm reporting line. The FRC Code and Guidance suggests that where an internal audit function does not exist, an important role of an audit committee is to assess on an annual basis this perceived gap in the control structure.<br><br>There is currently no internal audit function at Chocs, despite the external auditors having recommended this for the past few years; the latter having been rejected by Ben and Kenneth. The NEDs would appear to have been negligent in their risk oversight role by not having challenged this rejection. What else do they have to rely on to give them the assurance that they require to enable them to diligently fulfil their risk and control responsibilities?<br><br>The process of implementing a 'three lines of defence' risk control framework would enable Chocs to take a renewed, refreshed and much needed review of its whole approach to risk. It would ensure appropriate measures and controls were established holistically at the different levels within the organisation, rather than just leaving it to each site. Equally importantly it would ensure that the Chocs directors were taking a correct and proper approach to their accountability for the risks within the business. |

| Level | Mark | Descriptor |
|---|---|---|
| | 0 | No rewardable material. |
| **Level 1(Fail)** | 1-7 | • The answer gives a very basic definition and overview of the 'three lines of defence' and its relationship to risk control.<br>• The answer makes few, if any, links between theory and practice.<br>• The answer makes only limited use of the case-study material.<br>• The answer includes only limited comment as to how and why effective risk control is required within an organisation. |
| **Level 2 (Pass)** | 8-9 | • The answer gives a clear definition and overview of the 'three lines of defence' and its relationship to risk control.<br>• The answer illustrates and shows an understanding of how the theory of risk control and the use of a framework such as 'three lines of defence' is brought into practice in an organisation.<br>• The answer aligns the risk comments with the requirements in the case study organisation.<br>• The answer includes analysis as to how and why effective risk control is required within an organisation. |
| **Level 3 (Merit/Distinction)** | 10 -15 | • The answer gives a strong and comprehensive definition and overview of the 'three lines of defence' and its relationship to risk control.<br>• The answer illustrates and shows clear and strong links between the theory and practice of risk control (using a framework such as the 'three lines of defence') further illustrated by real-world examples.<br>• The answer makes good use of the case study material in identifying how the 'three lines of defence' could be used within the organisation.<br>• The answer includes an argued and detailed analysis as to how and why effective risk control is required within an organisation, illustrated by real-world examples. |

| Question number | Indicative content |
|---|---|
| 1(b)<br>10 marks | Answers require a definition and explanation of the meaning of Enterprise Risk Management (ERM). This then needs to identify the people that would be required at Chocs to delivera successful ERM initiative.<br><br>**Answers could include the following content:**<br><br>TheCOSO (Treadway Commission) definition of ERM is as follows, [whilst candidates would not be expected to replicate this in detail, the essence of it would need to be included within their answer]:<br>"Enterprise Risk Management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."<br><br>**Enterprise Risk Management (ERM)**<br>• An extension of the standard risk management process<br>• Important to recognise it as a 'process' that is still based around the core process of identification-assessment-monitoring-control<br>• The difference from a standard process is the three core aspects of the philosophy that underpins ERM:<br><br>1. Holistic focus<br>o ERM must applied across an entire organisation, recognising the interconnected nature of all processes, function, people and risks<br>o Avoidance of silo management and control<br>o Development of an integrated risk function, looking at risk across an organisation<br>o Chocs would need to consider how to develop a whole-business approach to risk, rather than its current fragmented approach.<br><br>2. Emphasis on value added risk management<br>o Under many standard models, risk control is seen as a cost applied to a business – eg Health and Safety which often has only an intangible benefit whilst reducing the bottom line of profitability<br>o In ERM each activity needs to be viewed as adding or protecting value. This requires an organisation to focus on more than its bottom-line profitability and to recognise the financial values associated with protection rather than just its income drivers<br>o Risk needs to be seen as a necessary part of any strategic project or process, the cost of risk control is therefore built into the viability from the start rather than (as often happens in standard risk control) being seen as a cost later in the process.<br>o At Chocs, risk control would appear to be seen as a reactive task rather than as a value-adding proactive process. An ERM approach would enable the directors of Chocs to assess and understand how and why a proactive approach to risk management can add value throughout an organisation by prevention rather than cure.<br><br>3. Blending of formal and informal tools and activities<br>o Formal aspects of the control process would include tangible systems, processes, |

procedures, policies, committees and forums

- Informal aspects of the control process would include organisational culture, social networks, and the internal and external perception of risk and risk management for a particular entity.
- The disparate approach at Chocs suggest that there are different approaches being taken to risk management at different sites. Not all of these Chocs approaches can be bad, or the business would not have continued to succeed in the way that it has. The directors could take an ERM approach to analyse and determine the optimal approach for a cross-business risk management structure.

**Roles and people involved in successful delivery of an ERM initiative**

- The **directors** retain ultimate accountability, set the strategic direction, recognise the risks associated with the strategic objectives, ensure that appropriate control measures are established. This basic understanding of ownership and accountability needs explaining and emphasising to the directors at Chocs.
- In an ERM scenario the role of **Chief Risk Officer (CRO)** (or its equivalent) is established to ensure that the risk management process is viewed from a holistic perspective. This person will
  - Support the board and the risk committee (or its equivalent)
  - Direct the work of the risk function within the organisation
  - Oversee risk management activities across all aspects of the organisation, ensuring uniformity of approach and alignment of differing drivers
  - Work with compliance and internal-audit functions as appropriate
- The **Risk Manager** will oversee, co-ordinate and facilitate risk management activities across a particular site or area within an organisation. This person is responsible to the CRO.
- The **Compliance Manager** will ensure that the design and ongoing operation of an organisation's risk management processes are compliant with all applicable rules, regulations and sector guidance, as appropriate. This person will need to work closely with the risk manager.
- It would be safe to assume that these latter three roles probably do not exist at Chocs, but the directors need to be aware that the tasks within each role still need to be fulfilled even if by a different person within the organisation.
- An I**nternal Audit** function (where it exists) will have a role in providing assurance that the risk management process is effective in terms of design and implementation. This role is to step back, look and listen and determine whether what was planned is actually happening, and if not, why not. As commented above, this role does not currently exist at Chocs despite the recommendation of the external auditors. This would appear to be a priority requirement for Chocs irrespective of whether they decide to follow an ERM approach.
- The **Company Secretary or Governance Professional** will often have a role in ensuring that the directors of an organisation have appropriate visibility of the core aspects of the process, and that relevant matters are included on the appropriate board and committee agenda. It is important that the Company Secretary at Chocs fully understands, is involved in, and helps to drive this initiative.

| Level | Mark | Descriptor |
|---|---|---|
| | 0 | No rewardable material. |
| **Level 1 (Fail)** | 1-4 | • The answer includes a basic description of ERM and the various roles involved.<br>• The answer demonstrates a limited understanding of ERM.<br>• There is little or no evidence of how ERM needs to be driven through an appropriate people structure.<br>• The answer makes limited use of the case-study scenario to differentiate between theory and practice in this area of risk control. |
| **Level 2 (Pass)** | 5-6 | • The answer includes a good description of ERM and the various roles involved.<br>• The answer demonstrates a reasonable understanding of ERM.<br>• There is good evidence of how ERM needs to be driven through an appropriate people structure.<br>• The answer makesuse of the case-study scenario to differentiate between theory and practice in this area of risk control. |
| **Level 3 (Merit/Distinction)** | 7-10 | • The answer includes a strong and robust description of ERM and the various roles involved.<br>• The answer demonstrates an in-depth understanding of ERM.<br>• There is strong evidence of how ERM needs to be driven through an appropriate people structure.<br>• The answer makes strong use of the case-study scenario to differentiate between theory and practice in this area of risk control.in practice. |

| Question number | Indicative content |
|---|---|
| 2(a)<br>15 marks | Answers need to identify a range of the risks that are apparent at Chocs, discuss how and why it is useful for directors to be able to define and understand risk and why the categorisation of risks can help in their management and control. As part of the overall discussion in the 'paper' that has been asked for, students need to be clear of the particular differentiations asked for in the question – risk versus uncertainty and controllable risks versus uncontrollable risks.<br><br>The tabular form included below is only a suggestion for clarity in this indicative answer.<br><br>**Answers could include the following content:**<br><br>It is apparent that risk is low on the Board agenda for the directors of Chocs, so we need to firstly understand what is meant by risk, and the type of risk that are identifiable at Chocs. Risk has different meanings within different contexts but generally refers to some type of exposure to danger, threat or change from an intended plan or route. In business the term risk often refers to unintended outcomes which directly or indirectly could cause monetary loss and hence challenge the viability of the organisation.<br><br>Risk is generally viewed with negative connotations, but the reality is that all organisations, and all people, need to take risk throughout their existence. The future is unknown, so to move forward into the future requires the taking of risk – how safe is it for me to cross the road?<br><br>The terms risk and uncertainty are often used interchangeably but there is a practical and distinct difference between them. They both indicate the exposure to danger, threat or change suggested above, however:<br>• risk is generally used to describe situations where two or more possible outcomes can be envisaged and can therefore be quantified – at a further level of complexity this forms the basis of much mathematical consideration of risk with the calculation of probability and the use of standard deviation to determine how, when and why there is correlation between risk drivers and the risk outcome.<br>• uncertainty is generally used to describe situations where it is recognised that there is more than one possible outcome, but it is not possible to define or quantify what the different outcomes might be<br>• if I press a light switch my 'risk' is that the light in the room to either work or not, the result will be obvious, I will know whether the light is on or off<br>•<br>if I press a fire alarm button, but do not then immediately hear any alarm sounding, I am 'uncertain' as to how or where any alarm might be sounding, or whether the switch is even working, I do not know whether my action has had any effect at all<br>A controllable risk is something where I have at least some choice as to whether or not I take the risk – to use the same analogy as above, I make the choice as to whether or not I cross a road, and where I cross it.<br>• At Chocs, there is a choice as to the level at which appropriate health and safety measures are implemented on the different sites<br><br>An uncontrollable risk is the potential for something to happen where I have no influence – a piece of brick falls off a building as I walk past and hits me.<br>• At Chocs, a particular site might be hit by a flood or a fire – whilst protective measures might have been put in place, the driving cause of a flood or a fire is likely to have been outside the control of management. |

**Categorisation of risks and examples at Chocs**

| Category | Impact | Chocs example |
|---|---|---|
| Business risk | the underlying business rationale fails often leading to successive losses | Susan has identified that business success varies from site to site and therefore so must the business risk<br><br>there is no mention of technology within the case-study, but an increasing awareness of cyber risk would be an important aspect of risk for the Chocs directors |
| Credit risk | restricted access to funds or supplies | there is no evidence of this at Chocs in the case-study, but this can be influenced by the reputation of the organisation, so recent accidents and the Indian media coverage might cause a problem |
| Market risk | customers start to use other suppliers | one of the reasons given for recent lower profitability is the increased competition – customers are going to alternative suppliers |
| Liquidity risk | cash not available to pay employees or other creditors | no evidence of this at Chocs |
| Operational risk | the supply chain or business chain fails | part of the review that is wanted by Susan is to look at the operational effectivenss of the different sites and potentially the need to move to specialisation |
| Reputational risk | image and integrity are damaged | the approach to the accidents and deaths by the Chocs directors suggests that they have little concept of reputational risk, in today's media world of rapid communication, the reputation of the entire business worldwide could be rapidly damaged by the reports that have appeared in the Indian media |

| Level | Mark | Descriptor |
|---|---|---|
| | 0 | No rewardable material. |
| **Level 1 (Fail)** | 1-7 | • The answer does not define risk.<br>• The answer does noexplain or identify different categories of risk.<br>• The explanations of risk, uncertainty and control are superficial and not linked to the case study.<br>• The answer illustrates only a basic understanding of risk and why it is important for the directors of the case study company. |
| **Level 2 (Pass)** | 8-9 | • The answer gives a reasonable definition of risk.<br>• The answer explains and explores well the different categories of risk.<br>• The explanations of risk, uncertainty and control are relevant and have been linked to the scenario from the case study.<br>• The answer illustrates anunderstanding of risk and why it is important for the directors of the case study company. |
| **Level 3 (Merit/Distinction)** | 10-15 | • The answer gives robust definition of risk using examples.<br>• The answer shows a deep understanding of the different categories of risk and why they matter to directors.<br>• The explanations of risk, uncertainty and control are developed and discussed with appropriate depth, and have been well linked to the scenario from the case study.<br>• The answer illustrates a clear and thorough understanding of risk and why it is important for the directors of the case study company. |

| Question number | Indicative content |
|---|---|
| 2(b)<br>10 marks | Answers should discuss the relevance of risk categorisation and also the risk management processes of identification, assessment, monitoring and control.<br><br>**Answers could include the following content:**<br><br>The purpose of using a risk management process or framework is to provide an organisational discipline, approach and consistency to the management of risk. Although many complex frameworks have been developed over the years, at their core they all include the four process basics mentioned in the question.<br><br>This fundamental approach would be useful for the Chocs business as it seems to have no uniform or structured approach to risk across the business. The ability to categorise risks as suggested in the answer to 2(a) requires an understanding and recognition of the risks and whether they are within the direct control or otherwise of the organisation.<br><br>**Identification**<br>• how do we (Chocs) know that a risk exists, who are we expecting to recognise, identify and categorise that risk?<br>• at each site we need to have risk officers who have a good knowledge of the site, its operations and its people, and use their network of contacts to bring risk awareness to all employees<br>• we (Chocs) need to develop a means for identified risk to be fed back to whoever has overall control of risks<br><br>**Assessment**<br>• we (Chocs)need to establish risk champions within the business, these would probably be at site level, but would need to report into a head-office function to ensure we are able to capture the holistic risk picture within the organisation<br>• we (Chocs) need to determine who the right person (or people) are to be able to assess the dimensions of identified risks – this will often plot likelihood against potential impact<br><br>**Monitoring**<br>• having established the existence and importance of a risk, we (Chocs) need to develop a means of monitoring that risk to the business and how it changes<br>• a risk is only ever a perception of one or more people at a moment in time, and different people will have different perceptions based on their biases, so we (Chocs) need to develop a robust process of consistent monitoring, with a resultant audit trail type record, to capture changes in the factors driving different risks<br><br>**Control**<br>• we (Chocs) need to determine the level of control that we can or cannot place on a particular risk<br>• we (Chocs) need to determine whether the 'threat is a risk which we can control, a risk which lies outside our control, or an uncertainty. In the case of the former we can place a control framework around the perceived risk and thus mitigate the likelihood of the risk delivering a negative outcome. In the case of the latter two, we can only look to mitigate any potential impact. |

| Level | Mark | Descriptor |
|---|---|---|
| | 0 | No rewardable material. |
| **Level 1 (Fail)** | 1-4 | • The answer does not to provide a differentiation between identification, assessment, monitoring and control.<br>• There is minimal or no use of the case study scenario in the answer.<br>• There are no recommendations as to how the case-study company could implement the risk control process. |
| **Level 2 (Pass)** | 5-6 | • The answer provides a clear differentiation between identification, assessment, monitoring and control.<br>• Each of the dimensions of the risk control process arelinked to the case study scenario.<br>• There are recommendations as to how the case-study company could implement the risk control process. |
| **Level 3 (Merit/Distinction)** | 7-10 | • The answer provides a detailed differentiation between identification, assessment, monitoring and controlillustrate the answer from the case study or other external examples.<br>• Each of the dimensions of the risk control process are fully linked to and use examples from the case study scenario.<br>• There are clear and challenging recommendations as to how the case-study company could implement the risk control process. |

| Question number | Indicative content |
|---|---|
| 3<br>25 marks | This question requires students to provide a comprehensive answer which brings together a number of areas from throughout the syllabus but within the context of emerging risks that resonate throughout Section C of the syllabus – risk and the business environment. The conjoined themes, as discussed separately below need to include board awareness, emerging risks, stakeholder challenge and the increasing awareness of and need for CSR (sustainability and social). The answer will need to demonstrate that the student is able to see how a common series of 'risk' threads run through each of these aspects of the business and its environment.<br><br>**The answers for each of these areas could include the following content:**<br><br>**[To score well it will be necessary to show how they are all inter-related; there is just one indicative version of this at the end of this answer, but there are many options that could be equally valid as an answer.]**<br><br>**Board awareness**<br>• A Board of directors has overall responsibility and accountability for the use of the assets of an organisation to drive success for the members, in the light of a sound board awareness of the stakeholder impact and expectations (Companies Act 2006 s172)<br>• The assets can be used in a number of ways on a dynamic from risk averse to risk seeking. In an ideal governance scenario the Board will be determining this approach (appetite) to risk, but as a minimum the Board (as the accountable body) needs to have a good awareness of all that is happening within the business, both in terms of risks being taken to deliver the operations, and risks that are anticipated in the delivery of the strategic objectives.<br>• At Chocs, based on the case-study provided, and the notes included towards the end, it is clear that there is very limited, if any board awareness. There is an inner sanctum of people (Ben, Susan and Jeremy)who meet to make all decisions (and it can be assumed this includes short and long-term risk decisions).<br>• There is a very apparent lack of independence around the Chocs board table, and it would be reasonable to surmise that most directors have only a limited awareness of operational risks being taken and the risks that are perceived through the strategy.<br><br>**Emerging risks**<br>• Emerging risks can fall broadly into two categories, known and unknown. This is mentioned by Susan at Chocs in her discussion with you as the company secretary. She has developed an awareness of the need to consider what are known as 'black swan' events, or sometimes called the unknown unknowns, as referred to by Donald Rumsfeld in 2002 when talking about whether Iraq was holding weapons of mass destruction.<br>• Known emerging risks can be anticipated, appropriate mitigation or protection can be determined and put into action. A Board of directors needs to be able to understand such risks, whilst challenging the appropriateness of the perceived action by the organisation.<br>• At Chocs such risks might emanate around Brexit, the advancement of IT and artificial intelligence, the political risks within the different countries that Chocs operates, and the likely restrictions on carbon emissions etc that are increasingly part of the 'green' agenda.<br>• Unknown emerging risks are, by their nature, difficult to protect or mitigate against. A board of directors needs to have an awareness of the existence of 'black swan' risks and to ensure that the organisational structure is agile and rigorous enough to handle such risks as they appear.<br>• At Chocs such risks are, but their nature, only to be imagined, otherwise they could be classified as known risks. Such 'unknown' organisational risks will however be driven by |

only a restricted number of drivers – people, politics, power – and the Board needs to be aware of how each of these areas is monitored and assessed to ensure that an the emergence of a 'black swan' risk is rapidly noticedwithin the business.

**Stakeholder challenge**

- The stakeholder agenda has become a dominant feature of corporate life. The Board of Chocs, as an AIM listed company, needs to have a keen awareness of their stakeholders and their accountability to such stakeholders.
- As already referred to, this is epitomised in the UK in s172 of the CA2006, together with the new s414 requirements for directors to state in their annual report, and on their website, how they have met their responsibilities
- In particular there is the need to recognise a short and long-term responsibility to shareholders, employees, customers, suppliers, government, local community and the wider environment within which a business operates.
- All we are really able to say with regard to Chocs in this regard is that the evidence from the case-study would lead to an assumption that such matters are never discussed at board meetings, but that they ought to be. Ignorance is no defence in law, directors' duties are a statutory requirement and each director at Chocs, not just the inner family group, need to take equal responsibility.

**Sustainability and social responsibility**

- The wider sustainability and corporate social responsibility expectations from organisations have grownexponentially within recent years. Boards of directors need to understand the impact that their organisation is having on the environment.
- At Chocs there will be a variety of differing expectations based around their different operating environments, each with their own country and political regulatory drivers. The reputational risk associated with these is that the media broadcast or publish stories (true or untrue) about the organisation which has a detrimental effect.
- The ethos of Chocs has always been to work with and support the farmers of the cocoa beans. This has recently been challenged, incorrectly it would seem, but the resultant media campaign might cause reputational damage to the whole organisation.
- Another aspect of this for Chocs to consider, given the nature of the business, might be the writing of an Integrated Report in line with the recommendations of the International Integrated Reporting Council.

All of these aspects are close aligned.

An organisation belongs to its members but has a much wider stakeholder responsibility. A Board of directors needs to have a finely tuned awareness of its stakeholder, their power and their expectations. These can be aligned to the current and the emerging risks of the organisation. It is quite possible that emerging risks can be managed more effectively through a closer stakeholder alignment, but that would require focused board awareness.

| Level | Mark | Descriptor |
|---|---|---|
| | 0 | No rewardable material. |
| **Level 1**<br>**(Fail)** | 1-12 | • The answer attempts to explain the importance of emerging risks but fails to align it to the stakeholder sustainability and board awareness.<br>• The answer provides few links to the case-study scenario.<br>• The answer makes few or no links between theory and practice.<br>• The answer includes no critical analysis of the stakeholder challenges at Chocs. |
| **Level 2**<br>**(Pass)** | 13-16 | • The answer provides an explanation of the importance of emerging risks and begins to explore why they need to be aligned to stakeholder sustainability and board awareness.<br>• The answer provides good alignment with the case-study scenario.<br>• The answer makes links between theory and practice.<br>• The answer includes critical analysis of the stakeholder challenges at Chocs. |
| **Level 3**<br>**(Merit/Distinction)** | 17-25 | • The answer provides a clear and focused explanation of the importance of emerging risks and explores why they need to be aligned to stakeholder sustainability and board awareness.<br>• The answer links the thought process to underlying theories and illustrates how and why the directors within the case-study scenario need to be challenged in their awareness of emerging risks.<br>• The answer makes strong links between theory and practice.<br>• The answer includes good critical analysis of the stakeholder challenges at Chocs. |

| Question number | Indicative content |
|---|---|
| 4 | Answers should be set out as a report and should demonstrate a robust understanding of the nature and purpose of a risk register, and be able to align this with facts and assumptions that can be made from the case study scenario. Answers should discuss the importance of the capturing of data (risks) to be included within the risk register and how the register could then be used as a stimulant to board discussion through summarised reporting and/or graphics.<br><br>**Answers could include the following content:**<br><br>**Risk registers**<br>• Used to store and monitor the results of risk assessment activities<br>• Acts as a database of past, current and perceived risks, to enable learning from the past and mitigation of the future<br>• Often an organisation has more than one risk register, these might be held by department, or by business function. From a director perspective it is important that there is a consistency of approach and method, together with a transparent and thought-out route for the distillation of risks on a number of registers to the main risk register which is used for board and committee reporting.<br>• The case study suggests that at Chocs there are individual risk registers at each site, but that there is no cohesive approach to their amalgamation or aggregation. Further than that the directors of Chocs seem to only ever have access to heavily summarised risk data in the form of charts, Whilst this type of presentation might not, in itself, be a problem, it is key that directors have visibility of and full access to the audit trail that sits behind such graphics.<br><br>**Risk identification and selection**<br>• There are a number of key questions that an organisation needs to answer before it starts to compile or maintain a risk register<br>  ○ How to identify and compile the risks that it faces?<br>  ○ How to devise appropriate metrics to decide whether or not a risk should appear on a risk register?<br>  ○ How to determine and measure likelihood and impact?<br>  ○ How to set the tolerance boundaries for the different risk registers that might exits for different areas and at different levels? EG a risk of a machine breaking down and interrupting a day of production might be significant at the shop-floor level but might be immaterial at the 'plc' level.<br>• At Chocs there does not seem to be any coherent or strategic approach to this gathering of risks. Each site keeps their own version of a register, and these are then amalgamated using a spreadsheet by the employees at the site in Ireland.<br><br>**Risk register structureand presentation**<br>• The structure of a risk register itself can be determined by an organisation. There is no right method, but there are plenty of wrong methods.<br>• The precursor is to decide what, as an organisation, you want to be able to see<br>• The need to set an appropriate level of granularity (this will clearly be quite low at an individual site or section, but much higher when it reaches board level). An important aspect of the controls is to ensure that low level, but high impact incidents manage to find their way through a series of layers to still appear at a board level, so directors have clarity as to what is happening. |

| | |
|---|---|
| | • This latter point would seem to be a serious 'gap' within the system at Chocs. The directors seem to have been made aware of the accidents and deaths, but there is no record of their level of concern or actions that they have taken in this regard.<br>• The danger of a cumulative risk register is that it becomes quickly over-populated with entries, there needs to be a way of segregating past, present and future – recognising that we are always faced with immediate risk at the present moment, but for most directors, in normal circumstances, it is the risk into the future that should maintain their focus.<br><br>• At Chocs, the aspects that could usefully be included, or available, at a Board level within a register, rather than perhaps just being shown in charts are:<br>o Tracking of H&S incidents as a cumulative business, but broken down into individual sites; this would need to include seriousness, frequency, and likelihood of any follow-through by a regulatory authority<br>o Clarity around deaths that have occurred on Chocs sites – this would need appropriate detail for directors to be able to take any action required. If UK, or UK related, there might be the risk of corporate manslaughter charges; in other countries similar legislation exists so the Chocs directors need total clarity. Such incidents can cause tangible damage through the pursuit of legal challenge but can also cause (often more quickly and with greater speed) significant reputational damage through media reporting, and word-of-mouth communication from employees.<br><br>• A well-constructed risk register would enable the Directors at Chocs to have better visibility and knowledge of the organisation through robust indicators, and granular details where there is a serious impact potential of the following key areas of risk:<br>o operational risk (what is happening on the ground at each site, probably with some sort of comparative rankings between the sites)<br>o financial risk to show the impact of strategic change in the business. It is implied that Reggie has control and oversight of this, but it is not clear that it is ever shared in detail with the whole<br>o cyber risk – there is no mention of this in the case study other than in the notes on Susan's concerns – this needs addressing immediately<br>o shareholder risk – concerns in the AIM market at declining financial performance from Chocs<br>o CSR and wider stakeholder and environmental risks – Stefan has raised this; Susan is concerned but so far it has not formed part of the board agenda |

| Level | Mark | Descriptor |
|---|---|---|
| | 0 | No rewardable material. |
| **Level 1 (Fail)** | 1-12 | • The answer shows minimal or no understanding of the purpose of a risk register.<br>• The answer makes only limited or no use of the case study scenario<br>• The answer makes a few or no links between theory and practice.<br>• The answer has little or no analysis or challenge of the principles and practice involved generically and within the case study scenario |
| **Level 2 (Pass)** | 13-16 | • The answer shows a reasonable understanding of the purpose of a risk register.<br>• The answer makes good use of the case study scenario and identifies many of the risks facing Chocs. |

| | | |
|---|---|---|
| | | • The answer makes relevant links between theory and practice.<br>• The answer has reasonable analysis or challenge of the principles and practice involved generically and within the case study scenario. |
| **Level 3 (Merit/Distinction)** | 17-25 | • The answer shows a good and thorough understanding of the purpose of a risk register and illustrates this with examples.<br>• The answer makes extensive use of the case study scenario identifying and expanding upon a range of different aspects of the risk scenario at Chocs.<br>• The answer makes strong links between theory and practice illustrating that the candidate has a thorough understanding of the area of risk and risk registers.<br>• The answer makes strong use of analysis or challenge in considering the principles and practice involved generically and within the case study scenario. |

# Section B

| Question number | Indicative content |
|---|---|
| 5<br>25 marks | Answers should be written in an appropriate manner to present to the new non-executive directors. It would be reasonable to expect such a paper to commence with some general comments as to the meaning of risk and why it matters to any organisation. In particular there should be a comment as to how and why organisational risk has to be owned and led by the directors and senior management of an organisation. As this is intended as a guidance note it might also be good to suggest some sort of alignment between risk culture, appetite and tolerance before discussing the details.<br><br>**Answers could include the following content:**<br><br>**Risk culture**<br>• Culture in general is often defined as "the way we do things around here", it is an intangible but important aspect of any organisation. It relates to the way in which employees collectively think, feel, perceive, act and behave.<br><br>• Risk culture is therefore a recognition of how risk fits within the wider culture of the organisation – if the organisation has a cautious and reserved approach to business, if so that is likely to also be its approach to risk; if the business has a market-challenging and bravado approach to its business, then that is likely to also be its approach to risk.<br><br>• Although there might be common traits, culture is unique to an organisation, driven by its particular mix of people. There is no right or wrong culture, culture exists at a moment in time but can also change through vision, drive or circumstance.<br><br>• In many businesses the assumption is that risk will be handled at the operational end of the business and that the directors only need to have broad summarised details, even with significant instances . This is never acceptable, and directors need to be kept fully informed.<br><br>• Risk culture will exist at different levels within any organisation and will often involve complex risk sub-cultures<br>• E.g. in an airline company a number of different risk cultures could easily be identified<br>o The board approach to risk culture will be defined by the directors in the aim of satisfying investor and stakeholder expectations (of course, these expectations may not always align with their own individual cultural beliefs and so will also be influenced by these).<br>o The risk culture of an individual flight will be determined by the pilot and his/her crew, and to a certain extent the weather. The crew reaction to stormy weather will change the 'culture' of the flight and will forward influence the reputation of the airline.<br>o The risk culture of each passenger will be determined by their own individual experience, fear or confidence, and expectations on that day from that flight.<br><br>• Risk culture within an organisation will influence, to a greater or lesser extent |

- The levels and types of risk that are taken
- The need for risk management and control procedures, and the importance attached to them: e.g. despite very similar operating expectations at all hospitals, the risk culture of any individual hospital will be established and led by the individual directors and management of that hospital, this will influence the employee and the patient experience.
- Approach and attitude to compliance
- Risk awareness throughout the organisation, which in turn will drive employee response to and reporting of perceived organisational risk

**Risk appetite**

- Risk appetite can be defined as the level of risk exposure that an organisation is prepared to accept; alternatively, it can be viewed as the willingness of an organisation to take risk in the pursuit of its strategic objectives. These two views are similar but subtly different
    - the former view aligns the risk to the organisation: e.g. by its nature a company mining for gold will be required to undertake risk as part of its modus operandi.
    - the latter view aligns the risk to the strategy of the organisation, with an underlying assumption that it is necessary for the organisation to take risk in order to deliver the strategic objectives: e.g. the same mining company might be prepared to take additional risks by mining deep mine shafts to reach a purer metal content, and therefore derive a high value product.

- Risk is a consequence of the need or desire to change.To understand risk appetite, we need to understand the need or desire from the perspective of the key players.

- Directors need to develop an understanding of their collective appetite for risk, and how this aligns with the views of the underlying owners of the organisational assets. In itself this can be an interesting process, because human bias would suggest that each director will have a slightly different tendency towards risk, so the first stage for a board of directors is to arrive at a collective perspective.The mans to achieve this will be partly determined by the underlying culture of the organisation.

- Risk appetite needs a close alignment with the wider company strategy. The governance iteration suggests that to achieve strategy will require risk, to undertake risk requires control, that control will then itself inform the realistic level of achievable strategic objectives.

- The textbook suggest that risk appetite has three core roles:
    - The support of risk management decisions
    - The support of strategic decision making
    - The underpinning of risk governance and internal control activities

**Risk tolerance and risk capacity**

- Risk tolerance is sometimes substituted for risk appetite, but they are different.

- Risk tolerance is however closely aligned with the concept of risk capacity
    - the capacity will suggest the maximum risk that could safely be encountered: e.g. a pharmaceutical company developing and testing new drugs will have the facilities to test ‘W’ number of patients before releasing the drug for governmental approval
    - the tolerance will suggest the advisable operating parameters – e.g. a minimum of G and a maximum of S; the same pharmaceutical company would need to

| | |
|---|---|
| | have tested ‘G’ number of patients as a minimum before seeking approval but knows that the testing authority would be happier if they had tested ‘S’ number fo patients<br><br>• Risk appetite is the need or desire to take risk, risk tolerance is the levels to which risk can or must be taken to maintain a viable business.<br><br>• Risk tolerance is usually measured through the use of metric measures. These apply on both sides of the risk dimension from a tolerance perspective. An organisation will have a minimum level of activity below which it must not fall and will have a maximum level of activity above which it should not operate.<br><br>• For example, in a manufacturing business there will be a minimal level of continuing orders that will be required to maintain the business, but there will also be a maximum number of orders that the capacity of the business can handle.<br><br>• Tolerance reporting is often linked to a Red Amber Green (RAG) approach where the boundary between the red and amber on both sides of a commercial projection is seen as the tolerance limit. Beyond those limits the risk can accelerate and cause long-term damage. |

| Level | Mark | Descriptor |
|---|---|---|
| | 0 | No rewardable material. |
| **Level 1 (Fail)** | 1-12 | • The answer attempts to differentiate between the three risk aspects identified in the question, but only provides a surface-level discussion.<br>• The answer demonstrates limited understanding of risk appetite, risk tolerance or risk culture.<br>• There is little or no understanding of the three risk aspects shown and no examples are given. |
| **Level 2 (Pass)** | 13-16 | • The answer differentiates well between the three risk aspects identified in the question, showing an understanding of how they are different.<br>• The answer demonstrates a good understanding of understanding of risk appetite, risk tolerance or risk culture. The answer illustrates clarity of thought as to how and why these aspects are essential perspectives in effective risk management.<br>• The answer shows a good understanding of the three risk aspects and includes examples. |
| **Level 3 (Merit/Distinction)** | 17-25 | • The answer provides a clear differentiation between the three risk aspects identified in the question, enhancing this through either example or direct comparison between the different approaches.<br>• The answer demonstrates a clear in-depth understanding of risk appetite, risk tolerance or risk culture. The answer include commentary as to when, how and why an organisation might use one or more of the different strategic pathways for development . The answer has been enhanced through developing the case-study scenario potential or through reference to other external organisations.<br>• There is a clear and detailed discussion of the three risk aspects; further enhanced by appropriate examples. |

| Question number | Indicative content |
|---|---|
| 6<br>25 marks | Answers need to show that risk is viewed as part of the underpinning structure for directors to deliver effective governance. In the UK Corporate Governance Code this is evidenced in Principle O which states<br><br>*"The board should establish procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives."*<br><br>There are many different ways in which this question could be answered, but to score good marks a student must be able to show a robust and through understanding of the relationship between risk and governance, and be able to recognise that the UK exists as one, but not the only model of governance, and further that in the UK our required approach to governance and risk is increasingly driven by the need to have a sound awareness of stakeholder expectations.<br><br>It is not expected that students will include any significant detail of non-UK corporate governance and risk approaches, but that they will simply identify a few key points so differentiation.<br><br>**Answers could include the following content:**<br><br>**FRC guidance and control**<br>In the UK corporate governance oversight currently rests with the Financial Reporting Council, although this non-statutory (member-led) organisation is in the process of being replaced by a regulatory organisation, reporting directly to the UK Government (NB possible name change to the Audit, Reporting and Governance Authority (ARGA)). As suggested above the core guidance around the alignment of risk with governance is covered in Principle O of the UK Corporate Governance Code, although there are, of course, many other mentions of risk throughout the various pieces of guidance.<br>Effective governance under Principle O could be interpreted as:<br>***Strategy*** *– what are we trying to achieve?*<br>***Risk*** *– how far can we risk the assets and reputation of the organisation to get there?*<br>***Control*** *– how do we know, as directors, what is happening in the daily operation of the organisation?*<br><br>**The UK comply or explain principle**<br>Corporate governance in the UK is built around the principle of 'comply or explain' The FRC Code obtains its validity through its adoption by the London Stock Exchange as a code of practice which it expects companies listed on its markets to adhere to. Such listed companies are expected to be able to demonstrate, and state in their annual report and accounts, that they **comply** with all aspects of the code. Where they do not think certain aspects of the code are appropriate to their particular organisation and its structure, they are able to **explain** how and why they are differing from the Code. It is then, generally, a matter of whether their market investors deem this to be appropriate or sufficient.<br><br>**Risk and the UK Corporate Governance Code 2018**<br>In addition to Principle O stated above there are two further main expectations<br>• The board should establish formal and transparent policies and procedures to ensure the independence and effectiveness of internal and external audit functions and satisfy itself on the integrity of financial and narrative statements.[7]<br>• The board should present a fair, balanced and understandable assessment of the company's |

position and prospects.

and further that

- The board should carry out a robust assessment of the company's emerging and principal risks. The board should confirm in the annual report that it has completed this assessment, including a description of its principal risks, what procedures are in place to identify emerging risks, and an explanation of how these are being managed or mitigated. (Provision 28 of UK Corporate Governance Code 2018)
- The board should monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness and report on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance controls. (Provision 29 of UK Corporate Governance Code 2018)

This underpins the robust approach that the UK take to the relationship between corporate governance and risk.

**The UK stakeholder approach**

A core aspect of 'governance' which has now entered the law in the UK is that of stakeholder awareness and transparency as to how a company is taking notice of the rights and expectations of its various stakeholders.

**The risk to directors here is that the governance within their organisation does not correctly fulfil all of the (now) statutory requirements and they could find themselves personally liable. Each director should know the details of section 172 Companies Act 2006 to ensure that their personal risk as a director is appropriately mitigated through**

- **robust boardroom discussion and challenge**
- **the new required reporting for companies classed as a Large Company under Companies Act 2006**

A reminder of section 172 CA 2006

*"A director of a company must act in the way he considers, in good faith, would be most likely to promote the success of the company for the benefit of its members as a whole and in doing so have regard (amongst other matters) to:*

*a) the likely consequences of any decision in the long term,*
*b) the interest of the company's employees,*
*c) the need to foster the company's business relationships with suppliers, customers and others,*
*d) the impact of the company's operations on the community and the environment*
*e) the desirability of the company maintaing a reputation for high standards of business conduct, and*
*f) the need to act fairly as between members of the company"*

The Companies (Miscellaneous Reporting) Regulations 2018 have added the following section into the Companies Act 2006:

**s414CZA**

***"A strategic report for a financial year of a company must include a statement (a "section 172(1) statement") which describes how the directors have had regard to the matters set out in section 172(1)(a) to (f) when performing their duty under section 172"***

This is applicable to all 'large companies as defined under the Act asone that satisfies 2 out of 3 of the following criteria:

- a turnover of more than £36million
- a balance sheet of more than £18million
- more than 250 employees

For the first time, directors of a significantly larger number of limited companies, not just the listed sector, now have a serious narrative reporting requirement – what is it that we do to comply with the

| | |
|---|---|
| | stakeholder expectations, and how can we evidence it, what is the risk if we fail to comply with this expectation?<br><br>**Other jurisdictions and different approaches**<br>• In Russia, Ivan will have been used to a corporate law structure regulated by the Civil Code of the Russian Federation. There is no specific regulation on corporate governance within Russia, but there are similar expectations around the behaviour of the various people involved within the corporate structure, but there is no mandatory reporting on social, environmental and ethical issues.<br>• Irish corporate governance regulations are very similar to those in the UK and their regulations for companies listed on the Irish Stock Exchange are included in the Irish Corporate Governance Annex<br>• Across Europe it has been challenging for different countries to develop a robust consistency, however one key point of difference is the composition of boards. In the UK we have a 'unitary' board structure, whereas countries like Germany have a 'dual' board structure comprising of a management board that reports to the supervisory board. The latter consists of external directors who are accountable to the shareholders.<br>• Some common aspects of risk and governance drive across Europe are<br>o The need for independent directors<br>o Enhanced disclosure requirements<br>o Encouragement of taking a long-term view of sustainability and moving away from a short-term profit-only vision.<br>• The World Bank has encouraged countries to focus on the promotion of transparency and accurate financial reporting, together with an improvement in the governance of state-owned enterprises.<br><br>*Rather than just continue this list in the sample answer, suffice to say that students who correctly mention one or two different regimes will be providing sufficient evidence of their understanding the UK way is not the only way!* |

| Level | Mark | Descriptor |
|---|---|---|
| | 0 | No rewardable material. |
| **Level 1 (Fail)** | 1-12 | • The answer provides only a basic definition and explanation of how governance and risk are aligned within the UK regulatory environment.<br>• The answer demonstrates a limited understanding of UK corporate governance and the risk dimension.<br>• The answer makes few or no links between theory and practice.<br>• The answer fails to mention any other corporate governance regimes and/or practices. |
| **Level 2 (Pass)** | 13-16 | • The answer provides a reasonable definition and explanation of how governance and risk are aligned within the UK regulatory environment.<br>• The answer demonstrates a good understanding of UK corporate governance and the risk dimension.<br>• The answer makes links between theory and practice.<br>• The answer discusses a non-UK corporate governance regime and/or practice. |

| | | |
|---|---|---|
| **Level 3 (Merit/Distinction)** | 17-25 | • The answer provides a strong definition and explanation of how governance and risk are aligned within the UK regulatory environment.<br>• The answer demonstrates a good and robust understanding of UK corporate governance and the risk dimension.<br>• The answer makes good links between theory and practice, using examples.<br>• The answer discusses a number of non-UK corporate governance regimes and/or practices. |