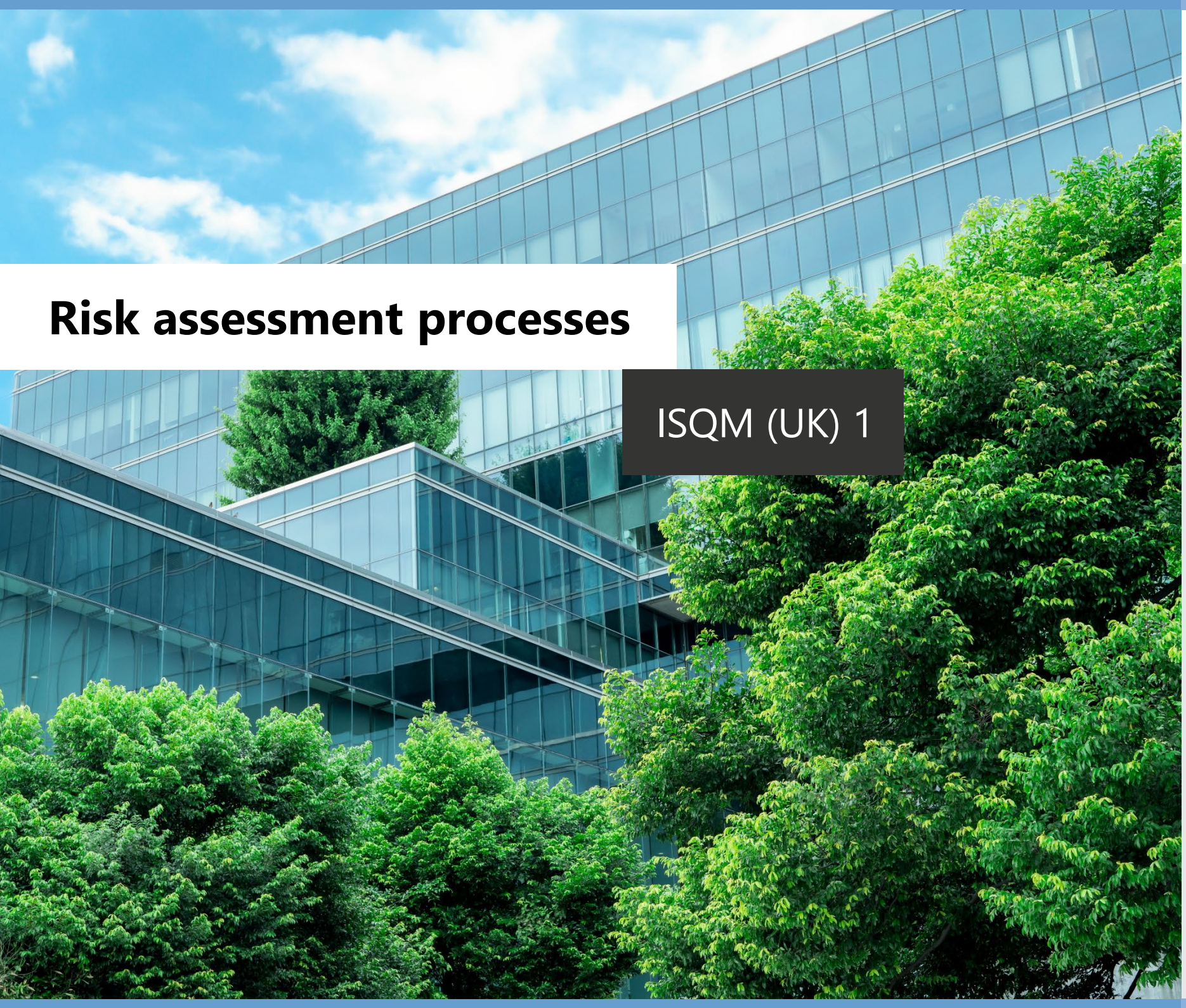


Financial Reporting Council

Risk assessment processes

ISQM (UK) 1

May 2026

Financial Reporting Council
13th Floor
1 Harbour Exchange Square
London
E14 9GE

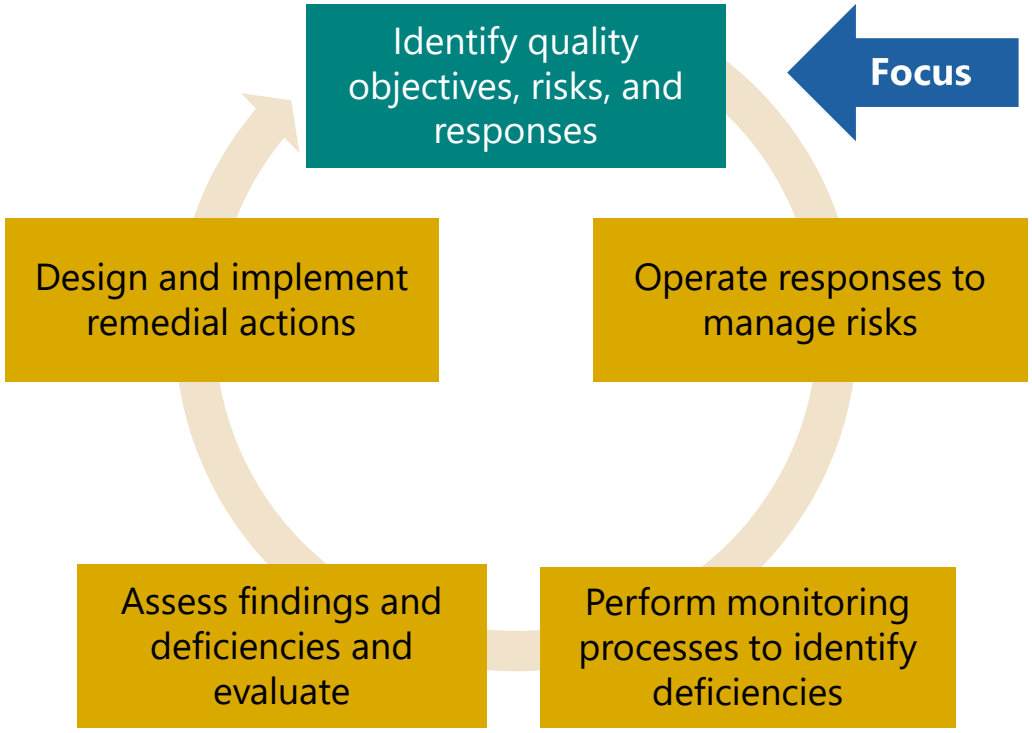
1. Introduction

Why are risk assessment processes important in a System of Quality Management ("SoQM")?

The purpose of the International Standards on Quality Management (ISQM (UK) 1) is to require firms to design, implement, and operate a system of quality management (SoQM) that is continuously tailored to the nature and circumstances of the firm and its engagements. The SoQM is intended to promote consistent engagement quality, protect the public interest, and support continuous improvement.

The standard is intended to move firms beyond complying with specific set policies and procedures towards a proactive and iterative approach to quality management. Firms are required to establish quality objectives, identify and assess quality risks, and continually evaluate how those risks evolve in response to internal and external factors. ISQM (UK) 1 requires tailored, yet still proportionate, responses to those risks, (i.e. the firm's policies and procedures, more commonly known as controls) alongside ongoing monitoring of the effectiveness of those responses. Monitoring outcomes informs whether responses need to be enhanced, supplemented or revised, and whether new or changing quality risks have emerged—supporting a continuous cycle of improvement.

Cycle for firms' operation of their SoQM



Robust risk assessment processes are essential for the initial development and ongoing operation of an effective SoQM.

Based on inspections so far, we have seen variations in how firms initially approached risk assessment and how their approaches have evolved. We have seen variations between and within firms of different sizes.

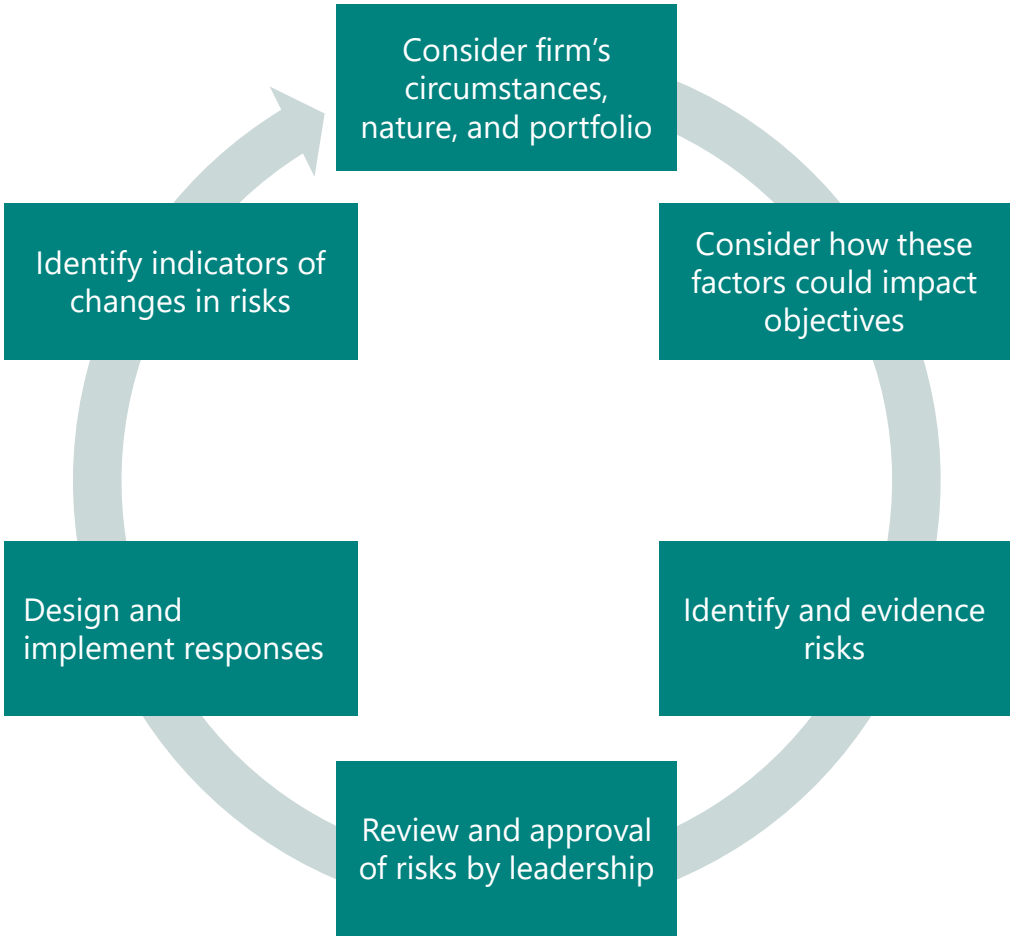
This has been an area of UK regulatory focus, with findings identified across firms of varied sizes. This area is key to our revised supervision model as we increase our emphasis on firms' SoQMs and how firms develop and tailor these proportionately, as a robust risk assessment is key to determining what mitigating responses and monitoring are proportionate for each firm. The FRC's supervisory activities will include inspecting firms' risk assessment processes and outputs, focusing on changes and considering how firms' risk assessments inform our risk-based approach to supervising firms.

1. Introduction - continued

What does the standard say about risk assessment?

ISQM (UK) 1 defines a quality risk as a risk that has a reasonable possibility of occurring; and that individually or in combination with other risks, would adversely affect the achievement of one, or more, quality objectives. When identifying risks ISQM (UK) 1 requires a firm to consider its operating and business model, its strategy, its environment, its resources, its network, the types of engagements it undertakes and the entities for which it undertakes engagements. Each firm's quality risks will be different and tailored. A firm's risk assessment needs to be sufficiently detailed, complete and clear to support identifying the nature and extent of mitigating responses.

Risk assessment cycle



Scope of this Thought Piece

This Thought Piece will cover insights on what firms may consider, with examples of good practice and pitfalls, in the following areas:

1) Process for identifying risks.
2) Granularity in risk identification.
3) Timing and iteration of risk assessment processes.
4) Risk assessment frameworks.
5) Governance processes over risk identification and assessment.

2. Considerations and examples

Process for identifying risks

Firms may consider a wide range of internal and external sources of information. These can include audit inspection findings, ethics breaches, results of root cause analysis, walkthroughs of processes to identify gaps, engagement with audit partners and operational leaders, internal risk management (e.g., internal audit reports or cyber and information security risk assessments), horizon scanning for emerging issues, professional and regulatory requirements, staff surveys, and expected risks set by networks. We expect variations in risks per firm, for reasons including:

Audit portfolio: size of portfolio, size of entities, sector spread and concentrations, number of international group audits, types of regulated entities.	Emerging issues or changing practices in entities and sectors audited.	Complexity: number of offices or business units, recent acquisitions, number of partners, mix of business lines, regulatory regimes.
Strategy: growth aspirations, expansion into new markets or sectors, plans for mergers and/or acquisitions, investment strategies.	Experience of leadership: size of leadership team, leadership structure, extent of day-to-day involvement in the practice.	Historical issues: trends in results of file inspections, trends in ethics breaches, complaints and investigations, regulatory feedback.
Network: participation in a network, size and formality of the network, extent of network requirements and resources provided.	Personnel: resourcing model, overseas staff, recruitment challenges, attrition, cultural aspirations and challenges, cultural maturity.	Resources: automated vs manual systems, use of emerging technology (e.g., AI), internal vs external resource development, use of service providers.

2. Considerations and examples - continued

Good practice	Common pitfalls
Determining a schedule of sources that need to be considered for each iteration of the risk assessment. Establishing a regular and frequent process to engage business process owners and leadership to identify changes. In smaller firms, engaging directly with partners and RIs. Mapping root causes for inspection findings and ethics breaches to risks to ensure they are all covered. Where a network or provider has set expected risks, tailoring these risks and rebutting those not relevant.	Boilerplate risks that aren't relevant or tailored to the firm. Only identifying risks that are not yet sufficiently mitigated, and excluding baseline risks where mitigations are in place. Excluding risks relating to individuals or teams not following policies and processes established by the firm. Excluding root causes that drove quality failings, e.g. lack of guidance. Not reflecting specific features in a firm's structure/model, e.g. firms with overseas staff not identifying any risks for culture or training for these staff. Lack of clear threshold for reasonable possibility so common risks are excluded with limited justification.

2. Considerations and examples (continued)

Granularity in risk identification

ISQM (UK) 1 does not prescribe a required level of detail or granularity for capturing risks, so firms need to determine what level is appropriate and meaningful for them to support effective design of responses. An example of a less granular risk would be the risk that the firm does not have sufficient personnel to undertake quality audits, while a more granular risk might be split between audit partners, senior staff, and junior staff or distinguish between personnel in different audit sectors or offices.

More granular

Advantages of more granular risks:

- Drives focus on specific risks.
- Helpful where new risks have arisen or more focus is needed.
- Prompts identification of targeted responses.
- Supports robust analysis of how responses mitigate risks.

Advantages of less granular risks:

- More stable with less frequent need for change.
- Fewer risks, allowing a simpler SoQM.
- Less chance that risks are missed, e.g., if a firm has identified risks on specific categories of human resources areas of risk could be missed.

Less granular

Good practice	Common pitfalls
Less granular risks, with a breakdown into granular identification of what could go wrong to assess the sufficiency of responses.	Broad risks with many/very broad mapped responses, where it is hard to see how the responses fully mitigate each risk.
Granular risks for specific sectors or processes where concerns have arisen.	Broad risks where it is hard to identify which element is most significant and, therefore, where responses should focus.
More granular risk where risks are newly emerged or have increased in significance.	Granular risks that do not capture all relevant risks.
More granular risks in areas of changes and ongoing quality initiatives.	Granular risks resulting in a very high number of risks and a very complex risk/response mapping.
Less granular risks on overarching emerging issues or areas of change to prompt review of where any new risks arise.	

2. Considerations and examples (continued)

Timing and iteration of risk assessment processes

Risk assessment processes need to be revisited regularly, on an at least annual basis. Firms shall consider, on an ongoing basis, if matters arise that change the risks relevant to the firm, or the nature or likelihood of existing risks. Firms often operate a combination of formal risk assessment processes, to ensure periodic revisiting of their risk assessment, and less formal mechanisms to identify and assess ad-hoc triggers. Examples of such triggers include emerging quality findings, emerging compliance or ethics breaches, significant changes to the audit portfolio, adoption of new technologies (including generative AI), changes to key service providers or resourcing models, significant investment or restructuring activity, changing macroeconomic factors, and the introduction of new standards or requirements.

Larger firms, with more complex SoQMs, benefit from more frequent, formal risk assessments to ensure potential changes to risks are identified and assessed on a timely basis. Smaller firms, with less complex SoQMs, are more likely to be able to identify possible changes through ongoing, informal management activities and so may require less frequent and formal risk assessments.

We have seen that firms' formal risk assessment processes range in frequency from annually to quarterly. The complementary informal mechanisms for identifying potential changes included regular management and leadership meetings, engagement with business process owners across the firm, and horizon scanning activities.

Good practice	Common pitfalls
Structured quarterly or triannual process where business process owners complete a checklist to identify areas of change. Risk assessment triggers built into other processes, e.g., in root cause analysis specifically assessing if causal factors indicate a new risk. At larger firms, regular fixed agenda items for management and oversight bodies. At larger firms, requiring all papers (to management and oversight bodies) to include analysis of impacts on quality risks.	Failing to update the risk assessment even annually. Insufficient assessment of whether SoQM deficiencies indicate changes to risks and only considering changes to responses. Insufficient assessment of how trends in root cause analysis results, quality findings and breaches indicate need for development of quality risks. Assuming no changes to quality risks following changes to governance and ownership structures. Assuming no changes to quality risks from increased or new uses of technology.

2. Considerations and examples (continued)

Framework for assessing risks

Most firms use their assessment process to rate risks. Risk ratings help drive proportionate responses and monitoring, by, for example:

- Requiring higher-rated risks to be addressed by preventative, as well as detective, responses, or by control-style processes as well as policies.
- More frequent and ongoing monitoring of higher rated risks, while allowing roll-forward of monitoring for less significant risks.
- Testing larger sample sizes when monitoring responses to mitigate higher rated risks.

Risk ratings are based on assessing the impact and likelihood of the risk crystallising, usually on a scale of 1-3/5, for each factor and combining these to determine the rating.

When determining impact, firms may consider financial, reputational, regulatory, quality, and operational factors, linking to the firm's ability to win, perform and complete audits. Firms may develop scenarios or thresholds for grading impact in these different areas, based on e.g., the number of personnel or teams that would be impacted, the number of engagements that could result in a breach or incorrect assurance opinion result, the scale of regulatory consequences, and the scope of reputational impact.

When determining likelihood, firms may consider at what scale to consider likelihood. For example, for some risks, it may be relevant to consider the likelihood of it occurring on one engagement and the likelihood of it being widespread, while for other risks (e.g., relating to governance or failure of technological resources) it may only be appropriate to consider occurrence at a population level.

Risks are usually rated on a gross basis, prior to identification of the mitigating responses. Some firms determine gross and net risk ratings, to evidence assessment of whether responses are sufficient to mitigate the risk in line with the firm's risk appetite. The formality of risk assessments will vary between firms. For smaller firms, a less formal approach may be more appropriate as there are fewer individuals involved in the risk assessment, and these individuals often have significant visibility of the audit practice's activities and challenges.

2. Considerations and examples (continued)

Good practice	Common pitfalls
Framework for determining impact and likelihood using structured questions. Setting quantitative and qualitative thresholds for financial, reputational, regulatory, quality, and operational impacts and for likelihood. Tracking risks that were not included as quality risk and documenting how they were assessed as low in likelihood and probability. Clear evidencing assessment of gross and net risk ratings and tying this through to the effectiveness assessments for responses.	Unclear if risk assessment is on a net or gross basis. Assessing risks on a net basis without assessing the effectiveness of responses. Lack of robust justification and evidence to support risk assessments. Assessments of likelihood not considering the results of SoQM monitoring. Lack of consistency in the assessment of different risks.

2. Considerations and examples (continued)

Governance processes over risk identification and assessment

Those with operational, and ultimate, responsibility for the SoQM need to have sufficient engagement with, and oversight of, the risk assessment in order to take ownership of evaluating whether quality risks have been adequately identified, assessed and mitigated to enable reasonable assurance over the attainment of the firm's quality objectives.

Appropriate governance processes will vary between firms based on their size, the complexity of leadership structures, and the day-to-day roles of those with operational, and ultimate, responsibility. Below we have considered examples of processes seen at different firms.

Informal discussion of risks and changes to risks through ongoing management activities.

Periodic evidence of approval.

Formal agenda items to discuss sources of information that drive risk assessment and proposed quality risks.

Log of changes with record of approval at leadership level.

Regular reporting on the assessment process, sources reviewed and identified changes to risks.

Structured engagement with business process owners to support stand-back.

Minuted discussions to evidence review, challenge and approval.

Evidence of approval at multiple levels of management and leadership.

2. Considerations and examples (continued)

Good practice	Common pitfalls
Evidence of discussion of emerging risks to support whether they meet the threshold for a quality risk. Discussion and challenge of risks entering and exiting the highest risk rating. Review of risks by business process owners who report to overall leadership. Ongoing engagement of leadership in the monitoring processes that drive changes in risk.	Lack of evidence of leadership being either involved in the underlying risk assessment process, or having robust discussion, review and challenge of the process; boilerplate sign-off only.

Financial Reporting Council

Financial Reporting Council

London office:
13th Floor, 1 Harbour Exchange Square,
London, E14 9GE

Birmingham office:
5th Floor, 3 Arena Central, Bridge Street,
Birmingham, B1 2AX

+44 (0)20 7492 2300

www.frc.org.uk

Follow us on

LinkedIn