MILLIMAN CLIENT REPORT

Commissioned by Ofcom

Report on principles-based best practices for online safety governance and risk management

31 October 2021

Chris Beck
Neil Cantle FIA
Dana-Marie Dick MSc
Adél Drew FIA
Yoke Hon Hue FIA
Darren Munday MBA, ACII, CFIRM
Amy Nicholson FIA
Despina Pantelide

Milliman

CONTENTS

1 ACKNOWLEDGEMENTS

Ofcom and Milliman acknowledge the academic contribution made by the Digital Leadership Research Centre, Bayes Business School[1] (formerly Cass), whose aim is to investigate the strategic and organisational implications of digital transformation.

[1] For more information, see the website at https://www.cass.city.ac.uk/faculties-and-research/centres/digital-leadership-research-centre.

2 INTRODUCTION

BACKGROUND AND CONTEXT

The draft Online Safety Bill presented to Parliament in May 2021 introduces a risk-based regulatory framework that will apply to in-scope firms that provide “user to user” or “search” services to UK users (regardless of where the company is based in the world). Social media firms, video sharing platforms, and some gaming and online communities would all fall within scope, but internet service providers and content published by a news publisher on its own site are excluded.

The draft Online Safety Bill defines online harms as content which gives rise to "a reasonably foreseeable risk of a significant adverse physical or psychological impact on individuals." The risk-based regulatory regime introduces safety duties that require services to (among other things):

- Minimise the presence and dissemination of priority illegal content
- Operate a service using systems and processes designed to protect children from encountering harmful content
- Set out in their terms and conditions how they will deal with content that is lawful but harmful to adults and apply the terms and conditions consistently

In-scope firms will need to take various steps to comply with the safety duties including: assessing the risks associated with their services (e.g., all services must carry out an illegal content risk assessment); taking proportionate steps to mitigate and manage the risk of harm to individuals identified in the relevant risk assessment; and producing annual transparency reports (for high-risk, high-reach firms only).

In-scope firms must meet the Online Safety standards that will be set out in legislation. These are standards that all in-scope firms must meet, albeit proportionately. When implementing the regulatory framework, Ofcom is expected to adopt a tiered, risk-based, approach. Regulatory expectations must be proportionate, and will vary depending upon the risk profile of each firm and the likely impact on the achievement of regulatory objectives.

PURPOSE OF REPORT

This report sets out best practice governance and risk management principles drawn from a wide range of sectors which exhibit similar risk behaviours to those associated with online harms. This includes, for example, financial services, motor sport, medical practice, construction and aviation. Given the broad scope of services that may fall within the Online Safety Bill, it is recognised, and expected, that firms will adopt different approaches to achieve particular outcomes, and that not all firms will aim to achieve best practice. This report is intended to provide practical examples of how to implement the principles, but it is recognised that, for example, smaller firms may wish to approach best practice in a manner that is proportionate to their resources. It is also true that larger corporate firms, with mature, widely embedded governance and risk management practices may, nevertheless, face additional complexities that will need to be taken into account. In the event that a regulator encourages, or expects, firms to comply with the principles set out in the report (or similar principles), it would be best practice for the regulator to have dialogue with firms to help them understand, directionally, how they are best able to implement the principles in an appropriate manner.

This report does not seek to set out Ofcom’s supervisory strategy and does not seek to provide answers to any questions which may arise, or issues which Ofcom may need to determine, in the context of the Online Safety Bill.

This report has been prepared subject to the reliances and limitations noted in Appendix C.

ECOSYSTEM

In order to understand the ways in which online harms can occur and propagate, it is helpful to consider the ecosystem within which they take place. The risk of online harm is highly complex and involves the interplay of a potentially large and varied number of actors, many of whom sit outside the boundary of any specific firm. There is

information asymmetry and an inability for a specific firm to directly "control" many of the actors influencing their risks. Another significant feature of the online harms ecosystem is that it is highly adaptive—even the notion of what "harm" is will be subject to the zeitgeist of societal judgement. This means that the types of risk management approaches employed by firms need to be capable of operating in that type of environment.

The best practices highlighted in this report are intended to illustrate how each firm can identify the complex set of risk drivers which is unique to them. Firms will then be in a position to take practical steps towards anticipating the risks of online harm and establishing strategies and processes to manage them. Enabling firms to anticipate risk enables more resources to be focussed on delivering the service in the long run[2]—reacting to events in the moment requires resources to be diverted, and can result in users receiving a suboptimal experience until the situation is remediated.

Additionally, the best practices highlighted in this report recognise the need for adaptation and agility. They illustrate how firms can not only build sound risk management for the current situation, but also develop the ongoing learning processes necessary to identify emerging risks and keep the organisation working well as things evolve in the future. The tension between the risk management system and governance framework, in conjunction with the supervisory regime, creates the momentum for an ongoing industry conversation about online harm which should enable sharing of knowledge, and ultimately lead to better user and business outcomes.

[2] See, for example, "The Value of Enterprise Risk Management," Hoyt & Liebenberg, The Journal of Risk & Insurance, December 2011, Vol 78, No 4.

3 EXECUTIVE SUMMARY

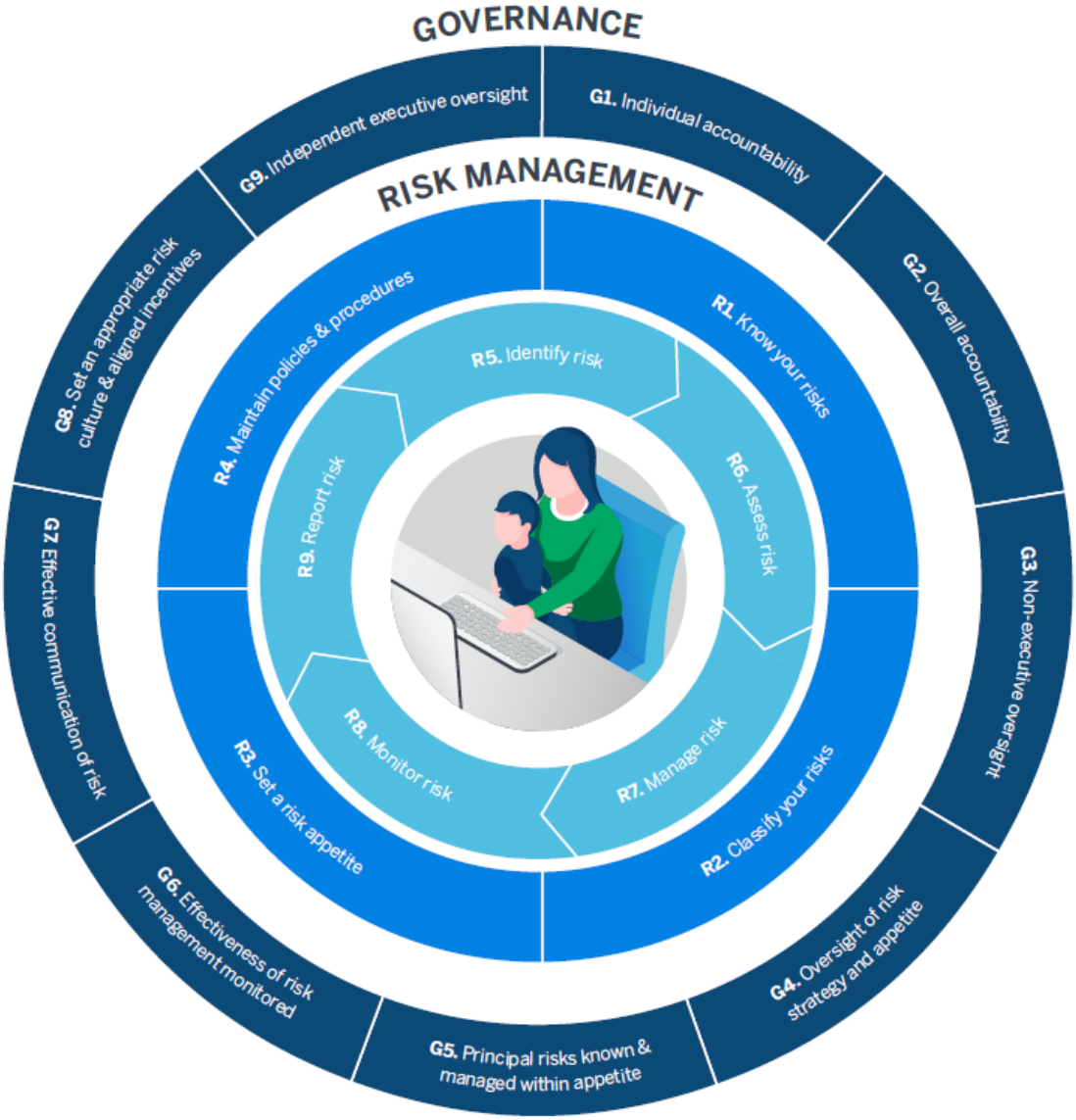
This report highlights best practice principles for the risk management system and its governance. The principles and practices discussed in this report are not meant to be prescriptive or exhaustive. They are valid for all types of firm covered by the Online Safety regime, and it is expected that individual firms will implement them using a proportionate and appropriate approach in relation to their particular circumstances.

As such, it is best practice for firms of all sizes to have a proportionate risk management system and governance framework in place which are aligned to these principles, which will mature over time as their business, and market practice, evolves. Smaller firms with fewer resources might, therefore, choose to outsource or combine certain functions in order to meet the principles, while larger firms, with potentially greater complexity, will look to more sophisticated approaches with dedicated resources.

It is also important to note that best practice risk management is intended to help firms anticipate risk, rather than react to events, thereby helping them to remain resilient and agile, delivering good user outcomes. Balancing risk management against the inefficiency of being reactive also helps to create attractive commercial outcomes.

Good risk management should therefore be seen as a forward-looking value-adding endeavour, rather than a backward-looking intrusive one. The principles are summarised in the diagram in Figure 1 and expanded upon below:

Figure 1: Governance and Risk Management



Risk management system

An effective risk management system is based on defining the risk environment and the approach to managing risk, and implementing an iterative, ongoing learning process to manage risk.

The key elements of understanding the risk environment and defining the approach to risk management include:

- **Know your risks:** It is important to understand the full range of risks faced.
- **Classify your risks:** This facilitates reporting and analysis of the risks faced. The approach to documenting key risk categories will vary across firms, but is required to remain compliant with the recordkeeping duties outlined in the draft Safety Bill.
- **Set a risk appetite:** This statement sets out a firm's attitude to risk, including the types and amount of risk it is willing to take. This is an important tool to ensure a mutual understanding of risk between all stakeholders, providing a reference for consistent decision-making and an important building block of a firm's risk culture.

- **Maintain risk policies and procedures:** These documents set out the risk environment within which the firm operates and the processes it follows to manage risk. These documents are important tools for formalising the risk culture and ensuring everyone within the firm has the same understanding of risk definitions, appetites, and processes. They also establish clear roles and responsibilities.

The process for managing risks comprises:

- **Identify risk:** Best practice is to identify risks regularly and systematically. Additionally, processes should exist to capture and escalate, where needed, risks that are identified outside formal review cycles.

- **Assess risk:** Risk assessment processes help firms to understand and prioritise risks. Risk assessment includes determining the likelihood of risks occurring and their potential impacts. The risk assessment should also measure the firm's performance against its stated risk appetite. Due to the complexity of the operating environment it is also essential to view risks as an interacting set of factors, not only looking at them individually.

- **Manage risk:** Risks are to be managed in a manner that is proportionate to their ability to cause harm. The person accountable for the risk is responsible for putting in place "risk controls," i.e., mitigating actions that reduce the likelihood of online harm events taking place, and helping manage and mitigate the impact of such events if they do occur. It is good practice for such controls to be used and implemented in the day-to-day activities of the firm, with the effectiveness of the controls being assessed on a regular basis by someone independent from those activities. It is also important to anticipate unintended consequences of the controls used, such as inadvertently restricting free expression.

- **Monitor risk:** The effectiveness and efficiency of the risk management system and risk management controls should be monitored on a regular basis. Both qualitative and quantitative metrics can be used.

- **Report risk:** It is best practice to regularly report on risk management activities to the governance body and risk governance body;[3] it can be made available to the regulator upon request. Risk reporting creates an important ongoing conversation about risk in the firm and helps to support firm-wide accountability. It enables firms to demonstrate their degree of compliance with best practice principles, for both internal and external purposes. This step ensures that risk management is embedded into governance processes and that there is effective oversight implemented across all stages of the risk management system.

[3] See Section 5 below for a full description of what is meant by "governance body" and "risk governance body."

Governance

Defining the appropriate risk governance structure is crucial and it can be done in many ways. The primary aim is to ensure that everyone in a firm is fully aware of, and understands, their own role regarding risk management and those of others. The governance structure should be able to deliver the required level of risk management in an optimised way, whilst demonstrating sufficient oversight and challenge that is independent from the business itself.

The Three Lines of Defence model is a widely adopted risk governance concept which is based on *individual accountability*. Under this governance structure, the senior managers accountable for risk-taking activity are the first line. Trusted advisors to the first line providing independent oversight and challenge (e.g., risk and compliance functions) are the second line. The third line, finally (e.g., internal and external auditors), provides independent assurance. The method of implementation varies according to the structure and resources of a particular firm. Some firms may be able to resource each line of defence with dedicated individuals. Others may use organisational design to try to ensure that oversight of particular tasks can be done by another individual in the firm who is not directly involved with that task. It is also common to use external resources where it is difficult, or impossible, to find an internal solution. The important objective is to ensure that firms find a way to achieve as much independent oversight and challenge as possible for each key task.

The *overall accountability* sits at the most senior level with a governance body which retains overall accountability for the principal risks and effectiveness of the risk management system. It is best practice to form a governance body which provides *nonexecutive oversight*. The governance body is ideally supported by a risk governance body which aims to facilitate focussed and informed discussion on risk-related matters. Where it is not possible to access nonexecutive resources the governance body should comprise the most senior individuals in the firm with as great a distance from day-to-day activity (i.e., risk-taking) as possible.

The risk governance body provides *oversight of the risk strategy and risk appetite* and the overall *effectiveness of risk management is monitored*. It also assesses the quality and appropriateness of the risk information and reporting to ensure that there is *effective communication of risk*. It is important for information about risk to flow upwards to the governance body in a clear and efficient way and for colleagues in the business to be able to learn about risk activity so that they can improve their processes.

The governance body should ensure that they *set an appropriate risk culture and aligned incentives*. It is important for the organisation to look ahead, by building an open, forward-looking risk culture. This enables the organisation to anticipate risks rather than react to them. As best practice, this should be embedded in a firm's activities and implemented through the risk strategy and risk appetite.

It is important to be able to deliver *independent executive risk oversight* and to effectively challenge the senior management approach to risks. For key decisions it is important that an independent challenge is available, to support the governance body's decision-making. This could be achieved with a dedicated risk function, as part of someone's role, if they can demonstrate a high level of independence, or in an external party.

4 RISK MANAGEMENT SYSTEM

INTRODUCTION

This part of the best practice guide highlights the principles that firms should consider if they wish to implement highly effective risk management systems for online harms. Whilst each principle represents best practice, it is understood that each firm will decide on a level of maturity for each element of its risk management system based upon its specific circumstances. It is also to be expected that, for any given principle, each firm may choose a different way to achieve it. The principles should, therefore, not be viewed as prescriptive or exhaustive, and their methods of implementation should be proportionate for any given firm.

It is best practice for each individual firm to tailor its risk management approach to its needs and characteristics, considering the firm's strategy and objectives. This is not intended to be a "one size fits all" approach, as the full government response[4] suggests, but instead reflects the diversity of the online services and harms spectrum.

Effective risk management is based on:

1. Understanding your risk environment and defining your approach to risk management:
    a. Risk profile
    b. Risk categories
    c. Risk policies and procedures
    d. Risk appetite
2. Defining the iterative processes to manage risk:
    a. Risk identification
    b. Risk assessment
    c. Risk management
    d. Risk monitoring
    e. Risk reporting

A structured approach to risk management is critical for successful implementation. It is best practice for the risk management system to continue to evolve in response to an ongoing evaluation of the risk environment. This requires a firm to consider the changing nature of the firm itself, the market, technological advancements and changing societal expectations over time. Firms following best practice are therefore able to continually improve the efficiency and effectiveness of their risk management processes.

PRINCIPLE R1: KNOW YOUR RISKS

It is best practice for a firm to have a good understanding of its risk profile based on the environment within which it operates and its specific business model

It is best practice for firms to identify and evaluate the full range of risks to which they are exposed, so that they adequately understand the risk environment. These risks will include the firm's general business risks, as well as the risks to users of the service (online harms) that impact the broader business risks. To achieve best practice, the full suite of risks identified should be recorded in the firm's risk profile document, which should be maintained and reviewed by the governance body[5] at least annually or whenever there are significant changes to or around the business.

[4] Online Harms White Paper: Full government response to consultation.

[5] See Section 5 below for a full description of what is meant by "governance body."

The risk profile of in-scope firms will likely vary based on the:

- Design and features of services offered
- Uses of the service
- Profile of the users (intended and otherwise)
- Number of users
- Reach of the content on the service
- Size of the firm
- Type of content the users are exposed to
- Nature and severity of the potential harm suffered by individuals
- The velocity of content spread

The design of a service and its features can be one of the key factors that contribute to the risk of harm occurring to a user. For example, the following service features are likely to pose greater risks of online harm to users: allowing children to be contacted by unknown adult users; allowing users (including children) to livestream themselves; and including private messaging channels where the content on those private channels is not or cannot be moderated.

The potential for harm is heightened if children, or other vulnerable people (such as those with mental health issues), are users of the service.[6] It is important for companies to have a good understanding of who their users are and what vulnerabilities they have. In practice, it may be quite difficult for firms to have adequate systems and processes in place to gather sufficiently granular levels of understanding of their users. Requesting sensitive personal data, such as health data, would be subject to General Data Protection Regulation[7] (GDPR) Article 9 and could be seen as a deterrent to users. Software could be used to track possible vulnerabilities through users' interactions with a service but this could raise privacy issues. Additional risk is introduced if a user's identity does not have to be disclosed to generate content on the platform. If users' true identities can remain anonymous, there is an increased potential for harm due to the lack of accountability and repercussions. An example of this is "fake users" or "trolls" with throwaway accounts that are often used to carry out cyberbullying and inflict psychological harm.[8] There are examples where certain platforms verify user profiles (usually those with significant influence or reach) and publicly indicate whether each user has a verified identity.

A service's popularity (and any sudden increase thereof) can be a source of risk for a firm. Having more users increases the reach of the content on the platform and hence the potential impact that content can have. Consideration should also be given as to whether individuals need to be registered users of a service to have access to its content. If not, the reach could be greater than known and the potential for harm increased.

The nature and severity of the potential harm to users should also be considered when determining the risk profile of a firm. The greater the likelihood and/or impact of harm to an individual user of the service, the greater the overall riskiness of the firm.

Best practice suggests that, if significant changes occur to any of the factors identified above, then the firm ought to carry out an ad hoc review of its risk profile. Firms with riskier profiles (high-risk and high-reach) are likely to be classified as Category 1 and would be subject to additional, or more stringent, regulation.

[6] UK Safer Internet Centre. People at Greater Risk Online. Retrieved 25 November 2021 from https://www.saferinternet.org.uk/blog/supporting-vulnerable-groups-online.
[7] EUR-Lex. Document 02016R0679-20160504. Retrieved 25 November 2021 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434.
[8] Ryan-White, G. (June 2021). Online Trolling and Abuse. Northern Ireland Assembly. Retrieved 25 November 2021 from http://www.niassembly.gov.uk/globalassets/documents/raise/publications/2017-2022/2021/justice/5121.pdf.

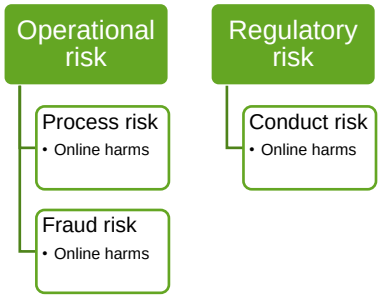
PRINCIPLE R2: CLASSIFY YOUR RISKS

It is best practice for a firm to maintain a risk register setting out the categories of risks to which it is exposed, with a risk owner assigned to each category

When considering the risks to which they are exposed, firms will primarily consider the key categories of risks posed to the overall operation and success of their business (i.e., financial risk, operational risk, regulatory risk), rather than only considering the risks to their customers or consumers of a firm's services. Best practice firms organise these key business risks into hierarchies, which provide more granular breakdowns of the components of each risk category. Under this approach, risks to the consumer are usually captured at a lower level within the hierarchy of risks. By embedding consumer-related risks within the wider risk hierarchy in this way, consideration of such risks becomes part of the overall risk culture of the firm, and enables a more effective risk management process which is tailored to the different types of risk that may arise.

Whilst the approach to documenting the key risk categories will vary across firms, and not all firms will maintain a formal risk register, the draft Online Safety Bill contains certain recordkeeping duties that firms will be required to comply with. As a general principle, firms should be able to demonstrate how the risk of online harm fits into their existing risk categories. For example, because the risk of online harm is likely to manifest within the categories of operational risk and regulatory risk, it may be categorised by the firm as shown in Figure 2.

Figure 2: Operational Risk and Regulatory Risk



Given the wide-ranging nature of online harms risk, and the different approaches that are likely to be adopted to manage such risks, best practice would be for firms to break this risk down into different classes and types of online harm. It is common for an industry to desire some level of consistency in the taxonomies used to classify risks, as it facilitates the sharing of knowledge between firms and enables the regulator to identify thematic trends.[9]

The definition of certain risk types, in particular risk types that are legal but harmful, is subject to interpretation and is unlikely to be understood consistently across the industry. Further, the approach to managing such material will vary across firms, with a less stringent approach potentially being taken by some firms. In sectors such as food hygiene,[10] for example, it has been useful to define such risk types to ensure that considerations which fall within the scope of the regulations, and the obligations with respect to such risks, are understood by firms.

In the dynamic and rapidly moving environment in which the online safety regime will operate, the categorisation and definition of online harms risk will inevitably evolve over time. It is, therefore, good practice for firms to make an initial attempt at embedding the categorisation of online harms risk into their existing risk categories, whilst acknowledging that this will require periodic review.

[9] See, for example, https://www.skybrary.aero/bookshelf/books/2301.pdf, which illustrates how the aviation industry benefits from knowledge sharing through the use of a common taxonomy for hazards.

[10] See, for example, https://www.food.gov.uk/business-guidance/how-risk-analysis-keeps-food-and-feed-safe, describing the ways in which risk classification helps to reduce the risk of poor hygiene impacting food supplies.

PRINCIPLE R3: SET A RISK APPETITE

It is best practice for a firm to have a risk appetite statement (with corresponding risk tolerances and limits) approved by the governance body

The governance body is responsible for establishing a firm's risk appetite statement or risk-based objectives. They are important tools, used to ensure mutual understanding of acceptable levels of risk between the governance body and executive management. It is important to link risk appetite statements to business objectives, of which regulatory requirements of the firm should be a consideration. Best practice is then for these risk appetite statements to be translated into risk tolerances at an enterprise level, which in turn cascade down into risk limits at business and operating levels.

Risk tolerances and limits reflect the acceptable variation of outcomes around a particular objective. A risk tolerance defines the absolute amount of risk a firm is willing to accept for a given objective. A risk limit acts as a warning mechanism for the business that risk levels are approaching a defined tolerance, and therefore allows appropriate time for corrective action to be taken. In addition to defining an acceptable degree of variation, it is best practice to define the acceptable reasons for variation. These "risk preferences" form an important cultural guide for the firm to highlight which activities are deemed unacceptable. A principle-based approach to risk appetite, tolerance and limit design enables firms to tailor these mechanisms to their specific business and objectives, and also to the exact characteristics of the risks they are exposed to. For example, risks that could arise suddenly may need much lower risk limits to enable suitable action to be taken within a given timeframe before a tolerance is breached.

The tolerances and limits, defined by the governance body, will be used later in the risk assessment process to judge whether an identified risk falls within the risk appetite levels of the firm. If it does not, corrective action should be taken. The type and speed of corrective action will also need to be defined by the governance body when setting the risk appetite statement. For example, a breach of a risk limit could require immediate escalation to the relevant risk owner while a breach of a risk tolerance could require immediate escalation to the governance body or regulator.

A well-developed risk appetite statement and process can:

- Help a firm inform its risk culture
- Help a firm better understand, and therefore manage, its risk exposure
- Help management make informed risk-based decisions
- Help improve transparency to users and the regulator

PRINCIPLE R4: MAINTAIN POLICIES AND PROCEDURES

It is best practice for a firm to have a set of documented risk policies and procedures that are approved, and reviewed at least annually, by the governance body

Policy and procedure documents set out, in writing, the risk environment within which a firm operates and the processes it follows to identify, assess, manage, monitor and report its risks. These documents are an important tool for articulating the desired risk culture and ensuring everyone within the firm has the same understanding of risk definitions, appetites and processes. They can easily be tailored to suit the size and complexity of a particular firm. They should be approved by the governance body and should be reviewed at least annually, or when needed to reflect changes in the operating environment.

A best practice set of risk management policy documents taking account of online harms could include:

- Management principles for risks from online harms
- Relevant regulatory requirements and how they are addressed
- Definition and taxonomy for company risks that take account of online harms
- Management objectives and goals relating to online harms

- Firm-wide processes and tools that business units are expected to adopt to manage online harms
- The organisational structure for managing risks from online harms
- Clearly defined roles and responsibilities for each aspect of online harms

PRINCIPLE R5: IDENTIFY RISK

It is best practice for a firm to implement deliberate and systematic processes to identify risks on a continuous basis

Risk identification is the first step in the iterative risk management process. The specific risks that may arise are a result of the firm's business environment, the processes it follows and the tools it uses. Under best practice, the identification of risks should be performed regularly, proactively and systematically to ensure all principal and emerging risks to the firm achieving its objectives are captured and logged. Additionally, processes should exist to capture and escalate, where needed, risks that are identified out of formal review cycles.

It is best practice for all levels within a firm to be involved in the risk identification process, whether this is during formal risk identification exercises or as a day-to-day expectation of being aware of potential issues and raising them to a line manager or risk manager. As a result, an open and transparent risk culture is important to enable everyone to speak up about issues they have identified. Looking at sectors where lives can be at stake (such as healthcare, construction or motor racing) you can see there is a huge incentive to try and identify potential risks in advance, enabling appropriate risk management strategies to be formulated which literally save lives. The risk identification process is key to being proactive rather than reactive.

In an online harms context, it makes sense to enable users to also be a part of risk identification practices. This can be achieved through ensuring, for example, that online content can be easily flagged, or through efficient and effective complaint procedures.

There are various risk identification processes firms can implement, for example:

- **Review lessons:** By analysing past experience, harms that have occurred, or near misses, are a useful indication of potentially similar risks.
- **External events:** As well as analysing harms that have occurred and near misses from its own experience, considering harms across the industry could also be a good prompt for understanding whether the firm could be exposed to similar events.
- **Risk prompt lists:** A firm's risk categorisation list can be used to ensure risks have been considered in all areas, e.g., operational risk and fraud risk.
- **Brainstorming:** Group discussions with internal or external experts can help identify a wider range of potential risks, both current and future. An open and honest risk culture is critical for these sessions to ensure everyone is empowered to speak up and be listened to.

When performing a best practice risk identification process, it is important for firms to consider emerging risks as well as existing risks. It is also advisable to not only consider standalone events but also where interactions of relatively benign risks could have a much larger impact than the sum of the parts.

PRINCIPLE R6: ASSESS RISK

It is best practice for a firm to implement risk assessment processes to understand and prioritise risks

Once risks have been identified it is best practice to assess them, to determine their likelihood and potential impacts, as part of an ongoing risk management process. This step enables risks to be prioritised, so that those risks with the potential to create the most harm are addressed first and allocated resources proportionately.

Expert judgement, along with analysis of past trends, will be useful in determining the likelihood of particular risk events occurring. The potential impact of the risk event will be a function of the scale, severity and complexity of the risk. Firms can use a risk matrix, for example, with likelihood (probability) and impact on the axes, as an assessment tool and a risk register to document their risk assessments. This would not be a requirement but, as a

minimum, firms should be able to demonstrate that they have analysed each identified risk in a consistent manner, assigned a person to be responsible for it, and determined what course of action, if any, should be taken. In field medicine, for example, it is clear that resources and time for action are limited. Medics use their risk assessments to prioritise so that they are able to achieve the best possible outcome, given the constraints they face. For online harms, firms should likewise be able to achieve an optimal allocation of resources by assessing the risks they face and ensuring that the aggregate level of risk is consistent with the stated risk appetite.

During this step of the risk management process, it is best practice to keep a record of near-miss events as well as risk events. This record should then be compared with the thresholds and limits set by the governance body for each risk class to determine whether a systemic issue exists. For example, if a start-up firm with a threshold for illegal activities of one event per year notices that it is repeatedly meeting or exceeding that threshold, it may indicate a potential area of deficiency in the design or use of its service and should prompt remedial action.

Best practice risk assessment is both quantitative and qualitative in nature. In the world of online harms, quantitative risk assessment could include measuring key risk indicators such as:

- Number of illegal or harmful activities that occur on the platform in a specified period
- Number of near-miss risk events that occur in a specified period
- Number of risk events reported by users versus flagged by staff or an artificial intelligence (AI) system
- The length of time content causing harm remained on the platform

Importantly, it is not sufficient to assess risks individually. Firms should give thought to how the various risks identified can interact with, and amplify, each other. Firms should also assess whether or not they have adequate resources in-house to manage multiple risk events occurring at once.

PRINCIPLE R7: MANAGE RISK

It is best practice for a firm to use controls to manage all identified risks in a manner proportionate to their ability to cause harm

Having identified and assessed the online harms risks to which users could be exposed, it is best practice for firms to use a combination of systems, processes and risk decisions (collectively, “controls”) to reduce the likelihood of online harm events taking place, and to determine the approach to manage and mitigate the impact of online harm events if they do occur. This could include, for example, the decision to avoid a risk entirely, such as deciding not to enable a certain feature on the platform if it was felt that it would be too challenging to manage.

In order to minimise the prevalence of online harm risks, best practice would be to manage these risks in a way that is proactive as well as reactive. It is therefore appropriate for firms to consider a variety of controls which are tailored to effectively manage the different types of online harm. They would include:

- Preventive controls, which aim to reduce the likelihood of online harm events taking place
- Identification controls, which aim to detect when an online harm event has taken place
- Remediation controls, which aim to rectify online harm events when they occur, and to limit their impact

For illustration purposes only, examples of such controls may include: user education and awareness initiatives to improve media literacy; age verification and parental controls; reporting mechanisms; and content monitoring, which could be achieved by the use of machine learning algorithms and artificial intelligence. It is important, however, that the use of particular controls does not inadvertently lead to new risks, such as the restriction of freedom of expression. It is also important to note that automated tools are not perfect and false positives can arise—actions taken as a result of a flag therefore need to be mindful of that possibility.

Scientific methods for identifying harmful content, understanding how harmful content spreads across networks, and effectively mitigating the effect of harmful content, are evolving, increasing in their sophistication. It is best

practice for firms to ensure that the controls they use are suitably advanced and that they evolve as the understanding in this field grows. It is also good practice for firms to consider the mindset of their users when using their platform, and their users' ability to detect harmful content, such as misinformation, which could impact the effectiveness of risk controls such as reporting mechanisms. As such, for controls that require user engagement, education on the use of these controls is likely to be critical.

It is best practice for such controls to be used and implemented in the day-to-day activities of the first line of defence, with the effectiveness of the controls being assessed on a regular basis by the second line. In order to take this approach, firms would need to determine the level of resources required to operate and assess these controls, including both technology and staffing requirements. Where firms are not able to fulfil these requirements internally, external options can be considered, such as the purchase of technologies and software, or the outsourcing of content monitoring activity.

Ofcom may consider flagging certain principles that represent best practice for firms' risk controls. For example, the principles that protection measures should be effective, easy to use, transparent, fair and evolving, as included within Ofcom's Video-Sharing Platform Guidance, could be incorporated into the online safety regime. In addition, Ofcom may consider the following aspects to incorporate into principles for risk controls:

- **The ability to manipulate controls**: For example, it should not be easy for children to override parental controls or age-gating measures, or for users to manipulate actions taken by the firm such as disabling of accounts. Risk controls should keep pace with increasingly sophisticated techniques adopted by users to circumvent controls.
- **The completeness of controls used**: Different controls should be used as appropriate and proportionate, to cover the broad spectrum of the different types of online harm.
- **The level of consistency across different platforms**: For example, Ofcom could consider encouraging the use of controls for collaboration across platforms, such as the use of databases for images or other content that should be removed across platforms.

The implementation of effective risk controls and approaches will inevitably require initial and ongoing investment by firms and may necessitate certain measures to be introduced that could discourage certain users from using a particular platform. Therefore, whilst other drivers, such as reputational drivers, are likely to encourage firms to make some investment in this area, there is likely to be a lack of incentive for firms to invest sufficiently without a regulatory driver. Ofcom's enforcement of risk management regulation will therefore be key to ensure that firms allocate adequate resources to this area.

PRINCIPLE R8: MONITOR RISK

It is best practice for a firm to monitor the effectiveness and efficiency of its risk framework and risk management controls on a regular basis

Whilst firms would be responsible for determining and embedding the risk management controls, under best practice they should be able to demonstrate the ongoing effectiveness and completeness of their controls, as well as the risk framework as a whole. Measuring the performance of those controls against online harms could be achieved through both quantitative and qualitative metrics, some examples of which are presented in the table in Figure 3. The list of examples is by no means explicit or exhaustive.

Figure 3: Quantitative and Qualitative Metrics

Examples of Quantitative Metrics	Examples of Qualitative Metrics
Precision of systems which identify and aim to remove harmful material	Survey results regarding user awareness and engagement

Number of terms and conditions (T&C) violations since last review	Proof independent reviews have been performed
Volume of harmful material reported	Type of harmful material reported
Recovery time of wrongfully suspended accounts	Documented proof of risk owners being involved in the process
Percentage of staff who have completed relevant annual training	Documented proof training has been rolled out to all relevant departments

Ofcom could consider providing guidance to firms in relation to performance targets regarding the content that violates policies and procedures. For instance, decreasing the prevalence of content that violates a site's hate speech policies or maintaining a specific median response time to users.

Where feasible, data should be collected on the usage and impact of the risk controls in place, with granularity on the level of harmful material and the harms that controls are attempting to mitigate. Data should be reviewed and monitored regularly and used as a tool for analysing past performance and trends to mitigate systemic issues.

Through the monitoring phase, any changes that could impact the risk profile or any emerging risks resulting from the regular review of the identification, assessment and management stages will be identified. However, when emerging risks appear, it is good practice for firms to make an initial attempt at embedding them into their existing risk categories, whilst acknowledging the fact that this will evolve over time and therefore require periodic review. When any new features or services are introduced, or where any changes are applied to a firm's existing services, an assessment of the impact on the risk framework and the firm's susceptibility to online harms should be made.

The internal and external environments for firms will constantly change, particularly in the area of online harms. This could be due to a diversified range of factors, including the evolving nature of technology and the increasing levels of user sophistication. Therefore, risk management controls need to evolve, improve and change over time to ensure continued relevance and effectiveness of the risk framework.

Furthermore, best practice would be to allocate individual responsibilities clearly within a firm. This includes the appointment of individuals to perform relevant regulatory control and legislative functions, where appropriate, within each firm, as well as Ofcom itself. This clear mapping of responsibilities will enhance the monitoring process. Failure to comply with the principles or a breach of the risk tolerance limits are a couple of examples where monitoring should ensure that escalation processes exist and are applied in a proportionate manner.

Ofcom will have a duty to consult on the codes and could assist all companies in understanding and fulfilling their responsibilities to ensure consistent compliance with the principles across the market, as well as identifying any areas for improvement. In some sectors, such as aviation, participants and the regulator have a very strong culture of knowledge-sharing about risk and a spirit of trying to collectively raise the bar.[11] Cooperation among the firms operating within the online spectrum could prove very effective in preventing online harms, by increasing transparency in the market and enabling firms to benefit from economies of scale.

PRINCIPLE R9: REPORT RISK

It is best practice for a firm to regularly report on its risk management activities to the governance body and the regulator, if and where appropriate

Risk reporting enables firms to demonstrate their compliance with the principles, for both internal and external purposes (e.g., the governance body and the regulator). This step ensures that risk management is embedded into governance processes and that there is effective oversight implemented across all stages of the risk management framework.

[11] See https://www.easa.europa.eu/domains/safety-management/safety-risk-management, for example.

Reporting should be treated as the vehicle of communication regarding the risk framework, through which any issues should be flagged as they arise and ensure that the firm operates within the risk appetite and tolerance limits that have been established.

One of the key requirements for effective risk management reporting is the need to produce reliable and accurate reporting to support the recipient in making well-informed decisions. It is best practice for any material decisions being requested from an executive committee, or governance body, to be supported by a risk opinion from the second line of defence—this provides the decision-makers with support in ensuring that the material risks associated with the decision have been considered.

The second requirement is the frequency of periodic risk reporting required. Recognition and documentation of procedures for when out-of-cycle risk reporting might be necessary will ensure adaptability and flexibility of the reporting process during extreme circumstances. For instance, consider an exception report on the breach of a risk tolerance limit. It is important that risk information is received in a timely manner which is consistent with the need to make decisions. In fast-moving environments, like a Formula 1 race, a rapid financial market movement or an operating theatre, it is important that risk information is received quickly to support decision-making by the first line of defence. In these types of situations, best practice involves the use of anticipatory reporting (such as scenario analysis) to supplement situational reporting about the current position to assist decision-makers in identifying the onset of a particular event.

The next significant requirement is to consider the parties involved in risk reporting. First, ownership for producing the risk reporting is required. This is normally based upon who "owns" the risk—often an expert in the business who understands the activity well or a manager who is responsible for the relevant process. Second, it is important to consider the audience of every document and the purpose for which they are receiving it. A good report will be appropriately detailed and well-articulated, to support recipients in meeting their objectives. The authors of these reports therefore need to consider the level of technical knowledge of the audience and ensure that the readers are not required to personally have a deep understanding of the topic in order to make good decisions.

Additional considerations are the enhancement of market integrity and confidence through reporting—a concept sometimes referred to as "freedom with publicity."[12] This could be a public report, based on enforcement data, further encouraging accountability of the firms, or a private report to Ofcom on more specific details—the use of public and private reporting can be a useful combination to ensure that a firm is able to inform the regulator about important risk information that could be commercially sensitive, for example.

[12] See https://www.cambridge.org/core/journals/annals-of-actuarial-science/article/abs/freedom-with-publicity-the-actuarial-profession-and-united-kingdom-insurance-regulation-from-1844-to-1945/7AE583713E2CBF14E4DA5F07D6545089, for example.

5 GOVERNANCE

INTRODUCTION

When addressing risk management, defining the appropriate risk governance structure is crucial—the risk management system is necessary but not sufficient. The risk governance structure creates a necessary tension between those taking risk in the business and a “governance body,” whose role is to ensure that the risk framework is operating appropriately. There are many different paths to implementing these governance principles which will be dependent upon each firm’s specific circumstances, e.g., mature versus start-up. The descriptions or names given to relevant governance bodies in a firm will vary depending on their size, structure or preference, e.g., some firms might have a truly independent governance body called “the Board of Directors,” whereas others might use a subgroup of the management team, or external support, to provide the necessary challenge and oversight. When reading this report the term “governance body” means a group of senior individuals who meet for the purpose of ensuring that good governance is taking place and who are as independent as possible from the daily risk-taking activity of the firm—it should therefore be interpreted appropriately for any particular firm. It is typical for a subset of the governance body to focus specifically on risk. Throughout this report we will refer to this subgroup as the “risk governance body.” Again, firms will have different names and structures for this—some will form "Board Risk Committees," while others may simply appoint an individual from the governance body to focus, at least part of their time, on risk. The primary aim for all firms, however, is that everyone in a firm is fully aware of, and understands, their own accountability regarding risk management and that of others. The goal is to achieve a risk governance structure which delivers the required level of risk management, whilst demonstrating sufficient oversight and challenge that are as independent as possible from the business itself.

With that in mind, we have highlighted a set of best practice governance principles that are aimed at supporting the implementation of an effective and efficient risk management framework. These are summarised in Figure 4.

Figure 4: Best Practice Governance Principles

PRINCIPLE G1: INDIVIDUAL ACCOUNTABILITY

The Three Lines of Defence model is a well-established organisational model built on a principle-based approach that assigns individual accountability and defines roles and responsibilities

The Three Lines of Defence model has been implemented across many sectors and has been endorsed by regulators, including the Financial Conduct Authority (FCA) in its efforts to assign executive accountability under the "Senior Managers & Certification Regime." The overarching principle of the Three Lines model is to align the strategy and purpose of the firm, whilst ensuring that individual accountability is clear.

A focus on good outcomes requires alignment across the Three Lines model, with clear accountability for managing the risk of online harms. It is important to clarify who owns, takes and manages these risks within the firm. The governance body is ultimately responsible for the risks. The risk takers comprise the first-line senior managers in the firm who are ultimately accountable for managing the risk of online harms, even though they typically delegate tasks to team members. The second line, e.g., risk and compliance functions in large firms or a senior manager with responsibilities for risk and compliance in smaller firms, fulfils the role of trusted advisor to the first line. They provide independent oversight and challenge, ensuring that risk assumptions are clear and that risk-taking is aligned with the firm's stated risk strategy and risk appetite framework. Finally, the third line, e.g., internal and external auditors, provides independent assurance. It should also be noted that firms sometimes find it appropriate to appoint an external party to fulfil a second-line or third-line role to achieve suitable independence without the need to recruit additional permanent resources.

Over the course of its implementation, it has been noted that the Three Lines model has some limitations—for example, three distinct lines are not always sufficient to enable clarity on roles and responsibilities.

In response to these limitations, some firms have deployed an "enhanced" approach that envisages a broader involvement of the second line. This approach expands on recurrent control activities, usually managed ex post facto, towards the adoption of a forward-looking mindset that supports and challenges first-line initiatives and includes:

- Having clearly defined roles and responsibilities for all senior managers.
- Having regular risk culture training sessions within the firm to ensure that management fully understands and appreciates the need to foster a healthy risk culture.
- Linking control objectives with business performance.
- Implementing automated technological controls that adopt a "safety first" mindset by design. This could include, for example: artificial intelligence; robotic process automation; and natural language processing.
- Encouraging the early involvement of the second line in the design phase of any business activities, product and/or process.
- Promoting stronger interaction between the first and second lines by creating opportunities for the second line to know and understand the business better.
- Incorporating risk management performance objectives into first-line variable compensation schemes.

Therefore, in meeting this principle, it is best practice for the governance body of a firm to:

- Ensure the first-line senior management is accountable for risk-taking that is supported by:
    - Performing a forward-looking risk assessment.
    - Proactively managing principal and emerging risks.
    - Aligning the risk strategy and risk appetite framework with the firm's business model and strategic objectives.
    - Collating risk-based management information and periodically presenting to the risk governance body.

- Establishing an internal control system that provides reasonable assurance that key controls are operating effectively. This could include elements such as: any technology a service chooses to make use of; partnerships with "trusted flaggers"; other fast-track content removal processes; how terms of service are agreed; and how decisions are made on broader safety measures.

- Ensure second line is responsible for providing independent oversight that includes:
  - Ensuring robust challenge of first-line risk-taking activities across the firm
  - Ensuring clear allocation of roles and responsibilities between the risk function and other second-line internal control functions, such as compliance
  - Preparing risk reporting that provides the risk governance body with independent assurance that the internal control system (including online safety management systems) is effective
- Ensure third line is responsible for providing independent assurance that includes:
  - Providing independent assurance to the risk governance body (and any entity responsible for reviewing the findings of internal and external audits) on the adequacy and effectiveness of the firm's governance, risk management system and internal control system, including the effectiveness of the second-line control functions.
  - Focussing on principal and emerging risks, significant control weaknesses and audit findings that may impact the firm's strategic objectives and overall risk profile.
  - Periodically assessing the quality and reliability of first-line and second-line risk reporting.
  - Where applicable, appointing an external third party to provide the technical skills and capabilities necessary to periodically complete an accountability and transparency audit of the online safety management systems to provide independent assurance. This audit should encompass all aspects of online safety, including how decisions on terms of service are agreed, and should not be limited to automated technological controls only.

PRINCIPLE G2: OVERALL ACCOUNTABILITY

It is best practice for a firm to ensure that overall accountability sits with the governance body, which is supported by a risk governance body with the aim of facilitating focussed and informed discussions on risk-related matters

- Ensure the governance body retains overall accountability for the firm's principal risks (including the risk of cross-platform migration) and for the effectiveness of the governance, risk management system and internal control system.
- Ensure the risk governance body is responsible for advising the governance body on matters including:
  - Providing consolidated oversight and challenge of first-line risk-taking activities, together with a concise summary of the committee's activities and matters considered
  - Seeking engagement with, and direction from, the governance body on key topics that may include those which have strategic importance to the firm (for example, business model adoption, development of new products and services)
  - Ensuring delegated risk-related responsibilities are clearly defined and coordinated amongst any other advisory committees that may exist
  - Facilitating the exchange of relevant risk information within groups of companies and key external stakeholders

PRINCIPLE G3: NONEXECUTIVE OVERSIGHT

It is best practice for the firm's risk governance body to be formed of both executive management and individuals who are independent from management and apply the spirit of UK Corporate Governance Code guidance on chair, composition, succession and evaluation criteria as far as possible

- Develop terms of reference, approved by the governance body, that clearly set out the risk governance body's responsibilities and duties, including standing agenda items and areas of delegated authority. This effort may include a standing invitation to other members of the governance body. Where they exist, the chief internal auditor, heads of internal control functions and a third-party auditor may also be invited.
- Ensure the risk governance body fulfils its nonexecutive status and does not take on the role of a first-line executive risk oversight body. For smaller firms, it might not be possible to access nonexecutive resources. In this case, the firm should ensure that the risk governance body comprises sufficiently independent internal and/or external resource(s) to be able to challenge those carrying out risk-taking activity in the business.
- Maintain an annual cycle of planned activity and ensure there is sufficient capacity for deep-dive or thematic reviews of the firm's specific exposures.
- Have an appropriate balance of skills, diversity and relevant industry expertise to fulfil the committee's function with recourse to external expert guidance and advice as required.

PRINCIPLE G4: OVERSIGHT OF RISK STRATEGY AND RISK APPETITE FRAMEWORK

It is best practice for the firm's risk governance body to provide the governance body with advice on the continued appropriateness of the risk strategy and risk appetite framework

- Develop a risk strategy that defines the overall approach to risk management, aligned to the business model, including its stated purpose, values, risk culture, corporate strategy and strategic objectives.
- Develop a risk appetite framework (approved by the governance body), including qualitative risk appetite statements and quantitative key risk indicators, that describe the aggregate types and the extent of risk that the firm is willing to assume (or avoid).
- Review the governance, risk management system and internal control system consistent with the risk strategy and risk appetite framework and recommend any material changes to the governance body. Such a review should be carried out periodically, or in the event of significant changes to or around the business. It would be best practice to appoint an external third party to complete a review at least once every few years.
- Consider whether there is appropriate alignment between the products and services and the risk strategy and risk appetite framework.
- Ensure there is a process whereby actual, or likely, material breaches of the risk appetite framework are escalated, including development of a risk acceptance process that manages the tension between the achievement of a firm's strategic objectives and risk control activities.

PRINCIPLE G5: PRINCIPAL RISKS KNOWN AND MANAGED WITHIN APPETITE

It is best practice for the firm's risk governance body to assess and advise the governance body on the principal and emerging risks and how they may affect the firm's likely fulfilment of its duty of care objectives and continued viability of its business model

- Challenge whether the first-line and second-line control functions have a sound understanding of the principal and emerging risks (including emerging categories of online harms), and the effectiveness of proposed or actual risk mitigation
- Periodically assess the effectiveness of the emerging risk identification and horizon scanning processes
- Consider the risks associated with proposed corporate actions, including significant changes to governance arrangements and legal structure, significant intragroup or outsourced service providers, operational resilience and business continuity arrangements for critical business services and impact on the continued viability of the business model

PRINCIPLE G6: EFFECTIVENESS OF RISK MANAGEMENT MONITORED

It is best practice for the firm's risk governance body to monitor and periodically advise the governance body as to the overall effectiveness of the firm's risk management system and internal control system

- Agree how the governance body will monitor and periodically assess the overall effectiveness of the firm's approach to managing the risk of online harms. This could include creating an online harms risk taxonomy that focusses on user risks.
- Consider whether individual and collective risk and control accountabilities are clearly and adequately documented and communicated.
- Ensure the business has embedded the internal control system and is periodically reporting the firm's: principal and emerging online harms risks; proposed or actual responses to these risks; and significant breaches of risk appetite.
- Ensure that the third-line audit function can review and advise the governance body of the results of independent assessments of the firm's risk management system and internal control system, including the effectiveness of the second-line internal control functions. The audit can be performed internally so long as the audit function is able to perform its duties independently and without interference from other stakeholders. The internal audit should focus on the governance and controls aspects of the risk management system and internal control system. The technical aspects of the risk assessment may be conducted by those who possess the technical capabilities to review and assess the risks, and may be supplemented by an external third party if additional expertise is required.

PRINCIPLE G7: EFFECTIVE COMMUNICATION OF RISK

It is best practice for the firm's risk governance body to assess and advise the governance body on the quality and appropriateness of the firm's risk information and reporting

- Consider a regular automated reporting mechanism, such as a risk dashboard, to provide risk information to the governance body that highlights significant matters relating to the effectiveness of protection measures. These risk matters should be monitored closely to ensure breaches are promptly resolved and do not re-materialise over time.
- Consider whether risk information and reporting presented to the governance body cover the full taxonomy of principal and emerging online harm risks in a manner that is comprehensible, enabling other stakeholders to understand, probe and challenge executive management effectively.

PRINCIPLE G8: SET AN APPROPRIATE RISK CULTURE AND ALIGNED INCENTIVES

It is best practice for the firm's risk governance body to periodically report to the governance body as to whether the firm's purpose, values and risk culture expectations are appropriately embedded in the risk strategy and appetite

- Assess and report to the governance body whether a statement of risk culture has been defined and communicated throughout the firm, i.e., the statement sets an expectation of understanding the consequences of online harms to better facilitate management of such risks
- Assess and report to the governance body whether ongoing risk culture monitoring activities are supported with useful metrics and indicators and have been embedded throughout the firm
- Provide a view to the governance body (and remuneration committee where one exists) on the appropriateness of the proposed risk-adjusted rewards for senior management and those engaged in risk-taking activities as well as ensure that there are no inappropriate incentives for second-line or third-line staff.

PRINCIPLE G9: INDEPENDENT EXECUTIVE OVERSIGHT OF RISK

It is best practice for the firm's risk governance body to safeguard the independence and objectivity of the individual responsible for overseeing risk management

- Appoint an individual to act as chief risk officer (CRO). This is ideally a dedicated individual with no first-line responsibilities who has the mindset, standing and gravitas to effectively challenge senior management's approach to online harms and be someone who has a good understanding of the firm, industry and the risks involved. In other firms this might form part of an executive's responsibilities or be an external party.
- Ensure that, for risk matters, the CRO has a reporting line to the chair of the risk governance body and direct access to the CEO.
- Ensure the CRO is supported by appropriate resources (referred to hereafter as the second-line risk function). These resources should be independent from the risk-taking being overseen and could be a dedicated independent internal or external team, or borrowed from another part of the firm. The second-line risk function is responsible for ensuring robust, independent oversight and challenge of risk-taking activities across the organisation. The members of the function should ensure they are not involved in risk-taking decisions that require their oversight.
- Periodically review and approve the risk management plan and activities of the second-line risk function, ensuring adequate resources are available to meet its obligations.
- Expect the CRO to produce risk reports for the governance body and the risk governance body that contain key concerns and matters relating to the management of online harms generated by the firm. There should be a standing agenda item at both the governance body and risk governance body to discuss the risk report. The report should include comments regarding the current risk profile of the firm and emerging online harms (both short-term and long-term), the appropriateness of the current management actions to deal with these risks and any incidents or breaches in the past which prompted regulatory intervention (including near-miss events).
- Allow the second-line risk function to support the organisation in identifying and adapting to material changes or developments in the internal or external environment, such as the use of technology to ensure online safety management systems are kept relevant and effective.

Appendix A – Glossary

Accountability	The ownership for ensuring an action is performed. Accountability for an action cannot be delegated, but responsibility for performing it can.
Business Model	A business model describes the rationale of how a company creates, delivers and captures value in economic, social, cultural or other contexts.
Challenge	The use of targeted questions to ensure completeness and reasonableness of understanding, views, ideas and assumptions.
Compliance Function	The person or collective group of people responsible for ensuring the controls and framework set in place are in line with both internal expectations and regulatory standards.
Consequence	The outcome of an event affecting the strategic objectives of a company. A consequence can be certain or uncertain and can have positive or negative and direct or indirect effects on objectives. It can be expressed qualitatively or quantitatively.
Online Safety Management System	The overall system that comprises the technology (including artificial intelligence, robotic process automation and natural language processing etc.), Terms of reference and broader safety measures that minimise the risk of harmful content being accessed by users via the firm's platform.
Control	A measure that maintains and/or modifies risk with the aim to mitigate the exposure of the company towards that risk. A control can mitigate the severity and/or likelihood of a risk. Controls refer to any system, process or decisions that could be implemented to mitigate the risk exposure.
Emerging Risk	A new or unforeseen risk that has not yet been fully understood. The available knowledge on these risks is usually limited and therefore requires careful consideration and monitoring.
Event	The occurrence or change of a particular set of circumstances. An event can have one or more occurrences, alongside several causes and consequences. An event can also be expected which does not happen, or something that is not expected which does happen. An event can also be a risk source.
External Risk	Risk that could arise from factors and circumstances beyond the company's control.
Governance	The structure on which a framework relies in order to operate efficiently and effectively.
Inherent Risk	An assessed level of risk in an activity or process that does not take account of any measures implemented to control the risk.
Internal Control Function	The people responsible for the implementation and monitoring of the internal control system within the company.
Internal Control System	The mechanisms, rules and procedures implemented and agreed by the governance body to ensure the integrity of the firm’s risk management system and the governance underlying it.
Key Risk Indicators	A set of useful information (i.e., metrics) that can be used to assess and measure the likely level of risk(s) in a specified setting.
Likelihood	The probability of an event occurring whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using either general terms or mathematically using the word “probability” or “frequency.”
Minimum Standards	This term refers to a set of standards defined by regulators which all firms subject to a particular regulatory regime must meet.
Near Miss	A situation where a risk event almost occurs, but is narrowly avoided.
Opportunity	An exploitable set of circumstances with uncertain outcomes requiring commitment of resources and involving exposure to risk.
Oversight	The overall review of the management to ensure that compliance with the principles being appointed by the regulator are met efficiently and effectively across all stages of the risk management process.

Principal Risk	The key risks the company is exposed to in relation to the firm's stated risk appetite and business model.
Residual Risk	The amount of risk or danger remaining after inherent risks have been reduced by risk controls. The company may or may not be aware that such risk exists in advance.
Risk	The uncertainty around the possibility of events occurring that could affect the likely achievement of a company's corporate strategy and objectives or legal and statutory requirements. An effect is a deviation from the expected and it can be positive, negative or both, and can address, create or result in opportunities and threats. Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.
Risk Acceptance	This occurs when a business or individual acknowledges that the potential benefit from taking on the risk outweighs the potential loss or consequences arising from it.
Risk Appetite	The aggregate types and extent of risk the governance body of each company is willing to take on and cope with, ensuring it lies within the company's risk tolerance to achieve its strategic objectives and deliver its business plan in both normal and stressed conditions.
Risk Appetite Framework	A key framework (approved by the governance body) designed to aid effective management decision-making, risk monitoring and reporting, and through which aggregate risk appetite is translated and cascaded into meaningful, calibrated risk thresholds, limits, metrics and indicators aligned to strategic objectives, and embedded throughout the company.
Risk Assessment	A dynamic process through which identified risks are assessed for likelihood, severity, scale, spread, complexity and seriousness of risks.
Risk Culture	The combination of a company's desired ethics, values, beliefs, knowledge, behaviours and understanding about risk, both positive and negative, that influences decision-making and risk-taking shared by a group of people with a common purpose.
Risk Dashboard	The graphical presentation of the company's key risk measures, often against their respective tolerance levels.
Risk Function	The people responsible for the implementation and monitoring of the risk management system within the company.
Risk Governance	The activity of oversight of a company's risk management system.
Risk Identification	A deliberate and systematic process of identifying both existing and emerging risks.
Risk Limits	The boundaries around the risk tolerance of different types of risks that the company should not breach as part of its compliance with the regulator and its strategic risk appetite statements. These limits are used by the first line to identify when there is a danger of exceeding the desired level of risk.
Risk Management	The application of resources to minimise and control the probability and impact of unfortunate events, or to maximise the realisation of opportunities.
Risk Management System	A set of strategies, processes and reporting procedures used to manage risks within an organisation with the aim of eliminating or minimising the impact of risks to the organisation. It should be well integrated into the organisational structure and decision-making processes of the firm.
Risk Thresholds	A lower-level boundary around the risk tolerance of different types of risks which flags that a risk is moving towards a breach of the relevant risk appetite statement.
Risk Profile	A breakdown of the threats that the company faces, or might face, along with a description of the severity and frequency of such threats. Determining a company's risk profile includes identifying the inherent risks within the design of the business and risks that may arise externally.
Risk Source	An element which alone or in combination has the potential to give rise to risk.
Risk Strategy	The company's overall approach towards risk management, which aims to achieve corporate objectives.

Risk Taker	An individual who is responsible for taking risks on behalf of the company, e.g., creating products or services, interacting with users, hiring staff etc.
Risk-Taking Activity	The process where an individual engages in an undertaking which involves risk(s) in anticipation of a better payoff or reward for the company.
Risk Taxonomy	This refers to the hierarchical categorisation of risk types based on exposure to aid mitigating actions.
Risk Tolerance	The maximum level of risk a company can take on, given its current level of resources, before breaching financial, operational, legal or regulatory limits.
Risk Universe	This term refers to the risk categories as described in the main report. A representation of a company's key sources and categories of risk.
Scenario Analysis	A process for selecting and analysing one or more changes to key variables and assumptions underlying a scenario to evaluate the impact on the output, including assessing the effectiveness of possible risk measures.
Stakeholder	This refers to a person or company that can affect, be affected by, or perceive themselves to be affected by a decision or activity. The term "interested party" can be used as an alternative.
Stress Testing	A process for selecting and analysing one or more extreme changes to key variables and assumptions underlying a scenario in order to evaluate the impact on the output, including assessing the effectiveness of possible risk measures.
Third Party	This often refers to an external stakeholder that could potentially become involved or is already involved with the process.

Appendix B – Desktop Research

Item	Title
1.	Audiovisual Media Services, Government response to public consultations on the government's implementation proposals (24 July 2019) https://www.gov.uk/government/consultations/requirements-for-video-sharing-platforms-in-the-audiovisual-media-services-directive/outcome/audiovisual-media-services-government-response-to-public-consultations-on-the-governments-implementation-proposals
2.	Online harms White Paper - Initial consultation response (15 December 2020) https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response
3.	Online harms White Paper: Full Government Response (FGR) to the consultation (15 December 2020) https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response
5.	Regulating video-sharing platforms - A guide to the new requirements on VSPs and Ofcom's approach to regulation (21 October 2020) https://www.ofcom.org.uk/__data/assets/pdf_file/0021/205167/regulating-vsp-guide.pdf
6.	Video-sharing platform - Guidance for providers on measures to protect from harmful material (24 March 2021) https://www.ofcom.org.uk/__data/assets/pdf_file/0028/216487/vsp-harms-draft-guidance.pdf
7.	The Risk Coalition - Raising The Bar: Principles-based guidance for Board risk committees and risk functions in the UK financial services sector (2019) https://riskcoalition.org.uk/the-guidance
8.	Input from Bayes Business School (formerly Cass Business School) - Digital Research Leadership Centre https://www.cass.city.ac.uk/faculties-and-research/centres/digital-leadership-research-centre
9.	FCA - Our Business Plan 2020/21 https://www.fca.org.uk/publications/corporate-documents/our-business-plan-2020-21
10.	Information Commissioner's Office https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/#:~:text=The%20UK%20data%20protection%20regime%20is%20set%20out,The%20ICO%20regulates%20data%20protection%20in%20the%20UK
11.	The IIA's Three Lines Model https://na.theiia.org/about-ia/PublicDocuments/Three-Lines-Model-Updated.pdf
12.	The Three Lines Model. CRO Forum. 2021 https://www.thecroforum.org/wp-content/uploads/2021/05/CRO-WG-Governance-.pdf
13.	Draft Online Safety Bill. 2021 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf
14.	Proposal of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC. European Commission. 2020 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72148
15.	Establishing a pro-active risk management culture. Swiss Re. This publication is no longer available publicly but can be made available upon request from: PUBLICATIONS@swissre.com 2010
16.	Transforming culture in financial services – Driving purposeful cultures. Discussion Paper DP 20/1. Financial Conduct Authority. 2020 https://www.fca.org.uk/publication/discussion/dp20-1.pdf
17.	How to hire a great Chief Risk Officer. A guide to the recruitment of Chief Risk Officers and other senior risk professionals. Institute of Risk Management. 2019 https://theirm.org/media/8461/how-to-hire-a-great-cro.pdf

18.	Positioning independent Risk Management to succeed. Protiviti. 2016 https://www.protiviti.com/IN-en/insights/bpro85
19.	Risk Management: Learn More from Near-Misses. Chemical processing. 2014 https://www.chemicalprocessing.com/articles/2014/risk-management-learn-more-from-near-misses/
20.	Charting A Way Forward: Online Content Regulation. Facebook. 2020 https://about.fb.com/wp-content/uploads/2020/02/Charting-A-Way-Forward_Online-Content-Regulation-White-Paper-1.pdf
21.	Addressing harmful online content. A perspective from broadcasting and on-demand standards regulation. Ofcom. 2018
22	What Corporate Boards Can Learn from Boeing's Mistakes. Harvard Business Review. June 2021 https://hbr.org/2021/06/what-corporate-boards-can-learn-from-boeings-mistakes

Appendix C – Reliances and Limitations

The information contained in this report is based upon a review of risk management "best practices" that have been observed through a review of academic and industry literature and directly through consulting work. The report does not represent a specific recommendation for the manner in which any firm should seek to achieve the principles outlined and does not intend to imply that following the principles outlined is guaranteed to produce a "no risk" outcome.

Where we have referred to practices described in third-party reports or articles, we have made reasonable endeavours to confirm the accuracy of the information but cannot guarantee that all sources used are entirely accurate. To the extent that any sources were significantly misleading, it is possible that the information we have presented could change. However, by using a wide range of sources, we believe that the chances of this are relatively low.

To the extent that we have included information in case studies, we have used publicly available information and are not aware of any restrictions relating to its inclusion in this report. To the extent that new information relating to a particular case study comes to light in future, then it is possible that the appropriateness of the case study to illustrate a particular point could be impaired. No reliance should be placed upon any draft version of this report.

This report has been prepared by Milliman for Ofcom as an internal resource to assist it during its considerations of the regulatory regime that is being developed for online safety. It must not be relied upon for any other purpose. Except with the written consent of Milliman, this report and any written or oral information or advice provided by Milliman must not be reproduced, distributed or communicated in whole or in part to any other person or relied upon by any other person.

The use of Milliman's name, trademarks or service marks, or reference to Milliman directly or indirectly in any media release, public announcement or public disclosure, including in any promotional or marketing materials, customer lists, referral lists, websites or business presentations is not authorised without Milliman's prior written consent for each such use or release, which consent shall be given in Milliman's sole discretion.

Milliman is among the world's largest providers of actuarial and related products and services. The firm has consulting practices in life insurance and financial services, property & casualty insurance, healthcare, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

milliman.com

CONTACT

Neil Cantle

neil.cantle@milliman.com