Continue

Share — copy and redistribute the material in any medium or format for any purpose, even commercially. Adapt — remix, transform, and build upon the material for any purpose, even commercially. The licensor cannot revoke these freedoms as long as you follow the license terms. Attribution — You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits. You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation . No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material. As a library, NLM provides access to scientific literature. Inclusion in an NLM database does not imply endorsement of, or agreement with, the contents by NLM or the National Institutes of Health. Learn more: PMC Disclaimer | PMC Copyright Notice . 2012 Feb;12(1):25–28. doi: 10.7861/clinmedicine.12-1-25 Health services are inherently risky: their core activities involve a response to unpredictable events where the potential for loss (both financial and non-financial) is high. Moreover, the responses themselves have uncertain consequences when things go wrong, and healthcare providers need to be aware of the risks they face in order to manage them in the interests of both patients and staff. Risk management has been defined as the systematic identification, assessment and evaluation of risk.1 Used properly in healthcare, it can not only be a process to report incidents, but also minimise the harm that clinical or resourcing errors can cause to patients and staff. From this perspective, the risk manager's remit in the NHS covers a wide range of activities–from the assessment and identification of risks through financial risk-transfer measures to investment in the quality of clinical care and beyond. The practice of risk management has developed and widened considerably in the NHS in the last decade in response to several key reports including An organisation with a memory,2 which highlighted the need to learn from clinical error, and Standards for better health, which outlined potential improvements to the quality of care across several dimensions.3 Moreover, risk management can be considered as part of the broader area of clinical governance which is defined by Chandraharan and Arulkumaran as a 'framework through which NHS organisations are accountable for continuously improving the quality of their services and safeguarding high standards of care by creating an environment in which excellence in clinical care will flourish'.4 Risk management encompasses many aspects of clinical governance, from risk reporting (and response to complaints) to audit, guidelines, risk assessments (risk registers) and training.1 In 2009, the Audit Commission recommended that trusts should 'review their risk management arrangements–including the way in which risks are reported to the board' and that the Department of Health as well as Monitor (the regulator of foundation trusts (FTs)) should 'consider further incentives and sanctions to reward good governance through greater autonomy and take action to address shortfalls where they arise'.5 This paper explores this theme–the inter-relationship between good governance, financial incentives and clinical risk management–and provides an overview of recent developments together with some evidence gleaned from views expressed by key decision takers within the NHS. Firstly, rating systems used within the NHS to classify hospitals according to the quality of their risk management activities are reviewed. A risk management programme was introduced by the NHS Litigation Authority (NHSLA) in 1995, although it was 2000 before it was fully implemented. The core of this programme is provided by a range of NHSLA standards and assessments, and it is a requirement of continued membership of the Clinical Negligence Scheme for Trusts (CNST) that hospitals are subject to audit by the NHSLA. A set of risk management standards for each type of healthcare organisation was developed incorporating organisational, clinical, and health and safety risks (www.nhsla.com). All the NHSLA standards are divided into three 'levels'. NHS organisations which achieve success at level one in the relevant standards receive a 10% discount on their CNST contributions, with discounts of 20% and 30% available to those passing to levels two and three respectively. Members of the CNST scheme are required to achieve level one compliance and are assessed on an annual basis until this is achieved. Organisations at level one are assessed against the relevant standard(s) once every two years and those at levels two and three at least once in any three-year period, although organisations may request an earlier assessment if they wish to move up a level. The discount earned by members is applied to contributions in the financial year following a successful assessment and is valid for two years. Organisations which fail an assessment are required to be assessed at the level assigned in the following financial year. Monitor uses the term governance to describe the effectiveness of an NHS FT's leadership. It uses performance measures, such as whether FTs are meeting national targets and standards (eg a reduction in methicillin-resistant Staphylococcus aureus (MRSA) rates), together with a range of other governance measures such as community representation, appropriate board roles and structures, clinical quality and service performance. Specifically, it requires evidence that boards address and resolve any risks that have been identified. Trusts are rated red (significant breach of terms of authorisation), amber-red (material concerns), amber-green (limited concerns) or green (no concerns). When assessing financial risk, Monitor's ratings reflect the likelihood of an actual or potential financial breach of the FT's terms of authorisation. The ratings are based on four criteria: achievement of financial plan, underlying performance, financial efficiency, and liquidity. Financial risk ratings are allocated using a scorecard which compares key financial information across all FTs. A rating of five reflects the lowest level of financial risk and a rating of one the greatest. If an NHS FT has failed to comply with the terms of its authorisation and this is significant–for example, if it consistently fails to meet required standards of care or is at significant financial risk–Monitor's board may decide to use its statutory powers of intervention. These range from closing a specific service, to removing any or all of the directors or governors and appointing replacements. To get a better appreciation of how risk management operates in NHS trusts, the views of nine acute NHS trust risk managers were obtained via exploratory telephone interviews in 2010 and 2011. Eight of the nine trusts selected had recently achieved an increase in their CNST risk management level. The main findings to emerge from these interviews were as follows: All trusts which achieved a risk management level increase claimed to have done so as part of a planned strategy–while this was mainly the responsibility of the risk management staff, other stakeholders, such as the board of directors and clinical staff, were also engaged. The declared motivations for seeking a risk management level increase involved both reputational and financial issues. From a reputational perspective, trusts see patient safety and quality benefits from obtaining higher risk management levels '…the push for level two was about reputation and how we looked as a trust'; 'It was a priority at board level to get to level three … to demonstrate that the trust's safety and quality agenda was in place and was embedded across the trust'. From a financial perspective, as discussed above, the NHSLA provides discounts on a trust's CNST contribution in return for the achievement of higher risk management levels and such discounts act as an incentive, as evidence by one interviewee: 'there also was the financial incentive–the 10% discount on the premium was substantial and this came at a time when financial pressures were starting to be considered'. Financial strength is seen as being important in order to obtain risk management level increases. Trusts that are in a position to commit financial resources to assist with an NHSLA assessment typically will do so, and find such investments to be more than justified if a successful outcome is obtained. Making such an investment is not felt to be a prerequisite to obtaining a risk management level increase but there is a general consensus that financially strong trusts are in a better position to do so as they have more resources to enable them to make such financial investments. Trusts with good governance structures believed that they were more likely to obtain risk management level increases. Eight of the nine trusts had recently increased their risk management level while all had recently acquired FT status. These tended to go hand in hand: one interviewee felt that trusts had to demonstrate good risk management arrangements as part of the process when applying for FT status, while another felt that a positive outcome of acquiring FT status was that it gave trusts a 'good governance structure which helped when applying for risk management level increases'. The governance structures in place as a result of acquiring FT status are said to be enhancing the risk management function within trusts. The new structures in FTs include public interest governors, staff governors and representation from the trust board. While such arrangements have taken time to settle down, they now 'work quite well and both public and staff governors are willing to support quality initiatives such as the patient experience'. From a financial perspective, FTs are also granted financial freedoms such as the ability to raise capital from both the public and private sectors within borrowing limits determined by projected cash flows–this is said to enhance the ability to invest in risk management level improvements. In summary, the consensus of the views obtained from our interviews with risk managers implied that there are definite relationships between governance structures, financial health and risk management activities–trusts typically have a plethora of external organisations to deal with on an annual basis and improvements made in governance relationships (as evidenced by acquiring FT status) are typically accompanied by improvements in a trust's financial position, and this improved financial health is an enabler to help them improve their risk management practices. From the views expressed by hospital risk managers, there would seem to be a strong a priori expectation that hospitals with good governance would perform well in relation to the management of clinical risks. Well run hospitals should have in place the structures to enable sound decisions about the allocation of resources, including those concerned with investment in patient safety measures. Moreover, hospitals with sound finances are expected to be best placed to manage clinical risk well; clearly, concerns about financial risks would be expected to constrain management in pursuing clinical risk management opportunities which require additional resources. To confirm whether this expectation was borne out by the evidence, the extent to which the ratings described above were correlated with each other were explored. The following tables show the results obtained by comparing the ratings given to 137 foundation hospitals as at 30 June 2011, including the CNST risk management levels as assessed by the NHSLA and current at that date. Tables 1 and 2 show the relationship between the CNST risk management levels and Monitor's finance and governance risk ratings respectively. Surprisingly, there appears to be little correlation between these, and this is confirmed by the Chi-squared tests reported at the foot of each table. By contrast, Table 3 shows a significant relationship between Monitor's ratings for financial and governance risk. It seems that Monitor's separate assessments of hospitals' exposure to risk is correlated, but bears little relationship to the quality of clinical risk management measures as audited by the NHSLA. CNST levels by finance ratings. CNST levels by governance ratings. Governance ratings by finance ratings. Part of the explanation for this conundrum may lie with the way that the NHSLA incentivises hospital managers to improve their risk management levels. Discounts of up to 30% on the CNST contributions are available for hospitals assessed at the highest level. This could conceivably lead to mixed consequences: hospitals with good governance and low financial risk may feel that the extra expense involved in acquiring higher standards is justified, but on the other hand hospitals facing financial problems could also feel that the contribution discounts are a way of easing those problems. So the relationship between governance, finance and clinical risk may be a complex one. To illustrate this, as part of a programme of research funded by the ESRC on public services quality, several studies exploring the link between the financial incentives for improved risk management and the responses by NHS hospitals were recently conducted. In one study, no relationship between the utilisation of diagnostic imaging tests and the risk management level attained was found.6 However, in another a positive relationship between higher risk management levels and a lowering of the hospital's MRSA infection rate was found.7 It has been speculated that certain types of patient care activity, including the use of diagnostic tests ordered by individual clinicians, may be less responsive to risk management incentives placed at the level of the hospital, whereas others, such as hospital infection control policies, are much more amenable to financial incentives at that level. In this paper the reasons why good hospital governance and sound finances are expected to be conducive to improved clinical risk management processes and outcomes have been set out. These expectations were shared by those risk managers interviewed in NHS hospitals–they clearly believed that there was a causal connection between their governance structures, the quality of their financial risk management, and the NHSLA's assessment of their clinical risk management standards. In practice, the current evidence from FTs does not bear this out, at least in the strict sense of a correlation between measurements of risk management standards across these categories. Why should this be so? There are a number of possible explanations. The measurement of risk management standards by Monitor and/or the NHSLA may be flawed, or the measurement may be accurate but the expected relationships are not there–they could be based on rhetoric not reality. Alternatively, the notion of risk management is something far more complex than can be captured by a single number for each hospital. Complex organisations can suffer from considerable inefficiencies, not least in terms of communications and internal incentives. Harris addresses such points explicitly to hospitals. He argues that the hospital is 'two firms in one': a medical staff and an administration, each with 'its own objectives, decision variables, and constraints'.8 Attempts to incentivise one of these groups to the exclusion of the other may end in failure. This problem is not a new one, but the widening remit of risk management in NHS hospitals does beg the question: whose risk is being managed? 1.Cottee C, Harding K. Risk management in obstetrics. Obstet Gynaecol Reprod Med 2008; 18: 155–62 10.1016/j.ogrm.2008.04.003 [DOI] [Google Scholar] 2.Department of Health. An organisation with a memory 2000London: DH [Google Scholar] 3.Department of Health. National standards, local action. Health and social care standards and planning framework 2005/7002 −− 60/.80 Annex 1 2004Leeds: DH [Google Scholar] 4.Chandraharan E, Arulkumaran S. Clinical governance. Obstet Gynaecol Repro Med 2007; 17: 222–4 10.1016/j.ogrm.2007.05.003 [DOI] [Google Scholar] 5.Audit Commission. Taking it on trust: a review of how boards of NHS trusts and foundation trusts get their assurance 2009London: Audit Commission [Google Scholar] 6.Fenn P, Gray A, Rickman N, et al. Enterprise liability, risk pooling and diagnostic care. J Pub Admin Res Theory 2010; 20: i225–42 10.1093/jopart/muq026 [DOI] [Google Scholar] 7.Fenn P, Gray A, Rickman N, Vencappa D, Rivero O. The impact of risk management standards on patient safety: the determinants of MRSA infections in acute NHS hospitals, 2001–2008. 2011 Centre for Risk and Insurance Studies Working Paper. [Google Scholar] 8.Harris JE. The internal organisation of hospitals: some economic implications. Bell J Econ 1976; 8: 467–82 [Google Scholar] Articles from Clinical Medicine are provided here courtesy of Royal College of Physicians Risk management in healthcare is a means of identifying, assessing, prioritising and controlling risks across an organisation. It is a key element of good governance and underpins the ability to provide safe and effective care and supports to people who use health and social care services. Risk management is a continuous process which demands a proactive approach by an organisation to prevent harm or loss. In HCI's research paper "The Healthcare System: Will We Ever Learn? – A Review of the Common Themes arising from UK and Ireland Healthcare Inquiries", HCI found that Risk Management was one of the common themes arising between Ireland and UK serious events. The inquiries reviewed identified systematic failings in the organisations risk management approaches that directly impacted on quality and safety of the services provided to patients. For example, the Liverpool Community Health NHS Trust was found to have no clear and effective system in place to manage risk or to communicate identified risks to senior management within the wider NHS. The Scally Report identified inherent weaknesses in the CervicalCheck risk management processes, including the manner in which the risks were identified, communicated and managed, and in particular the processes by which serious risks could be escalated. In the Portlaoise Hospital Report HIQA found that risks were not comprehensively reviewed or addressed at senior level, all known risks were not captured, and staff were not confident in local and regional systems. In this blog we detail the principles of Risk Management, some of the advantages and challenges and provide some guidance on service indicators that can be used to support the identification of risks. Principles of Risk Management The following principles of risk management are identified in the HIQA Guidance on Risk Management (2014): The identification, assessment and management of risk promotes the independence and social inclusion of older people. The assessment of risk highlights both the negative and positive aspects of any situation. Risks change as circumstances change and need to be reviewed on a regular basis. Information used and recorded needs to be as comprehensive and accurate as possible. Identification of risk carries a duty to do something about it. Involvement (SU, family, advocates, professionals / staff) improves the quality of risk assessment, management and decision making. Risk taking involves everyone working together to achieve positive outcomes. The Advantages of Risk Management Risk management has many real benefits for a healthcare organisation, including: Provides a safe, quality service to service users and staff. Improves Governance. Gain a true understanding of an organisation and its services: Improves organisational learning and communication. Improves mandatory and voluntary reporting. Improves stakeholder confidence and trust. Work proactively to identify and treat risk as needs changes. Increase staff awareness on risk areas. Improves the organisation's safety culture. Leads to more effective decision making. The Challenges of Risk Management As discussed in HCI's Research Paper there are challenges with risk management which can have negative consequences that directly impact on the quality and safety of the services provided to the service users. Some of the challenges include: Can be time consuming. Often difficult to know where to start. Paperwork and duplication across the risk registers. Roles and responsibilities eg. who is responsible for what area of the risk register. Active monitoring of risks and updating of risk register. Prioritisation of risks. Service indicators to support identification of risks Healthcare organisations need to be able to effectively use service indicators to understand their organisation and be responsive to risk. Indicators which are harnessed from real time data, can provide a true reflection of the service activities and support the identification of issues or potential risk areas. The areas of service where indicators may arise from include: patient-safety incidents and other incidents involving patients and staff complaints, concerns and compliments findings from risk assessments / gap analysis legal claims audits satisfaction surveys findings and recommendations from national and international reviews and investigations casemix, activity and performance data. Where the information from these indicators is effectively gathered, extracted and analysed, it can provide real oversight of the service and can be effectively utilised to manage risk and develop quality improvement initiatives. Conclusion Historically risk management was a reactive model, but we can see that being proactive with risk management enables the service to get out ahead of potential issues and work to identify controls that can minimise risks or reduce the potential impact of an issue. Although risk management is viewed as everyone's business, it must be driven by senior management to ensure that it is seen as a priority. At HCI, we help providers of health and social care make intelligence driven decisions to attain, manage and improve quality, safety and regulatory compliance. Since 2005, we have supported health and social care organisations to build comprehensive risk management systems to effectively manage and reduce risks in their organisations. If you would like support in developing a Risk Management System, contact HCI at info@hci.care. Download a copy of the HCI Research Paper Discover the crucial role of risk management in healthcare leadership and how it ensures safe and efficient operations. Explore the importance of identifying, assessing, and mitigating risks to protect patients, staff, and the organisation's reputation. When it comes to delivering high-quality healthcare, being an effective leader requires you to make the right decisions, set the most appropriate priorities, motivate others and ensure activities under your remit to function soundly and as efficiently as possible. How does risk management fit in? If you already work in or aspire to hold leadership and management positions within the UK National Health Services (NHS) or other country's health and social care providers, you'll be aware of the importance not only of ensuring things run smoothly and safely, but also continuously evaluating and improving the quality of healthcare systems and services. As well as overseeing day-to-day activities, healthcare leaders need to quickly identify and competently deal with any problems and challenges which may arise. Planning, ideally averting and preparing to tackle such issues, both likely and unlikely, is essentially what risk management is all about. It concerns the clinical and administrative systems, processes, procedures, and reporting structures designed to detect, monitor, assess, mitigate, and prevent risks to patients and staff. It could be something as simple as ensuring health practitioners and visitors to health establishments regularly use hand sanitiser to avoid spreading infections to patients. Alternatively, in the event of a major incident which involves hundreds or thousands of casualties with a range of injuries, triage systems and multi-agency cooperation may be needed. Are leadership and management different? Does it matter in healthcare? Read our guide: Why is risk management in healthcare important? Managing risk is an ongoing strategic and operational responsibility in any healthcare setting as it informs the decision-making that affects everything from training and recruitment to resource allocation and procurement. At a strategic level, medical risk management protects patients and staff from medical errors or harm, and the organisation from any financial or legal repercussions, such as a lawsuit or cyber attack, both of which could cause irreparable damage to the organisation's reputation. Operationally, it provides guidance and clarity to the many individuals involved in delivering healthcare services, for example, through surgical checklists, cleaning regimes and disinfection procedures or monitoring essential training and certification. This enables all members of staff to work more effectively together, providing a safe, quality service to service users and staff, employing the same shared (and understood) systems, procedures and processes and proactively identifying and dealing with risks as and when they happen. How do you develop a strategy for risk management in healthcare? Most larger healthcare establishments will have at least one role dedicated to quality, compliance, risk management and/or patient safety, however, all healthcare staff will probably be expected to participate in the identification, assessment, planning and management of clinical and non-clinical risks. As a head of service, team leader or other senior manager, you'll be expected to encourage risk awareness among staff and be required to keep and regularly review a detailed risk register, prioritising risks and escalating any risks that actually occur in accordance with any pre-prepared protocols and procedures. The volume and variety of risks is potentially huge and be aware that they will exist at different levels, for example: Strategic risks: risks that affect ability to deliver corporate strategy or function as an organisation as a whole. Corporate operational risks: risks that affect the delivery of an operational plan or common team risks that require a corporate response. Team risks: risks related to the delivery of departmental operations and objectives. Programmes and project risks: risks associated with specific activities, which may be short, medium or long-term. It is likely that your employer will have its own guidance for risk management, so always check first. If not, the UK-based Health and Safety Executive (HSE) outlines five key steps for risk management which provide a useful starting point: Identify risks: what might cause harm, what practices are safe/unsafe, are any dangerous substances or equipment in use? Assess the risks: who might be harmed and how, what is the likelihood of this happening, how and who can prevent or control the risks, what action is needed? Control the risks: can you get rid of the risk altogether, is what you are already doing sufficient, what more needs to be done? Record your findings: document the risks in a risk register, stating who might be harmed and how, the likelihood and what is being done to manage the risks? Review the controls: based on recent or past events, does anything need to be changed, are there any new risks that need adding, has the risk register been effective? Why should I study the MSc in Healthcare Leadership? Central to the curriculum of our MSc in Healthcare Leadership is the development of your ability to reflect on the practices, personality and approaches required for good leadership in a variety of healthcare systems worldwide. In doing so, you'll develop the same perspective, context, critical thinking, analytical and decision-making skills required to manage risks and enhance your own practice and that of those around you. The Supporting Change, Innovation, and Problem-Solving module will be of particular relevance, teaching you how to evaluate the effectiveness of strategies to promote and implement change, be that managing risk or anything else. Promoting Quality and Safety in Healthcare is focused on evidence-based models of best practice to improve the quality of care delivery and maximise patient safety, while the Global Perspectives on Healthcare Policy module will also help you better understand how to develop policies, including risk management, at the macro, meso, and micro level. Are you ready to take your healthcare or clinical career to the next level? Discover the University of Hull Online's part-time MSc in Healthcare Leadership: The National Quality Board (NQB) was established in 2009 to champion and drive strategic alignment for quality across health and care, on behalf of NHS England, the Care Quality Commission (CQC), the UK Health and Security Agency (UKHSA), the National Institute for Health and Care Excellence (NICE), the Office for Health Improvement and Disparities (OHID), the Department of Health and Social Care (DHSC), Healthwatch England, the Health Services Safety Improvement Body (HSSIB) and the National Guardian's Office (NGO). This document is part of a wider suite of guidance developed by the NQB for integrated care systems (ICSs), notably: the Shared Commitment to Quality (2021); Guidance on System Quality Groups (2021) and; Guidance on Quality Risk Response and Escalation (2022). All of the NQB's guidance is available on the webpage: NHS England » National Quality Board publications for integrated care systems The NQB would like to specifically thank the NHS England South West Clinical Quality Team for its work in developing these principles. This document complements the National Quality Board's (NQB) other guidance for integrated care systems (ICSs), and particularly the National Risk Response and Escalation Guidance which sets out how quality risks and concerns should be managed in ICSs. The document sets out key principles to use when assessing risks in environments or scenarios that are rapidly changing or based on multiple factors (e.g. multiple services/organisations involved). Whether it is unprecedented levels of pressure, unit and care home closures, new technologies, IT systems or medicines coming onto the market, pandemics or public health emergencies, health and care organisations are faced with increasing complexity. Individual health and care organisations, including providers, Integrated Care Boards (ICBs) and Local Authorities, must ensure their approach to risk management meets recognised standards and best practice (key guidance on risk assessment in health and care includes the National Patient Safety Agency's Risk Matrix for Risk Managers, 2008), including: agreed risk appetite statements; common language and scoring; and risk frameworks clearly linked to associated accountability and governance frameworks, which cover quality alongside wider risk frameworks (e.g. operational, financial). However, in multi-factorial and complicated situations, collaborative approaches and whole system solutions are also required. This document has been designed to help those working in these scenarios. It does not provide detailed operational guidance on "the how"; how to develop common language and scoring, how to develop system risk appetites etc. However, it does provide a set of guiding principles, and through testing with systems we hope to provide more detailed learning on deploying the principles set out in the document. Care quality is understood according to the NQB shared commitment's definition, as care that is safe, effective and provides a personalised experience. This care should also be delivered in a way that is well-led, sustainable and addresses inequalities. This means that it enables equality of access, experiences and outcomes across health and care services*. Whilst developed to align with the NQB guidance, the approach also draws on Emergency Preparedness, Resilience and Response (EPRR) principles and can be used to support decision makers to fulfil their statutory responsibilities in planning for and responding to incidents. Annex A provides recent case studies to illustrate usage of the framework, covering mental health and ambulance services. *The concept of high quality health and social care must take due account of requirements in relation to the Equality Act 2010 and the Public Sector Equality Duty and relevant requirements in relation to reducing health inequalities introduced by the Health and Social Care Act 2012 and/or in the current Health and Care Bill. This aligns with the CQC's 2021 strategy. These principles sit alongside the other NQB guidance, as well as the National Oversight and Assessment Framework (OAF), the National Patient Safety Strategy and wider frameworks (e.g. EPRR, Emerging Concerns Protocol). The NQB has published a suite of guidance to help systems put in place effective leadership, culture, governance, structures and systems to manage and improve quality. This guidance has set out the expected purpose and function of System Quality Groups* and articulated the framework and mechanisms for managing and escalating quality risks and concerns, which the NQB sees as core to effective quality, including safety, management. Systems may also find it helpful to consider the four areas associated with Safety management system frameworks. *System Quality Groups (SQGs) replaced Quality Surveillance Groups in the 2022 updated NQB guidance. All ICSs must have a SQG to bring together system partners to drive intelligence sharing and quality improvement across the ICS. Key members are: Integrated Care Boards (ICBs), Local Authorities, NHS England, CQC, primary care, local maternity systems (LMS), patient safety specialist(s) and at least two lay members, including Healthwatch. The NQB's framework for managing quality risks, the National quality risk response and escalation guidance, is based on an open culture and learning system, proactive and transparent intelligence sharing, system working and the need to manage risks as close to the point of care as possible. The guidance is clear that mitigation and management of risks and concerns often requires whole system approaches and solutions, involving partners from across health, social care and other services in places, systems, regions and nationally. The guidance also clarifies the mechanisms to be used to manage risk, most notably Rapid Quality Reviews and Quality Improvement Groups, alongside wider governance structures. The NQB's Guidance on Risk Response and Escalation is being implemented to manage risks at provider, place, system, regional and national level, however effective risk assessment and management across systems remains an area of priority, challenge and complexity. Providers and systems are having to manage significant pressures in workforce, service capacity and finances, changing population health needs, and the need to balance and share risks in multiple areas across settings. In rapidly changing and multi-factorial situations, such as closures of care homes or mental health units, or highly pressured urgency and emergency care (UEC) departments, collaborative and dynamic approaches to risk assessment are required to decide upon the best possible or least worse course (or multiple courses) of action*. *This approach is in line with the JESIP (Joint Emergency Services Interoperability) principles – Principles for joint working – JESIP Website. The people, teams, services and organisations involved from across NHS, local authority and voluntary, community and social enterprise (VCSE) partners must be able to answer questions such as: do we have a sufficiently good understanding of the risk profile and mitigating actions within and across our organisations, pathways, services and places or are there emerging risks that are not being addressed? are all staff clear and sighted on the organisation and local system approach to risk sharing and what that means for individual staff and staff groups? how do we best work together as organisations across a place, integrated care system and Partnership to manage risks? how do risks across the pathway/organisations in our system aggregate and interrelate to impact on the overall summarised risk profile presented? To answer these questions, it is important to consider risks from the perspective of different organisational/outcome lenses to understand connectivity and where resources should best be applied, and to support decision-making in rapidly changing and multi-factorial situations where collaborative solutions may be required to achieve a risk reduction across the system. An overview of risk management is presented in Figure 1 below, taken from the ISO 31000 Risk Management – Guidelines (2018). Figure 1: Overview of risk management Image description: The image depicts the risk management process as a circular flow diagram. The main steps are: scope, context, criteria risk assessment (including identification, analysis, and evaluation) monitoring and review risk treatment recording and reporting The steps are connected by arrows showing the iterative nature of the risk management cycle. A risk is the effect of uncertainty which, should it occur, will impact either positively or negatively on those who use the service, staff, the organisation and/or the system. Risk management can be described as a coordinated set of activities and methods that is used to direct an organisation and to control and mitigate the risk(s). Risk assessment is the process of determining the probability of a risk occurring and the likely consequences. It is made up of three processes: risk identification, risk analysis and risk evaluation. Risk assessment is an iterative and collaborative process which draws on the knowledge and view of stakeholders. It should use the best available information, supplemented by further enquiry, as necessary. Risk appetite is defined by the Institute of Risk Management as the amount of risk that an organisation or system is willing to seek or accept in the pursuit of its long-term objective. Whilst there is a standard framework for risk management, a key principle of effective risk management is the need to base is on the local risk appetite and intelligence, which will be unique to each provider, pathway or system. Risk assessment is common across all health and care organisations, with most organisations likely to use a matrix approach to risk recording comprised of a 'Likelihood X Consequence' model. Typically, risk is recorded in a format like the example below: ExampleConsequenceLikelihoodScoreThere is a risk that..... caused by... this would lead to an impact/effect on...444X4= 16 Figure 2: A typical '5×5' risk matrix Image description: The image is a 5×5 grid depicting a risk assessment matrix. The rows represent the consequence levels from Minimal to Severe, while the columns show the likelihood levels from Rare to Almost certain. Each cell in the matrix contains a risk score based on the combination of consequence and likelihood. The risk scores range from Very low 1 to Extreme 25. The color-coding provides a visual indication of the risk level, with green representing lower risk, yellow for medium risk, and red for higher risk. Risk assessment is often a pre-planned, systematic evaluation of potential risks, typically done before an activity starts and on an ongoing basis at set intervals. It identifies hazards and controls based on known conditions, and typically within single organisations. In most scenarios, existing risk processes and frameworks should be used, however in multi-factorial, fast-changing environments, there is a need for an approach that also analyses risk from the perspective of different organisations/ services and considers how risks may be shared across the system. The table below sets out the types of environments and contexts to which this document applies (on the right side): Standard riskRisk in multi-factorial, fast changing environmentsUsually simple risks based on linear cause and effectReflective of a changeable set of internal/environmental states – often speculativeMore easily predictable and therefore assessableLess easily predictable and more complicated to assessTends to support risk trajectory from high towards lowWhen viewed from different perspectives; concludes a least worse/best possible option, which may not reduce all risksA single risk, within the remit of a single team, department or organisationRisk within a system or network, with recognised connectivity and contagionBased on historical knowledge/patternsCan be unpredictable and often unknown/novel conditionsCommonly the factors used in corporate risk assessmentsCommonly associated with unknown situations or emerging informationAssessment requires a variation from a set of known baseline conditions. Requires assessment of a number of interconnecting factors (e.g. pathways, organisations, time). Determines the reasonably practicable measures to be taken. Examples in health and care may include: When a decision is made in a short time frame to close a care home or a home care agency hands back a contract. Staff in those teams may need to make quick decisions about how to provide safe, ongoing care for the people being treated by the provider, including alternative provision and/or early discharge. When there are unexpected medicines shortages or dispensing issues within a community, place or system, such as recent examples of ADHD medication, pancreatic enzyme replacement therapy and antibiotics. Service continuity plans based on national guidance should be in place, alongside local support and services. In a busy emergency department (ED), a sudden rise in admissions may place unexpected pressure on paramedic and ED teams. Staff in those teams may need to make 'on the spot' decisions to keep people using services, families and staff at lowest risk – be it diverting ambulances, opening up temporary escalation spaces or increasing early discharge. The OPEL (Operating Pressure Escalation Level) framework can help teams decide what actions and escalations are needed to manage risks, however they need to be viewed collectively and dynamically. Other examples include a public emergency (e.g. large fire) or the withdrawal of medication from the market. In these cases, there will be a need for teams to make rapid decisions that involve multiple perspectives and partners. The risk profile in one or more organisations may need revising, or there may be a need to share risk across the system in order to achieve a decision that is least worse, best possible or for the 'greater good'. Who will own and manage the shared risks? How will the response be coordinated and who will monitor it? What changes are needed? In order to answer these questions, those involved must follow a number of key principles. These principles cover culture, systems, structures, policy and support, all of which are needed for effective risk assessment and management. Person-centred: Actively focus on the experience of people using services, carers, family, staff, students and learners, across all risk management activities. What does quality, including safety, look like from their perspective? What are the key concerns and risks? How are we using feedback from these groups to assess, mitigate, manage and monitor risks? Collaboration and engagement: Across places, pathways and systems, involving all key organisations, services, and teams, from across health, social care and wider services. The collaboration should be in line with the system strategy (e.g. ICP Strategy, Joint Strategic Needs Assessments (JSNA)), NQB Quality Risk Response and Escalation Guidance and wider policy (e.g. EPRR policy, OPEL framework, Better Care Fund plans, annual safeguarding reports). This ensures that a comprehensive understanding of risks is achieved and that the best possible strategies are co-developed. Open and proactive intelligence sharing: Key to successful assessment and decision-making, this means being able to answer questions such as: what data/information are we using across the system to assess the risks? Where are we getting this information from and are there gaps? Are there any cultural issues getting in the way of intelligence sharing? Common risk profile, language and scoring: It is key that the services and organisations involved have a common risk profile, language and scoring, against which shared risk appetite levels should be set. This requires using consistent risk matrixes and, if possible, agreed thresholds for levels of risk defined by reference to common, objective measures. Clear roles and coordination of responsibilities: All relevant teams and organisations must be clear on roles, responsibilities and accountabilities, including: who is responsible for monitoring, reviewing and updating the information and assessment? who will ensure that resources are identified and coordinated to support improvement? Processes fail when there is no accountability to deliver and no mechanism to coordinate and assure, which is where the system role is important. Ensuring that accountability lines are clearly defined and communicated to everyone involved, including timescales and ongoing maintenance, is a priority. The ICB's role in providing objective challenge on risk assessments for health should also be recognised. A Memorandum of Understanding (MoU) across system partners may be helpful. The role of System Quality Groups in coordinating improvement and risk management should also be understood and agreed, as well as System Coordination Centres for health. Clear reporting, recording and monitoring: As above, a shared risk appetite should be in place. The 'weighting' of some areas of impact may be considered greater than others, which should be clearly documented. The outcomes of the assessment should be recorded alongside jointly agreed priorities and improvement plans. The documentation should include a recording of time to provide an audit trail, as the assessment may need updating over a period of time. The individual Boards in all relevant system organisations, including Integrated Care Boards and Local Authorities, must have visibility of assessment and outcomes, including being notified of any actions that may increase risk share in a part of the pathway/ system or that deviate from national policy and standards (with clear justification as to why and a timeframe). The CQC should also be informed of any actions that increase risk and how they were agreed. Board assurance frameworks of all relevant organisations should be populated to include the decisions. Effective action planning and mitigation: Goals should be SMART (Specific, Measurable, Attainable, Relevant and Time-based), with clear information on timelines, action holders and inter-dependencies, aligned to accountability frameworks. Escalation: where quality risks cannot be managed at system level, they should be escalated to NHS England regions in alignment with the National Quality Board guidance or via alternative required routes (e.g. Emergency Preparedness, Resilience and Response Process, local authority or safeguarding governance). Competent decision-making: A distinguishing feature is the need for competent decision-makers who can judge risks in real-time and through a system lens. This requires training, communication and support to recognise potential threats, understand their implications and make crucial decisions swiftly and effectively within a wider learning system. Equalities and inequalities: A focus on equalities and inequalities should underpin the assessment and response. Are particular population groups at higher risk or more likely to receive an adverse impact from the mitigations/management? Are there gaps in insight from an equality and diversity perspective? External factors consideration: Consider external factors such as regulatory changes, technological advancements and public health trends that can impact care and outcomes. Dynamic and regular review: Dynamic and regular review and monitoring is needed to adjust strategies and interventions to mitigate potential risks. Organisations and systems must also learn from past incidents, as well as where things have gone well, to refine their processes. This document sets out the need to review how risk management is implemented in fast-changing and multi-factorial environments, and the key principles to support this approach. In working with systems, we intend to develop more detailed understanding of how to apply these principles and frameworks, including the role of ICBs vis-à-vis wider system partners. Below, we set out a first step in terms of how risk matrixes can be updated to be used in integrated care systems. Further examples are provided in Annex A. The example in Figure 3 below has been system tested when developing these principles and refers to significant pressure in the urgent and emergency care pathway, and assessment as to whether ambulances should be diverted to another provider. In the example: The dimensions of assessment – risks and areas of impact – have been identified, agreed and articulated by the different organisations in the system. They will vary according to local circumstances. Risks might cover parts of a service, pathway or system. Areas of impact might include quality (e.g. safety, experience), inequalities, performance (e.g. access, treatment times), finance, workforce (e.g. capacity, morale, training programmes, placements), environmental, or be aligned to the taxonomy used in the SEIPS framework (i.e. technology/tools/equipment; people/persons; tasks; physical environment; organisation; and external environment/context). The changes to the assessment post-intervention have been clearly articulated. The re-assessment and reporting should be undertaken regularly, and the least worse scenario maintained for as short a period as possible. Scenario: Decision to divert ambulances from one organisation due to exceptional pressures within the Emergency Department. Figure 3: Example of risk assessment across an integrated care system Image description: The image is a risk assessment matrix that evaluates various organisational entities across different areas of impact. The risk scores range from 4 to 25, with color-coding to indicate low (green), medium (yellow), and high (red) risk levels. The matrix shows the initial risk assessment for Organisation A, which had an "extreme/high risk" rating. The revised assessment for Organisation A reduced the risk to "medium." For Organisation B, the initial and revised assessments both indicated "medium risk." Organisation C also had a "medium risk" rating in both the initial and revised assessments. The initial assessment for Organisation D, which involves sub-contracted alcohol assessment, referral, and advice, resulted in a "high risk" rating. The revised assessment for Organisation D is not shown. In the example: for the trust diverting ambulances (org A) the decision to divert ambulances may result in reduced pressure and therefore reductions in patient harm (outcomes), environmental risks (trips, falls etc. associated with overcrowding), workforce (human factors), as well as improvements in experience of care however, the ambulance trust (org B) may experience increased risks to patient harm (outcomes) and experience due to travelling larger distances to convey patients to hospital, therefore increasing their response times the organisation receiving diverted ambulances (org C) may be under pressure and hence see increased risks to outcomes, environment workforce and experience the sub-contracted organisation offering alcohol assessment, referral and advice (org D), working out of the ED that is diverting the ambulances, may also see a reduction in risks to environment, workforce, and experience. However there may not be a service within the receiving trust and therefore care outcomes may be impacted The example illustrates how assessment through a system lens opens up new mitigations/ interventions based on least worse/best possible scenarios, but also the need to continue assessing dynamically to mitigate the risks as best as possible. The example could be broadened to assess risks in other parts of the system. For example, the decision to divert ambulances may make it harder for discharge teams at organisation C to discharge people and may mean that the person being discharged may consequently require more community, social care and primary care support. As risk management within health and care continues to mature, it has become more important than ever to ensure that risk assessment is effective, systems-based and responsive. The organisations involved in delivering and commissioning health and care must ensure that their risk frameworks and processes are being used effectively in line with key standards, and that those assessing risks have the skills and capabilities needed to do this effectively. At the same time, there is also a need to consider the role of a collaborative approach to risk assessment in today's operating environment: one that recognises that different organisations and system partners must not only understand each other's key risks and priorities, but also support each other to manage them. The NQB hopes that the principles set out in this document provide a useful reference and starting point to those assessing and managing risks across integrated care systems. Scenario: Decision to close an independent hospital due to quality concerns raised by the CQC and removal of the provider's registration within a short time frame (such as 28 days closure). many years of the provider being in and out of "special measures" with CQC a high number of commissioners using the service to place people far from home* (e.g. 22 different ICB's for 80 people) the ICB in which the hospital service is located does not use this provider, and therefore does not have clear oversight of the service limited quality oversight from placing commissioners for people without a learning disability and autism diagnosis a large number of community providers in the placing ICB with different approaches to managing people on their caseload lack of specialism despite being a specialist service, and a lack of a clear clinical model* long lengths of stay for all inpatients* high levels of distress in patients being managed in non-local environments above average physical health concerns for inpatients patients are frequently described as 'hard to place' by commissioners and hypothesis is this is leading to acceptance of standard of care high levels of restrictive practices are noted* provider has low levels of safeguarding which doesn't reflect clinical activity, and safeguarding concerns are completed retrospectively by provider above average staff turnover and recruitment above average staff sickness high levels of agency use constant key changes to the senior leadership team financial constraints of the provider due to CQC restrictions resulting in no new admissions into the service the hospital is not physically near other services and therefore is isolated from system support and visitor footfall* Higher Education Institution (HEI) healthcare training programmes impacted with sudden loss of available clinical placements including for mental health students and trainees currently on placement at the Trust *Known risk factors for closed cultures in mental health hospitals, which can lead to breaches of people's human rights, including patient abuse. Image description: The image is a 5×5 risk assessment matrix that evaluates various risk factors across areas like setting, safety, experience, workforce, and regulation. Each risk factor is assigned a numerical risk score ranging from 4 to 20, with color-coding to indicate low, medium, and high risk levels.The matrix provides a structured way to assess and compare different risk factors across the key impact areas for this organisation.The image is a 5×5 risk assessment matrix that evaluates various risks across different areas including setting, safety, experience, workforce, and regulation. Each risk factor is assigned a numerical risk score ranging from 4 to 20, with color-coding to indicate low, medium, and high risk levels.The risk assessment matrix provides detailed risk scores for various factors like primary care team with patient awaiting ambulance, ambulance response time, ambulance to hospital queuing and handover, trust decision to admit delays, boarding to wards, infection control, and more. The matrix allows for a structured evaluation of risks across multiple organisational areas.Publications reference: PRN01589 The effective management of risk is becoming both more complex and more important as we move into working as systems. Provider boards will need to be well sighted on system-wide risk, risks accruing from place-based and other collaborations and co-operative ventures in addition to managing risk within their own organisations. While it has always been the case that changes within a nearby provider presented both risk and opportunities, now the chance to plan together also presents the right set of circumstances to maximise opportunities collectively and to minimise the likelihood and impact of risks. However, system working will also mean increased complexity. It will make it more difficult for boards to be sufficiently well sighted on all of the ventures in which they are involved to be confident that they have adequate assurances of the right quality. In this chapter Rob Kurau provides some fresh insights into the essentials of risk management that even experienced risk practitioners are likely to find useful. What is risk management? A risk is defined as "an uncertain event or set of circumstances that, should it occur, would have an impact on an organisation's objectives". More simply, a risk is something that could go wrong. Providers share exposure to similar risk types and risk categories. A standard set of definitions is set out in Appendix 1. The principal benefits of effective risk management to providers are: it helps the provider maintain patient safety it ensures the provider can provide value to its communities it minimises harm and damage it drives organisational learning it helps the provider build credibility in the eyes of its stakeholders. Clearly, provider boards need to recognise that for the organisation to meet its strategic objectives, effective risk management will be essential. For this reason, setting out an enterprise-wide risk management system or framework will be critical; broadly encompassing the activities relating to the identification, assessment, control, monitoring and reporting of risk. Each component of a good practice risk management framework in place at a leading provider has been summarised below: Risk vision and strategy – How we articulate our risk management priorities and how they are aligned to our strategy. Risk culture – How our risk decisions are shaped by culture. Risk appetite – How much risk we can take in order to deliver our strategy while ensuring we can provide safe and effective patient outcomes. Policy and governance – How we organise ourselves, make decisions and take approved risks. Risk assessment and control – How we understand risks and limit undesirable outcomes from occurring. Incident management – How we respond when things go wrong, how we learn and stop the same things happening again. Monitoring and assurance – How we check that controls are working and highlight when risks require attention. An example of a risk management framework summary is set out at Appendix 2. Risk vision and strategy It is important that risk management considerations are properly reviewed as part of the provider board's strategy setting process. If a review of the provider's strategic risks is not properly undertaken, financial and non-financial resources to mitigate these risks may not be allocated, potentially leading to unacceptable clinical risks and poor patient outcomes. The mitigation of such risks part way through the strategic planning cycle could be more difficult to achieve, compared to when risk remediation plans are agreed and funded at the outset. A risk management vision and strategic risk priorities should set out the themes of risk management activity that will be undertaken to contribute to the delivery of the provider's overall vision and strategy. In the current context, that will no doubt include capturing risks which impact the organisation derived from system working, provider collaboratives and partnerships including at place. Developing this may also enhance the alignment between the provider's overall strategy and the supporting risk management priorities. These priorities should then be reflected within departmental plans and the provider's longer-term strategy, with progress monitored by relevant management groups (for departmental plans) and assurance committees (for the strategy). We would expect the provider's strategy to feed into and align with the strategy (or strategies) of relevant ICSs. Risk culture Risk culture includes the values and behaviours that shape risk decisions. It is acknowledged that the risk management framework will only be truly effective if operating within an appropriate culture. When viewed through a 'risk lens', culture encompasses the values, beliefs, knowledge, understanding and practical application of risk management, which is embodied by the board and shared and adopted by all employees across the provider. Culture stems from the 'tone from the top' and is shaped by the influence of every employee in their daily interactions and specifically through the adoption and promotion of the provider's behaviours. Every employee therefore has a role to play in creating an appropriate culture. For more on organisational culture see our chapter on problem sensing and culture. Risk appetite Since we wrote the third edition of this compendium, we have noted an increased emphasis on provider boards engaging with the topic of risk appetite. As set out within the 'Orange Book – Risk Appetite guidance note', Government Finance Function (October 2020), risk appetite is defined as the level of risk within which the organisation aims to operate. By defining a risk appetite, the provider board will be able to clearly set the optimal position in pursuit of its strategy and vision. The benefits of adopting a risk appetite include: supporting informed decision-making reducing uncertainty improving consistency across governance mechanisms and decision-making supporting performance management enabling the board to focus and prioritise resources. If one of the key roles of the board is to ensure that the organisation is taking the right level of risk within which to meet its strategic objectives, then the risk appetite is a significant tool in helping boards to understand the organisation's risk management boundaries within which to deliver the overall strategy and vision. The risk appetite approach should set out: the principles within which the risk appetite has been set the common risk language to be used, against which risk appetite levels should be set the risk appetite methodology, including the appetite levels and how these are defined a set of qualitative risk appetite statements and quantitative exposure limits for each risk type and category the controls and reporting mechanisms that have been put in place to enable the board to track management's adherence to risk appetite. Once the board has approved the risk appetite, it is essential that management considers the best way to embed their approach into day-to-day planning and management. Key processes, where it is important for risk appetite to be taken into account, include within the strategy setting process, board decision making and risk appetite adherence reporting. For illustration purposes, Appendix 3 sets out a case study with an example Board-level risk appetite, aligned to each risk type and category, as well as risk appetite statements. This information has been derived from The Leeds Teaching Hospitals NHS Trust – Risk Appetite 2021/22. The board may of course find itself in a position where its risk appetite differs to that of neighbouring trusts, partners, regulators or indeed its ICS. This publication focuses primarily on the roles and responsibilities of the trust board, which are of course to determine risk appetite for the organisation – however we can assist in facilitating wider discussions through the NHS Providers' Board development programme where more tailored conversations are appropriate. Policy and governance Providers are expected to have appropriate systems of risk management and internal control in place. This manifests itself through a board and committees, a set of policies, board assurance reporting mechanisms and an annual control statement, as part of the provider's Annual Report. Risk management committees are now more commonplace in NHS providers. We have observed the role of a risk management committee is to consider the provider's most material risks and receive updates to its risk profile, progress with risk remediation plans and key risk escalations from clinical service units and corporate functions or equivalent. Typically risk management committees should also provide periodic updates to the board. Where providers have not established a dedicated risk management committee, we have observed that some providers deal with risk management matters through an Audit & Risk Committee or directly at the Board. Any of these approaches may be suitable, though should be considered within the context of the provider's circumstances. A policy is a document that articulates what must be done (or is permitted within prescribed boundaries) and, where appropriate, what must not be done by employees in their day-to-day activities and in pursuit of their strategic objectives. The attributes of a policy are that it directs and limits the actions of employees in pursuit of their strategic objectives and that it defines the scope within which decisions can be taken. The board assurance framework (BAF) is a significant tool in helping provider boards to understand the implementation of strategy in the context of risk management. The BAF sets out the provider's strategic objectives, the risks to achieving them and the controls and assurance mechanisms that have been put in place to manage risk and deliver the objectives. An industry good practice example of a BAF template as well as a review by PwC across a range of NHS sector BAF documents can be found on the NHS Providers website . The annual governance statement (AGS) is a key section within the provider's annual report, signed by the provider's chief executive. The AGS includes the system of internal control across the provider and includes its capacity to handle risk; risk and control framework; resourcing levels; any data governance serious incidents and key controls; and overall effectiveness of internal control. Risk assessment and control A risk assessment is the process for estimating the amount of risk and is important to the provider as it enables management to understand the nature and extent of the risks that the organisation faces and to prioritise actions where appropriate. Risks should be assessed based upon a combination of the likelihood of the risk occurring and the potential impact upon the organisation and its patients should the risk occur. Such risks can sometimes be categorised based on whether they are near-term risks versus those that are longer-term, horizon risks. All risks should be assessed on an inherent (without controls) and residual (with controls) basis using the provider's risk scoring matrix. Controls are repeatable actions taken to reduce risks and they are important as they should reduce the likelihood of risks occurring and/or their impact should they occur. Risk assessment should not be a one-off exercise but one which is repeated to take account of the progress of mitigating actions and any change in circumstances. For illustration purposes, Appendix 4 sets out a good practice risk scoring matrix from a leading provider. Following periodic risk assessments, risk registers should be used for recording and tracking risks and associated action plans. They are important as they enable management to understand the nature and extent of the risks that the organisation faces and supports the progress of actions to address them. Once the risk assessment has been undertaken, it is good practice for management ownership to be assigned, a risk mitigation plan to be documented, a review to be held by the executive team, with subsequent escalation via the risk management committee to the board, if necessary. An industry good practice risk register template is available on the NHS Providers Board Development resources webpage. Incident management As part of the NHS England emergency preparedness, resilience and response (EPRR) framework, providers must show they can effectively respond to major, critical and business continuity incidents whilst maintaining services to patients. Providers are usually required to undertake an annual self-assessment against the full set of core EPRR standards. The introduction of the integrated care board (ICB) has resulted in a change to the process in that the self-assessment is submitted to the ICB who provide local assurance prior to submission to NHS England and the Local Heath Resilience Partnership. Providers are also expected to have a whistleblowing process (also known as 'Freedom to Speak Up') to enable their employees to be able to raise concerns about any wrongdoing that could affect others. This is important as it lets the provider know if things are going wrong, which otherwise it might not have found out about. All concerns raised through the whistleblowing channel should then be subject to review and investigation. Where concerns are substantiated, appropriate action should be taken to address the concern and where possible to seek to prevent a re-occurrence. Monitoring and assurance The three lines of defence model is

an accepted regulated framework designed to facilitate an effective risk management system. This model is used across the public and private sector because it provides a standardised and comprehensive risk management process that clarifies roles, and reduces cost and effort. Different departments play a distinct role within this model. The first line of defence is responsible for the ongoing management of risks within the provider. In managing these risks, departments will adopt a variety of operational level risk and control monitoring mechanisms, such as holding risk workshops, maintaining risk registers and tracking key performance indicators. Examples include clinical service units and other front-line patient services. The second line of defence is responsible for oversight of day-to-day management of risk by the first line. These activities should include supporting, coaching, facilitating, monitoring, challenging, reporting and instructing on first line risk management practices. Examples include departments such as quality, finance and human resources. The third line of defence is responsible for providing an independent and objective opinion to the board on the adequacy and functioning of the system of internal control. Given the size and complexity of some providers, it is commonplace for providers to use a third-party firm to deliver internal audit services to the board. Looking to the future It is clear that risk management across the NHS must go beyond compliance and support the delivery of outcomes for the benefit of patients and other key stakeholders. Since we wrote the third edition of this compendium, we have observed providers taking forward initiatives to further mature their own and the wider system's risk management capabilities. We hope that this section will make a further contribution with this work and provide some practical assistance. Create intelligent forms to trigger adaptable sequence workflows for any industry and department (HR, IT, Healthcare, etc). Identification, evaluation and control of risks For other uses, see Risk (disambiguation). For business risks, see Risk analysis (business). For the magazine, see Risk Management (magazine). "Risk Analysis" redirects here. For the academic journal, see Risk Analysis (journal). This article needs additional citations for verification. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed.Find sources: "Risk management" – news · newspapers · books · scholar · JSTOR (January 2014) (Learn how and when to remove this message) Example of risk assessment: A NASA model showing areas at high risk from impact for the International Space Station Business administration Accounting Management accounting Financial accounting Audit Business entity (list) Corporate group Corporation sole Company Conglomerate Holding company Cooperative Corporation Joint-stock company Limited liability company Partnership Privately held company Sole proprietorship State-owned enterprise Corporate governance Annual general meeting Board of directors Supervisory board Advisory board Audit committee Corporate law Commercial law Constitutional documents Contract Corporate crime Corporate liability Insolvency law International trade law Mergers and acquisitions Corporate title Chairman Chief business officer/Chief brand officer Chief executive officer/Chief operating officer Chief financial officer Chief human resources officer Chief information officer/Chief marketing officer Chief product officer/Chief technology officer Economics Commodity Public economics Labour economics Development economics International economics Mixed economy Planned economy Econometrics Environmental economics Open economy Market economy Knowledge economy Microeconomics Macroeconomics Economic development Economic statistics Finance Financial statement Insurance Factoring Cash conversion cycle Insider dealing Capital budgeting Commercial bank Derivative Financial statement analysis Financial risk Public finance Corporate finance Managerial finance International finance Liquidation Stock market Financial market Tax Financial institution Capital management Venture capital Types of management Asset Brand Business intelligence Business development Capacity Capability Change innovation Commercial Marketing Communications Configuration Conflict Content Customer relationship Distributed Earned value Electronic business Enterprise resource planning management information system Financial Human resource development Incident Knowledge Legal Materials Network administrator Office Operations services Performance Power Process Product life-cycle Product Project Property Quality Records Resource Risk crisis Sales Security Service Strategic Supply chain Systems administrator Talent Technology Organization Architecture Behavior Communication Culture Conflict Development Engineering Hierarchy Patterns Space Structure Trade Business analysis Business ethics Business plan Business judgment rule Consumer behaviour International business Business model International trade Trade route Business process Business statistics Business and economics portalvte Risk management is the identification, evaluation, and prioritization of risks,[1] followed by the minimization, monitoring, and control of the impact or probability of those risks occurring.[2] Risks can come from various sources (i.e, threats) including uncertainty in international markets, political instability, dangers of project failures (at any phase in design, development, production, or sustaining of life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters, deliberate attack from an adversary, or events of uncertain or unpredictable root-cause.[3] Retail traders also apply risk management by using fixed percentage position sizing and risk-to-reward frameworks to avoid large drawdowns and support consistent decision-making under pressure. There are two types of events viz. Risks and Opportunities. Negative events can be classified as risks while positive events are classified as opportunities. Risk management standards have been developed by various institutions, including the Project Management Institute, the National Institute of Standards and Technology, actuarial societies, and International Organization for Standardization.[4][5][6] Methods, definitions and goals vary widely according to whether the risk management method is in the context of project management, security, engineering, industrial processes, financial portfolios, actuarial assessments, or public health and safety. Certain risk management standards have been criticized for having no measurable improvement on risk, whereas the confidence in estimates and decisions seems to increase.[2] Strategies to manage threats (uncertainties with negative consequences) typically include avoiding the threat, reducing the negative effect or probability of the threat, transferring all or part of the threat to another party, and even retaining some or all of the potential or actual consequences of a particular threat. The opposite of these strategies can be used to respond to opportunities (uncertain future states with benefits).[7] As a professional role, a risk manager[8] will "oversee the organization's comprehensive insurance and risk management program, assessing and identifying risks that could impede the reputation, safety, security, or financial success of the organization", and then develop plans to minimize and / or mitigate any negative (financial) outcomes. Risk Analysts [9] support the technical side of the organization's risk management approach: once risk data has been compiled and evaluated, analysts share their findings with their managers, who use those insights to decide among possible solutions. See also Chief Risk Officer, internal audit, and Financial risk management § Corporate finance. Risk is defined as the possibility that an event will occur that adversely affects the achievement of an objective[10]. Uncertainty, therefore, is a key aspect of risk.[11] Risk management appears in scientific and management literature since the 1920s.[12] It became a formal science in the 1950s, when articles and books with "risk management" in the title also appear in library searches.[13] Most of research was initially related to finance and insurance.[14][15] One popular standard clarifying vocabulary used in risk management is ISO Guide 31073:2022, "Risk management — Vocabulary".[4] Ideally in risk management, a prioritization process is followed.[16] Whereby the risks with the greatest loss (or impact) and the greatest probability of occurring are handled first. Risks with lower probability of occurrence and lower loss are handled in descending order. In practice the process of assessing overall risk can be tricky, and organisation has to balance resources used to mitigate between risks with a higher probability but lower loss, versus a risk with higher loss but lower probability. Opportunity cost represents a unique challenge for risk managers. It can be difficult to determine when to put resources toward risk management and when to use those resources elsewhere. Again, ideal risk management optimises resource usage (spending, manpower etc), and also minimizes the negative effects of risks. Opportunities first appear in academic research or management books in the 1990s. The first PMBoK Project Management Body of Knowledge draft of 1987 doesn't mention opportunities at all. Modern project management school recognize the importance of opportunities. Opportunities have been included in project management literature since the 1990s, e.g. in PMBoK, and became a significant part of project risk management in the years 2000s,[17] when articles titled "opportunity management" also begin to appear in library searches. Opportunity management thus became an important part of risk management. Modern risk management theory deals with any type of external events, positive and negative. Positive risks are called opportunities. Similarly to risks, opportunities have specific mitigation strategies: exploit, share, enhance, ignore. In practice, risks are considered "usually negative". Risk-related research and practice focus significantly more on threats than on opportunities. This can lead to negative phenomena such as target fixation.[18] For the most part, these methods consist of the following elements, performed, more or less, in the following order: Identify the threats. Assess the vulnerability of critical assets to specific threats. Determine the risk (i.e. the expected likelihood and consequences of specific attacks on specific assets). Identify ways to reduce those risks. Prioritize risk reduction measures. The Risk management knowledge area, as defined by the Project Management Body of Knowledge PMBoK, consists of the following processes: Plan Risk Management – defining how to conduct risk management activities. Identify Risks – identifying individual project risks as well as sources. Perform Qualitative Risk Analysis – prioritizing individual project risks by assessing probability and impact. Perform Quantitative Risk Analysis – numerical analysis of the effects. Plan Risk Responses – developing options, selecting strategies and actions. Implement Risk Responses – implementing agreed-upon risk response plans. In the 4th Ed. of PMBoK, this process was included as an activity in the Monitor and Control process, but was later separated as a distinct process in PMBoK 6th Ed.[19] Monitor Risks – monitoring the implementation. This process was known as Monitor and Control in the previous PMBoK 4th Ed., when it also included the "Implement Risk Responses" process. The International Organization for Standardization (ISO) identifies the following principles for risk management:[5] Create value – resources expended to mitigate risk should be less than the consequence of inaction. Be an integral part of organizational processes. Be part of the decision-making process. Explicitly address uncertainty and assumptions. Use a systematic and structured process. Use the best available information. Be flexible. Take human factors into account. Be transparent and inclusive. Be dynamic, iterative and responsive to change. Be capable of continual improvement and enhancement. Continual reassessment. Benoit Mandelbrot distinguished between "mild" and "wild" risk and argued that risk assessment and management must be fundamentally different for the two types of risk.[20] Mild risk follows normal or near-normal probability distributions, is subject to regression to the mean and the law of large numbers, and is therefore relatively predictable. Wild risk follows fat-tailed distributions, e.g., Pareto or power-law distributions, is subject to regression to the tail (infinite mean or variance, rendering the law of large numbers invalid or ineffective), and is therefore difficult or impossible to predict. A common error in risk assessment and management is to underestimate the wildness of risk, assuming risk to be mild when in fact it is wild, which must be avoided if risk assessment and management are to be valid and reliable, according to Mandelbrot. According to the standard ISO 31000, "Risk management – Guidelines", the process of risk management consists of several steps as follows:[5] This involves: observing the context (the environment of the organization) the social scope of risk management the identity and objectives of stakeholders the basis upon which risks will be evaluated, constraints. defining a framework for the activity and an agenda for identification developing an analysis of risks involved in the process mitigation or solution of risks using available technological, human and organizational resources After establishing the context, the next step in the process of managing risk is to identify potential risks. Risks are about events that, when triggered, cause problems or benefits. Hence, risk identification can start with the source of problems and those of competitors (benefit), or with the problem's consequences. Source analysis[21] – Risk sources may be internal or external to the system that is the target of risk management (use mitigation instead of management since by its own definition risk deals with factors of decision-making that cannot be managed). Some examples of risk sources are: stakeholders of a project, employees of a company or the weather over an airport. Problem analysis[citation needed] – Risks are related to identified threats. For example: the threat of losing money, the threat of abuse of confidential information or the threat of human errors, accidents and casualties. The threats may exist with various entities, most important with shareholders, customers and legislative bodies such as the government. When either source or problem is known, the events that a source may trigger or the events that can lead to a problem can be investigated. For example: stakeholders withdrawing during a project may endanger funding of the project; confidential information may be stolen by employees even within a closed network; lightning striking an aircraft during takeoff may make all people on board immediate casualties. The chosen method of identifying risks may depend on culture, industry practice and compliance. The identification methods are formed by templates or the development of templates for identifying source, problem or event. Common risk identification methods are: Objectives-based risk identification [citation needed] – Organizations and project teams have objectives. Any event that may prevent an objective from being achieved is identified as risk. Scenario-based risk identification – In scenario analysis different scenarios are created. The scenarios may be the alternative ways to achieve an objective, or an analysis of the interaction of forces in, for example, a market or battle. Any event that triggers an undesired scenario alternative is identified as risk – see Futures Studies for methodology used by Futurists. Taxonomy-based risk identification – The taxonomy in taxonomy-based risk identification is a breakdown of possible risk sources. Based on the taxonomy and knowledge of best practices, a questionnaire is compiled. The answers to the questions reveal risks.[22] Common-risk checking[23] – In several industries, lists with known risks are available. Each risk in the list can be checked for application to a particular situation.[24] Risk charting[25] – This method combines the above approaches by listing resources at risk, threats to those resources, modifying factors which may increase or decrease the risk and consequences it is wished to avoid. Creating a matrix under these headings enables a variety of approaches. One can begin with resources and consider the threats they are exposed to and the consequences of each. Alternatively one can start with the threats and examine which resources they would affect, or one can begin with the consequences and determine which combination of threats and resources would be involved to bring them about. Main article: Risk assessment Once risks have been identified, they must then be assessed as to their potential severity of impact (generally a negative impact, such as damage or loss) and to the probability of occurrence. [26] These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of an unlikely event, the probability of occurrence of which is unknown. Therefore, in the assessment process it is critical to make the best educated decisions in order to properly prioritize the implementation of the risk management plan. Even a short-term positive improvement can have long-term negative impacts. Take the "turnpike" example. A highway is widened to allow more traffic. More traffic capacity leads to greater development in the areas surrounding the improved traffic capacity. Over time, traffic thereby increases to fill available capacity. Turnpikes thereby need to be expanded in a seemingly endless cycles. There are many other engineering examples where expanded capacity (to do any function) is soon filled by increased demand. Since expansion comes at a cost, the resulting growth could become unsustainable without forecasting and management. The fundamental difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kinds of past incidents and is particularly scanty in the case of catastrophic events, simply because of their infrequency. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for intangible assets. Asset valuation is another question that needs to be addressed. Thus, best educated opinions and available statistics are the primary sources of information. Nevertheless, risk assessment should produce such information for senior executives of the organization that the primary risks are easy to understand and that the risk management decisions may be prioritized within overall company goals. Thus, there have been several theories and attempts to quantify risks. Numerous different risk formulae exist, but perhaps the most widely accepted formula for risk quantification is: "Rate (or probability) of occurrence multiplied by the impact of the event equals risk magnitude."[vague] Risk mitigation measures are usually formulated according to one or more of the following major risk options, which are: Design a new business process with adequate built-in risk control and containment measures from the start. Periodically re-assess risks that are accepted in ongoing processes as a normal feature of business operations and modify mitigation measures. Transfer risks to an external agency (e.g. an insurance company) Avoid risks altogether (e.g. by closing down a particular high-risk business area) Later research[27] has shown that the financial benefits of risk management are less dependent on the formula used but are more dependent on the frequency and how risk assessment is performed. In business it is imperative to be able to present the findings of risk assessments in financial, market, or schedule terms. Robert Courtney Jr. (IBM, 1970) proposed a formula for presenting risks in financial terms. The Courtney formula was accepted as the official risk analysis method for the US governmental agencies. The formula proposes calculation of ALE (annualized loss expectancy) and compares the expected loss value to the security control implementation costs (cost–benefit analysis). Planning for risk management uses four essential techniques. Under the acceptance technique, the business intentionally assumes risks without financial protections in the hopes that possible gains will exceed prospective losses. The transfer approach shields the business from losses by shifting risks to a third party, frequently in exchange for a fee, while the third-party benefits from the project. By choosing not to participate in high-risk ventures, the avoidance strategy avoids losses but also loses out on possibilities. Last but not least, the reduction approach lowers risks by implementing strategies like insurance, which provides protection for a variety of asset classes and guarantees reimbursement in the event of losses.[28] Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories:[29] Avoidance (eliminate, withdraw from or not become involved) Reduction (optimize – mitigate) Sharing (transfer – outsource or insure) Retention (accept and budget) Ideal use of these risk control strategies may not be possible. Some of them may involve trade-offs that are not acceptable to the organization or person making the risk management decisions. Another source, from the US Department of Defense (see link), Defense Acquisition University, calls these categories ACAT, for Avoid, Control, Accept, or Transfer. This use of the ACAT acronym is reminiscent of another ACAT (for Acquisition Category) used in US Defense industry procurements, in which Risk Management figures prominently in decision making and planning. Similarly to risks, opportunities have specific mitigation strategies: exploit, share, enhance, ignore. This includes not performing an activity that could present risk. Refusing to purchase a property or business to avoid legal liability is one such example. Avoiding airplane flights for fear of hijacking. Avoidance may seem like the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits. Increasing risk regulation in hospitals has led to avoidance of treating higher risk conditions, in favor of patients presenting with lower risk.[30] Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. For example, sprinklers are designed to put out a fire to reduce the risk of loss by fire. This method may cause a greater loss by water damage and therefore may not be suitable. Halon fire suppression systems may mitigate that risk, but the cost may be prohibitive as a strategy. Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and effort applied. By effectively applying Health, Safety and Environment (HSE) management standards, organizations can achieve tolerable levels of residual risk.[31] Modern software development methodologies reduce risk by developing and delivering software incrementally. Early methodologies suffered from the fact that they only delivered software in the final phase of development; any problems encountered in earlier phases meant costly rework and often jeopardized the whole project. By developing in iterations, software projects can limit effort wasted to a single iteration. Outsourcing could be an example of risk sharing strategy if the outsourcer can demonstrate higher capability at managing or reducing risks.[32] For example, a company may outsource only its software development, the manufacturing of hard goods, or customer support needs to another company, while handling the business management itself. This way, the company can concentrate more on business development without having to worry as much about the manufacturing process, managing the development team, or finding a physical location for a center. Also, implanting controls can also be an option in reducing risk. Controls that either detect causes of unwanted events prior to the consequences occurring during use of the product, or detection of the root causes of unwanted failures that the team can then avoid. Controls may focus on management or decision-making processes. All these may help to make better decisions concerning risk.[33] Briefly defined as "sharing with another party the burden of loss or the benefit of gain, from a risk, and the measures to reduce a risk." The term 'risk transfer' is often used in place of risk-sharing in the mistaken belief that you can transfer a risk to a third party through insurance or outsourcing. In practice, if the insurance company or contractor go bankrupt or end up in court, the original risk is likely to still revert to the first party. As such, in the terminology of practitioners and scholars alike, the purchase of an insurance contract is often described as a "transfer of risk." However, technically speaking, the buyer of the contract generally retains legal responsibility for the losses "transferred", meaning that insurance may be described more accurately as a post-event compensatory mechanism. For example, a personal injuries insurance policy does not transfer the risk of a car accident to the insurance company. The risk still lies with the policyholder namely the person who has been in the accident. The insurance policy simply provides that if an accident (the event) occurs involving the policyholder then some compensation may be payable to the policyholder that is commensurate with the suffering/damage. Methods of managing risk fall into multiple categories. Risk-retention pools are technically retaining the risk for the group, but spreading it over the whole group involves transfer among individual members of the group. This is different from traditional insurance, in that no premium is exchanged between members of the group upfront, but instead, losses are assessed to all members of the group. Risk retention involves accepting the loss, or benefit of gain, from a risk when the incident occurs. True self-insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that either they cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed to war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great that it would hinder the goals of the organization too much. Main article: Risk management plan Select appropriate controls or countermeasures to mitigate each risk. Risk mitigation needs to be approved by the appropriate level of management. For instance, a risk concerning the image of the organization should have top management decision behind it whereas IT management would have the authority to decide on computer virus risks. The risk management plan should propose applicable and effective security controls for managing the risks. For example, an observed high risk of computer viruses could be mitigated by acquiring and implementing antivirus software. A good risk management plan should contain a schedule for control implementation and responsible persons for those actions. There are four basic steps of risk management plan, which are threat assessment, vulnerability assessment, impact assessment and risk mitigation strategy development.[34] According to ISO/IEC 27001, the stage immediately after completion of the risk assessment phase consists of preparing a Risk Treatment Plan, which should document the decisions about how each of the identified risks should be handled. Mitigation of risks often means selection of security controls, which should be documented in a Statement of Applicability, which identifies which particular control objectives and controls from the standard have been selected, and why. Implementation follows all of the planned methods for mitigating the effect of the risks. Purchase insurance policies for the risks that it has been decided to transferred to an insurer, avoid all risks that can be avoided without sacrificing the entity's goals, reduce others, and retain the rest. Initial risk management plans will never be perfect. Practice, experience, and actual loss results will necessitate changes in the plan and contribute information to allow possible different decisions to be made in dealing with the risks being faced. Risk analysis results and management plans should be updated periodically. There are two primary reasons for this: to evaluate whether the previously selected security controls are still applicable and effective to evaluate the possible risk level changes in the business environment. For example, information risks are a good example of rapidly changing business environment. Main article: Enterprise risk management Enterprise risk management (ERM) defines risk as those possible events or circumstances that can have negative influences on the enterprise in question, where the impact can be on the very existence, the resources (human and capital), the products and services, or the customers of the enterprise, as well as external impacts on society, markets, or the environment. There are various defined frameworks here, where every probable risk can have a pre-formulated plan to deal with its possible consequences (to ensure contingency if the risk becomes a liability). Managers thus analyze and monitor both the internal and external environment facing the enterprise, addressing business risk generally, and any impact on the enterprise achieving its strategic goals. ERM thus overlaps various other disciplines - operational risk management, financial risk management etc. - but is differentiated by its strategic and long-term focus.[35] ERM systems usually focus on safeguarding reputation, acknowledging its significant role in comprehensive risk management strategies.[36] Risk in Banking Main article: Financial risk management As applied to finance, risk management concerns the techniques and practices for measuring, monitoring and controlling the market- and credit risk (and operational risk) on a firm's balance sheet, due to a bank's credit and trading exposure, or re a fund manager's portfolio value; for an overview see Finance § Risk management. A traditional measure in banking is value at risk (VaR) – the possible loss due to adverse credit and market events. Banks seek to hedge these risks, and will hold risk capital on the net position. The Basel III framework governs the parallel regulatory capital requirements, including for operational risk. Fund managers employ various strategies to protect their fund value; these given their mandate and benchmark. Non-financial firms focus on business risk more generally, overlapping enterprise risk management: i.e. those events and occurrences which could negatively impact cash flow or profitability, and hence result in a loss of business value or a decline in share price. See also: Contract management The concept of "contractual risk management" emphasises the use of risk management techniques in contract deployment, i.e. managing the risks which are accepted through entry into a contract. Norwegian academic Petri Keskitalo defines "contractual risk management" as "a practical, proactive and systematical contracting method that uses contract planning and governance to manage risks connected to business activities".[37] In an article by Samuel Greengard published in 2010, two US legal cases are mentioned which emphasise the importance of having a strategy for dealing with risk:[38] UDC v. CH2M Hill, which deals with the risk to a professional advisor who signs an indemnification provision including acceptance of a duty to defend, who may thereby pick up the legal costs of defending a client subject to a claim from a third party,[39] Witt v. La Gorce Country Club, which deals with the effectiveness of a limitation of liability clause, which may, in certain jurisdictions, be found to be ineffective.[40] Greengard recommends using industry-standard contract language as much as possible to reduce risk as much as possible and rely on clauses which have been in use and subject to established court interpretation over a number of years.[38] Customs risk management is concerned with the risks which arise within the context of international trade and have a bearing on safety and security, including the risk that illicit drugs and counterfeit goods can pass across borders and the risk that shipments and their contents are incorrectly declared.[41] The European Union has adopted a Customs Risk Management Framework (CRMF) applicable across the union and throughout its member states, whose aims include establishing a common level of customs control protection and a balance between the objectives of safe customs control and the facilitation of legitimate trade.[42] Two events which prompted the European Commission to review customs risk management policy in 2012-13 were the September 11 attacks of 2001 and the 2010 transatlantic aircraft bomb plot involving packages being sent from Yemen to the United States, referred to by the Commission as "the October 2010 (Yemen) incident".[43] Main article: Risk management (cultural property) ESRM is a security program management approach that links security activities to an enterprise's mission and business goals through risk management methods. The security leader's role in ESRM is to manage risks of harm to enterprise assets in partnership with the business leaders whose assets are exposed to those risks. ESRM involves educating business leaders on the realistic impacts of identified risks, presenting potential strategies to mitigate those impacts, then enacting the option chosen by the business in line with accepted levels of business risk tolerance[44] For medical devices, risk management is a process for identifying, evaluating and mitigating risks associated with harm to people and damage to property or the environment[45]. Risk management is an integral part of medical device design and development, production processes and evaluation of field experience, and is applicable to all types of medical devices. The evidence of its application is required by most regulatory bodies such as the US FDA. The management of risks for medical devices is described by the International Organization for Standardization (ISO) in ISO 14971:2019, Medical Devices—The application of risk management to medical devices, a product safety standard. The standard provides a process framework and associated requirements for management responsibilities, risk analysis and evaluation, risk controls and lifecycle risk management. Guidance on the application of the standard is available via ISO/TR 24971:2020. The European version of the risk management standard was updated in 2009 and again in 2012 to refer to the Medical Devices Directive (MDD) and Active Implantable Medical Device Directive (AIMDD) revision in 2007, as well as the In Vitro Medical Device Directive (IVDD). The requirements of EN 14971:2012 are nearly identical to ISO 14971:2007. The differences include three "(informative)" Z Annexes that refer to the new MDD, AIMDD, and IVDD. These annexes indicate content deviations that include the requirement for risks to be reduced as far as possible, and the requirement that risks be mitigated by design and not by labeling on the medical device (i.e., labeling can no longer be used to mitigate risk). Typical risk analysis and evaluation techniques adopted by the medical device industry include hazard analysis, fault tree analysis (FTA), failure mode and effects analysis (FMEA), hazard and operability study (HAZOP), and risk traceability analysis for ensuring risk controls are implemented and effective (i.e. tracking risks identified to product requirements, design specifications, verification and validation results etc.). FTA analysis requires diagramming software. FMEA analysis can be done using a spreadsheet program. There are also integrated medical device risk management solutions. Through a draft guidance, the FDA has introduced another method named "Safety Assurance Case" for medical device safety assurance analysis. The safety assurance case is structured argument reasoning about systems appropriate for scientists and engineers, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment. With the guidance, a safety assurance case is expected for safety critical devices (e.g. infusion devices) as part of the pre-market clearance submission, e.g. 510(k). In 2013, the FDA introduced another draft guidance expecting medical device manufacturers to submit cybersecurity risk analysis information. Main article: Project risk management Project risk management must be considered at the different phases of acquisition. At the beginning of a project, the advancement of technical developments, or threats presented by a competitor's projects, may cause a risk or threat assessment and subsequent evaluation of alternatives (see Analysis of Alternatives). Once a decision is made, and the project begun, more familiar project management applications can be used:[46][47][48] Planning how risk will be managed in the particular project. Plans should include risk management tasks, responsibilities, activities and budget. Assigning a risk officer – a team member other than a project manager who is responsible for foreseeing potential project problems. Typical characteristic of risk officer is a healthy skepticism. Maintaining live project risk database. Each risk should have the following attributes: opening date, title, short description, probability and importance. Optionally a risk may have an assigned person responsible for its resolution and a date by which the risk must be resolved. Creating anonymous risk reporting channel. Each team member should have the possibility to report risks that he/she foresees in the project. Preparing mitigation plans for risks that are chosen to be mitigated. The purpose of the mitigation plan is to describe how this particular risk will be handled – what, when, by whom and how will it be done to avoid it or minimize consequences if it becomes a liability. Summarizing planned and faced risks, effectiveness of mitigation activities, and effort spent for the risk management. Megaprojects (sometimes also called "major programs") are large-scale investment projects, typically costing more than $1 billion per project. Megaprojects include major bridges, tunnels, highways, railways, airports, seaports, power plants, dams, wastewater projects, coastal flood protection schemes, oil and natural gas extraction projects, public buildings, information technology systems, aerospace projects, and defense systems. Megaprojects have been shown to be particularly risky in terms of finance, safety, and social and environmental impacts. Risk management is therefore particularly pertinent for megaprojects and special methods and special education have been developed for such risk management.[49] It is important to assess risk in regard to natural disasters like floods, earthquakes, and so on. Outcomes of natural disaster risk assessment are valuable when considering future repair costs, business interruption losses and other downtime, effects on the environment, insurance costs, and the proposed costs of reducing the risk.[50][51] The Sendai Framework for Disaster Risk Reduction is a 2015 international accord that has set goals and targets for disaster risk reduction in response to natural disasters.[52] There are regular International Disaster and Risk Conferences in Davos to deal with integral risk management. Several tools can be used to assess risk and risk management of natural disasters and other climate events, including geospatial modeling, a key component of land change science. This modeling requires an understanding of geographic distributions of people as well as an ability to calculate the likelihood of a natural disaster occurring. The management of risks to persons and property in wilderness and remote natural areas has developed with increases in outdoor recreation participation and decreased social tolerance for loss. Organizations providing commercial wilderness experiences can now align with national and international consensus standards for training and equipment such as ANSI/NASBLA 101-2017 (boating),[53] UIAA 152 (ice climbing tools),[54] and European Norm 13089:2015 + A1:2015 (mountaineering equipment).[55][56] The Association for Experiential Education offers accreditation for wilderness adventure programs.[57] The Wilderness Risk Management Conference provides access to best practices, and specialist organizations provide wilderness risk management consulting and training.[58] The text Outdoor Safety – Risk Management for Outdoor Leaders,[59] published by the New Zealand Mountain Safety Council, provides a view of wilderness risk management from the New Zealand perspective, recognizing the value of national outdoor safety legislation and devoting considerable attention to the roles of judgment and decision-making processes in wilderness risk management. One popular models for risk assessment is the Risk Assessment and Safety Management (RASM) Model developed by Rick Curtis, author of The Backpacker's Field Manual.[60] The formula for the RASM Model is: Risk = Probability of Accident × Severity of Consequences. The RASM Model weighs negative risk—the potential for loss, against positive risk—the potential for growth. Main article: IT risk management IT risk is a risk related to information technology. This is a relatively new term due to an increasing awareness that information security is simply one facet of a multitude of risks that are relevant to IT and the real world processes it supports. "Cybersecurity is tied closely to the advancement of technology. It lags only long enough for incentives like black markets to evolve and new exploits to be discovered. There is no end in sight for the advancement of technology, so we can expect the same from cybersecurity."[61] ISACA's Risk IT framework ties IT risk to enterprise risk management. Duty of Care Risk Analysis (DoCRA) evaluates risks and their safeguards and considers the interests of all parties potentially affected by those risks.[62] The Verizon Data Breach Investigations Report (DBIR) features how organizations can leverage the Veris Community Database (VCDB) to estimate risk. Using HALOCK methodology within CIS RAM and data from VCDB, professionals can determine threat likelihood for their industries. IT risk management includes "incident handling", an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. According to the SANS Institute, it is a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.[63] Main article: Operational risk management Operational risk management (ORM) is the oversight of operational risk, including the risk of loss resulting from: inadequate or failed internal processes and systems; human factors; or external events. Given the nature of operations, ORM is typically a "continual" process, and will include ongoing risk assessment, risk decision making, and the implementation of risk controls. For the offshore oil and gas industry, operational risk management is regulated by the safety case regime in many countries. Hazard identification and risk assessment tools and techniques are described in the international standard ISO 17776:2000, and organisations such as the IADC (International Association of Drilling Contractors) publish guidelines for Health, Safety and Environment (HSE) Case development which are based on the ISO standard. Further, diagrammatic representations of hazardous events are often expected by governmental regulators as part of risk management in safety case submissions; these are known as bow-tie diagrams (see Network theory in risk assessment). The technique is also used by organisations and regulators in mining, aviation, health, defence, industrial and finance. The principles and tools for quality risk management are increasingly being applied to different aspects of pharmaceutical quality systems. These aspects include development, manufacturing, distribution, inspection, and submission/review processes throughout the lifecycle of drug substances, drug products, biological and biotechnological products (including the use of raw materials, solvents, excipients, packaging and labeling materials in drug products, biological and biotechnological products). Risk management is also applied to the assessment of microbiological contamination in relation to pharmaceutical products and cleanroom manufacturing environments.[64] Main article: Supply chain risk management Supply chain risk management (SCRM) aims at maintaining supply chain continuity in the event of scenarios or incidents which could interrupt normal business and hence profitability. Risks to the supply chain range from everyday to exceptional, including unpredictable natural events (such as tsunamis and pandemics) to counterfeit products, and reach across quality, security, to resiliency and product integrity. Mitigation of these risks can involve various elements of the business including logistics and cybersecurity, as well as the areas of finance and operations. Travel risk management is concerned with how organisations assess the risks to their staff when travelling, especially when travelling overseas. In the field of international standards, ISO 31030:2021 addresses good practice in travel risk management.[65] The Global Business Travel Association's education and research arm, the GBTA Foundation. found in 2015 that most businesses covered by their research employed travel risk management protocols aimed at ensuring the safety and well-being of their business travelers.[66] Six key principles of travel risk awareness put forward by the association are preparation, awareness of surroundings and people, keeping a low profile, adopting an unpredictable routine, communications and layers of protection.[67] Traveler tracking using mobile tracking and messaging technologies had by 2015 become a widely used aspect of travel risk management.[66] This section is an excerpt from Risk communication.[edit] Risk communication is a complex cross-disciplinary academic field that is part of risk management and related to fields like crisis communication. The goal is to make sure that targeted audiences understand how risks affect them or their communities by appealing to their values.[68][69] Risk communication is particularly important in disaster preparedness,[70] public health,[71] and preparation for major global catastrophic risk.[70] For example, the impacts of climate change and climate risk effect every part of society, so communicating that risk is an important climate communication practice, in order for societies to plan for climate adaptation.[72] Similarly, in pandemic prevention, understanding of risk helps communities stop the spread of disease and improve responses.[73] Risk communication deals with possible risks and aims to raise awareness of those risks to encourage or persuade changes in behavior to relieve threats in the long term. On the other hand, crisis communication is aimed at raising awareness of a specific type of threat, the magnitude, outcomes, and specific behaviors to adopt to reduce the threat.[74] Risk communication in food safety is part of the risk analysis framework. Together with risk assessment and risk management, risk communication aims to reduce foodborne illnesses. Food safety risk communication is an obligatory activity for food safety authorities[75] in countries, which adopted the Agreement on the Application of Sanitary and Phytosanitary Measures. Risk communication also exists on a smaller scale. For instance, the risks associated with personal medical decisions have to be communicated to that individual along with their family.[76] Business continuity Catastrophe modeling Cost engineering Cost-plus contract Crossing the river by touching the stones Disaster risk reduction Environmental Risk Management Authority (NZ) Financial risk management International Institute of Risk & Safety Management ISO 31000 IT risk management Risk Management Framework Loss-control consultant Moral hazard National Safety Council (USA) Optimism bias Pest risk analysis Precautionary principle Reference class forecasting Representative heuristic Risk appetite Risk aversion Risk management tools Risk premium Roy's safety-first criterion Security management Social risk management Stranded asset Supply-chain risk management Three lines of defence Gordon–Loeb model

^ Cybellium. Risk Management Exam Review: A Comprehensive Guide to Excelling in Risk Management Exams. Cybellium. p. 3. ISBN 978-1-83679-348-9. ^ a b Hubbard, Douglas (2009). The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons. p. 46. ISBN 9781119522034. ^ Ata, Nabil Abu el; Schmandt, Rudolf (2016-05-17). The Tyranny of Uncertainty: A New Framework to Predict, Remediate and Monitor Risk. Springer. p. 7. ISBN 978-3-662-49104-1. ^ a b ISO 31073:2022 — Risk management — Vocabulary. Feb 2022. Retrieved 17 July 2024. ^ a b c ISO 31000:2018 — Risk management — Guidelines. Feb 2018. Retrieved 17 July 2024. ^ ISO 31000:2018 – Risk management – A Practical Guide (1 ed.). ISO, UNIDO. 2021. ISBN 978-92-67-11233-6. Retrieved 17 December 2021. ^ Bhandari, Ashok (2021-10-27). 10X Execution: For Extra-ordinary Business Growth & Success. The PrintWorks. p. 310. ISBN 978-81-949109-2-3. ^ "Risk Manager" Society for Human Resource Management ^ "What Are Risk Analysts & Risk Managers?", CFA Institute ^ Office of Financial Management, State of Washinton (July 1, 2017). ""Risk Assessment"" (PDF). Office of the Financial Management. Retrieved June 27, 2025. ^ Hardy, Karen (2014-11-10). Enterprise Risk Management: A Guide for Government Professionals. John Wiley & Sons. p. 121. ISBN 978-1-118-91102-0. ^ Yang, Kai (2024-01-04). Quality in the Era of Industry 4.0: Integrating Tradition and Innovation in the Age of Data and AI. John Wiley & Sons. p. 242. ISBN 978-1-119-93244-4. ^ Dionne, Georges (2013). "Risk Management: History, Definition, and Critique: Risk Management". Risk Management and Insurance Review. 16 (2): 147–166. doi:10.1111/rmir.12016. S2CID 154679294. ^ "Risk Management and Insurance". NBER. Retrieved 2024-12-03. ^ "Forex ea". 2022-11-30. Retrieved 2024-12-03. ^ "Risk Management- Em Asst". 2021-06-30. SSRN 3737157. Retrieved 2024-12-03. ^ "The ascent of risk". www.pmi.org. Retrieved 2021-12-13. ^ "Target fixation in risk management. Arguments for the bright side of risk". Stefan Morcov. 2021. Retrieved 2021-12-13. ^ Morcov, Stefan (2021). Managing Positive and Negative Complexity: Design and Validation of an IT Project Complexity Management Framework. KU Leuven University. Available at ^ Mandelbrot, Benoit and Richard L. Hudson (2008). The (mis)Behaviour of Markets: A Fractal View of Risk, Ruin and Reward. London: Profile Books. ISBN 9781846682629. ^ "Risk Identification" (PDF). Comunidad de Madrid. p. 3. ^ CMU/SEI-93-TR-6 Taxonomy-based risk identification in software industry. Sei.cmu.edu. Retrieved on 2012-04-17. ^ "Risk Management Systems Checklist (Common Items)" (PDF). www.fsa.go.jpn. ^ Common Vulnerability and Exposures list. Cve.mitre.org. Retrieved on 2012-04-17. ^ Crockford, Neil (1986). An Introduction to Risk Management (2 ed.). Cambridge, UK: Woodhead-Faulkner. p. 18. ISBN 0-85941-332-2. ^ Neil Hodge (2021). "How to Address Low-Probability, High-Impact Risks", Risk Management ^ "CRISC Exam Questions". Retrieved 23 Feb 2018. ^ Baldzhy, Maryna (2023-12-25). "Risk Management Strategies in the Global Business Environment: Analysis of Complex Dependencies and Effectiveness of Measures" (PDF). Economic Affairs. 68 (4). doi:10.46852/0424-2513.4.2023.20. ^ Dorfman, Mark S. (2007). Introduction to Risk Management and Insurance (9 ed.). Englewood Cliffs, N.J: Prentice Hall. ISBN 978-0-13-224227-1. ^ McGivern, Gerry; Fischer, Michael D. (1 February 2012). "Reactivity and reactions to regulatory transparency in medicine, psychotherapy and counseling" (PDF). Social Science & Medicine. 74 (3): 289–296. doi:10.1016/j.socscimed.2011.09.035. PMID 22104085. Archived from the original (PDF) on 21 April 2018. Retrieved 20 April 2018. ^ IADC HSE Case Guidelines for Mobile Offshore Drilling Units Archived 2017-05-03 at the Wayback Machine 3.2, section 4.7 ^ Roehrig, P (2006). "Bet On Governance To Manage Outsourcing Risk". Business Trends Quarterly. Archived from the original on 2018-09-01. Retrieved 2007-09-07. ^ Shashi; Centobelli, Piera; Cerchione, Roberto; Ertz, Myriam (2020). "Managing supply chain resilience to pursue business and environmental strategies". Business Strategy and the Environment. 29 (3): 1215–1246. Bibcode:2020BSEnv..29.1215S. doi:10.1002/bse.2428. ISSN 0964-4733. S2CID 213432044. ^ Snedaker, Susan (2014). Business continuity and disaster recovery planning for IT professionals. Chris Rima (2nd ed.). Waltham, MA: Syngress. ISBN 978-1-299-85332-4. OCLC 858657442. ^ Institute of Enterprise Risk Practitioners "Distinguishing between ERM and ORM approaches". ^ "Taking the risk out of risk management: Holistic approach to enterprise risk management". Strategic Direction. 32 (5): 28–30. 2016-01-01. doi:10.1108/SD-02-2016-0030. ISSN 0258-0543. ^ University of Tromsø, Contractual Risk Management (C-RM), accessed 6 January 2021 ^ a b Greengard, S. (2010), The Difference Is in the Details, Engineering Inc., September/October 2010, pages 13–15 ^ UDC–UNIVERSAL DEVELOPMENT, L.P., Cross–Complainant and Respondent, v. CH2M HILL, Cross–Defendant and Appellant, Court of Appeal, Sixth District, California, 15 January 2010, accessed 7 January 2021 ^ State of Florida, Witt v. La Gorce Country Club, Third District Court of Appeal, 10 June 2009, accessed 6 January 2021 ^ European Commission, Customs Risk Management Framework (CRMF), accessed 28 March 2023 ^ European Commission, Customs risk management in details, accessed 28 March 2023 ^ European Commission, Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee on Customs Risk Management and Security of the Supply Chain, COM(2012) 793 final, page 3, published 8 January 2013, accessed 27 December 2023 ^ ASIS ^ Gübitz, B.; Klinger, U. (2023). ""Risk Management for Medical Devices in Compliance with EN ISO 14971"". Medical Devices and In Vitro Diagnostics. Reference Series in Biomedical Engineering: 1–32 – via Springer. ^ Lev Virine and Michael Trumper. Project Decisions: The Art and Science. (2007). Management Concepts. Vienna. VA. ISBN 978-1-56726-217-9 ^ Lev Virine and Michael Trumper. ProjectThink: Why Good Managers Make Poor Project Choices. Gower Pub Co. ISBN 978-1409454984 ^ Peter Simon and David Hillson, Practical Risk Management: The ATOM Methodology (2012). Management Concepts. Vienna, VA. ISBN 978-1567263664 ^ Oxford BT Centre for Major Programme Management ^ Berman, Alan. Constructing a Successful Business Continuity Plan. Business Insurance Magazine, March 9, 2015. ^ Craig Taylor; Erik VanMarcke, eds. (2002). Acceptable Risk Processes: Lifelines and Natural Hazards. Reston, VA: ASCE, TCLEE. ISBN 9780784406236. Archived from the original on 2013-12-03. ^ Rowling, Megan (2015-03-18). "New global disaster plan sets targets to curb risk, losses". Reuters. Archived from the original on 2016-03-04. Retrieved 2016-01-13. ^ "American National Standard ANSI/NASBLA 101-2017: Basic Boating Knowledge—Human Propelled" (PDF). Retrieved 2018-11-01. ^ "UIAA Standard 152: Ice Tools" (PDF). Archived from the original (PDF) on 2020-08-20. Retrieved 2018-11-01. ^ "EN 13089 Mountaineering equipment – Ice-tools – Safety requirements and test methods (includes Amendment A1:2015)". Retrieved 2018-11-01. ^ "Irish Standard I.S.EN 13089:2011+A1:2015 Mountaineering equipment – Ice-tools – Safety requirements and test methods" (PDF). Retrieved 2018-11-01. ^ "Association for Experiential Education". Retrieved 2018-11-01. ^ "NOLS Risk Services". Retrieved 2018-11-01. ^ Haddock (2013). Outdoor safety : risk management for outdoor leaders. Wellington, NZ: New Zealand Mountain Safety Council. ISBN 9780908931309. ^ Schneider, Ari (23 May 2018). Outdoor Leadership and Education. Xalibu LLC. ISBN 9781732348202. ^ Arnold, Rob (2017). Cybersecurity: A Business Solution. Threat Sketch. p. 4. ISBN 978-0692944158. ^ "Duty of Care Risk Analysis Standard (DoCRA)". DoCRA. Archived from the original on 2018-08-14. Retrieved 2018-08-22. ^ SANS Glossary of Security Terms Retrieved on 2016-11-13 ^ Saghee, M; Sandle, T; Tidswell, E, eds. (2011). Microbiology and Sterility Assurance in Pharmaceuticals and Medical Devices (1 ed.). Business Horizons. ISBN 978-8190646741. ^ International Organization for Standardization (ISO), ISO 31030:2021 Travel risk management — Guidance for organizations, Edition 1, published in 2021, accessed on 22 January 2025 ^ a b GBTA Foundation, Overwhelming Majority of Companies Keep Travelers Safe Through Travel Risk Management Protocols, published on 19 May 2015, accessed on 23 January 2025 ^ Global Business Travel Association Risk Committee, Keeping Safe with Some Solid Advice: Travel Risk Awareness Clarified, published on 20 July 2022, accessed on 23 January 2025 ^ Risk Communication Primer—Tools and Techniques. Navy and Marine Corps Public Health Center ^ Understanding Risk Communication Theory: A Guide for Emergency Managers and Communicators. Report to Human Factors/Behavioral Sciences Division, Science and Technology Directorate, U.S. Department of Homeland Security (May 2012) ^ a b Rahman, Alfi; Munadi, Khairul (2019). "Communicating Risk in Enhancing Disaster Preparedness: A Pragmatic Example of Disaster Risk Communication Approach from the Case of Smong Story". IOP Conference Series: Earth and Environmental Science. 273 (1): 012040. Bibcode:2019E&ES..273a2040R. doi:10.1088/1755-1315/273/1/012040. S2CID 199164028. ^ Motarjemi, Y.; Ross, T (2014-01-01), "Risk Analysis: Risk Communication: Biological Hazards", in Motarjemi, Yasmine (ed.), Encyclopedia of Food Safety, Waltham: Academic Press, pp. 127–132, ISBN 978-0-12-378613-5, retrieved 2021-11-12 ^ "Risk communication in the context of climate change". weADAPT | Climate change adaptation planning, research and practice. 2011-03-25. Retrieved 2021-11-12. ^ "RISK COMMUNICATION SAVES LIVES & LIVELIHOODS Pandemic Influenza Preparedness Framework" (PDF). World Health Organization. 2015. ^ REYNOLDS, BARBARA; SEEGER, MATTHEW W. (2005-02-23). "Crisis and Emergency Risk Communication as an Integrative Model". Journal of Health Communication. 10 (1): 43–55. doi:10.1080/10810730590904571. ISSN 1081-0730. PMID 15764443. S2CID 16810613. ^ Kasza, Gyula; Csenki, Eszter; Szakos, Dávid; Izsó, Tekla (2022-08-01). "The evolution of food safety risk communication: Models and trends in the past and the future". Food Control. 138: 109025. doi:10.1016/j.foodcont.2022.109025. ISSN 0956-7135. S2CID 248223805. ^ Stevenson, Mabel; Taylor, Brian J. (2018-06-03). "Risk communication in dementia care: family perspectives". Journal of Risk Research. 21 (6): 692–709. doi:10.1080/13669877.2016.1235604. ISSN 1366-9877. S2CID 152134132.

Risk management resources, Global Risk Institute Risk knowledge library, Risk and Insurance Management Society Risk Journals, Risk.net Glossary of financial risk management terms, Risk.net DoD Risk Management Guide for Defense Acquisition Programs Archived 2017-07-04 at the Wayback Machine (2017) Risk management at Wikipedia's sister projects:Media from CommonsResources from WikiversityData from Wikidata Retrieved from " In the healthcare industry, patients, staff and even organizations themselves are exposed to risk on a daily basis. Risks to patient care, financing, accreditation, market share and reputation are unavoidable, making a strong risk management program an essential component to any well-run healthcare organization. Risk management in healthcare encompasses all of the steps taken to identify, assess, mitigate, monitor and prevent risks from causing significant damage. In order for proactive risk assessment and response to have a meaningful impact in the midst of a health crisis, risk management should constantly remain a top priority. Risk Management in Healthcare Organizations Traditionally, the role of risk management focused on patient care and safety, but in our modern world, new technologies, cybersecurity concerns, medical science advancements and an ever-confusing regulatory landscape have driven risk management to become a much more complex and intricate process. In an organism as large as the healthcare industry, risks come in many different shapes and sizes. Whether it be working directly with patients, clinical research or healthcare administration, an unidentified or unaddressed risk can have a rippling effect impacting more than a single department or system. Nowadays, the way an entity approaches risk will have a significant effect on the value it brings to clients and ultimately, it's financial performance. The role of risk management has evolved from a reactive measure meant to limit legal exposure to become a preventative, comprehensive program capable of safeguarding the entire healthcare ecosystem. Proactively implementing a risk management strategy helps to prevent an incident from occurring or minimize the effects of one that cannot be eliminated altogether, thus improving the quality of the organization. While the role of risk management in healthcare is growing, the adoption of more sophisticated processes has been slow to come about. This lack of preparation can lead to dire consequences in a crisis: compromised patient and provider safety, increased risk of liability and financial losses. How Risk Management Works in Practice Throughout an organization, time should be taken to identify and assess risks. All potential risks need to be prioritized so that you can address those with highest potential to negatively impact your operations in any way. After that, you'll be able to develop an organizational-specific risk management plan. Developing a plan, of course, is not a simple, quick process. You first need to begin by performing a risk-specific analysis that answers these questions: What could possibly happen? To answer this question takes a considerable amount of research to ensure you have the latest information on everything from regulations to scientific studies. Every healthcare provider should constantly review new guidelines, studies and directives announced by governing bodies such as the Food and Drug Administration (FDA), the Department of Health and Human Services (HHS) or the American Society for Healthcare Risk Management (ASHRM). In addition to gathering external information, internal policies, procedures and processes should also be reviewed. How likely is a risk to occur? In order to determine this, you need to engage those in your organization who are familiar with daily operations and can assess the probability of a risk. A qualitative assessment can be used to determine the likelihood by using an established scaled (such as low, medium or high). This subjective rating system depends on assessor expertise to be the most accurate. If a risk occurs, how severe will the effects be? In order to gain more insight about your risk mitigation process, a quantitative assessment attaches numerical values to your analysis such as money or time. By using values such as money, time or lost assets to determine risk impact, a quantitative risk assessment provides an accurate reflection of your threat landscape By understanding the severity of a risk, you are able to rank and prioritize threats to deal with the most immediate and dangerous. How can the likelihood of a risk occurring be mitigated? In general, your risk mitigation strategy will fall into one of these categories: risk avoidance, risk limitation, risk transference or risk acceptance. How you proceed depends on your risk experts' analysis of the risk in question. How can we reduce a risk's impact? After you have chosen a strategy, you will take steps to implement it. For example, doctors will transfer the risk of medical error causing significant financial loss by purchasing malpractice insurance. What cannot be proactively avoided? Some risks are impossible to adequately prepare for in advance, and careful consideration should be taken to make sure you've prepared as well as possible. You can't plan for every eventuality, but you can anticipate that at some point, a crisis will occur. The role of risk management in healthcare is to help you prevent a crisis from occurring and be as prepared as possible when the unexpected does happen. The Role of Risk Management in Crisis During health crises, such as the COVID-19 pandemic, risk management is an important component to focus on. Chaotic situations can be full of uncertainty; uncertainty is unknown and unpredictable. Risk however, is measurable, relying on objective data and analysis. Having a plan for identifying, assessing, mitigating and monitoring risks will keep your organization on track and focused on keeping all patients, care providers and the institution safe. The Role of Risk Management Software From building assessments to evaluating data, ComplianceBridge Risk helps you to manage each step and make your job easier. This versatile software brought to you by ComplianceBridge allows you to manage risk on as many as six different dimensions. You have the ability to customize question sets and even to weigh questions to improve measurement of risk with conditional logic. Respondents can delegate assessments or reassign specific questions to the most qualified individual. Assessments can also be divided up among teams, departments or individuals, adding more flexibility to the process. Results can be viewed in real-time from a manager dashboard. ComplianceBridge Risk will allow your company to manage risk on a regular basis. It improves reporting and giving you more accurate data to aid in choosing an appropriate risk mitigation strategy. Learn more about our risk management software today by scheduling a demo!

Enjoy sharper detail, more accurate color, lifelike lighting, believable backgrounds, and more with our new model update. Your generated images will be more polished than ever.See What's NewExplore how consumers want to see climate stories told today, and what that means for your visuals.Download Our Latest VisualGPS ReportData-backed trends. Generative AI demos. Answers to your usage rights questions. Our original video podcast covers it all—now on demand.Watch NowEnjoy sharper detail, more accurate color, lifelike lighting, believable backgrounds, and more with our new model update. Your generated images will be more polished than ever.See What's NewExplore how consumers want to see climate stories told today, and what that means for your visuals.Download Our Latest VisualGPS ReportData-backed trends. Generative AI demos. Answers to your usage rights questions. Our original video podcast covers it all—now on demand.Watch NowEnjoy sharper detail, more accurate color, lifelike lighting, believable backgrounds, and more with our new model update. Your generated images will be more polished than ever.See What's NewExplore how consumers want to see climate stories told today, and what that means for your visuals.Download Our Latest VisualGPS ReportData-backed trends. Generative AI demos. Answers to your usage rights questions. Our original video podcast covers it all—now on demand.Watch Now