**Business Risk Assessment Guidance Document**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Review date:** | **Edited by:** | **Approved by:** | **Comments:** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1 Introduction 3](#_Toc49417646)

[1.1 Guidance statement 3](#_Toc49417647)

[1.2 Status 3](#_Toc49417648)

[1.3 Training and support 3](#_Toc49417649)

[2 Scope 3](#_Toc49417650)

[2.1 Who it applies to 3](#_Toc49417651)

[2.2 Why and how it applies to them 4](#_Toc49417652)

[3 Definition of terms 4](#_Toc49417653)

[3.1 XYZ 4](#_Toc49417654)

[3.2 Reasonably foreseeable incident 4](#_Toc49417655)

[3.3 Reasonably foreseeable impact 4](#_Toc49417656)

[3.4 Likelihood 4](#_Toc49417657)

[3.5 Risk 4](#_Toc49417658)

[3.6 Risk matrix 4](#_Toc49417659)

[3.7 Accreditation 4](#_Toc49417660)

[4 Basic risk assessment principles 5](#_Toc49417661)

[4.1 Overview 5](#_Toc49417662)

[4.2 Duties and responsibilities 5](#_Toc49417663)

[4.3 Making competency-based judgements 6](#_Toc49417664)

[4.4 Documentation 6](#_Toc49417665)

[5 Conducting business related risk assessments 6](#_Toc49417666)

[5.1 Aim of a business risk assessment 6](#_Toc49417667)

[5.2 The principles of risk assessment 7](#_Toc49417668)

[5.3 Calculating risk(s) 7](#_Toc49417669)

[5.4 Business risks and where they may be found 7](#_Toc49417670)

[5.5 A consistent approach 8](#_Toc49417671)

[5.6 Business risk assessment considerations 9](#_Toc49417672)

[5.7 Structuring a business risk description using XYZ methodology 9](#_Toc49417673)

[5.8 A business risk impact scale 10](#_Toc49417674)

[5.9 Likelihood of occurrence (factors) 11](#_Toc49417675)

[5.10 Likelihood descriptions 12](#_Toc49417676)

[5.11 XYZ impact descriptors 12](#_Toc49417677)

[5.12 Multiple locations with similar risks 13](#_Toc49417678)

[5.13 Grouping risks 14](#_Toc49417679)

[5.14 Risk control strategies 14](#_Toc49417680)

[5.15 Managing resources 15](#_Toc49417681)

[5.16 Business risk action planning 15](#_Toc49417682)

[5.17 Third party risk considerations 16](#_Toc49417683)

[5.18 Additional controls 16](#_Toc49417684)

[5.19 Reviewing business risks 17](#_Toc49417685)

[5.20 Monitoring risks 17](#_Toc49417686)

[5.21 Residual risk 17](#_Toc49417687)

[5.22 Additional business considerations 18](#_Toc49417688)

[5.23 Quality assurance and administration 18](#_Toc49417689)

[5.24 Audits and review 19](#_Toc49417690)

[6 Additional information 19](#_Toc49417691)

[6.1 Recommended resources 19](#_Toc49417692)

[7 Summary 19](#_Toc49417693)

[Annex A 20](#_Toc49417694)

# Introduction

## Guidance statement

Business risk assessments are often perceived as being complicated and very time consuming. This guidance is provided to assist assessors to complete a suitable and sufficient assessment of business risk and manage it in context with others. It must be understood that, whilst this guide contains information and explanations of some of the broader principles of business risk, it is not intended to cover every aspect or circumstance.

Often the natural instinct when undertaking a business risk assessment is simply to assess what is perceived to be ‘the problem’, devise certain controls with which to approach it and to consider this to have completed the task. This guidance document is aimed at supporting assessors’ knowledge and their approach to risk assessments, as well as improving the quality of the risk assessments they may have already undertaken.

## Status

The organisation aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this aide-memoire might have regarding the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment.

## Training and support

The organisation will provide guidance and support to help those to whom it applies to understand their rights and responsibilities under this guidance document. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this document.

# Scope

## Who it applies to

This document applies to all staff at [insert organisation name]. Other individuals performing functions in relation to the organisation, such as agency workers, locums and contractors, are encouraged to use it.

## Why and how it applies to them

This document has been produced to provide staff at [insert organisation name] with an overview of how the organisation can undertake a suitable and sufficient assessment, whilst giving the necessary level of information to understand how the process is undertaken and the benefits that can be gained for both the organisation and their patients.

# Definition of terms

## XYZ

A methodology for assessing business risks

## Reasonably foreseeable incident

A reasoned prediction of what and why an incident may occur

## Reasonably foreseeable impact

An impact (or level of consequence) that could reasonably be anticipated

## Likelihood

The likelihood of an incident (or exposure) occurring

## Risk

Impact (multiplied by) likelihood

## Risk matrix

A numerical scale of impact (consequence) and likelihood of occurrence

## Accreditation

The action or process of officially recognising someone or an organisation as having a particular status or being qualified to perform a particular activity

# Basic risk assessment principles

## Overview

It will be of huge benefit to adopt a systematic approach to the identification, assessment and management of business risk which will enable a much better understanding of what needs to be managed and to what extent.

Risk related information is broadly set against the standards promoted by organisations such as the Institution of Occupational Safety and Health (IOSH)[[1]](#footnote-1) and the International Institute of Risk and Safety Management (IIRSM).[[2]](#footnote-2)

The general requirements to undertake risk assessments are set out in the Management of Health and Safety at Work Regulations 1999 (MHSWR) and its Approved Code of Practice (ACOP) which takes precedence[[3]](#footnote-3).

## Duties and responsibilities

The following duties and responsibilities are detailed in the Health and Safety at Work etc. Act 1974 (HASAWA):[[4]](#footnote-4)

* **Employers** have the responsibility for ensuring health and safety requirements are put into practice and this is accepted to be via the line management structure. This means that, on a day to day basis, managers hold the duty of the employer. Ultimate responsibility is held by the most senior person within the organisation.
* **Managers** are responsible for reasonably foreseeable risks being identified, evaluated, prioritised and then controlled so far as is reasonably practicable. Managers at all levels are also accountable for those risks over which they have the authority and/or budgetary control to act.
* **Employees** have a responsibility to ensure that they conduct their activities in a safe manner, following policy or as directed by their line manager(s). When off-site and/or working independently, employees should conduct themselves in a safe manner at all times.

As a point of note, managers cannotbe accountable for risks over which they do not have authority or budgetary control to act but they are responsible for identifying and evaluating risks that arise from their work and passing information to those who do have accountability to act.

## Making competency-based judgements

It is important that those involved with the business risk assessment process have an appropriate level of demonstrable competence to undertake the risk assessment and manage the process end to end.

There are many opinions as to what is meant by the term ‘competency’. However, it is generally accepted to be a blend of the following factors:

* Knowledge, experience, ability, skill and training underpinned by an individual’s clear understanding of their own limitations

Competency must also play its part in the decision-making process as to when, as well as when not, to undertake a business risk assessment

## Documentation

The important aspect of a business risk assessment is the content. A template has been provided at Annex A to assist assessors in documenting the required information.

This will enable assessors to construct a reflective risk assessment at [insert organisation name]. It is the assessor’s responsibility to ensure that the data contained within the business risk assessment is reflective of the organisation’s own specific conditions.

If any risk assessment is generic and its content is challenged, responsible individuals may, at the very least, be criticised by an enforcement officer or other regulator for failing to provide a suitable and sufficient risk assessment.

The methodology for risk assessments is set out within the [Risk Assessment Guidance Document](https://practiceindex.co.uk/gp/forum/resources/risk-assessment-guidance-document.1519/).

# Conducting business related risk assessments

## Aim of a business risk assessment

Before understanding how to conduct any business risk assessment, there is one key learning point to remember and that is the aim of a risk assessment, which is:

The core function of any risk assessment is to identify its relative priority.

There are many differing matrices and approaches to risk assessment. Irrespective of this, as long as the assessment clearly demonstrates its relative priority, the content is reflective of circumstances and the methodology consistently applied, then the risk assessment should be valid.

## The principles of risk assessment

In order to be successful when undertaking a business risk assessment, it is important to acknowledge that risk is calculated by the sum (by multiplying together) of two independent variables, with key descriptions that are represented numerically one to five on an X and Y axis.

These independent variables (that cannot influence or affect each other) are nominally called consequence and likelihood. In order to undertake a risk assessment, assessors must undertake an assessment of consequence and a separate assessment of likelihood and rate each independently.

## Calculating risk(s)

Using the broad principle of risk, supported by the risk matrix, will enable assessors to calculate the level of risk by using the numerical values of both consequence and likelihood. These numerical values, when multiplied together, give a numerical value of risk: Impact (Consequence) x Likelihood = risk.

A picture containing large

Description automatically generated

Image Source: [Risk Management Policy and Procedure](https://www.sth.nhs.uk/clientfiles/File/Enclosure%20K%20-%20RiskManagementPolicyStrategy.pdf)

Risks are graded and given a rating as shown below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk rating** | | | |
| Low 1 **–** 3 | Moderate 4 **–** 6 | High 8 **–** 12 | Extreme 15 **–** 25 |

Image Source: [Risk Management Policy and Procedure](https://www.sth.nhs.uk/clientfiles/File/Enclosure%20K%20-%20RiskManagementPolicyStrategy.pdf)

## Business risks and where they may be found

It is important that each manager has an appreciation as to from where potential risks may arise. This should then prompt the following questions:

1. Which risks should we be concerned with?
2. What risks may impact on achieving current business objectives?

The table below provides an overview of some of the potential subjects which may have an associated risk. Please note this list is not exhaustive.

|  |  |
| --- | --- |
| Subject | Consideration(s) |
| Staff | Training and development, travel and lone working, training matrix management, personal development reviews (PDRs), recruitment and retention, health, safety and welfare, professional registration and competencies, consultation, co-ordination, communication and co-operation |
| Patients | Patient records, communication, contact and safety |
| Premises | Infrastructure, equipment servicing/maintenance (gas safety, water, electricity etc.), external technical assessments/reports (fire and asbestos etc.), service providers/suppliers, media (TV, local paper and social media), contractors (third party cleaning services, maintenance etc.) |
| Systems | Policies and procedures, quality management, information technology, data protection and confidentiality, clinical activities, health and safety, purchasing and budgets |
| Finance | Financial liability, fraud, income versus expenditure, rent, rates, utilities, salaries/drawings, insurance etc. |
| Planning | Succession plan, business continuity plan, fire and emergency evacuation plan etc. |
| Other | Political, Economic, Sociological, Technological, Environmental, Legal (PESTEL analysis) |

Not all risk is necessarily bad or negative. In fact, risk can have a positive influence, or an upside, and this can include:

* + Events that we want to happen
  + Impacts that are beneficial
  + Doing something pro-actively to create and exploit an opportunity

Positive risks should be open to the same kind of analysis as negative risks. However, most organisations do not do this very well, if at all.

## A consistent approach

As detailed in the [Risk Assessment Guidance Document](https://practiceindex.co.uk/gp/forum/resources/risk-assessment-guidance-document.1519/), most health and safety risk assessments are task based. Therefore, risk assessors need to ensure they are assessing the tasks that staff and/or patients undertake (or are potentially exposed to the risks from other tasks being performed) whilst on the premises or elsewhere. The same risk assessment template could be adapted for use in assessing business risks.

However, when assessing business risks, the task-based approach cannot always be applied and a slightly different approach may be required. Irrespective of any methodology used, assessors must ensure that there is a consistent approach to the assessment process. If the approach is consistent then, whatever the resulting risks are, they should easily be comparable with other risks.

## Business risk assessment considerations

There may be the potential for multiple business impacts in any given circumstance, for example a fatal fire. Such an event would undoubtedly impact on service delivery, reputation, community access to services, finance, future staff recruitment/retention and other core business subjects.

Bearing the aforementioned in mind, there is often a temptation for managers to try to explain every eventuality by placing lots of data within the general impact description. Unfortunately, a mass of information can be counterproductive, as it can potentially disguise the reasonably foreseeable impact which may adversely influence the application of the impact score, its risk rating and ultimately its relative priority.

This could mean those ultimately responsible for making decisions and allocating resources may over or under-resource the risk. Therefore, the anticipated impact outcome would benefit from being singular in its description with additional impacts annotated in the organisation’s risk register and dealt with using a comprehensive action plan.

It is important that clarity and consistency are achieved when describing business risks, using a structured methodology that can be used to deliver a short but meaningful risk description. There are differing methods of describing business risk, with the XYZ model being the methodology of choice.

## Structuring a business risk description using XYZ methodology

The XYZ methodology is designed to illustrate how impact information (risk description) can be briefly and meaningfully articulated. XYZ is best constructed as a whole sentence but, when broken down into its constituent parts, the broad description of each element is as follows:

**X** **–** Briefly describes the nature of the problem

**Y –** Gives an illustrative reason why this event might occur

**Z –** Indicates an anticipated outcome that is reasonably foreseeable (at worst)

The following are simple hypothetical examples that reflect the use of the **XYZ** methodology for describing the risk impact:

1. **X –** Failing to meet CQC expectations, **Y –** due to having poor management systems, **Z –** resulting in loss of service provision
2. **X** – Lack of inward financial investment, **Y** – due to unclear priorities, **Z** – resulting in key equipment upgrades being delayed
3. **X** – Key member of staff being suddenly indisposed, **Y** – with no succession plan in place, **Z** – resulting in a significant business knowledge gap
4. **X** – Failing to maintain appropriate core staffing levels in key business areas, **Y –** due to limitations of local resources, **Z –**resulting in poor service delivery and/or increased locum costs
5. **X –** Key equipment breakdowns, **Y –** due to ineffective maintenance/failure to recognise wear and tear, **Z –**resulting in failing to deliver quality healthcare services
6. **X –** Failing to develop skills of existing staff, **Y –** due to lack of investment, **Z –**resulting in disincentivised staff with ongoing retention issues
7. **X –** Failing to provide sufficient training to achieve mandatory requirements, **Y –** due to staff availability/time restrictions, **Z –** resulting in non-compliance with statutory/mandatory requirements
8. **X –** Increase in volume of quality complaints, **Y –** due to a lack of due diligence and/or process failure, **Z –** resulting in reputational damage of the organisation
9. **X** – Inability to fully comply with new COVID-19 requirements, **Y** – due to physical space restrictions within the premises, **Z** – resulting in limitations being placed upon service delivery, resulting in an increase in complaints

It is important for any organisation to define what a particular impact may mean in the context of their own circumstances. It is therefore recommended that, if not already in place, a meaningful and localised business impact scale should be developed.

## A business risk impact scale

Each number on the business impact scale must have an agreed value to the business that must be meaningful, reflective and written in context. Illustrative examples are shown in tabular form overleaf:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Impact rating | Reputation damage | Health, safety & wellbeing | Recruitment and/or retention | Fire | Financial |
| 5 | Sustained national media coverage of a negative event | Fatality or multi fatality and/or prosecution at Crown Court for regulatory non-compliance | Inability to recruit/retain staff leading to core service suspension or service delivery failure | Permanent loss of premises | >£1 million anticipated cost of a significant or negative event |
| 4 | Sustained regional or local media coverage of a negative event | Non-recoverable injury | Short term < 3 months ability to recruit to key roles and/or loss of several key staff | Loss of part of premises > 4 weeks | >£100K but < £1 million  anticipated cost of a negative event |
| 3 | Single front- page article of general criticism in local newspaper | Recoverable injury requiring hospital treatment | Temporary unplanned loss > 1 week of > 2 staff from same department | Loss of part of premises < 4 weeks | < £100K but > £10K  anticipated cost of a negative event |
| 2 | Multiple general (minor) complaint letters from public or patients | Minor injury to a person and/or damage to equipment | Temporary unplanned loss < 1 week of a staff member | Loss of part of premises for up to 72 hours, e.g. damage from a flood or break-in etc. | > £500  anticipated cost of a negative event |
| 1 | Single letter of complaint on a minor matter | Minor damage but no injury from an accident | < 48 hours absence of 1 member of staff | Temporary loss of room or part of premises | <£500  anticipated cost of a negative event |

## Likelihood of occurrence (factors)

When making a judgement about the likelihood of occurrence, the relevant factors that will contribute to the judgement (where reasonable) should be evidence based and articulated in context. It is recommended that a minimum of three to four relevant factors are used to support the likelihood judgement.

It is to be noted that additional data and/or related information can be utilised in a business context, such as compliance statements, investment data, policy effectiveness, relevant records or communications, delivery and/or lead-times, partner and/or other organisational factors as well as joint enterprise information.

Further information on likelihood factors (from a safety perspective) can be found in the Risk Assessment Guidance Document.

## Likelihood descriptions

The table below has been produced to help to translate what is meant by likelihood when used in context with the risk matrix (Section 5.3).

|  |  |  |
| --- | --- | --- |
| Ref | Matrix description likelihood | Likelihood interpretation |
| 5 | Almost certain | There are no significant controls in place or, those that are, are only ‘nominally’ in place but are never actually practiced, managed or in any way effective. Often compounded by very poor behaviour of those involved |
| 4 | Likely | Limited controls in place, often not very effective and involve frequent significant lapses in practice or application. Often limited competency of those involved and/or a lack of supervision leading to poor behaviours |
| 3 | Possible | Some controls in place which are mostly effective but occasional significant lapses in practice or application do occur. General competencies may vary, but generally positive with reasonable behaviours and supervision |
| 2 | Unlikely | Controls are generally quite effective, in a reasonable work environment with infrequent minor lapses in practice or application of controls. Behaviour of those involved is generally good |
| 1 | Rare | Controls are very robust and are effectively practiced each and every time with good behaviours exhibited. Usually very good levels of supervision, higher levels of competency and good motivation from those involved |

## XYZ impact descriptors

Sometimes managers identify the outcome, or even a reason why something might happen in the first instance, meaning that the person undertaking the business risk assessment may have to work backwards to enable the description to make sense for others. Imagine a manager has a concern, such as:

*“They are worried that they might be prosecuted’*

On its own, the above statement has little context. Therefore, the above outcome (Z) needs to be supported by meaningful information to give more context.

As the (Z) is notionally about being prosecuted, in this instance we would need to work backwards to construct the rationale for why this prosecution could occur.

There are a host of different reasons that could be used as a rationale, however all that is required is to describe a single illustrative reason (Y) that is reasonably foreseeable.

*e.g.* **–** *‘Due to a lack of due diligence (****Y)***

Taking this process to its final step (when working backwards), the final question (to identify X) should be, what is the nature of the problem?

*e.g. The Fire Service Inspectorate stated categorically that they could almost certainly prosecute if the current non-compliance continued.*

The above information needs to be broken down into component parts then put in chronological order so that it becomes a meaningful short sentence (risk description).

This risk description (XYZ) can then be impact rated, using an agreed matrix (Section 5.9) and would be rated 5 on the illustrated business impact scale.

The above example has been expanded to include likelihood factors and is shown below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| XYZ risk description | Impact rating | Likelihood of occurrence | Likelihood rating | Risk rating |
| **(X)** Compliance with enforcement requirements not achieved, (**Y)** due to lack of due diligence on regulatory compliance actions, (**Z)** resulting in a potential prosecution | 5 | No progress has been made since being notified in writing 2 months ago, with practice manager now on long term sick, no interim PM has yet been appointed  Contractor requested to quote for improvement works, lead time is 8 weeks, with Fire Service re-inspection due next month  Currently non-compliant with RIDDOR, due to failure to report on time | 4 | 20 |

## Multiple locations with similar risks

For organisations operating from multiple premises, it would not be unusual for similar risks to exist in each location. If a risk assessment was conducted in location A and it is later identified that the same risk is present at location B, the level(s) of risk may be the same.

It may be that each location can manage their risk(s) independently with existing resources. The correct risk management approach will depend on the levels of risk at each location, the availability of local resources and any variances of relevant local conditions.

## Grouping risks

It may prove beneficial for an overarching business risk assessment to be conducted, enabling a number of individual risks of the same subject to be grouped with the option of using hyperlinks to the individual risk assessments. These risks could be overseen centrally but managed locally to achieve a common purpose.

This would enable risks to be connected so that informed decisions could be made in context with all information readily available. This, in turn, would enable managers to select an appropriate risk control strategy.

It must be noted that, depending on circumstances, the level of the combined business risk may differ from the original level of the individual risks due to their collective impact and likelihood.

## Risk control strategies

There are various strategies that can be deployed to control risk. Some professional bodies may also offer or advocate strategies for specific business orientated subjects. The table below details basic strategies for consideration:[[5]](#footnote-5)

|  |  |
| --- | --- |
| **Strategy** | **Comment** |
| Eliminate | Discontinue the activity in its entirety so that the risk is removed. Although this should always be considered, it may not be reasonable. |
| Reduce | By the allocation of resources. It is worth noting that, in most circumstances (whilst there are exceptions), the likelihood of occurrence is usually influenced more than the potential impact. |
| Tolerate | This is a level of risk that the business will essentially ‘put up with’, whilst actively managing the risk using existing, effective control measures. |
| Transfer | This is when (usually with written consent) a risk is transferred in its entirety to another organisation. |

The strategy is recorded on the organisations risk register.

## Managing resources

Managers may occasionally struggle to define or deploy resources for a particular risk (or group of similar risks) as every organisation will have varying levels of resources at their disposal. Furthermore, several considerations need to be made including:

* The time and effort that can be allocated by individuals/teams
* The people available (including their competencies)
* Levels of supervision and monitoring
* Equipment and supplies

It is advisable that all relevant legal and/or safety requirements are met in the first instance.

The level of resources allocated to a particular risk can be determined by the following principles:

* Higher level risks where assessed (numerically) are to be more deserving of resources than lesser medium and lower level risks
* Medium level risks where assessed (numerically) are less than higher level risks but still more deserving of resources than lower level risks
* Lower level risks where assessed (numerically) may require resources based upon their relative priority

It is important to recognise that, irrespective of the level of risk, if there is a failure to supervise, monitor or review risks effectively and proportionately, then it is not unreasonable for any risk to have the potential to increase. It is further advised that, if a statutory requirement cannot be met, then the activities that may be adversely affected should be suspended until adequate arrangements are put in place.

## Business risk action planning

When articulating a new control that is required, it is important to be clear about what controls are being introduced in order to reduce the level of risk. The most appropriate manner in which this can be achieved is by constructing the control in terms of SMART, that is Specific, Measurable, Achievable, Realistic and Time bound. SMART is advocated by the Chartered Management Institute (CMI).[[6]](#footnote-6)

When any changes to existing control measures are made, or when new control measures are introduced, it is imperative that they are communicated to the whole team.

## Third party risk considerations

Organisations work with a range of partner organisations, contractors and other service providers and, as a result, additional risks may be identified. Therefore, organisations should consider the following:

* What are the risks that the organisation may expose a third party to whilst conducting day to day business?
* What are the risks that the third party may expose the organisation to whilst conducting operations?
* What new, changed or combined risks may arise from interacting with third parties?

Contractors can often present significant challenges whilst on the premises so therefore the management of contractors must be a business risk consideration. Further information is available via the HSE.[[7]](#footnote-7)

## Additional controls

Existing control measures may require improvement or new controls may be necessary. The hierarchy of controls[[8]](#footnote-8) below should be considered. Further information on the risk control hierarchy is available on the HSE website.

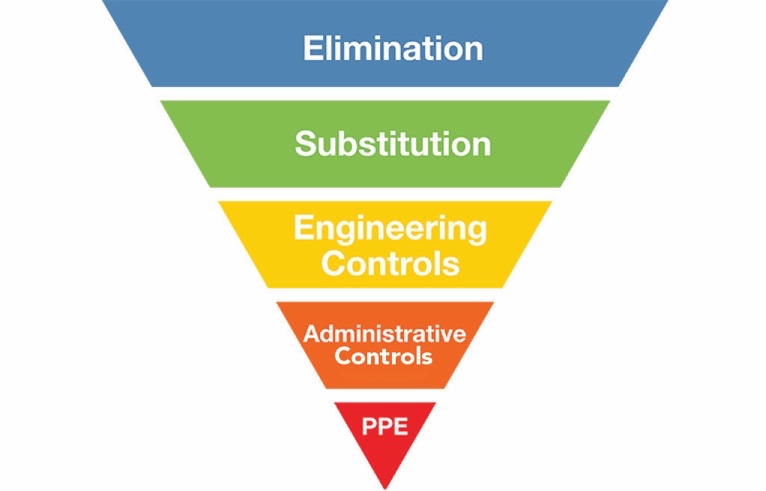


Image source: [safetyandhealthmagazine.com](https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.safetyandhealthmagazine.com%2Farticles%2F16790-the-hierarchy-of-controls&psig=AOvVaw1ja7TKyVASFuSlYKbQuSmC&ust=1598104890244000&source=images&cd=vfe&ved=2ahUKEwj4vdLjuqzrAhUS4BoKHefGBvYQr4kDegUIARC7AQ)

Due to the range of business risks that may be assessed, there is no single strategy or hierarchy of controls that would meet every potential eventuality. Therefore, it is advised that, irrespective of the business subject risk, the controls that are either already in place, or are required, are identified as being fit for that specific purpose and relevant to the nature and extent of the risk itself.

## Reviewing business risks

A business risk assessment is a legal document and, by virtue, is disclosable to certain third parties. Additionally, it may be required as evidence for either criminal or civil court actions. Therefore, regular reviews are essential and should be conducted at least annually.

Managers should have a robust system in place that ensures the controls that are in place are maintained and remain effective, that any amendments that are required are actioned and key information is made available to those who may be affected by the risk(s).

The date of the review must be recorded on the assessment and the subsequent review date annotated. The most effective way to determine how often a risk assessment should be reviewed is by looking at its relative priority (numerically) then using the illustrative guide within the risk review profile detailed in the risk assessment template at Appendix 1 of the Risk Assessment Guidance Document.

If challenged by HSE, the CQC or other regulatory bodies, practice managers and/or the responsible person will have to justify the periodicity for the review of documents and the effectiveness of such reviews. If it cannot be evidenced that a review was undertaken, then it did not happen.

## Monitoring risks

It is recommended that business risks are monitored in line with their relative priority, as you may be required to demonstrate that you are monitoring the risks in addition to carrying out regular reviews.

Risk monitoring can also involve:

* + Ensuring required actions are taken
  + Tracking risk control progress
  + Identifying changes in operations, finance and/or strategy
  + Reviewing the effectiveness of reporting structures
  + Identifying new/changed risks

Monitoring can be included on the organisation’s risk register. If it cannot be evidenced that a risk was monitored, then it did not happen.

## Residual risk

Residual risk is the remaining risk after all the additional control measures have been implemented and are deemed to be working effectively. Until this point, the actual level of risk is managed in terms of its relative priority. This is essentially a competency-based judgement with the aspiration that the risk will reduce numerically.

Assessors must be mindful that, whilst the general objective is to reduce risk numerically, if the control is not suitable, it could increase the risk, rather than decrease it.

## Additional business considerations

In order to ensure that managers are aware of all elements of organisational activity, they should consider the following:

* Is there confidence in the current arrangements that enable a clear understanding of the key business risks that currently affect the organisation?
* How effectively does the organisation compare and contrast risks from different elements of core business (e.g. comparing a financial risk against an operational risk)?
* Is there confidence that adequate time and resource is currently given to risk management?

The management of business risk is a proactive process, enabling an organisation to obtain reasonable assurance that its business objectives can be met through the most effective deployment of controls in context with their relative priorities.

## Quality assurance and administration

The important aspect of a business risk assessment is the content. Using the template at Appendix 1 of the [Risk Assessment Guidance Document](https://practiceindex.co.uk/gp/forum/resources/risk-assessment-guidance-document.1519/), the following points are to be completed as they are considered to be the principles of good risk assessment administration:

1. Confirm risk description
2. Insert organisation name
3. Create/insert local risk assessment reference
4. Insert date risk assessment completed
5. Create/insert relevant documents reference
6. Insert risk assessor’s name and job role
7. Insert the name and job role of any contributors to the risk assessment
8. Insert manager’s name and job role
9. Insert name and job role of who reviewed the risk assessment (see risk review profile – how often the document and content must be reviewed)
10. Check content of risk assessment for relevance and general accuracy
11. Check that the additional control measures required are SMART
12. Check all of the ratings are correct and that the risk rating is a result of multiplication
13. Once the controls have been implemented, then revisit the risk assessment and calculate the residual risk
14. Complete the risk register (PLUS document)

## Audits and review

It is recommended that all safety management systems (including business risk assessments) are subject to review with a periodic audit to enable compliance and thereby provide assurance to all stakeholders.

In order to ensure that business risk assessments remain valid and controls remain effective, it is also important to supervise activities proportionally to the level of risk that they present.

Other circumstances that would prompt a systems review include, but are not limited to, a significant change of staff, changes in funding, location, equipment or process.

# Additional information

## Recommended resources

Additional sources of information are available from a variety of related organisations, including but not restricted to the following:

[The Health and Safety Executive](http://www.hse.gov.uk/)

[International Institute of Risk & Safety Management](http://www.iirsm.org/)

[IOSH (Institution of Occupational Safety & Health)](https://iosh.com/)

[Chartered Institute of Environmental Health](https://www.cieh.org/)

[Chartered Management Institute](file:///C:\Users\Brookfield\Downloads\Chartered%20Institute%20of%20Environmental%20Health)

[Financial Ombudsman](https://www.financial-ombudsman.org.uk/)

# Summary

The function of a business risk assessment is to establish its relative priority to enable risk effective management to take place. The function of risk management is to allocate resources against your priorities. There is no such thing as a perfect business risk assessment. However, any risk assessment that is considered suitable and sufficient must reflect local circumstances. Key findings must be communicated and be subject to review by using the risk review profile.

Business risk assessors and managers must understand the range of business risks that they face and their relative level (priorities), understand the resources at their disposal and then allocate those resources in a meaningful way.

# Annex A

**Business risk assessment and control form**

Brief task description: [Insert task description]

Organisation name: [Insert organisation name] Risk assessment reference: [Insert local reference number]

Date completed: [Insert date completed] Relevant documents reference: [Insert supporting document name/reference numbers]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk description**  (XYZ and/or hyperlink to risk assessment) | **Impact rating** | **Likelihood** | **Likelihood rating** | Risk rating  (Colour coded) | Additional control measures required (summary) | **To be implemented by who and by when?** | **Residual risk**  **(*Risk - after all additional controls are implemented)*** |
| (**X**) Compliance with enforcement requirements not achieved, (**Y**) due to lack of due diligence on regulatory compliance actions, (**Z**) resulting in a potential prosecution. | 5 | No progress has been made since being notified in writing 2 months ago, with practice manager now on long term sick, no interim PM has yet been appointed.  Contractor requested to quote for improvement works, lead time is 8 weeks, with Fire Service re-inspection due next month.  Currently non-compliant with RIDDOR, due to failure to report on time. | 4 | 20 | Secure services of interim PM  Communicate with Fire Service stating current circumstances against planned improvement. Progress with remedial works.  Report RIDDOR | Business manager (BM), 31.08.2020  BM, 31.08.20  BM, 21-08-20 | 10 |

**General Administration**

|  |  |  |
| --- | --- | --- |
| **Risk assessor’s name:** | **Contribution to risk assessment by:** | **Manager approval** |
| [Insert name of risk assessor] | [Insert name of any contributors] | [Insert name of manager] |
| **Risk assessor’s job role:** | **Contributor’s job role:** | **Date of approval** |
| [insert job role] | [insert job role] | [insert date] |

|  |  |  |  |
| --- | --- | --- | --- |
| **This document was reviewed/updated by:** | **Job role:** | **On date:** | **Next planned review due:** |
| [Insert name of assessor] | [insert job role] | [insert date] | [insert date] |

|  |  |
| --- | --- |
| **Risk review profile** | **Recommended risk assessment and risk controls review periodicity.**  ***Guidance Note:*** *The principle of review is that the more significant the risk level, the more often it must be reviewed.*  **Always review if an incident has occurred:** |
|  | If the risk is 15 – 25 (Very high) Review at least every 1 – 3 months |
|  | If the risk is 8 – 12 (High) Review at least every 6 – 12 months |
|  | If the risk is 4 – 6 (Moderate) Review at least every 12 – 18 months |
|  | If the risk is 1 – 3 (Low) Review at least every 18 – 24 months |

1. [Institution of Occupational Safety and Health](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjfmMmiiKzrAhUSsXEKHV-aBCAQFjABegQIARAC&url=https%3A%2F%2Fiosh.com%2F&usg=AOvVaw0c8sZfNP5lhyOZkS37kZyp) [↑](#footnote-ref-1)
2. [International Institute of Risk and Safety Management](https://www.iirsm.org/) [↑](#footnote-ref-2)
3. [Management of Health and Safety at Work Regulations 1999](https://www.legislation.gov.uk/uksi/1999/3242/contents/made) [↑](#footnote-ref-3)
4. [Health and Safety at Work etc. Act 1974](https://www.hse.gov.uk/legislation/hswa.htm) [↑](#footnote-ref-4)
5. [HSE ALARP Suite of guidance](https://www.hse.gov.uk/managing/theory/index.htm) [↑](#footnote-ref-5)
6. [SMART](http://www.managers.org.uk/) [↑](#footnote-ref-6)
7. [HSE Managing contractors](https://www.hse.gov.uk/managing/delivering/do/organising/managing-contractors.htm) [↑](#footnote-ref-7)
8. [HSE Hierarchy of controls](https://www.hse.gov.uk/risk/faq.htm#hierarchy) [↑](#footnote-ref-8)