Qualsys

Risk management workshop guide

Qualsys helps businesses comply with global regulations, such as

ISO

FDA 21 CFR Part 11

GXP QUALITY SYSTEMS

An effective management system takes more than a single software solution or achieving a certificate for the wall. It takes time, energy, commitment and investment.

Qualsys's software and solutions give businesses the tools and knowledge they need to effectively plan, monitor and improve performance.

We've worked with worldwide brands such as Sodexo, BT and Diageo, as well as hundreds of SMEs, to help them make good practice natural and invisible.

Founded in 1995, Qualsys Ltd is now one of the largest privately-owned governance, risk and compliance software providers in the UK.

Our software solutions are used every day in more than 100 countries across the globe, helping all kinds of businesses meet a wide range of standards and regulations.

CQI | IRCA

ISOQAR REGISTERED | UKAS MANAGEMENT SYSTEMS 0026

www.qualsys.co.uk

Get in touch

Mike Pound
Managing Director
+44(0) 114 282 3338
mike.pound@qualsys.co.uk

Brands we work with

YAZAKI, DIAGEO, BUNZL, Accolade Wines, NHS, Honeywell, UNIVERSITY OF LEEDS, Unilever, BT, sodexo

Welcome to your risk workshop

Chris Owen

Services Director

Risks speak for themselves. We all know the danger of risk, but not everybody addresses it properly.

For a business, unchecked risks mean incidents and accidents - which mean lost money, time and reputation.

Not identifying risks means no preventative action can be taken, which creates a reactive rather than proactive culture. And the whole cycle repeats itself.

Today's workshop will give you the insights, ideas, tools and techniques you need to get ahead of the risks your business faces.

We've built today's itinerary around not only core risk principles and standards like ISO 31000:2018, but also the experience and expertise accrued by the Qualsys team.

As a quality management system supplier for some of the world's largest businesses, we've had to embed robust risk-based thinking across our operation.

Sharing the lessons we've learnt and answering the questions we used to ask allows us to offer you the most valuable support we can.

We hope you enjoy today's session and leave feeling more confident, informed and risk-ready than when you arrived.

Agenda

The risk management workshop

Description	Time
Introduction and overview of risk and ISO 31000	9.00 - 9.45
Risk principles and risk framework	9.45 - 10.30
Coffee	10.30 - 10.45
The risk process	10.45 - 11.15
Risk context and identification	11.15 - 12.15
Lunch	12.15 - 13.00
Risk analysis and evaluation	13.00 - 13.45
Risk treatment	13.45 - 14.30
Afternoon tea	14.30 - 14.45
Risk monitoring and review	14.45 - 15.15
Cultural change	15.15 - 15.45
Round up	15.45 - 16.00

Your risk challenges

“Transitioning to ISO 9001, ISO 14001 and ISO 45001”
“Understanding which parts of the standards require risk assessment”
“Having a standard risk assessment system that everyone understands”
“Identifying risk”
“Creating a relevant risk register”
“Engaging the board with risk management”
“Effective gap analysis”
“Implementing solutions in the real world”
“Learning how others manage risk”
‘How to run an ISO-compliant management system”
“Looking at internal and external risks and how they affect the business”
“Management of assets (maintenance and repairs)”
“Communicating to all employees”

The economic uncertainty of the past few years has had a major effect on how companies operate. Companies that used to operate smoothly with the help of forecasts and projections now refrain from making business judgements that are set in stone. Now, companies have a renewed focus: to manage risk.

Risk is the main cause of uncertainty in any organisation. So companies increasingly focus more on identifying risks and managing them before they even affect the business. GRC commentator Michael Rasmussen has identified a 'perfect storm' of risk elements arriving before 2020 - so the ability to manage risk is more vital than ever to help companies act more confidently on future business decisions and make themselves more profitable and efficient.

Helping your business reach this target is the focus of today's session.

ISO 31000 Risk Management Workshop

22 March 2018

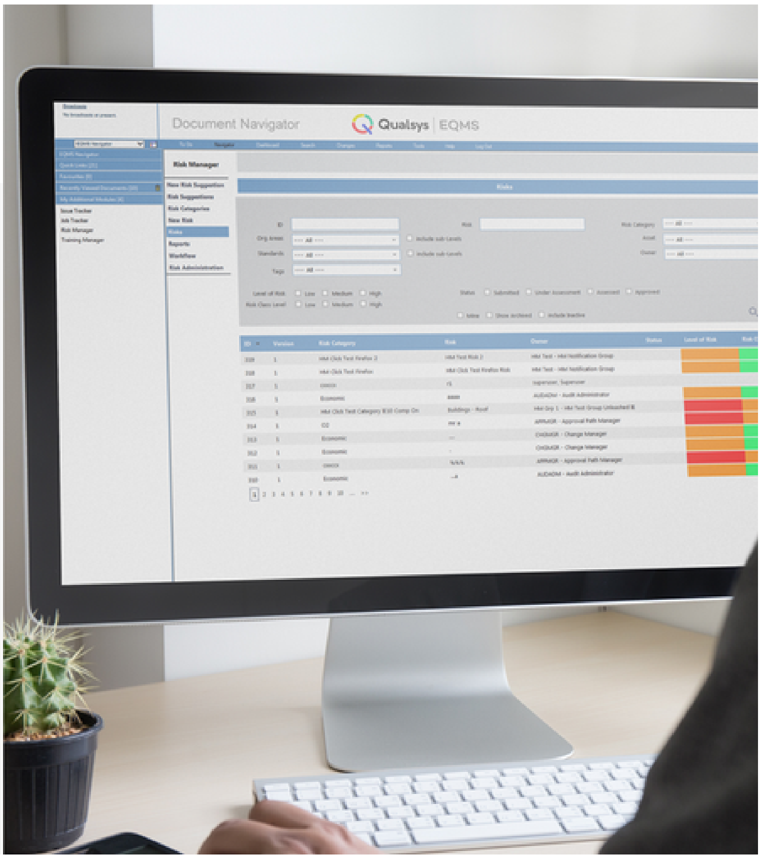
Your team today

Liam Pollard

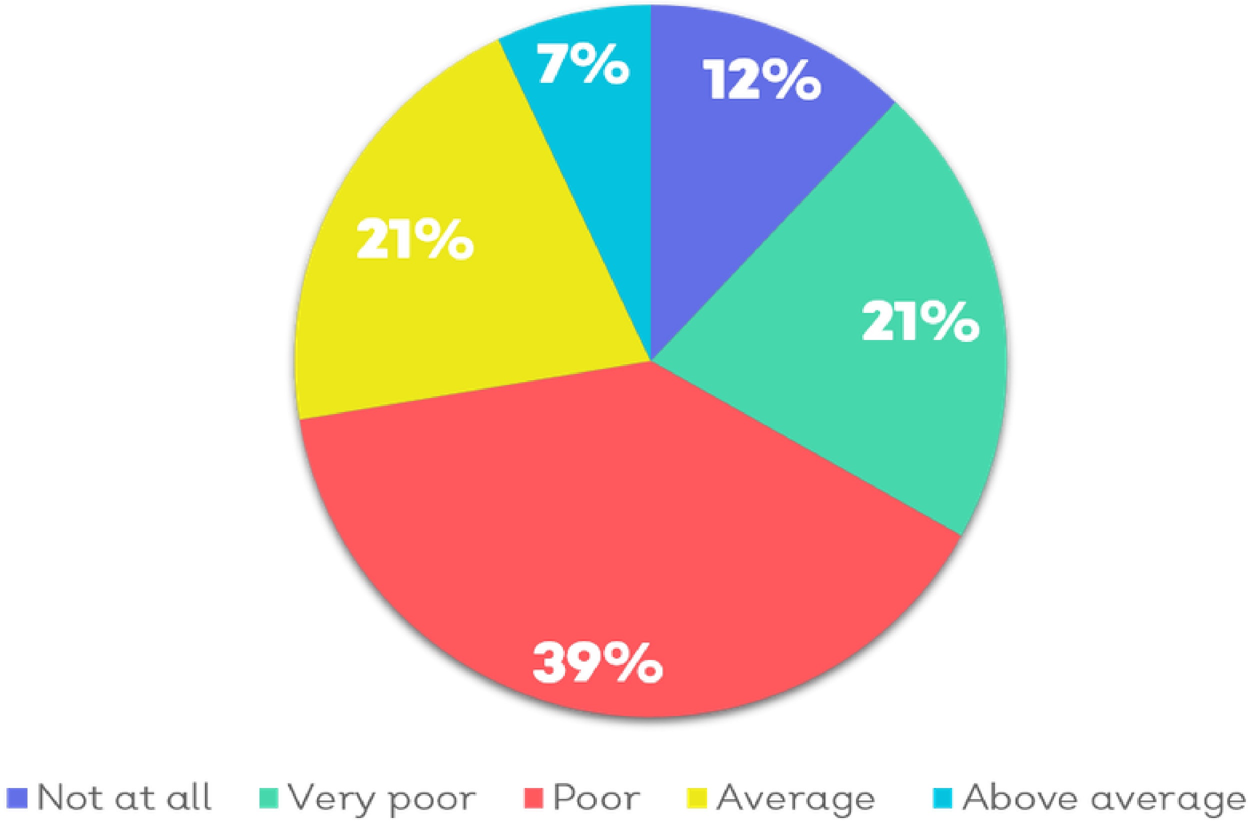
Service Implementation Manager

Chris Owen

Services Director



How effective is your business at employing ‘risk-based thinking’?



Results of Qualsys Global Quality Survey, January 2018

- 62% say their business does not proactively manage risk
- 72% say their business is not effectively employing risk-based thinking

Download the free report:

quality.eqms.co.uk/global-grc-report-2018

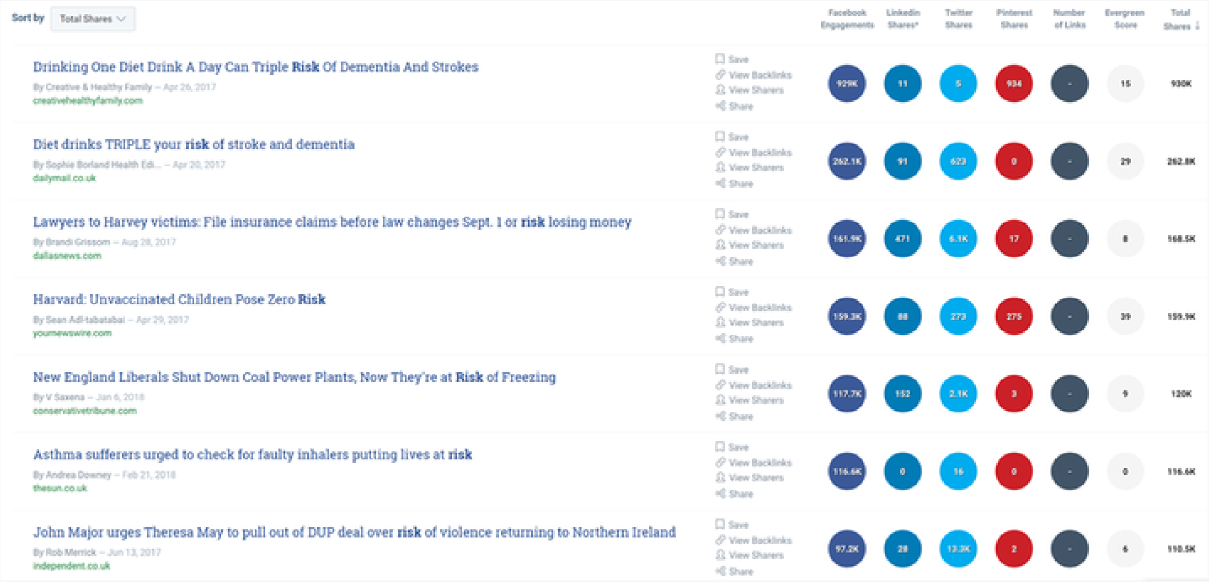
Risk and ISO 31000

Introduction and overview of risk & ISO 31000 – 9.00

- Welcome
- What is risk? Why is it important to manage risk?
- Introduction to risk-based thinking
- Overview of ISO 31000

Understanding the true scope, nature, and impact of risks may be the greatest challenge organisations face today.
- OCEG

Risk is everywhere



Sort by Total Shares

		Facebook Engagements	LinkedIn Shares*	Twitter Shares	Pinterest Shares	Number of Links	Evergreen Score	Total Shares ↓
Drinking One Diet Drink A Day Can Triple **Risk** Of Dementia And Strokes By Creative & Healthy Family – Apr 26, 2017 creativehealthyfamily.com	Save View Backlinks View Sharers Share	929K	11	5	934	-	15	930K
Diet drinks TRIPLE your **risk** of stroke and dementia By Sophie Borland Health Edi... – Apr 20, 2017 dailymail.co.uk	Save View Backlinks View Sharers Share	262.1K	91	623	0	-	29	262.8K
Lawyers to Harvey victims: File insurance claims before law changes Sept. 1 or **risk** losing money By Brandi Grissom – Aug 28, 2017 dallasnews.com	Save View Backlinks View Sharers Share	161.9K	471	6.1K	17	-	8	168.5K
Harvard: Unvaccinated Children Pose Zero **Risk** By Sean Adl-tabatabai – Apr 29, 2017 yournewswire.com	Save View Backlinks View Sharers Share	159.3K	88	273	275	-	39	159.9K
New England Liberals Shut Down Coal Power Plants, Now They're at **Risk** of Freezing By V Saxena – Jan 6, 2018 conservativetribune.com	Save View Backlinks View Sharers Share	117.7K	152	2.1K	3	-	9	120K
Asthma sufferers urged to check for faulty inhalers putting lives at **risk** By Andrea Downey – Feb 21, 2018 thesun.co.uk	Save View Backlinks View Sharers Share	116.6K	0	16	0	-	0	116.6K
John Major urges Theresa May to pull out of DUP deal over **risk** of violence returning to Northern Ireland By Rob Merrick – Jun 13, 2017 independent.co.uk	Save View Backlinks View Sharers Share	97.2K	28	13.3K	2	-	6	110.5K

- Most shared articles on risk [Buzzsumo]

What is risk and why is it important?

Qualsys

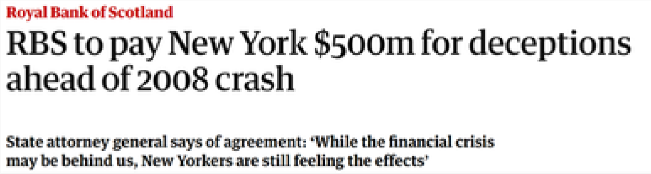
- Risk is *uncertainty*
- Risk can be both positive and negative
- Risk management involves understanding, analysing, and addressing risk
- Risk management must be proportionate to the complexity and type of organisation

requirements
QMS
GDPR
new
ISO
business
quality
security
Security
standards
systems
change
control
process
Risk
data
time
clientsrisk
customer
Transition
certification
system
standard
transition
commitment
documentation
implement
consulting
Keeping
growth
company
training
document
Audit
Data
audit
supplier

12,000+ GRC professionals answer: What is your main business challenge?

Cost of poor risk management

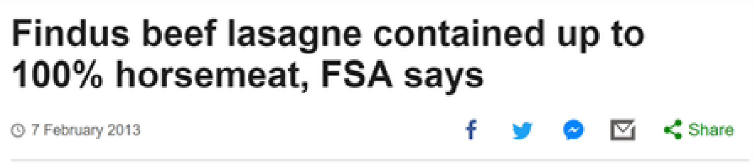
Qualsys



Royal Bank of Scotland

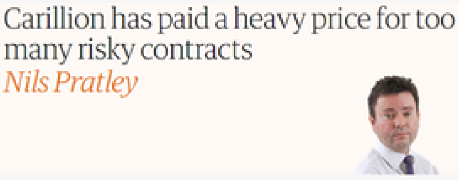
RBS to pay New York $500m for deceptions ahead of 2008 crash

State attorney general says of agreement: 'While the financial crisis may be behind us, New Yorkers are still feeling the effects'



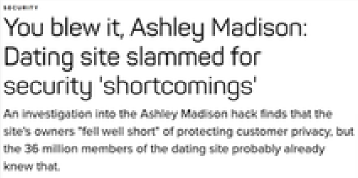
Findus beef lasagne contained up to 100% horsemeat, FSA says

7 February 2013



Carillion has paid a heavy price for too many risky contracts

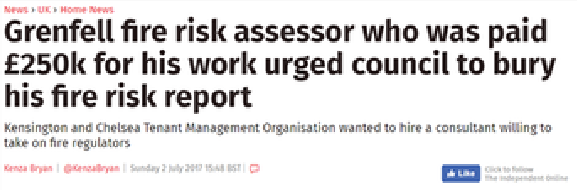
Nils Pratley



SECURITY

You blew it, Ashley Madison: Dating site slammed for security 'shortcomings'

An investigation into the Ashley Madison hack finds that the site's owners "fell well short" of protecting customer privacy, but the 36 million members of the dating site probably already knew that.

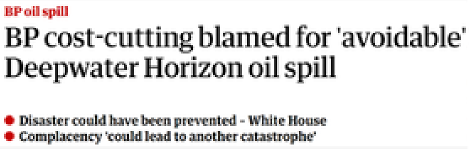


News › UK › Home News

Grenfell fire risk assessor who was paid £250k for his work urged council to bury his fire risk report

Kensington and Chelsea Tenant Management Organisation wanted to hire a consultant willing to take on fire regulators

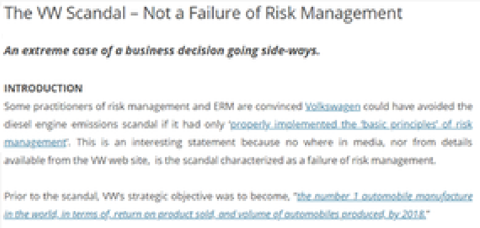
Kenza Bryan | @KenzaBryan | Sunday 2 July 2017 15:48 BST |



BP oil spill

BP cost-cutting blamed for 'avoidable' Deepwater Horizon oil spill

- Disaster could have been prevented - White House
- Complacency 'could lead to another catastrophe'



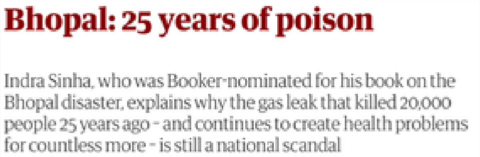
The VW Scandal – Not a Failure of Risk Management

An extreme case of a business decision going side-ways.

INTRODUCTION

Some practitioners of risk management and ERM are convinced Volkswagen could have avoided the diesel engine emissions scandal if it had only 'properly implemented the 'basic principles' of risk management'. This is an interesting statement because no where in media, nor from details available from the VW web site, is the scandal characterized as a failure of risk management.

Prior to the scandal, VW's strategic objective was to become, "*the number 1 automobile manufacture in the world, in terms of, return on product sold, and volume of automobiles produced, by 2018.*"



Bhopal: 25 years of poison

Indra Sinha, who was Booker-nominated for his book on the Bhopal disaster, explains why the gas leak that killed 20,000 people 25 years ago – and continues to create health problems for countless more – is still a national scandal

Breakout session

Take three minutes to consider:

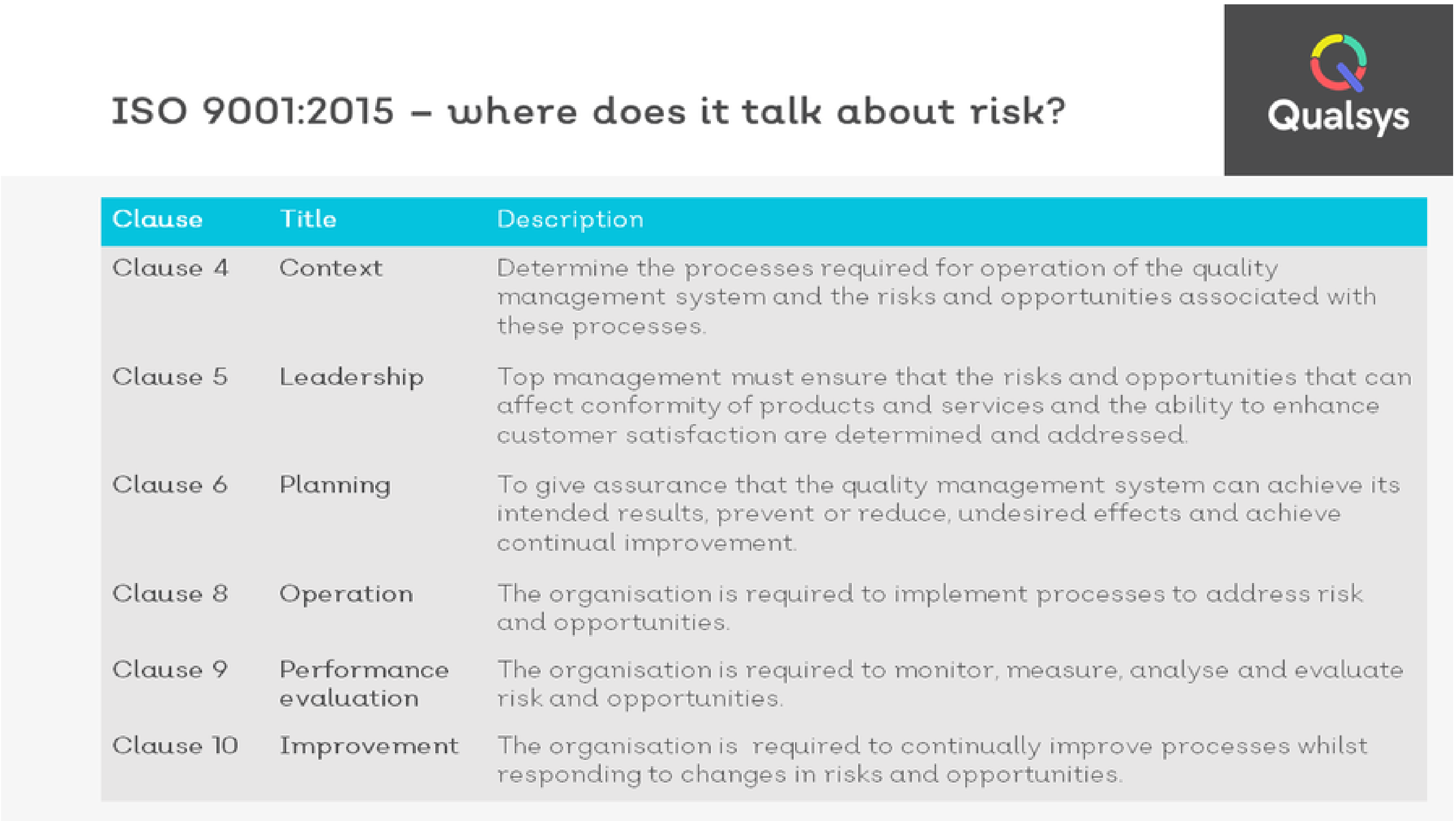
Why should businesses implement a risk management system?

What are the three biggest risks your business faces?

What has happened recently in the media that might also affect your business?

Who currently manages your business risks?

ISO 31000 definition of risk: ‘the effect of uncertainty on objectives’



ISO 9001:2015 – where does it talk about risk?

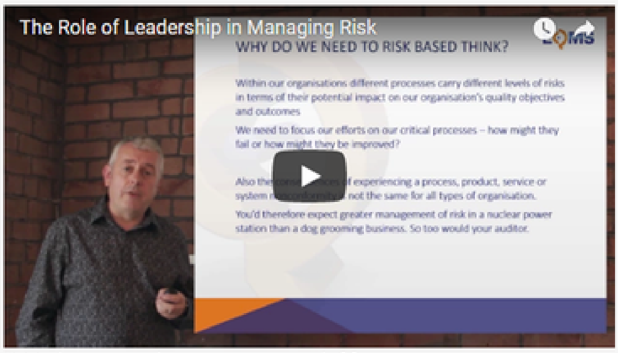
Clause	Title	Description
Clause 4	Context	Determine the processes required for operation of the quality management system and the risks and opportunities associated with these processes.
Clause 5	Leadership	Top management must ensure that the risks and opportunities that can affect conformity of products and services and the ability to enhance customer satisfaction are determined and addressed.
Clause 6	Planning	To give assurance that the quality management system can achieve its intended results, prevent or reduce, undesired effects and achieve continual improvement.
Clause 8	Operation	The organisation is required to implement processes to address risk and opportunities.
Clause 9	Performance evaluation	The organisation is required to monitor, measure, analyse and evaluate risk and opportunities.
Clause 10	Improvement	The organisation is required to continually improve processes whilst responding to changes in risks and opportunities.

Risk-based thinking: Determine, consider and where necessary take action to address any risks and opportunities that impact your organisation's ability to deliver it's intended results.

What is risk-based thinking?

1. **Determining the risks** and opportunities
2. **Planning actions** to address them
3. **Implementing them** in a **quality management system**
4. **Evaluating** their effectiveness

Risk-based thinking



The Role of Leadership in Managing Risk

WHY DO WE NEED TO RISK BASED THINK?

Within our organisations different processes carry different levels of risks in terms of their potential impact on our organisation's quality objectives and outcomes

We need to focus our efforts on our critical processes – how might they fail or how might they be improved?

Also the consequences of experiencing a process, product, service or system nonconformity is not the same for all types of organisation.

You'd therefore expect greater management of risk in a nuclear power station than a dog grooming business. So too would your auditor.

"Within our businesses, different processes carry different levels of risks in terms of their potential impact on our organisation's quality objectives and outcomes. We need to focus our efforts on our critical processes – how might they fail or how might they be improved."

Watch video: http://quality.eqms.co.uk/blog/leadership-and-risk-iso-90012015-requirements

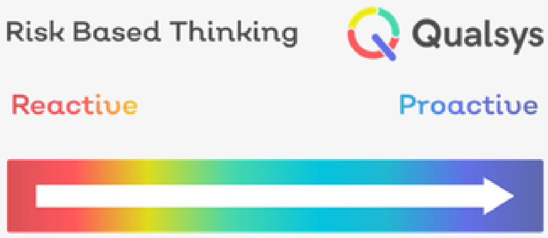
1. Annex SL brought a systematic approach to the management of risk
2. Plan, do, check, act
3. Risk based thinking now explicit requirement

References to 'preventative action' have disappeared. The core concept of identifying and addressing potential mistakes before they happen very much remains.

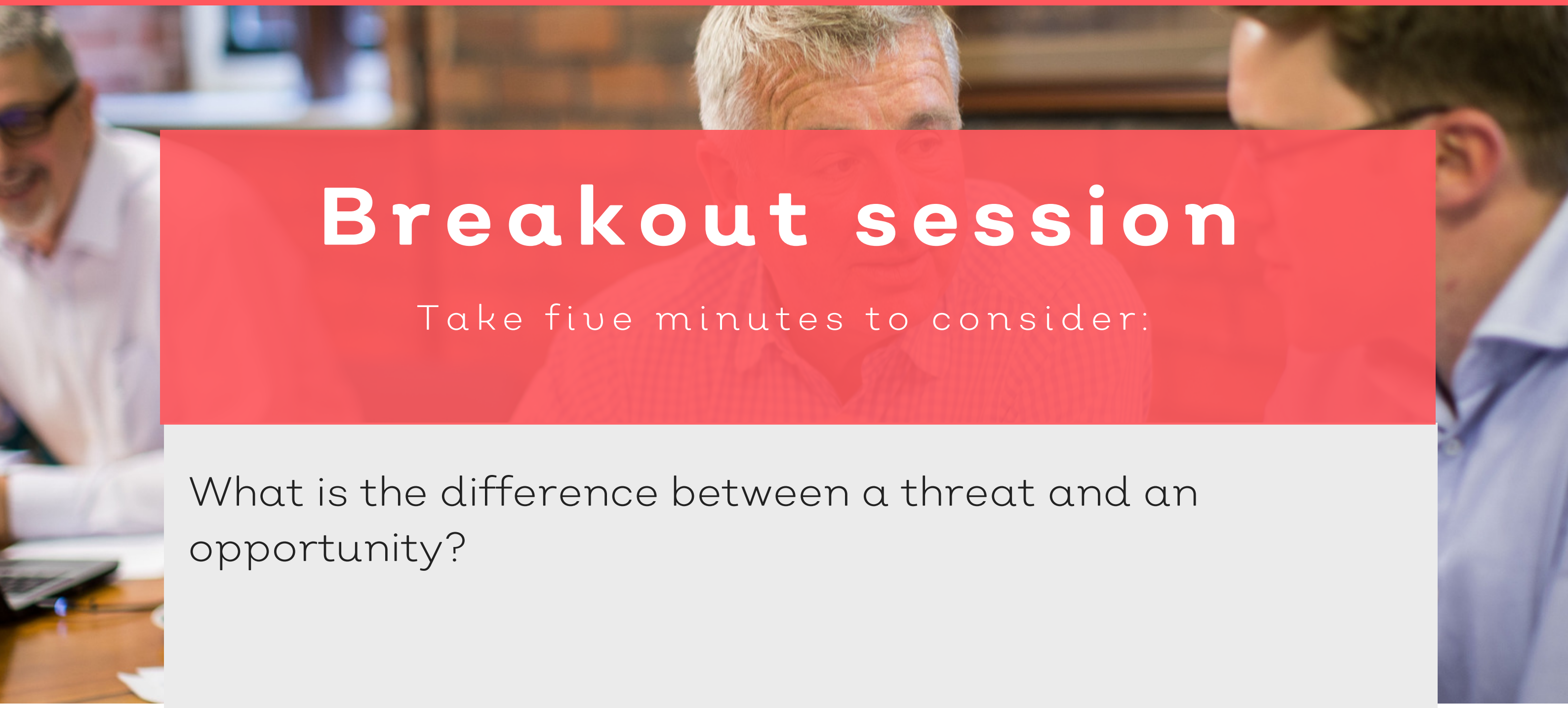
The risk-based approach to ISO standards

Risk-based thinking:

- Improves governance
- Establishes a proactive culture of improvement
- Assists with statutory and regulatory compliance
- Assures consistency of quality of products and services
- Improves customer confidence and satisfaction



Notes



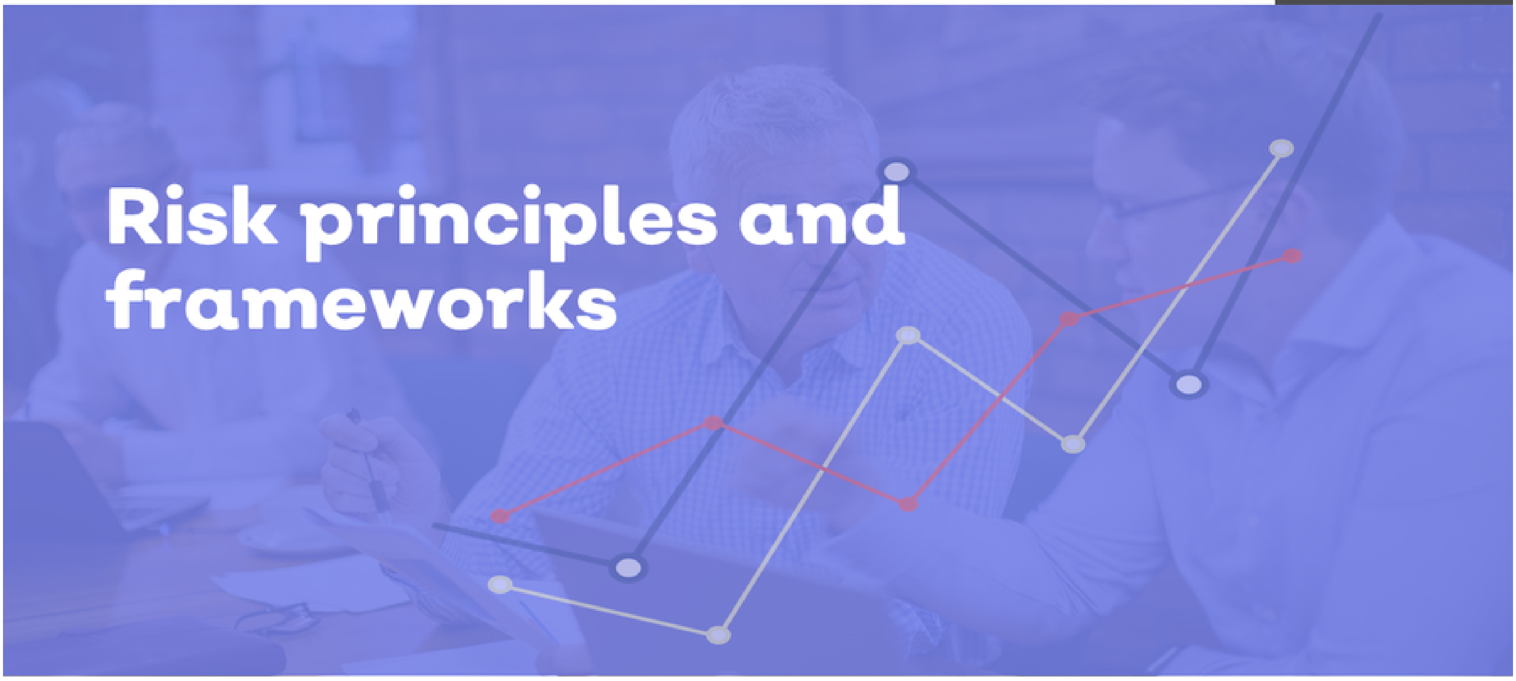
Breakout session

Take five minutes to consider:

What is the difference between a threat and an opportunity?

What would be an example of an opportunity as opposed to a threat?

How do you think opportunities should be managed?

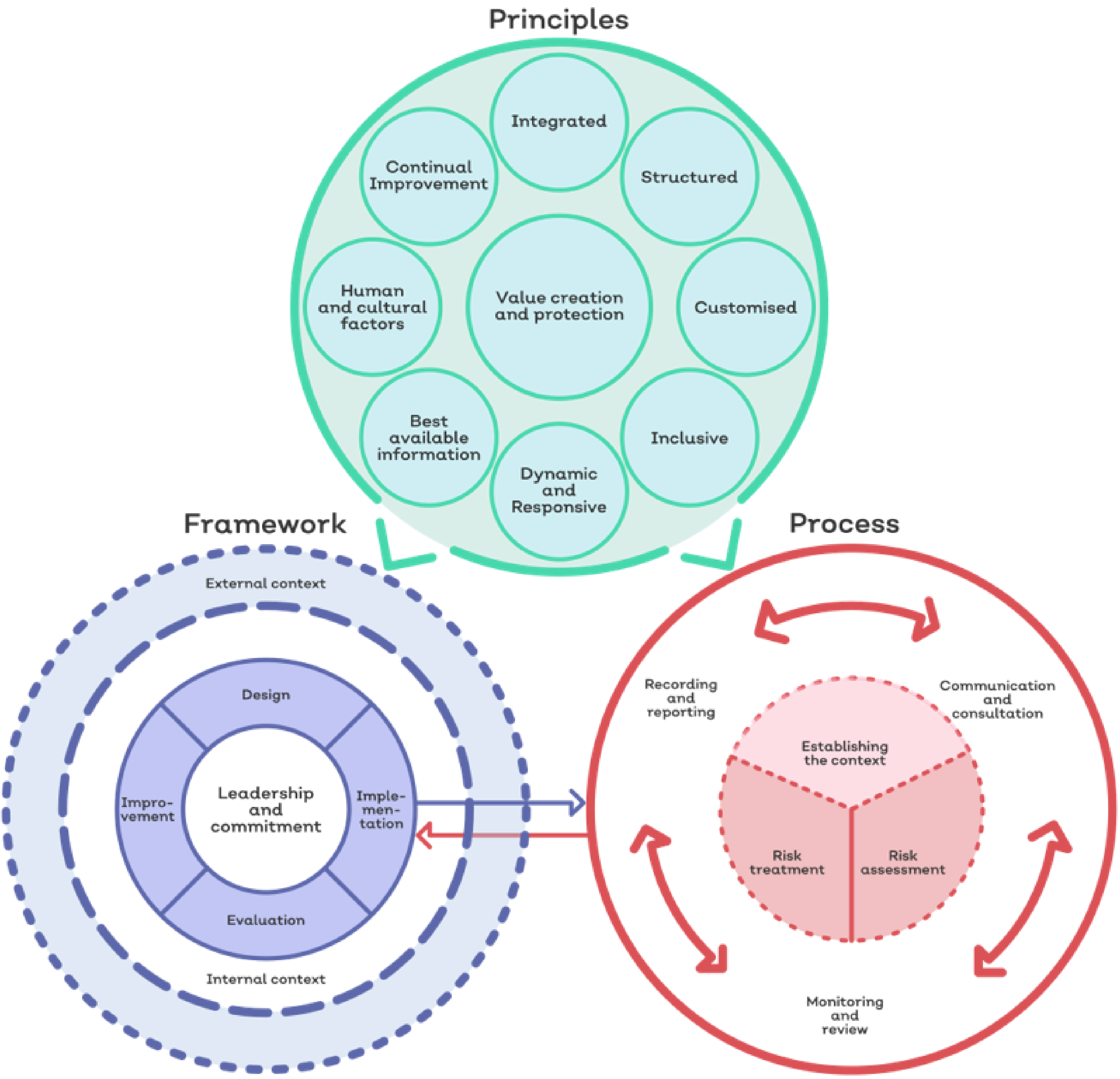


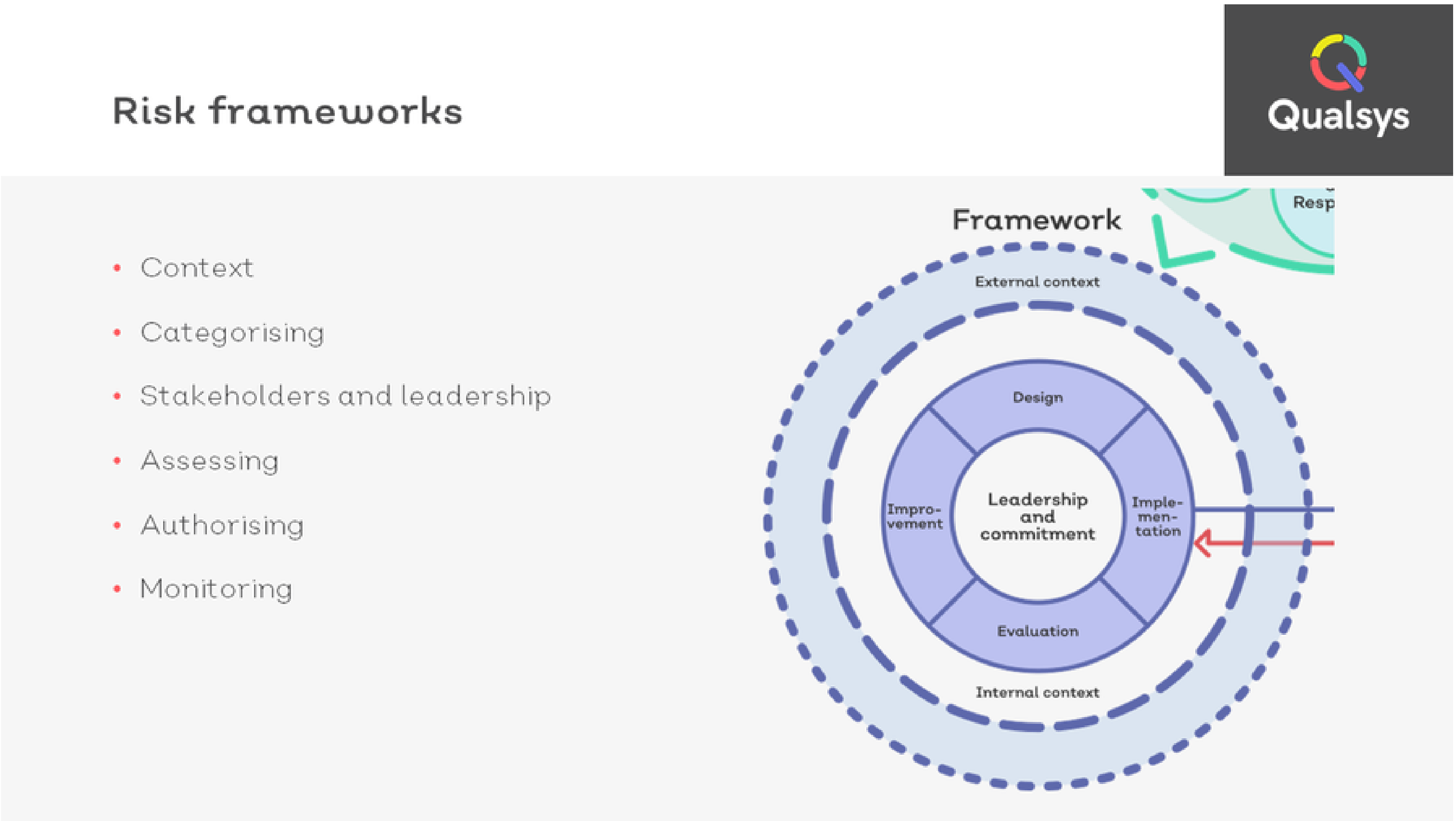
Risk principles and frameworks

Risk principles and frameworks – 9.45

- Risk principles
- Risk frameworks
- Risk management framework examples
- Risk assessment process
- Risk management principles

- Establishing the context
- Risk assessment
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment
- Monitoring and review
- Communication and consultation





Risk frameworks

- Context
- Categorising
- Stakeholders and leadership
- Assessing
- Authorising
- Monitoring

Breakout session

Take two minutes to list:

Three examples of internal quality risks

1.
2.
3.

Three examples of external risks

1.
2.
3.

Notes

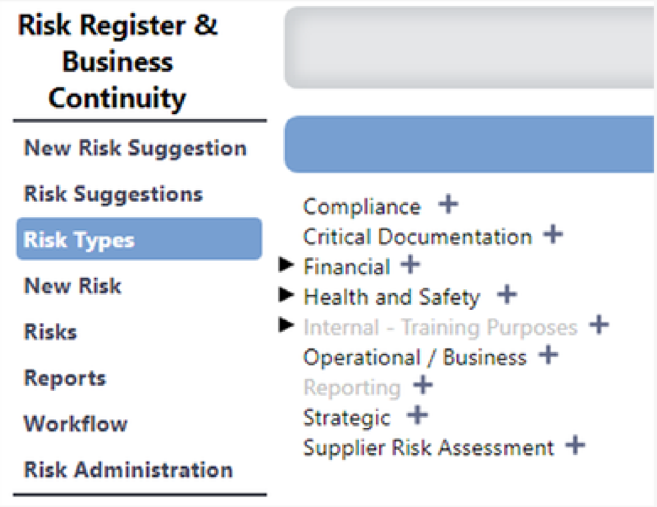
Risk examples

Internal risks

- Stability
- Organisational structure
- Politics and mismanagement
- Resources
- Innovation
- Incentives

External risks:

- Economy
- Political-legal factors
- Socio-cultural factors
- Technology
- Shareholders



Hint!

Organise your risk categories into business areas and request risk suggestions in the same area to engage your entire business.

Risk stakeholders

- Understanding – Risk Stakeholders should strive to understand the risks which are being discussed.
- Informing – Risk Stakeholders may be required to provide specialist information to an organisation.
- Identifying – Risk stakeholders may help to identify risk.
- Providing – Some stakeholders may be expected to provide the necessary resources for the chosen action plan.
- Training – If an action plan requires education of staff or customers, someone must carry out the training.
- Communicating – Information may need to be widely spread as part of the risk management process.

External	Internal
Government Authorities Regulators Customers Trade bodies Emergency services Staff dependents Competitors Suppliers Business owners Bank Business partners Contractors	Contractors Business partners Staff • Management • Quality / Compliance • Health and safety • Risk management teams • Business development • Marketing • HR • Finance • Purchasing • Facilities and estates • Manufacturing • Procurement

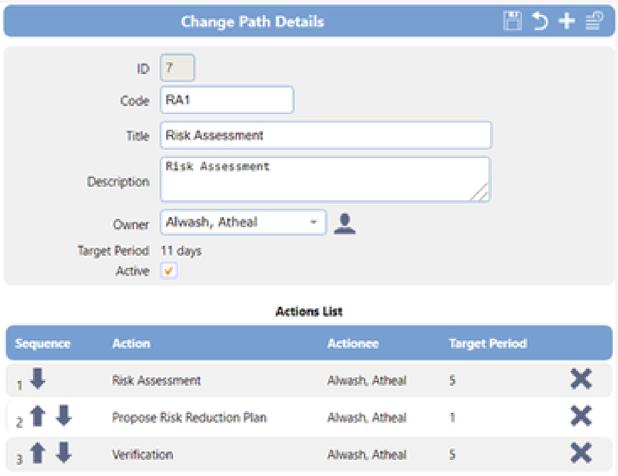
Leadership

ISO 9001 prescribes two key responsibilities:

1. General oversight, such as:
   - Determine the risk appetite
   - Ensuring the effectiveness of the quality management system
   - Ensuring the intended results are achieved
   - Mindful of external and internal threats that could prevent them from delivering the intended results
   - Mindful of opportunities which will facilitate the realisation of the intended results.

2. Promote risk based thinking, such as:
   - Explicitly promote risk based thinking in respect of their quality management system
   - Evidence support of a risk based approach

Leadership responsibilities



Change Path Details

ID	7
Code	RA1
Title	Risk Assessment
Description	Risk Assessment
Owner	Alwash, Atheal
Target Period	11 days
Active	☑

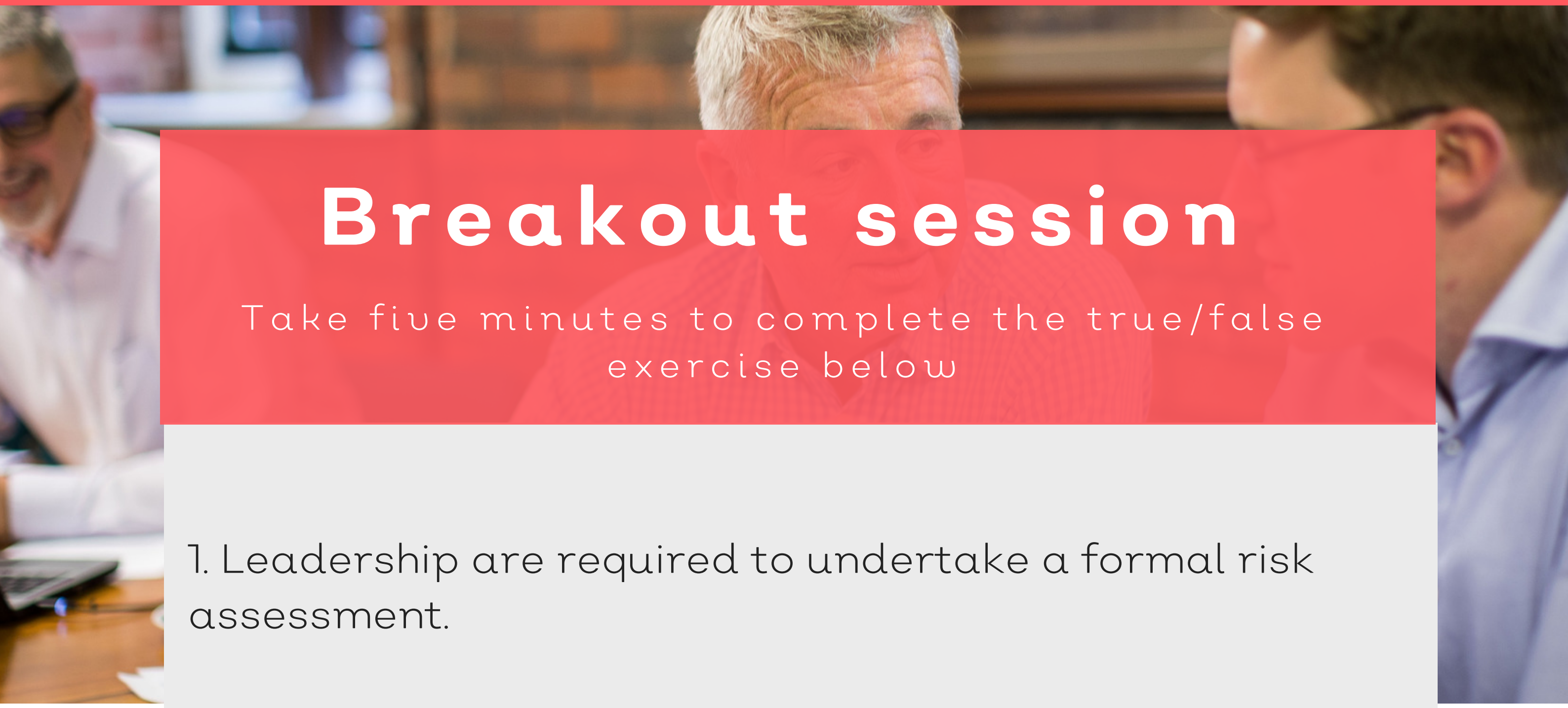
Actions List

Sequence	Action	Actionee	Target Period	
1 ↓	Risk Assessment	Alwash, Atheal	5	✕
2 ↑ ↓	Propose Risk Reduction Plan	Alwash, Atheal	1	✕
3 ↑ ↓	Verification	Alwash, Atheal	5	✕

Hint!

Make it easy for your top management team to knowexactly what you need and by what date using workflows with checklists.

- Developing policies and procedures around risk that are consistent with the organisation's strategy and risk appetite.
- Following up on management's implementation of risk management policies and procedures.
- Following up to be assured that risk management policies and procedures function as they are intended.
- Taking steps to foster risk awareness.
- Encourage a culture of risk adjusting awareness.
- Annual formal review of risk management systems



Breakout session

Take five minutes to complete the true/false exercise below

1. Leadership are required to undertake a formal risk assessment.

2. Leadership must determine the risk appetite.

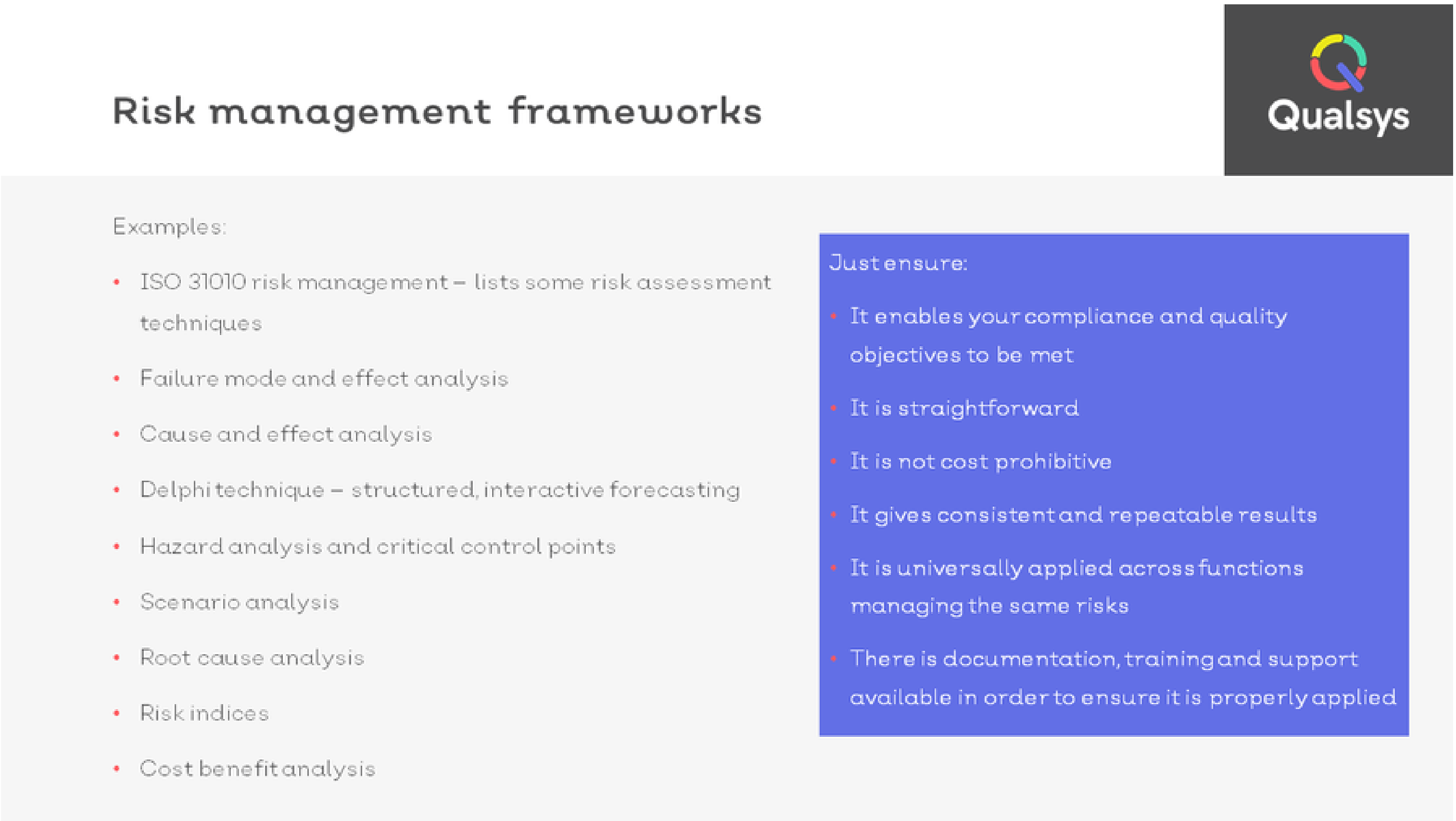
3. Leadership must be mindful of opportunities which will help the business.

4. Leadership can delegate their risk management responsibilities to a well-trained management representative.

5. Leadership can demonstrate commitment to managing risk by investing in risk management systems which are available for the entire business.

6. Leadership must promote risk-based thinking.

7. Leadership must determine the review and reporting requirements of the accountable individuals involved in delivering and monitoring risk processes.



Risk management frameworks

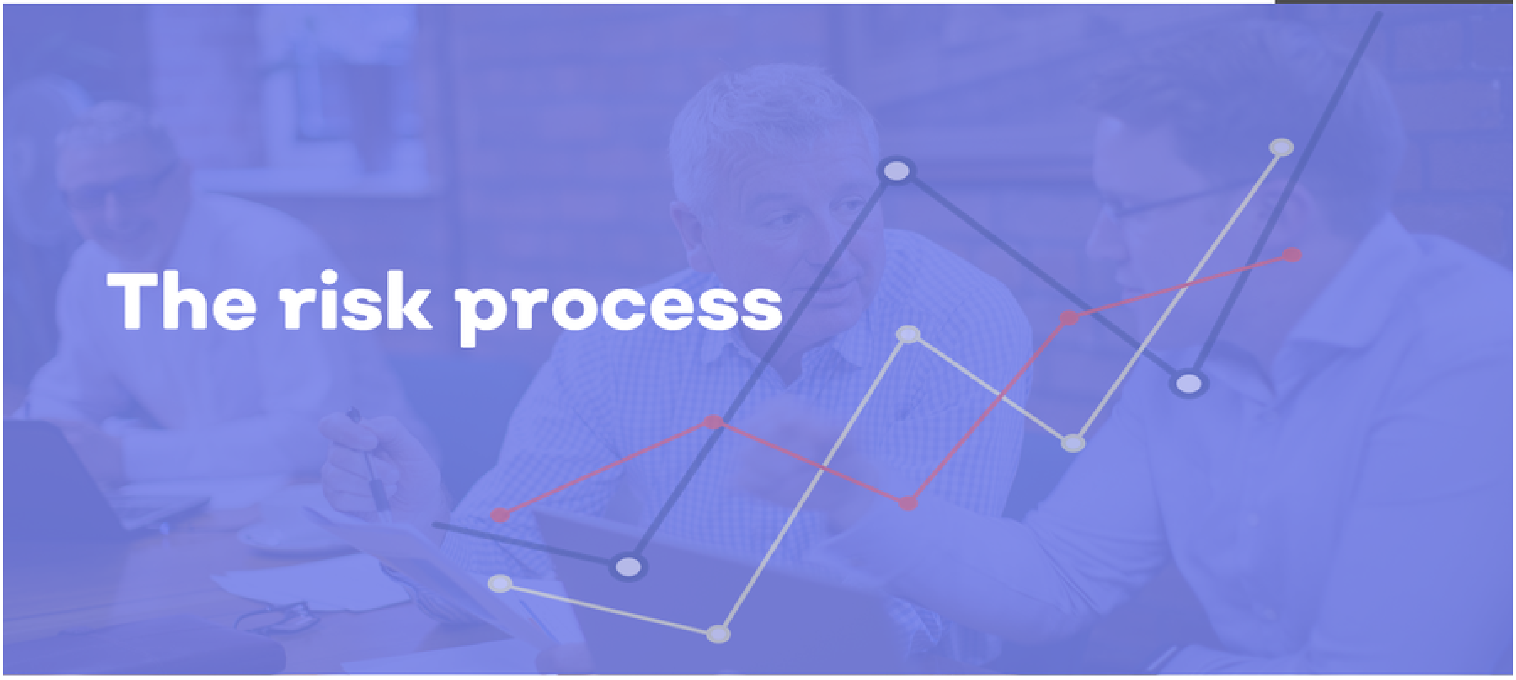
Examples:

- ISO 31010 risk management – lists some risk assessment techniques
- Failure mode and effect analysis
- Cause and effect analysis
- Delphi technique – structured, interactive forecasting
- Hazard analysis and critical control points
- Scenario analysis
- Root cause analysis
- Risk indices
- Cost benefit analysis

Just ensure:

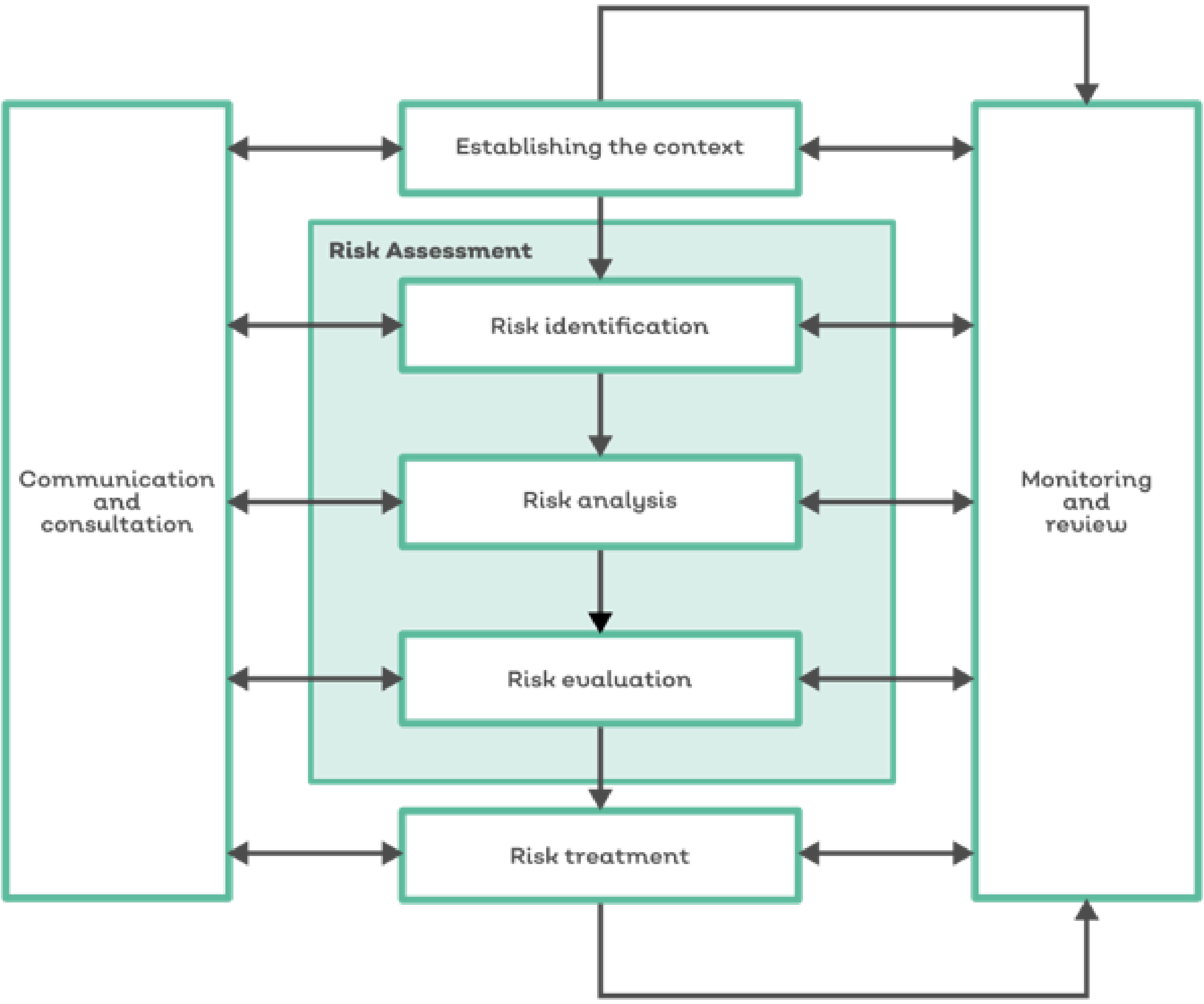
- It enables your compliance and quality objectives to be met
- It is straightforward
- It is not cost prohibitive
- It gives consistent and repeatable results
- It is universally applied across functions managing the same risks
- There is documentation, training and support available in order to ensure it is properly applied

Notes



The risk process

- Establishing the context
- Risk assessment
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment
- Monitoring and review
- Communication and consultation



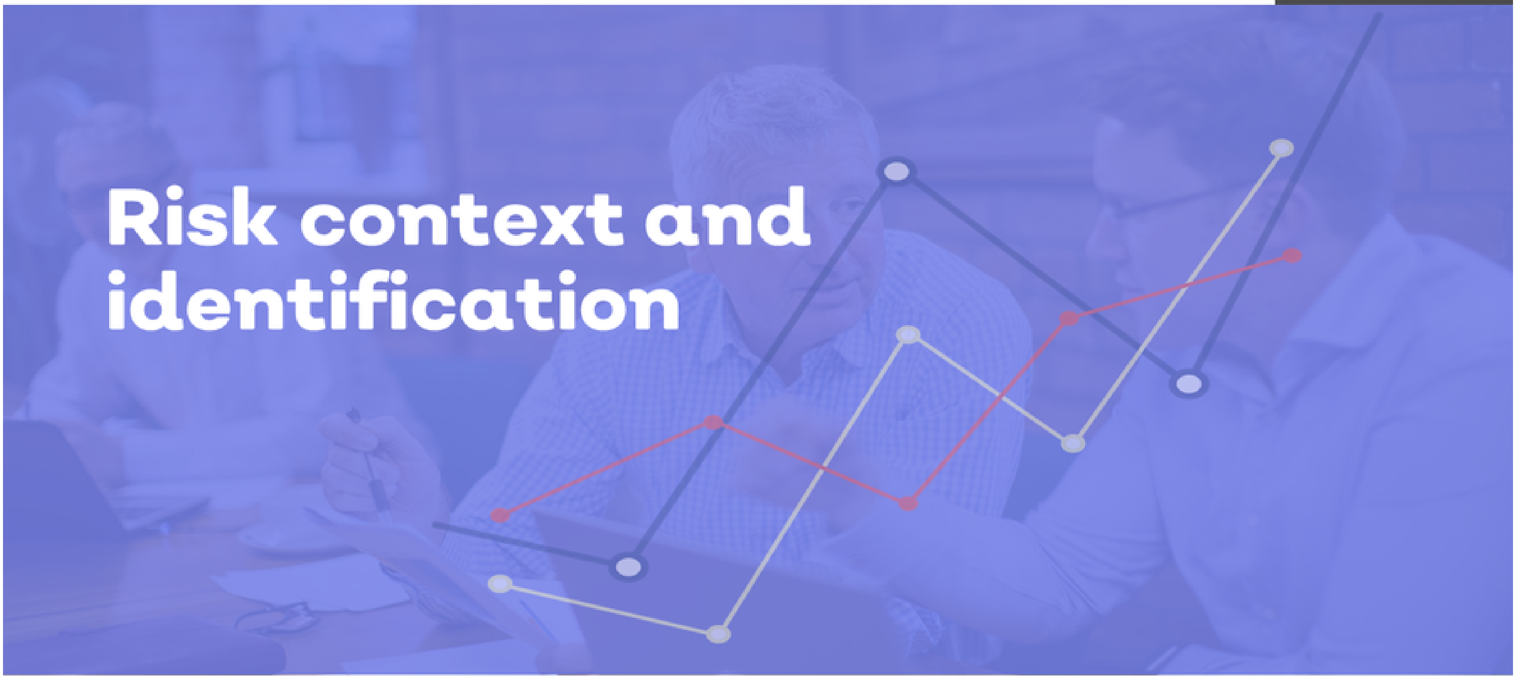
ISO 27001, GDPR

- Risk-based approach
- Privacy by design – GDPR
- Privacy impact assessment

GDPR workshop next month:

https://qualsys.co.uk/knowledge-centre/training/gdpr-training-course/

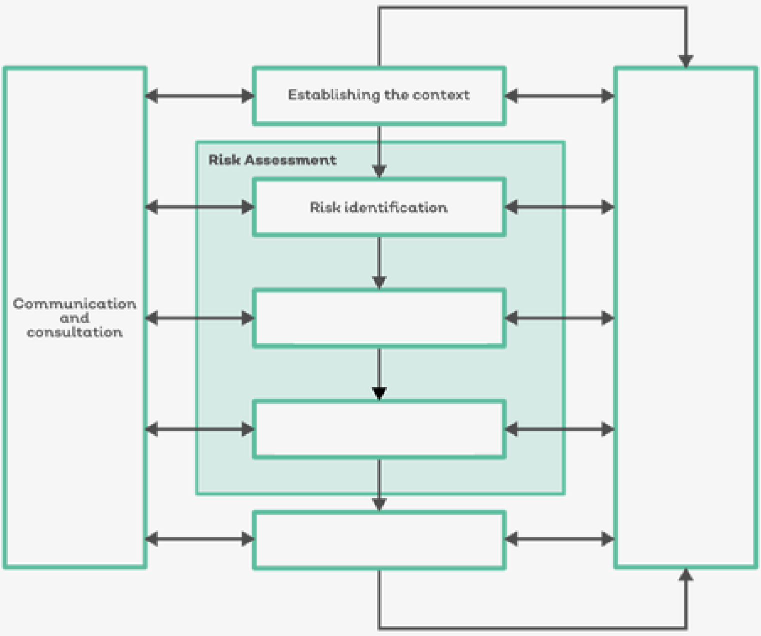
Notes



Risk context and identification

Risk context and identification – 11.15

- Risk context
- Organisational risk appetite
- Leadership
- Identification strategies

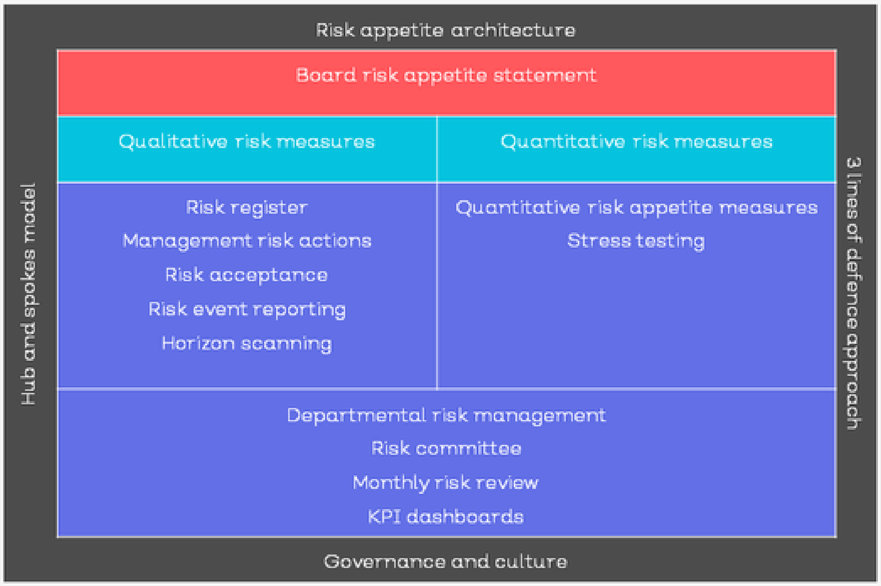


Risk context:
“Define the external and internal parameters that your organisation must consider when you manage risk.”

Risk context

The context should consider:

- Time, location, specific inclusions/exclusions
- Business objectives and activities
- Resources, including accountability and responsibilities
- Records, including where they are kept and a standard reporting process



Risk appetite architecture

Board risk appetite statement

Qualitative risk measures	Quantitative risk measures
Risk register Management risk actions Risk acceptance Risk event reporting Horizon scanning	Quantitative risk appetite measures Stress testing

Departmental risk management
Risk committee
Monthly risk review
KPI dashboards

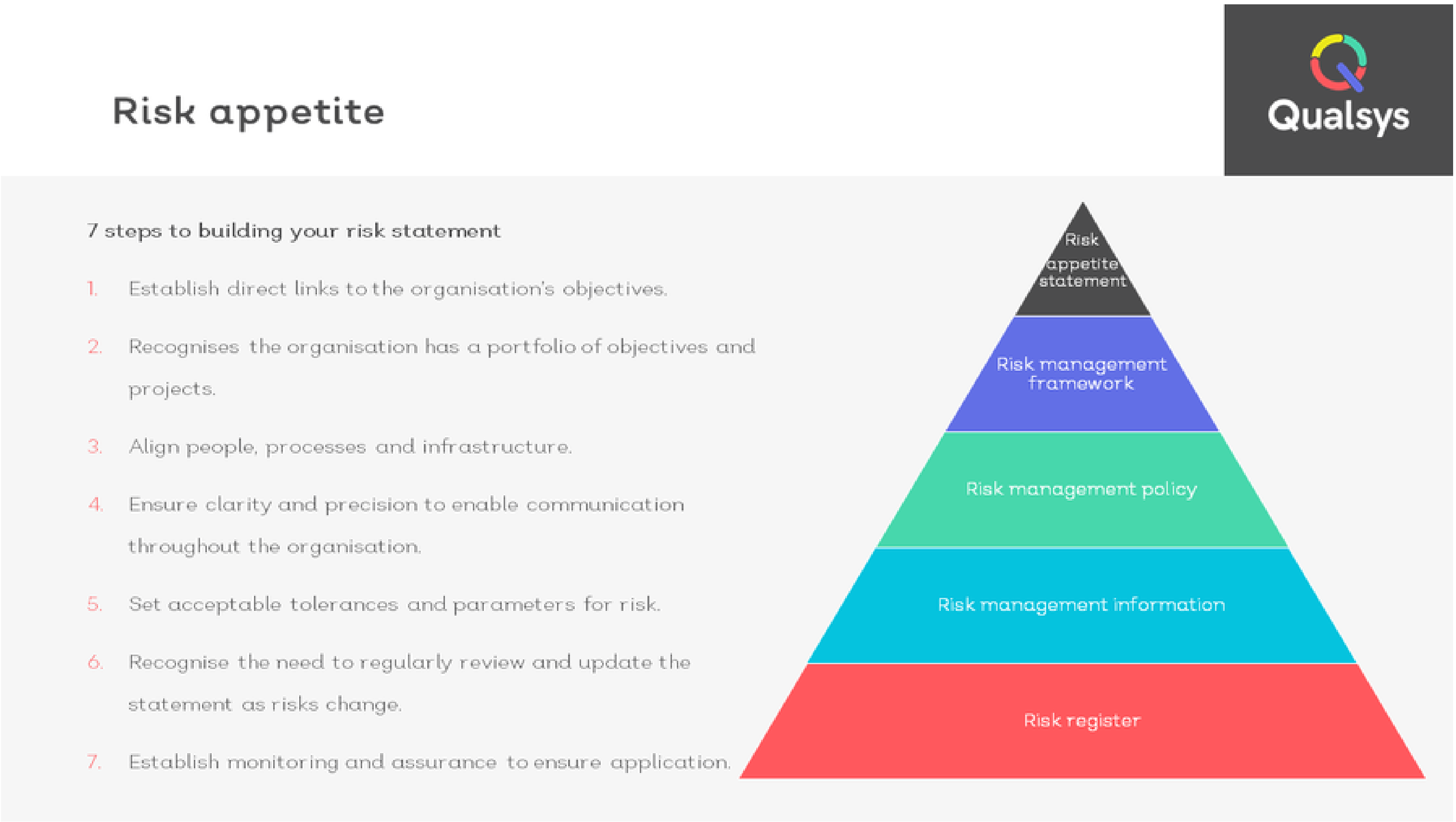
Governance and culture

Hub and spokes model

3 lines of defence approach

3 lines of defence: http://quality.eqms.co.uk/blog/defending-from-the-front-how-to-adopt-the-three-lines-of-defence

Risk appetite:
“The amount and type of risk that an organisation is willing to take in order to meet their strategic objectives.”

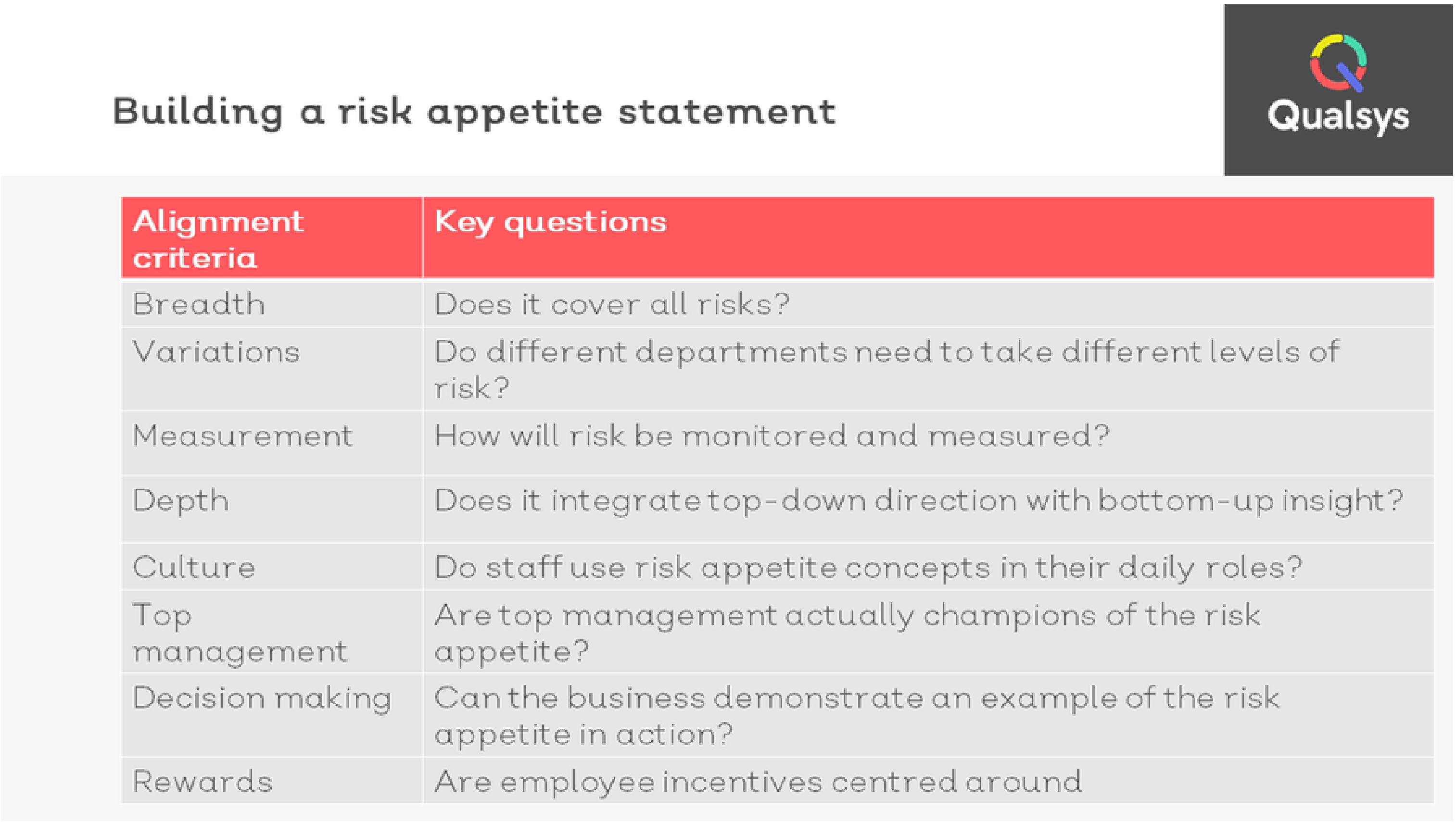


Risk appetite

Qualsys

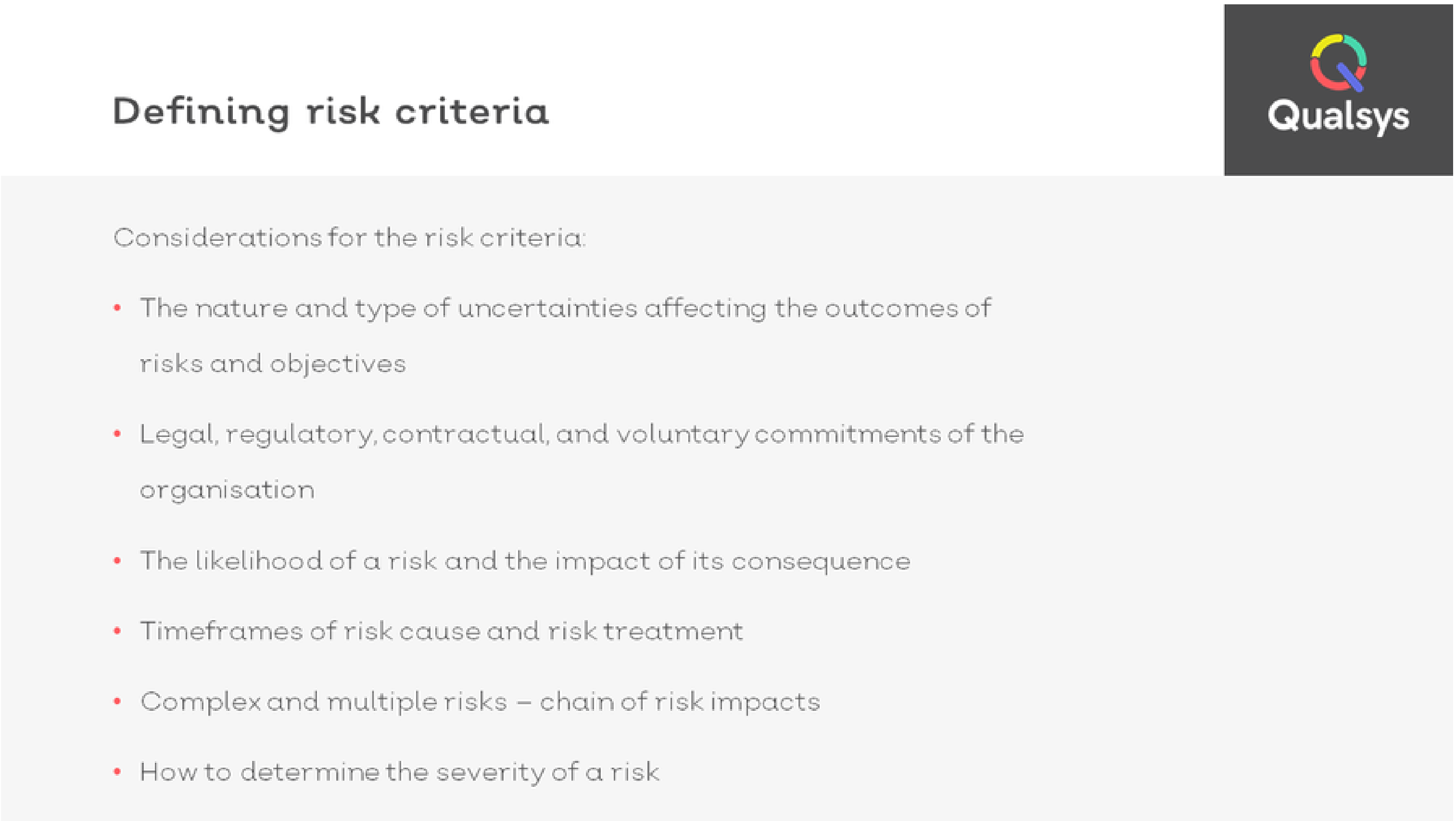
7 steps to building your risk statement

1. Establish direct links to the organisation’s objectives.
2. Recognises the organisation has a portfolio of objectives and projects.
3. Align people, processes and infrastructure.
4. Ensure clarity and precision to enable communication throughout the organisation.
5. Set acceptable tolerances and parameters for risk.
6. Recognise the need to regularly review and update the statement as risks change.
7. Establish monitoring and assurance to ensure application.



Building a risk appetite statement

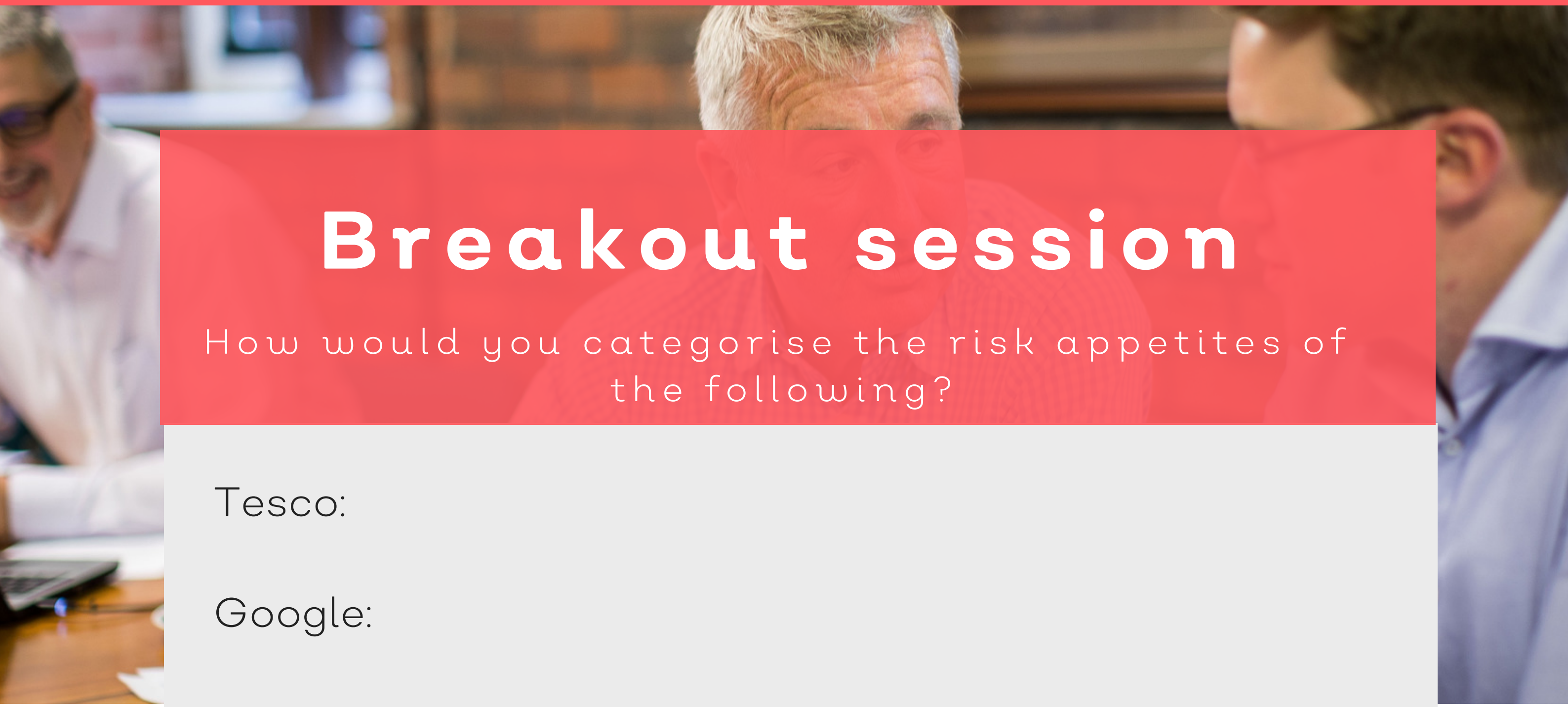
Alignment criteria	Key questions
Breadth	Does it cover all risks?
Variations	Do different departments need to take different levels of risk?
Measurement	How will risk be monitored and measured?
Depth	Does it integrate top-down direction with bottom-up insight?
Culture	Do staff use risk appetite concepts in their daily roles?
Top management	Are top management actually champions of the risk appetite?
Decision making	Can the business demonstrate an example of the risk appetite in action?
Rewards	Are employee incentives centred around



Defining risk criteria

Considerations for the risk criteria:

- The nature and type of uncertainties affecting the outcomes of risks and objectives
- Legal, regulatory, contractual, and voluntary commitments of the organisation
- The likelihood of a risk and the impact of its consequence
- Timeframes of risk cause and risk treatment
- Complex and multiple risks – chain of risk impacts
- How to determine the severity of a risk



Breakout session

How would you categorise the risk appetites of the following?

Tesco:

Google:

Hairdressing Salon:

RBS:

The Sun:

Averse

Avoidance of risk is a key business objective

Cautious

Preference for ultra-safe options: low risk, limited potential for reward

Neutral

Preference for safe options: low degree of risk and may only have a limited potential reward.

Open

Willing to consider all potential options and choose the one most likely to result in successful delivery while also providing an acceptable level of reward and value for money.

Hungry

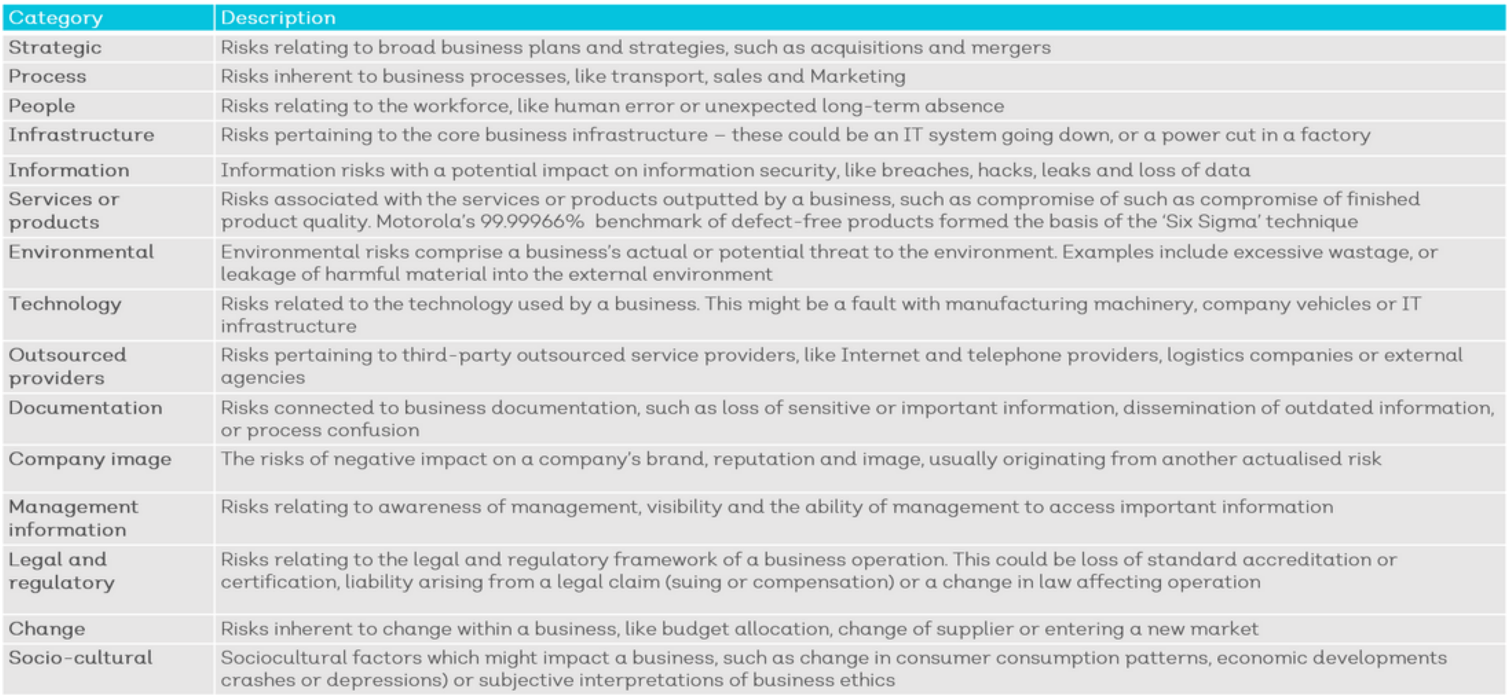
Eager to be innovative and to choose options offering potentially higher business rewards despite greater inherent risk.

Risk identification

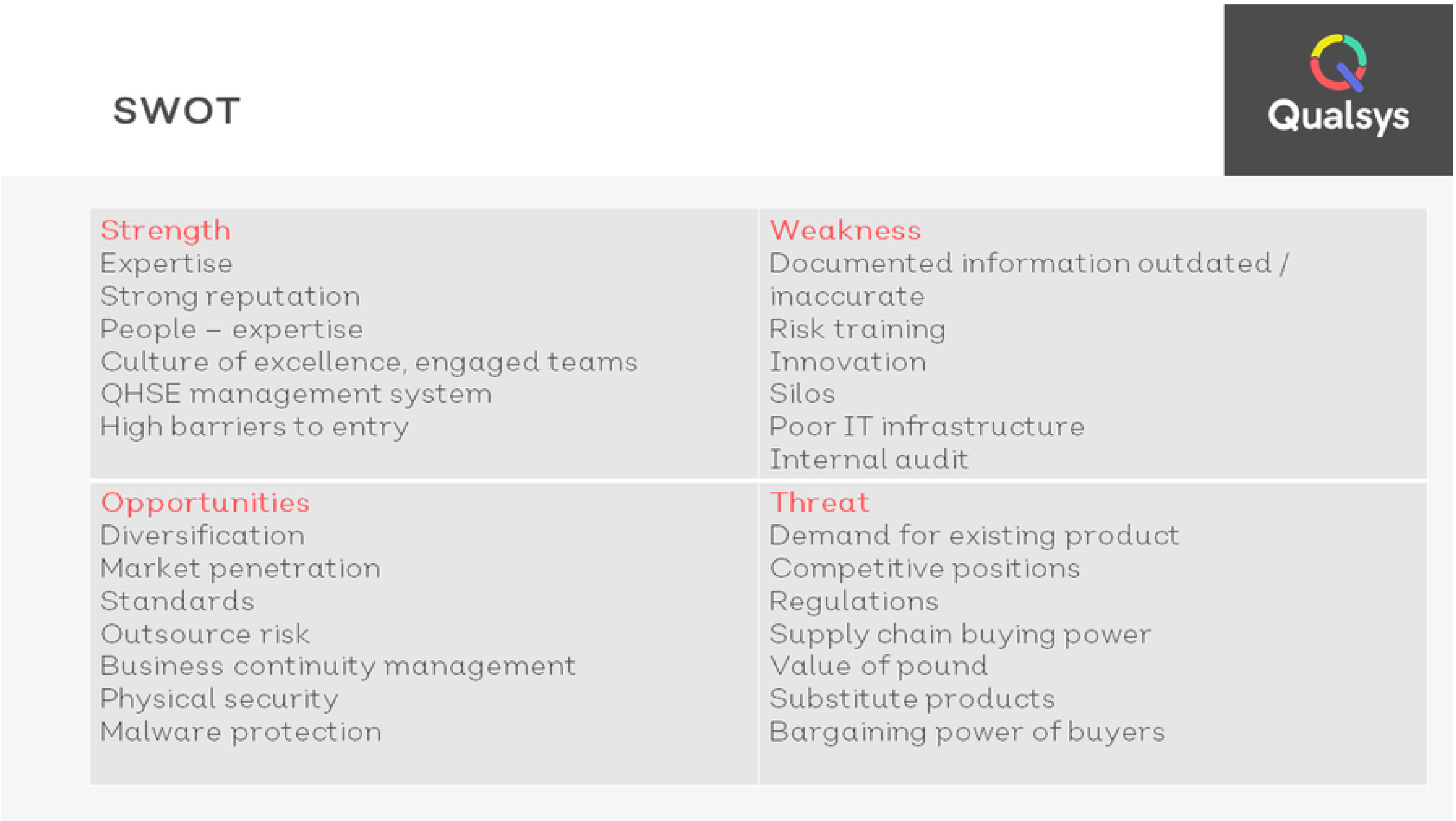
Example risk identification techniques

Qualsys

- Review lessons
- Brainstorming (SWOT)
- Risk committee
- Risk prompts list
- Risk breakdown structure



Category	Description
Strategic	Risks relating to broad business plans and strategies, such as acquisitions and mergers
Process	Risks inherent to business processes, like transport, sales and Marketing
People	Risks relating to the workforce, like human error or unexpected long-term absence
Infrastructure	Risks pertaining to the core business infrastructure – these could be an IT system going down, or a power cut in a factory
Information	Information risks with a potential impact on information security, like breaches, hacks, leaks and loss of data
Services or products	Risks associated with the services or products outputted by a business, such as compromise of such as compromise of finished product quality. Motorola's 99.99966% benchmark of defect-free products formed the basis of the 'Six Sigma' technique
Environmental	Environmental risks comprise a business's actual or potential threat to the environment. Examples include excessive wastage, or leakage of harmful material into the external environment
Technology	Risks related to the technology used by a business. This might be a fault with manufacturing machinery, company vehicles or IT infrastructure
Outsourced providers	Risks pertaining to third-party outsourced service providers, like Internet and telephone providers, logistics companies or external agencies
Documentation	Risks connected to business documentation, such as loss of sensitive or important information, dissemination of outdated information, or process confusion
Company image	The risks of negative impact on a company's brand, reputation and image, usually originating from another actualised risk
Management information	Risks relating to awareness of management, visibility and the ability of management to access important information
Legal and regulatory	Risks relating to the legal and regulatory framework of a business operation. This could be loss of standard accreditation or certification, liability arising from a legal claim (suing or compensation) or a change in law affecting operation
Change	Risks inherent to change within a business, like budget allocation, change of supplier or entering a new market
Socio-cultural	Sociocultural factors which might impact a business, such as change in consumer consumption patterns, economic developments crashes or depressions) or subjective interpretations of business ethics



SWOT

Strength Expertise Strong reputation People – expertise Culture of excellence, engaged teams QHSE management system High barriers to entry	Weakness Documented information outdated / inaccurate Risk training Innovation Silos Poor IT infrastructure Internal audit
Opportunities Diversification Market penetration Standards Outsource risk Business continuity management Physical security Malware protection	Threat Demand for existing product Competitive positions Regulations Supply chain buying power Value of pound Substitute products Bargaining power of buyers

Breakout session: DIY SWOT

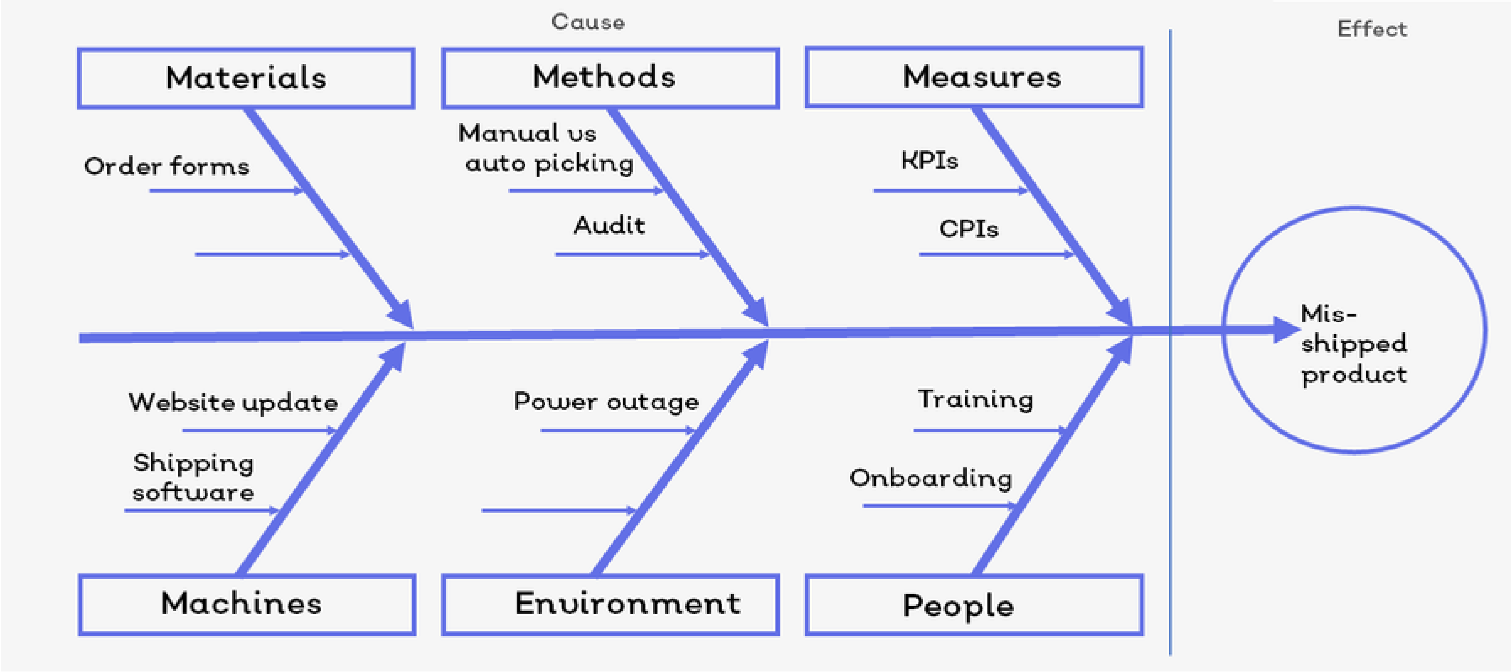
Strength	Weakness
Opportunities	Threat

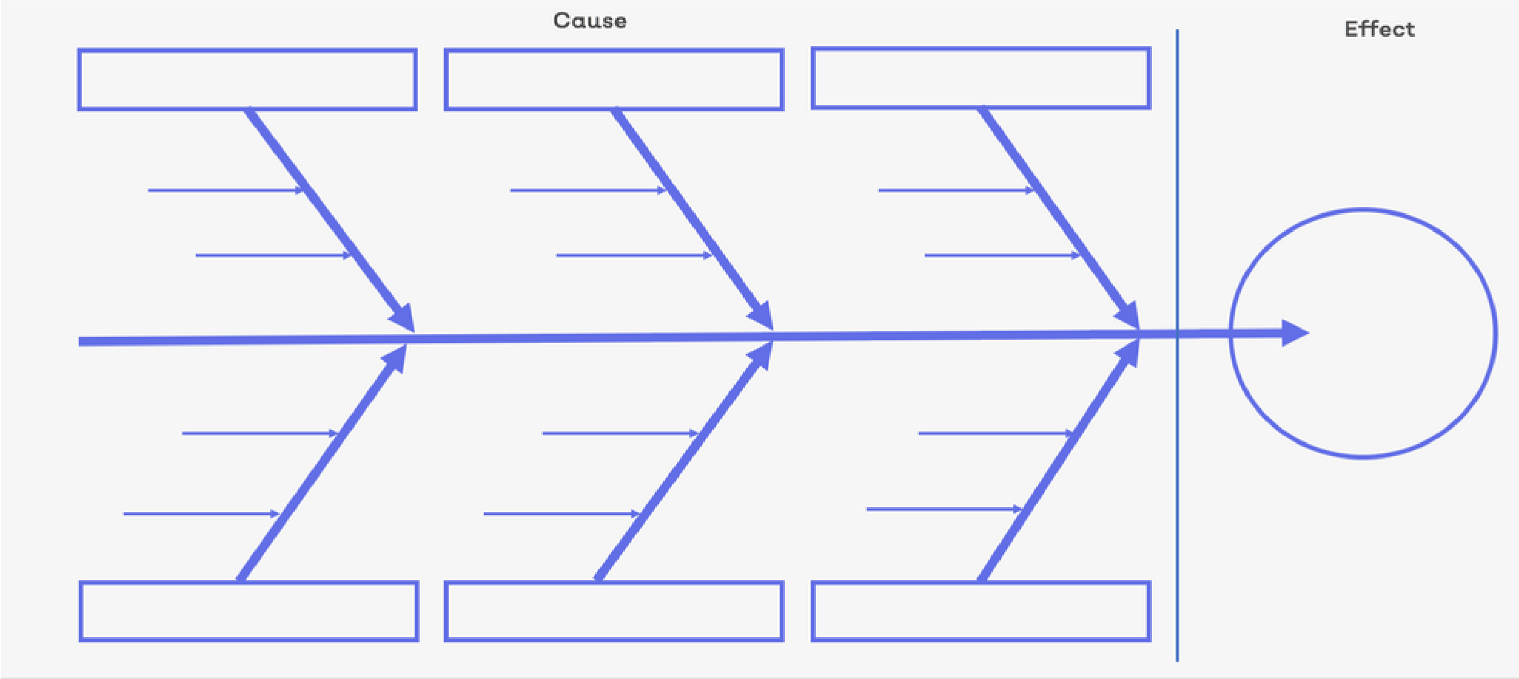
6 rules for identifying risks

An effective risk identification process should include the following steps:

1. Create a systematic process
   - A risk register
2. Gather information from various sources
   - Each department responsible for identifying and documenting risks in their risk register
3. Apply risk identification tools and techniques
4. Document the risks
5. Document the risk identification process
6. Assess the process effectiveness

Breakout session: create your own fishbone

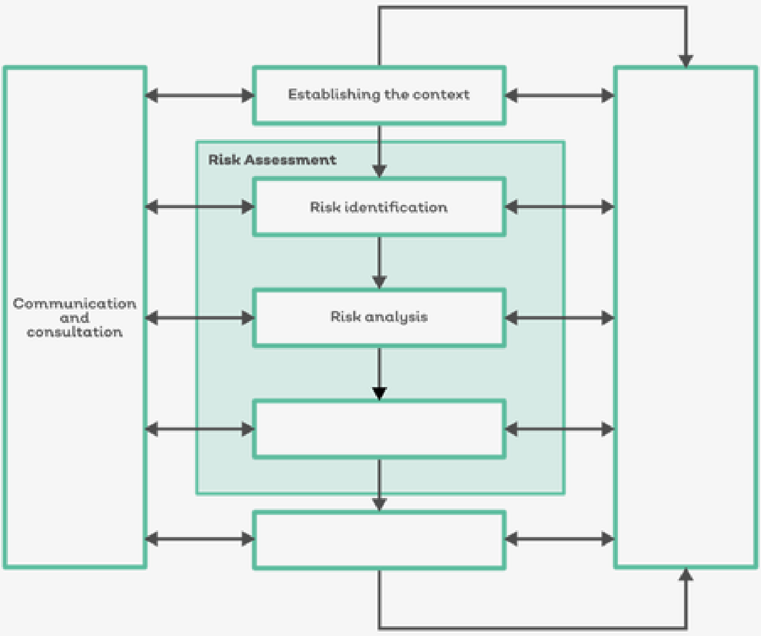




Risk analysis and evaluation

Risk analysis and evaluation – 1.00

- Risk register
- Categorising risks
- Effectiveness of criteria definition
- Which risks are high priority?



A risk register is a tool that helps you to track issues and address problems as they arise.

What does a risk register contain?

- Risk category to group similar risks
- The risk breakdown structure identification number
- A brief description or name of the risk to make the risk easy to discuss
- The *impact* (or *consequence*) if event actually occurs rated on an integer scale
- Probability and likelihood of its occurrence rated on an integer scale
- The *Risk Score* (or *Risk Rating*) is the multiplication of Probability and Impact and is often used to rank the risks.
- Common *mitigation steps* are identify, analyse, plan response, monitor and control.

Breakout session

Take five minutes to take the first steps on your Risk Register handout

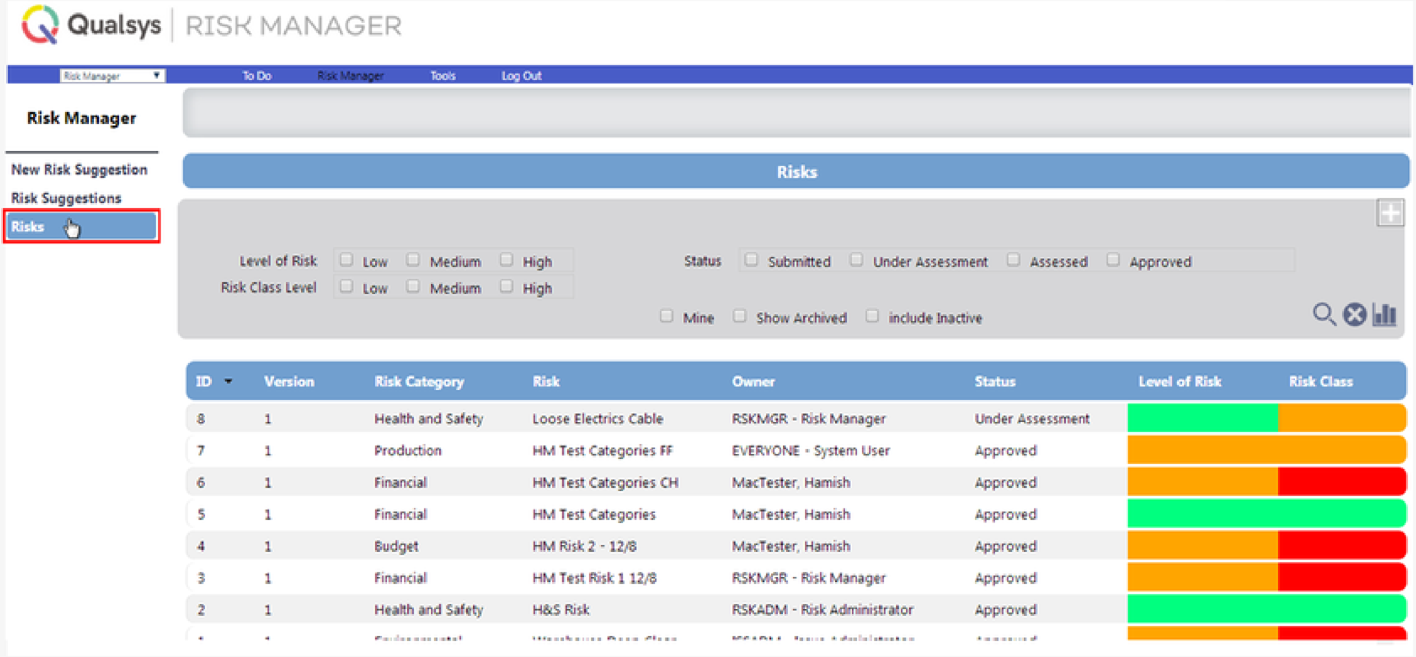
1. Identify three of your business risks and add them to your Risk Register handout

2. Identify the category of each risk and fill in the Category section of your handout

3. Identify which asset (s) is/are affected by the risk e.g. reputation, workforce, machinery etc.

Notes

Recording and assessing



Qualsys | RISK MANAGER

Risk Manager

- New Risk Suggestion
- Risk Suggestions
- Risks

Risks

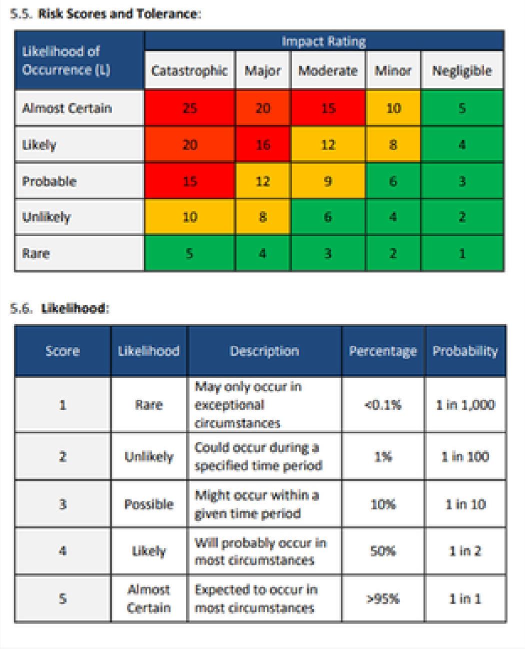
Level of Risk ☐ Low ☐ Medium ☐ High

Risk Class Level ☐ Low ☐ Medium ☐ High

Status ☐ Submitted ☐ Under Assessment ☐ Assessed ☐ Approved

☐ Mine ☐ Show Archived ☐ include Inactive

ID ▾	Version	Risk Category	Risk	Owner	Status	Level of Risk	Risk Class
8	1	Health and Safety	Loose Electrics Cable	RSKMGR - Risk Manager	Under Assessment	🟩	🟧
7	1	Production	HM Test Categories FF	EVERYONE - System User	Approved	🟧	🟧
6	1	Financial	HM Test Categories CH	MacTester, Hamish	Approved	🟧	🟥
5	1	Financial	HM Test Categories	MacTester, Hamish	Approved	🟩	🟩
4	1	Budget	HM Risk 2 - 12/8	MacTester, Hamish	Approved	🟧	🟥
3	1	Financial	HM Test Risk 1 12/8	RSKMGR - Risk Manager	Approved	🟧	🟥
2	1	Health and Safety	H&S Risk	RSKADM - Risk Administrator	Approved	🟩	🟩
1	1	Environmental	Warehouse Door Glass	ISSADM - Issue Administrator	Approved	🟧	🟥

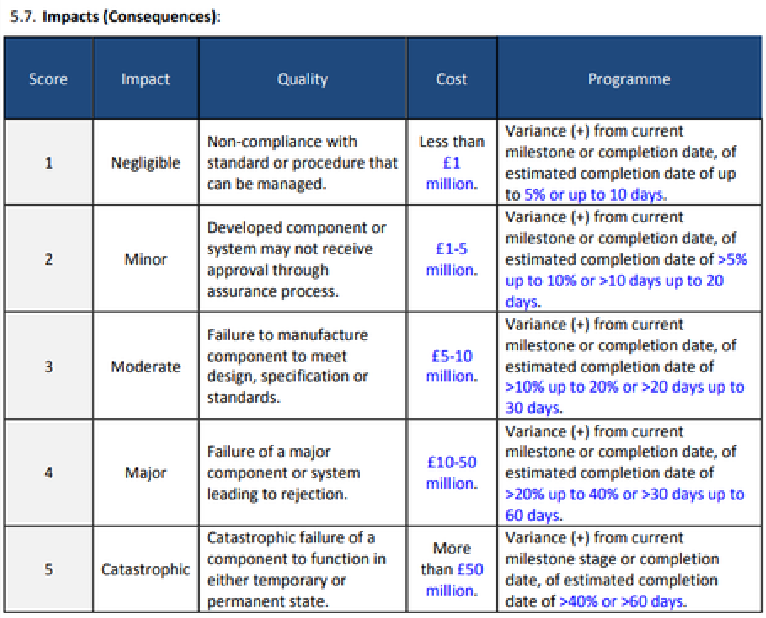


5.5. Risk Scores and Tolerance:

Likelihood of Occurrence (L)	Impact Rating				
	Catastrophic	Major	Moderate	Minor	Negligible
Almost Certain	25	20	15	10	5
Likely	20	16	12	8	4
Probable	15	12	9	6	3
Unlikely	10	8	6	4	2
Rare	5	4	3	2	1

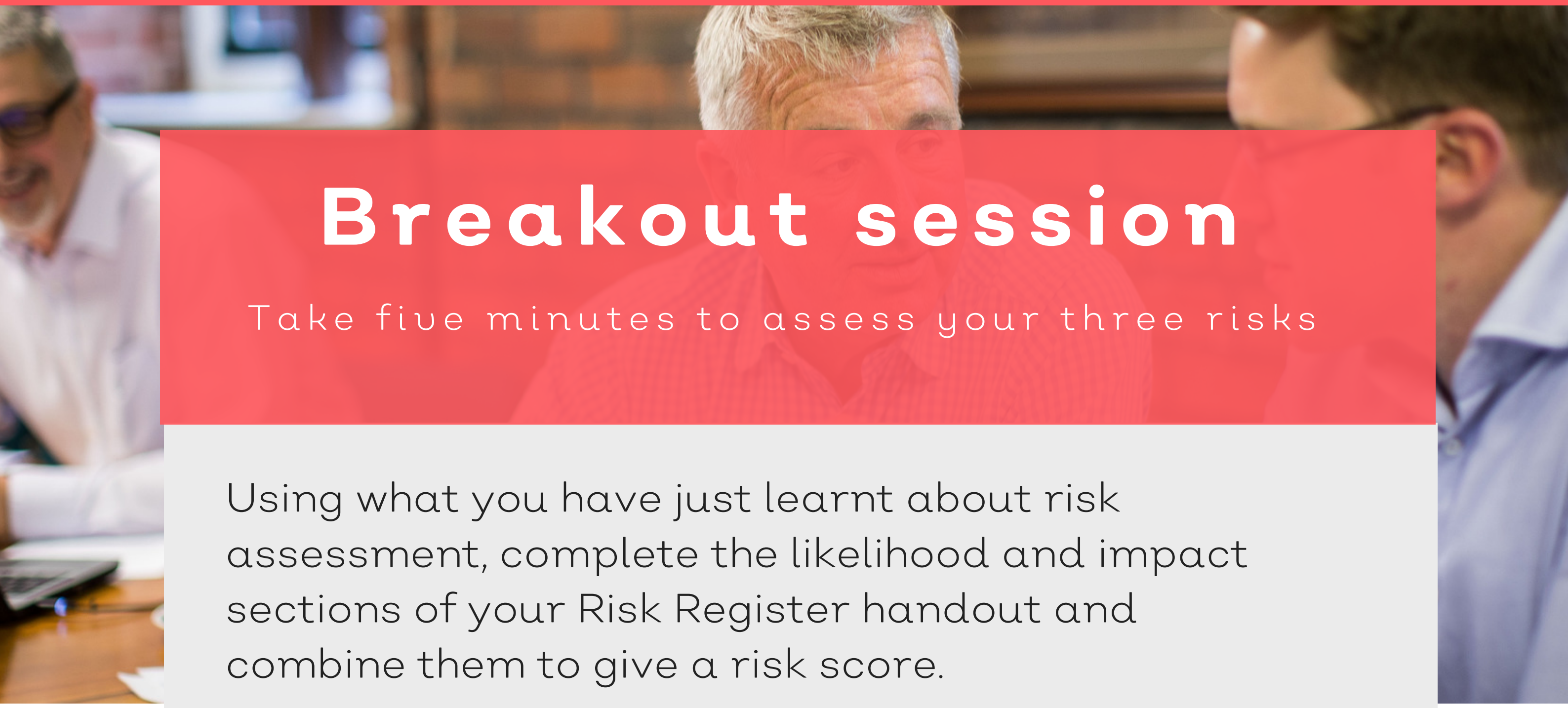
5.6. Likelihood:

Score	Likelihood	Description	Percentage	Probability
1	Rare	May only occur in exceptional circumstances	<0.1%	1 in 1,000
2	Unlikely	Could occur during a specified time period	1%	1 in 100
3	Possible	Might occur within a given time period	10%	1 in 10
4	Likely	Will probably occur in most circumstances	50%	1 in 2
5	Almost Certain	Expected to occur in most circumstances	>95%	1 in 1



5.7. Impacts (Consequences):

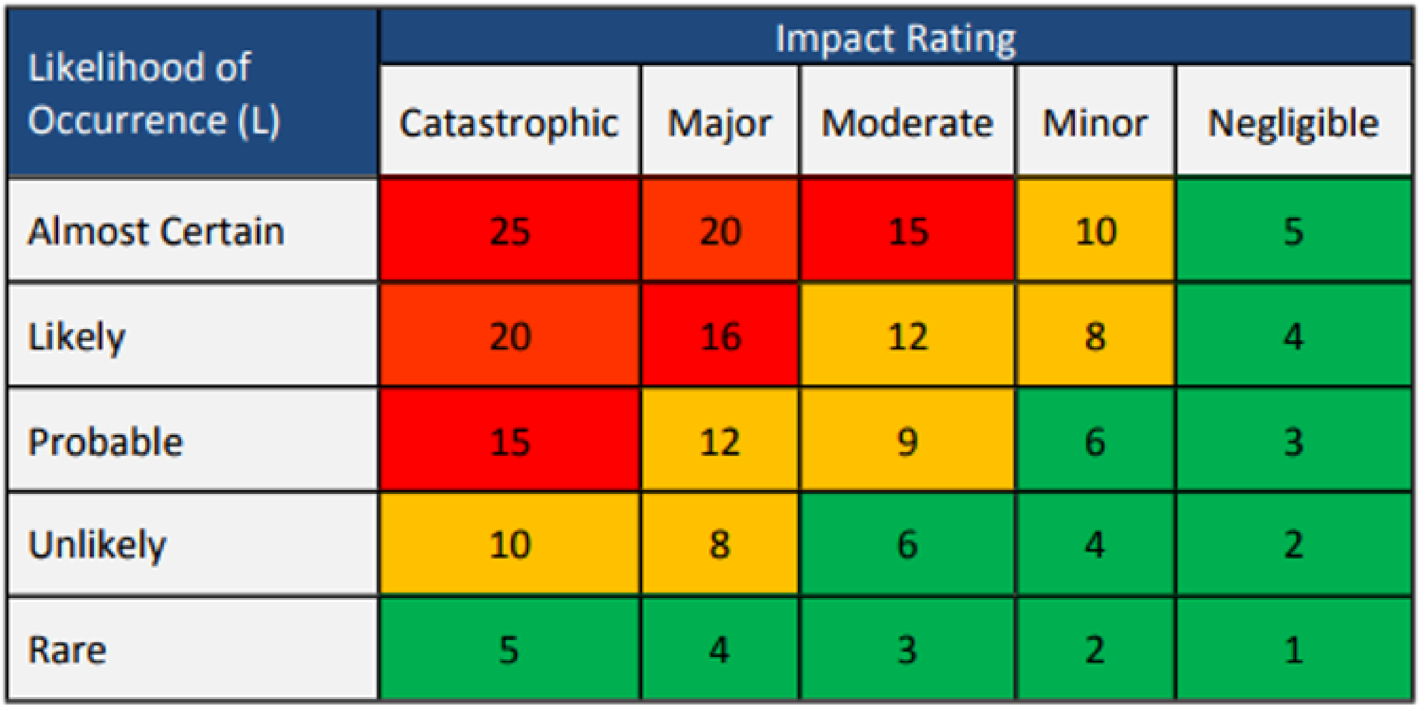
Score	Impact	Quality	Cost	Programme
1	Negligible	Non-compliance with standard or procedure that can be managed.	Less than £1 million.	Variance (+) from current milestone or completion date, of estimated completion date of up to 5% or up to 10 days.
2	Minor	Developed component or system may not receive approval through assurance process.	£1-5 million.	Variance (+) from current milestone or completion date, of estimated completion date of >5% up to 10% or >10 days up to 20 days.
3	Moderate	Failure to manufacture component to meet design, specification or standards.	£5-10 million.	Variance (+) from current milestone or completion date, of estimated completion date of >10% up to 20% or >20 days up to 30 days.
4	Major	Failure of a major component or system leading to rejection.	£10-50 million.	Variance (+) from current milestone or completion date, of estimated completion date of >20% up to 40% or >30 days up to 60 days.
5	Catastrophic	Catastrophic failure of a component to function in either temporary or permanent state.	More than £50 million.	Variance (+) from current milestone stage or completion date, of estimated completion date of >40% or >60 days.



Breakout session

Take five minutes to assess your three risks

Using what you have just learnt about risk assessment, complete the likelihood and impact sections of your Risk Register handout and combine them to give a risk score.

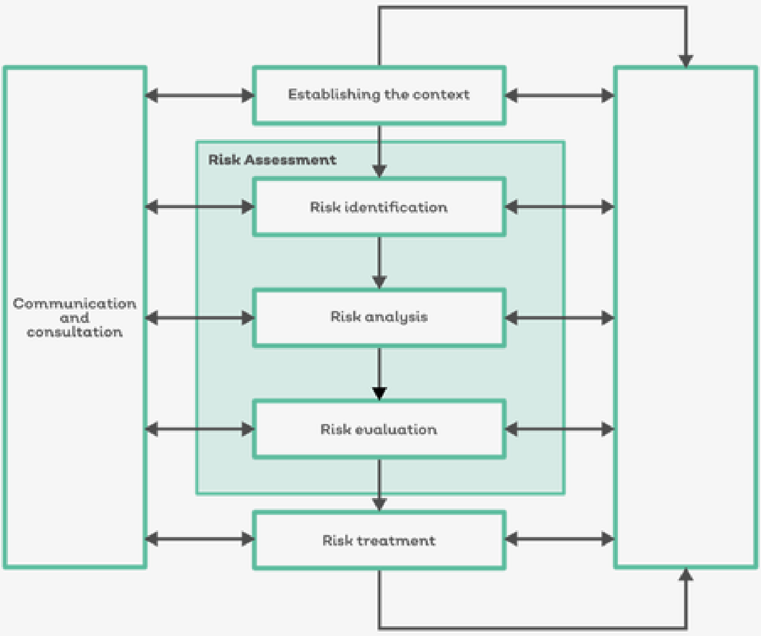


Likelihood of Occurrence (L)	Impact Rating				
	Catastrophic	Major	Moderate	Minor	Negligible
Almost Certain	25	20	15	10	5
Likely	20	16	12	8	4
Probable	15	12	9	6	3
Unlikely	10	8	6	4	2
Rare	5	4	3	2	1

Risk treatment

Risk treatment – 1.45

- Risk treatment strategies
- Risk controls
- Risk culture



Establishing the context

Risk Assessment

Risk identification

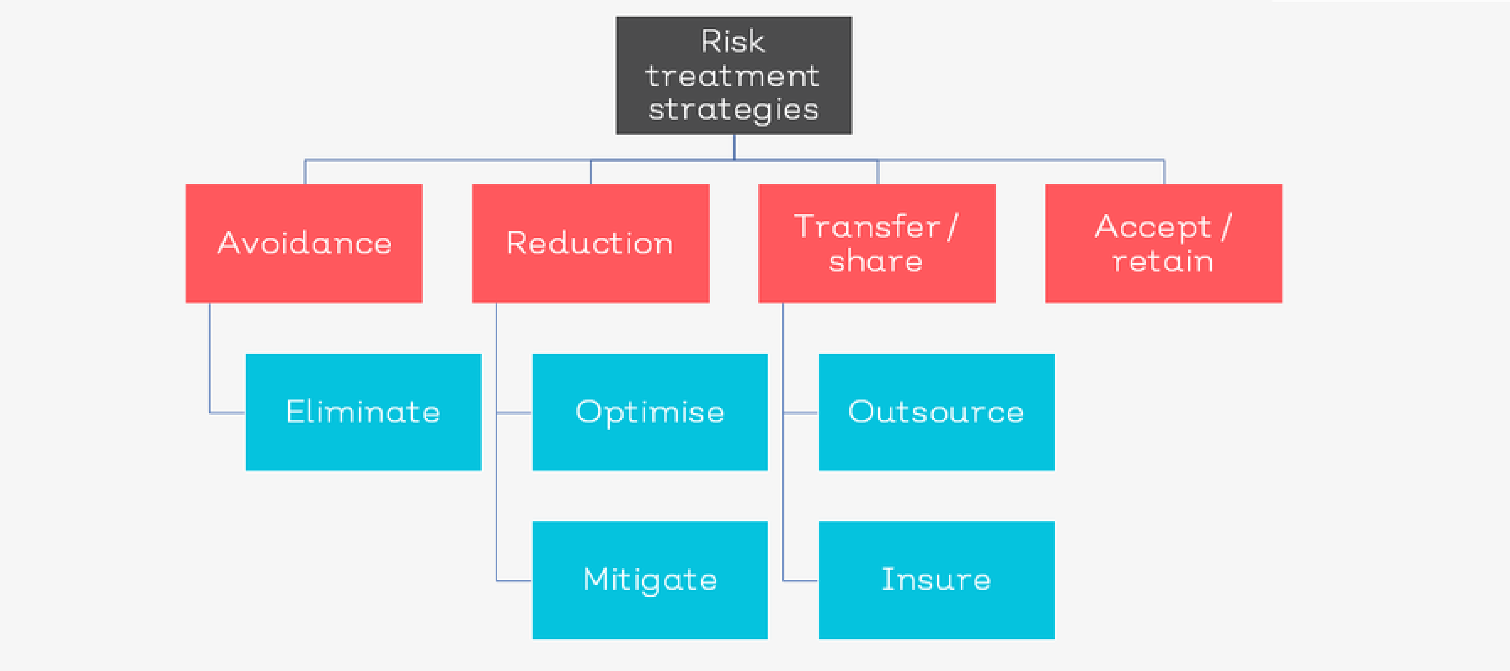
Risk analysis

Risk evaluation

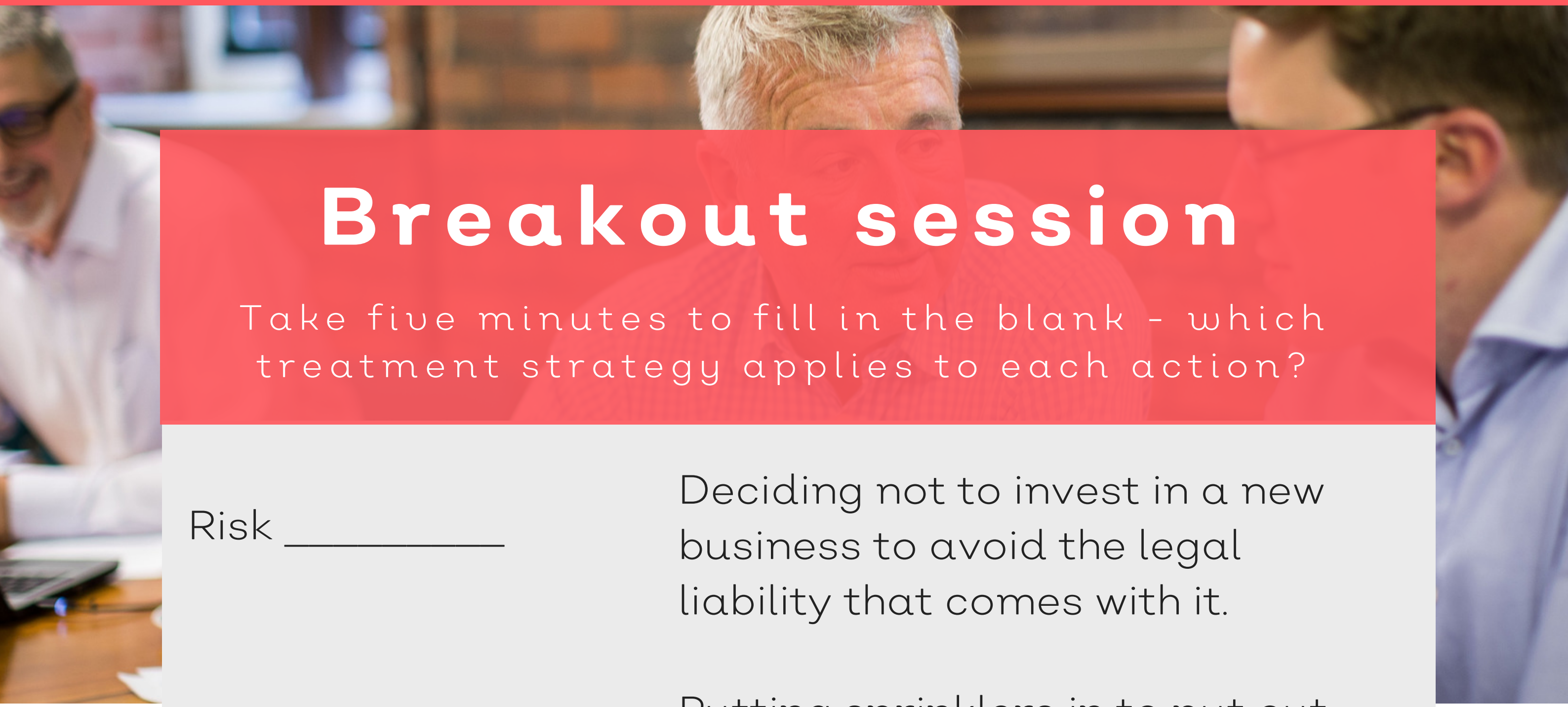
Risk treatment

Communication and consultation

Risk treatment strategies



A risk control is any measure or action that modifies risk – ISO 31000



Breakout session

Take five minutes to fill in the blank - which treatment strategy applies to each action?

Risk ___________ Deciding not to invest in a new business to avoid the legal liability that comes with it.

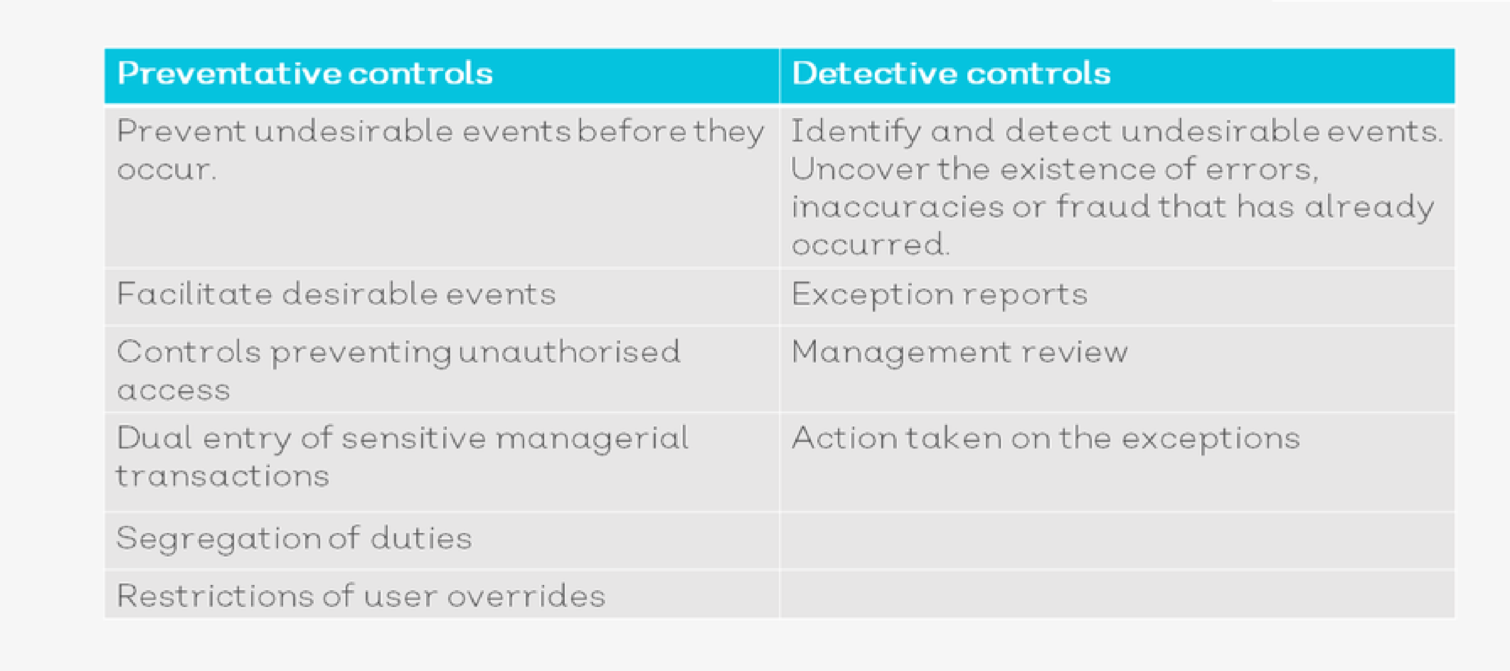
Risk ___________ Putting sprinklers in to put out a fire to reduce the risk of loss.

Risk ___________ Outsourcing customer service.

Risk ___________ Launching a new product in a competitive market.

Notes

2 types of control



Preventative controls	Detective controls
Prevent undesirable events before they occur.	Identify and detect undesirable events. Uncover the existence of errors, inaccuracies or fraud that has already occurred.
Facilitate desirable events	Exception reports
Controls preventing unauthorised access	Management review
Dual entry of sensitive managerial transactions	Action taken on the exceptions
Segregation of duties	
Restrictions of user overrides	

Notes

Breakout session

Take five minutes to complete your Risk Register handout

1. Add controls to the risks on your Risk Register handout, considering the risk treatment strategies we've discussed

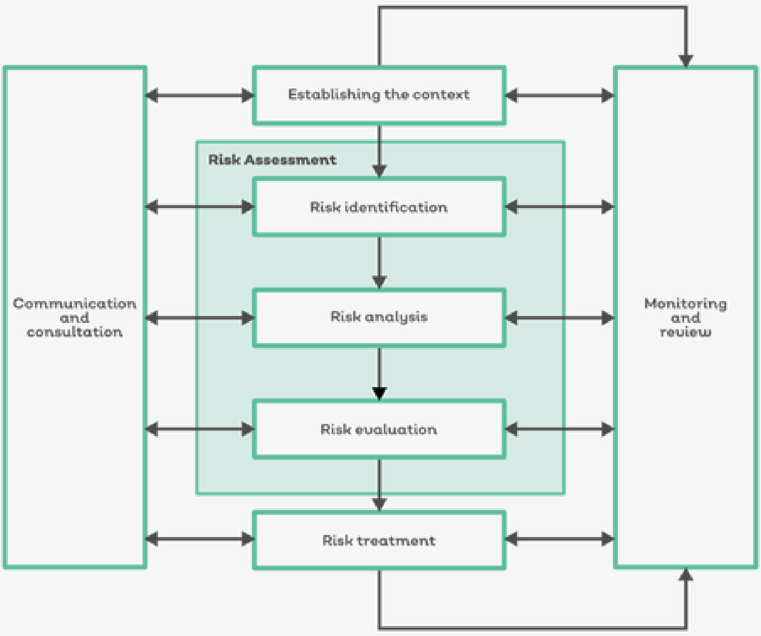
2. After the controls, conduct a new risk likelihood/impact assessment to give your residual risk scores

Notes

Risk monitoring and review

Risk monitoring and review – 2.45

- ISO 31000 clause 6.6. monitor and review
- Risk KPIs
- Training
- Communications
- Integrated systems



Establishing the context

Risk Assessment

Risk identification

Risk analysis

Risk evaluation

Risk treatment

Communication and consultation

Monitoring and review

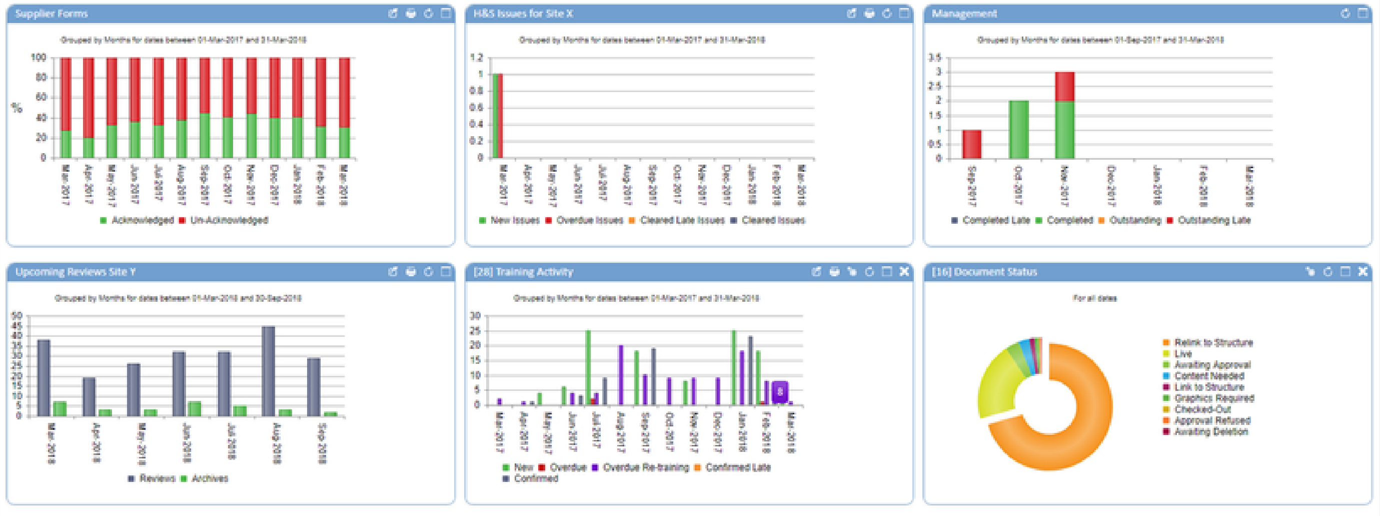
ISO 31000: Clause 6.6 Monitor and Review

- Internal and external changes will require you to monitor and review your risks
- Up to leadership to determine the review and reporting requirements
- Risk culture
- Training
- Communications
- Establishing KPIs

> “You need to give every employee a channel where they can communicate risk.”
>
> - Richard Green, Kingsford Consultancy Services Ltd

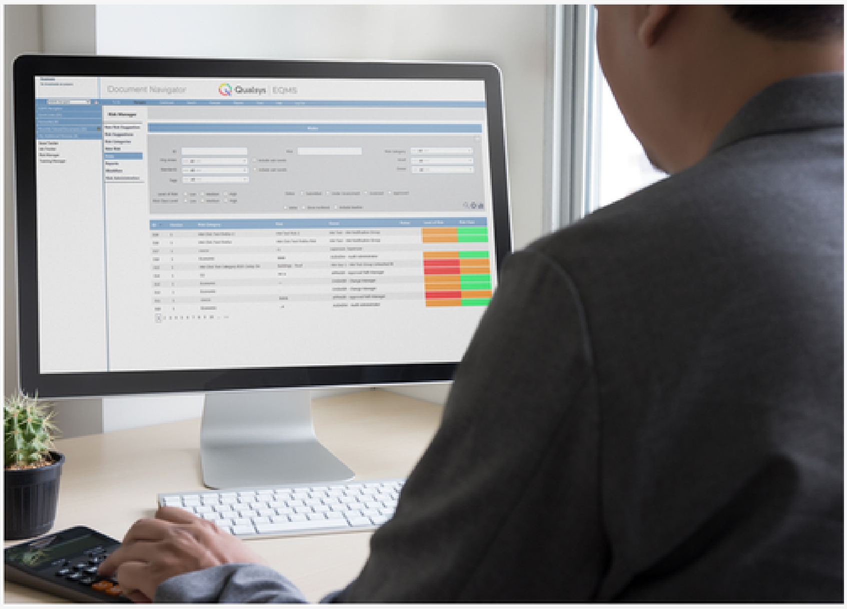
Watch here: https://qualsys.wistia.com/medias/tqspoowtgf

Single source of truth



Importance of communication

- Ideas and insights
- You can't be everywhere all the time
- Experts across your business
- Collaborate for stronger decision making



Roles & responsibilities

As a
Risk owner

I must
Document and manage the risk

So that
I can ensure the risks are well managed

As a
Technology Owner

I must
document changes to procedures

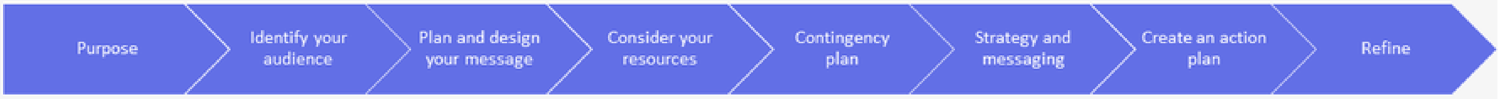
So that
I can be confident we are compliant

As a
Manager

I must
Encourage my team to identify and talk about risk

So that
We can get better data

8-step communications plan



Purpose

Identify your audience

Plan and design your message

Consider your resources

Contingency plan

Strategy and messaging

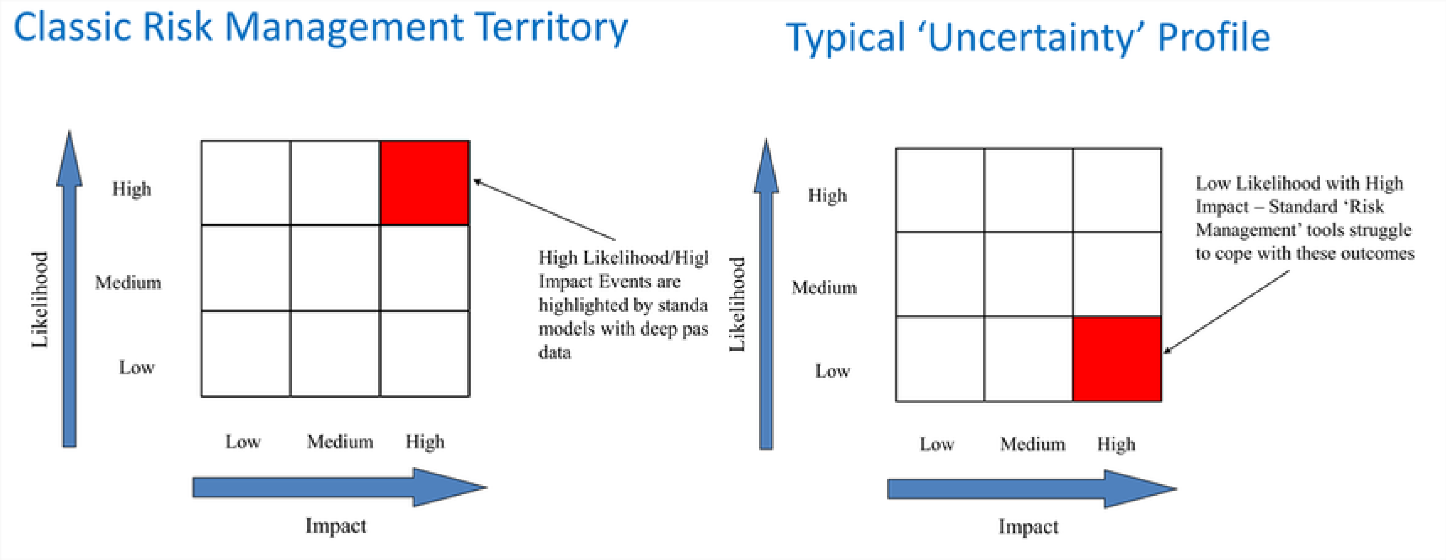
Create an action plan

Refine

Developing your communication plan

- Top-down engagement
- Implement a data protection policy
- Build data protection in from the ground up
- Communications, training and development
- Access management

But be warned!



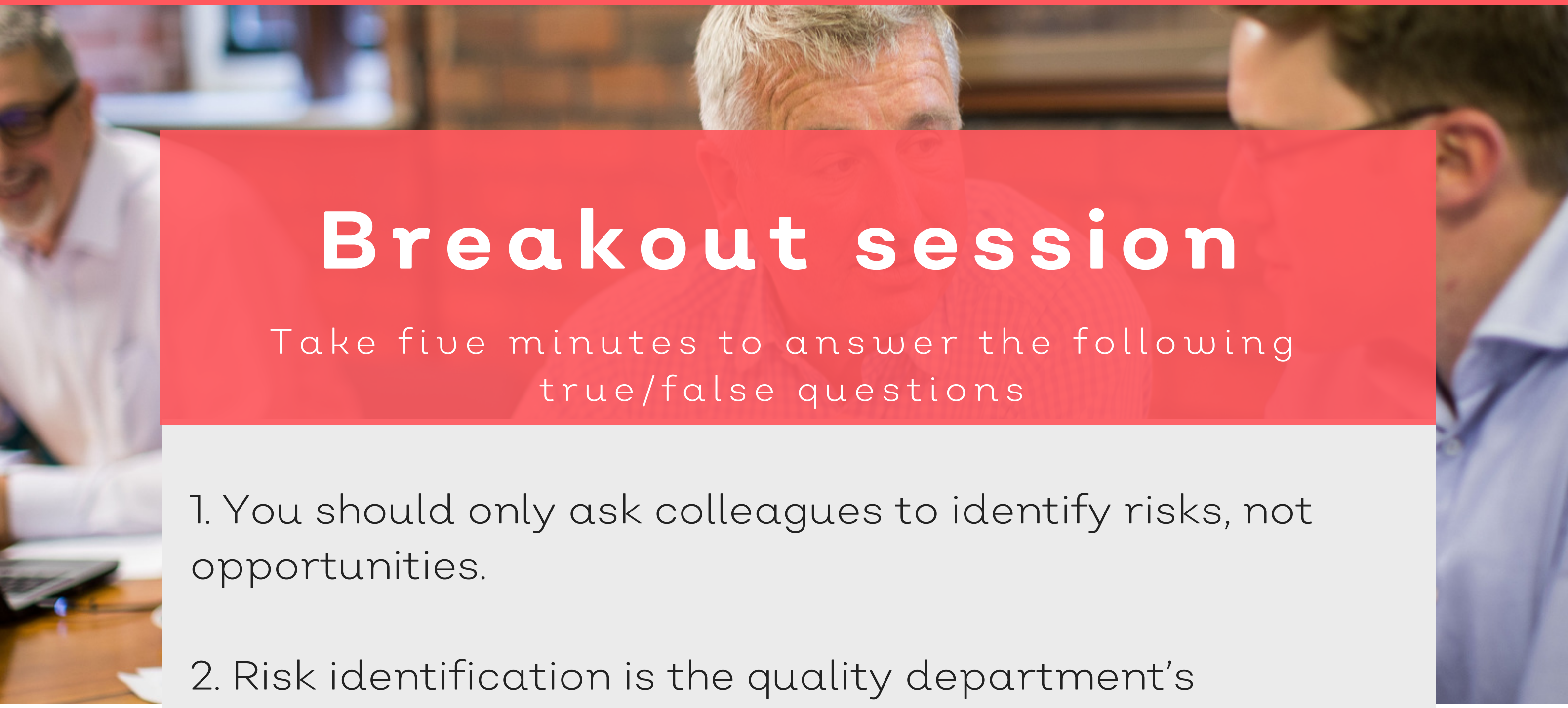
Classic Risk Management Territory

High Likelihood/Higl Impact Events are highlighted by standa models with deep pas data

Typical 'Uncertainty' Profile

Low Likelihood with High Impact – Standard 'Risk Management' tools struggle to cope with these outcomes

http://quality.eqms.co.uk/blog/rethinking-risk-cqi-conference-2016-part-1



Breakout session

Take five minutes to answer the following true/false questions

1. You should only ask colleagues to identify risks, not opportunities.

2. Risk identification is the quality department's responsibility.

3. Effective risk controls lower your risk score.

4. Risk registers should comprise both tangible and intangible assets.

5. Every risk needs to have the lowest possible risk score.

6. A core risk management principle is explicitly addressing uncertainty.

7. Risk matrices assess the likelihood and impact of a risk event.

8. ISO 9001:2015 mandates a formal risk assessment and risk register.

9. Senior management and boards need to take an active role in risk management.

10. Most risks and non-conformances arise from human error.

Cultural change

Cultural Change – 3.15

- Engaging the business
- 6 essential building blocks for a strong, functioning risk culture
- Starting the conversation
- Tips on managing cultural change

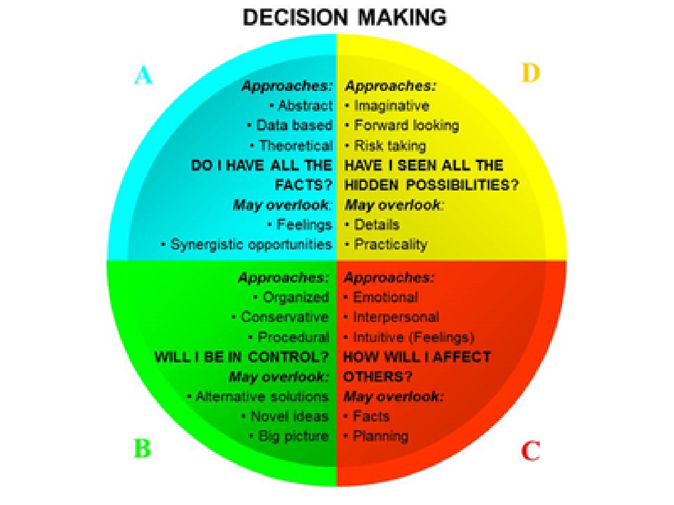
Engaging the business

- Reiterate importance of risk management
- Relates to everyone
- Guidance needs to be from the top down
- Imperative to involve and empower staff

Building blocks for a strong, functioning risk culture

Do you have...

1. Leadership sending consistent and clear messages on acceptable levels of risk?
2. Risk and risk appetite discussions as part of key strategic decisions?
3. Considerations of what might go wrong and deciding upon appropriate tolerance levels when considering targets and performance?
4. Adequate risk reporting, monitoring and incident reporting based upon clearly defined risk appetite?
5. A system of accountability with sanctions for those taking inappropriate levels of risk?
6. Appropriate levels of resource to address risks?



DECISION MAKING

A

Approaches:
- Abstract
- Data based
- Theoretical

DO I HAVE ALL THE FACTS?

May overlook:
- Feelings
- Synergistic opportunities

D

Approaches:
- Imaginative
- Forward looking
- Risk taking

HAVE I SEEN ALL THE HIDDEN POSSIBILITIES?

May overlook:
- Details
- Practicality

B

Approaches:
- Organized
- Conservative
- Procedural

WILL I BE IN CONTROL?

May overlook:
- Alternative solutions
- Novel ideas
- Big picture

C

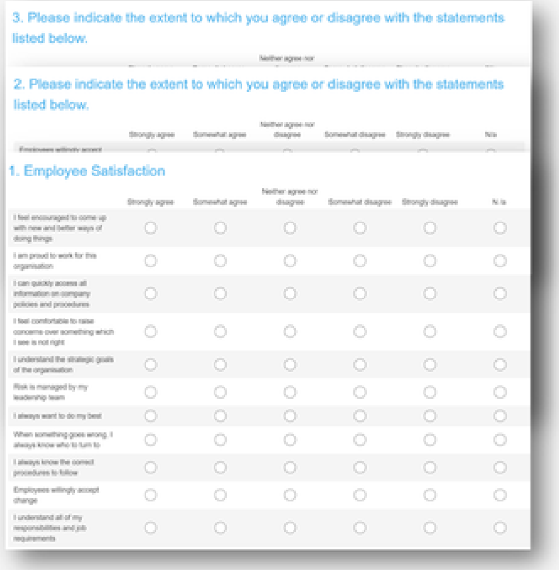
Approaches:
- Emotional
- Interpersonal
- Intuitive (Feelings)

HOW WILL I AFFECT OTHERS?

May overlook:
- Facts
- Planning

Start the conversation

- Formal structures
  - Suggestions process
  - Every single employee engaged
- Meetings with employees
  - Audits
  - Monthly drop in sessions and quality council
- 'Voice of the business' survey
  - Values & organisational culture
  - Training and development
  - Leadership
  - Systems & structure
  - Ask for ideas
  - Example: https://www.surveymonkey.co.uk/r/employee-feedback-survey-grc
  - What are your employees telling you? Top management will want to know.
  - Identify gaps and issues



3. Please indicate the extent to which you agree or disagree with the statements listed below.

2. Please indicate the extent to which you agree or disagree with the statements listed below.

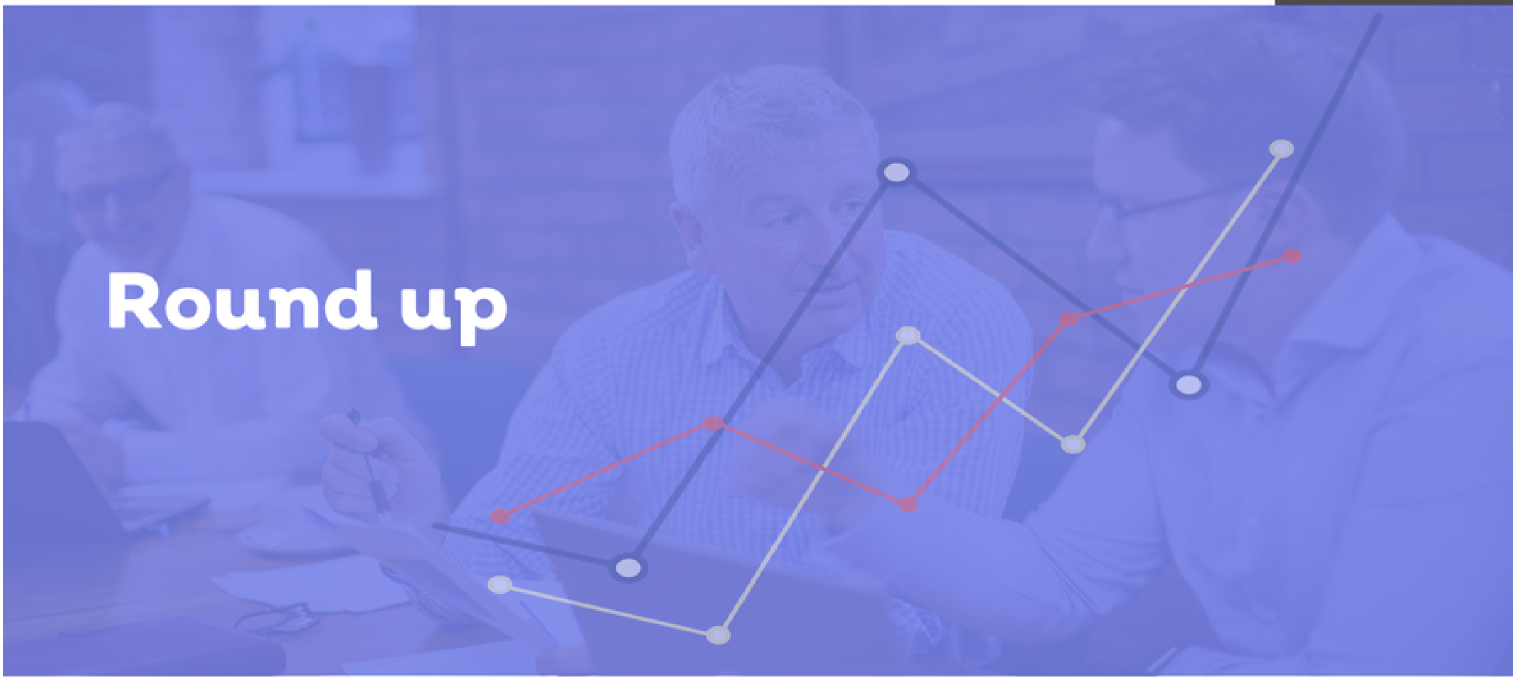
1. Employee Satisfaction

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree	N/a
I feel encouraged to come up with new and better ways of doing things	○	○	○	○	○	○
I am proud to work for this organisation	○	○	○	○	○	○
I can quickly access all information on company policies and procedures	○	○	○	○	○	○
I feel comfortable to raise concerns over something which I see is not right	○	○	○	○	○	○
I understand the strategic goals of the organisation	○	○	○	○	○	○
Risk is managed by my leadership team	○	○	○	○	○	○
I always want to do my best	○	○	○	○	○	○
When something goes wrong, I always know who to turn to	○	○	○	○	○	○
I always know the correct procedures to follow	○	○	○	○	○	○
Employees willingly accept change	○	○	○	○	○	○
I understand all of my responsibilities and job requirements	○	○	○	○	○	○

Watch Leadership, ISO 9001:2015 and Risk: https://qualsys.wistia.com/medias/9mizntocg2

Tips on managing cultural change

- Quantitatively measure your current cultural values
- Align culture, strategy and structure
- Ensure staff and stakeholder participation
- Communicate and demonstrate the change
- Manage the emotional response
- Reiterate importance of risk management
- Relates to everyone
- Guidance needs to be from the top down
- Imperative to involve and empower staff



Round up

Round Up – 3.45

- Best practice from the Risk Masters
- Challenges managing risk
- Risk management mistakes to avoid
- Useful resources

Best practices from the Risk Masters

1. Create shareholder value from risk management by linking risk to business performance
2. Involve the risk organisation in key decision-making processes
3. Invest in continuous improvement
4. Integrate risk management across the organisation and business units for a more consistent approach
5. Engage a higher level of commitment to analytics and risk modelling in an increasingly complex risk environment
6. Go beyond compliance - Risk Masters were identified as better at developing relationships with regulatory agencies
7. Statistically, high performing risk organisations are more likely to have an Enterprise Risk Management program

90%

of Risk Masters have an ERM in place

Challenges managing risks

- Speed of information exchange is elevating the need for more robust risk oversight
- Risk management leaders need to speak the language of the business
- The complexity of business may outweigh an individual's capacity to assess risk
- Risk oversight and strategy need to be better integrated
- Overlooking ethical culture may lead to an organisation's biggest risk

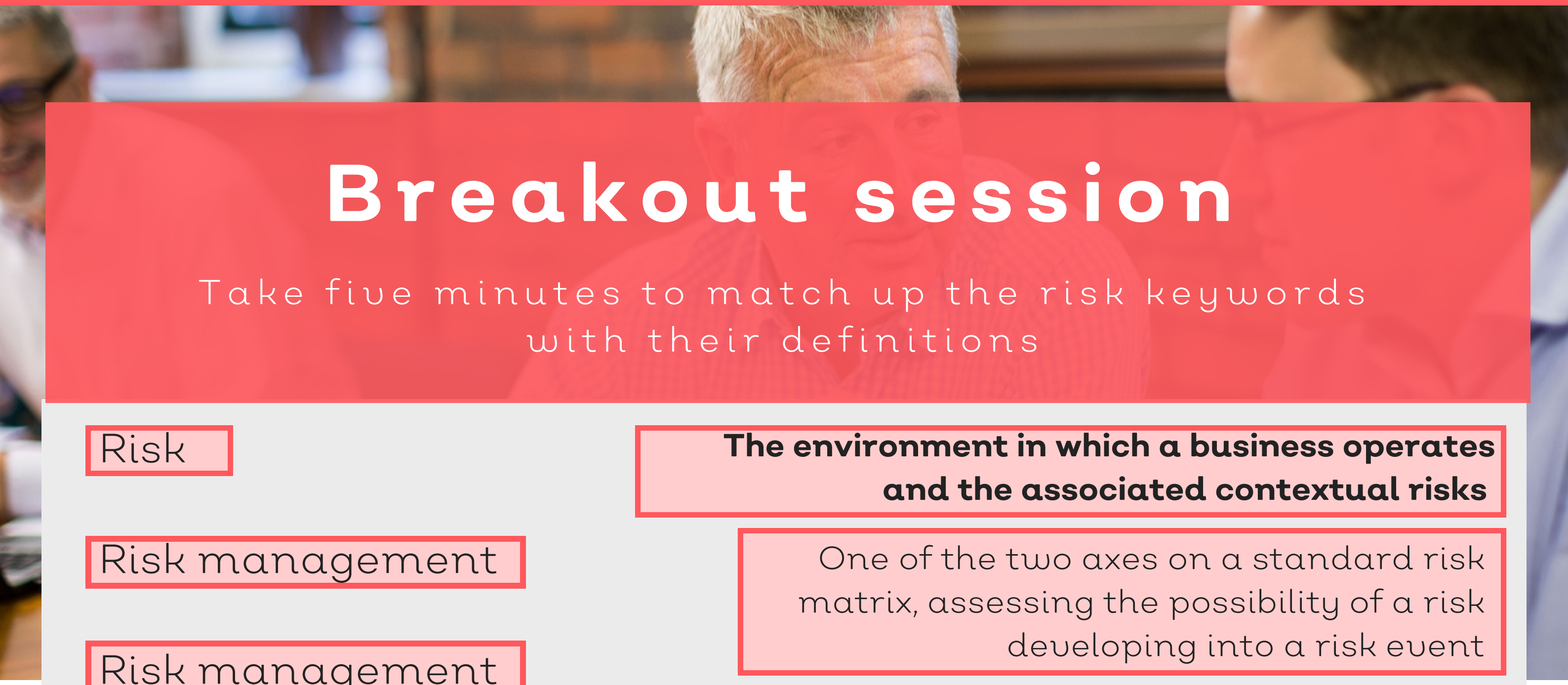
6 risk management mistakes

1. Relying on historical data
2. Focusing on narrow measures
3. Overlooking knowable risks
4. Overlooking concealed risks
5. Failing to communicate
6. Not managing risks in real time

https://hbr.org/2009/03/six-ways-companies-mismanage-risk

Useful resources

- Handouts / Slides: http://quality.eqms.co.uk/risk-management-post-workshop-resources
- ISO 27001 toolkit: http://quality.eqms.co.uk/iso-27001-toolkit
- ISO 31000 toolkit: http://quality.eqms.co.uk/iso-31000-risk-management
- More training / workshops: https://qualsys.co.uk/knowledge-centre/training/



Breakout session

Take five minutes to match up the risk keywords with their definitions

Risk

Risk management

Risk management policy

Risk management plan

Risk owner

External context

Internal context

Risk identification

Risk event

Risk source

Likelihood

Risk treatment

Residual risk

The environment in which a business operates and the associated contextual risks

One of the two axes on a standard risk matrix, assessing the possibility of a risk developing into a risk event

The level of risk after risk treatment has been applied

A control placed onto a risk to decrease its likelihood, severity or both

The actualisation of risk into a specific occurrence, such as an accident, data breach or loss of employee

An area of uncertainty with real or potential impact on business objectives

The broad process of minimising, controlling and mitigating risk to an acceptable level

The process of analysing a business or business area to map out the risks within

The individual responsible for monitoring a particular risk and taking action where necessary

The area of a business where a risk can originate and develop into a risk event

The structure of a business operation and its connected contextual risks

A document demonstrating how your business manages risk

A formulated strategy for identifying, addressing, controlling and reviewing risk

Contact details

Aizlewood's Mill, Nursery
Street, Sheffield, S3 8GG

info@qualsys.co.uk
+44 (0) 114 282 3338
www.qualsys.co.uk

Talk to us

More questions about risk management or GRC? Talk to us today.