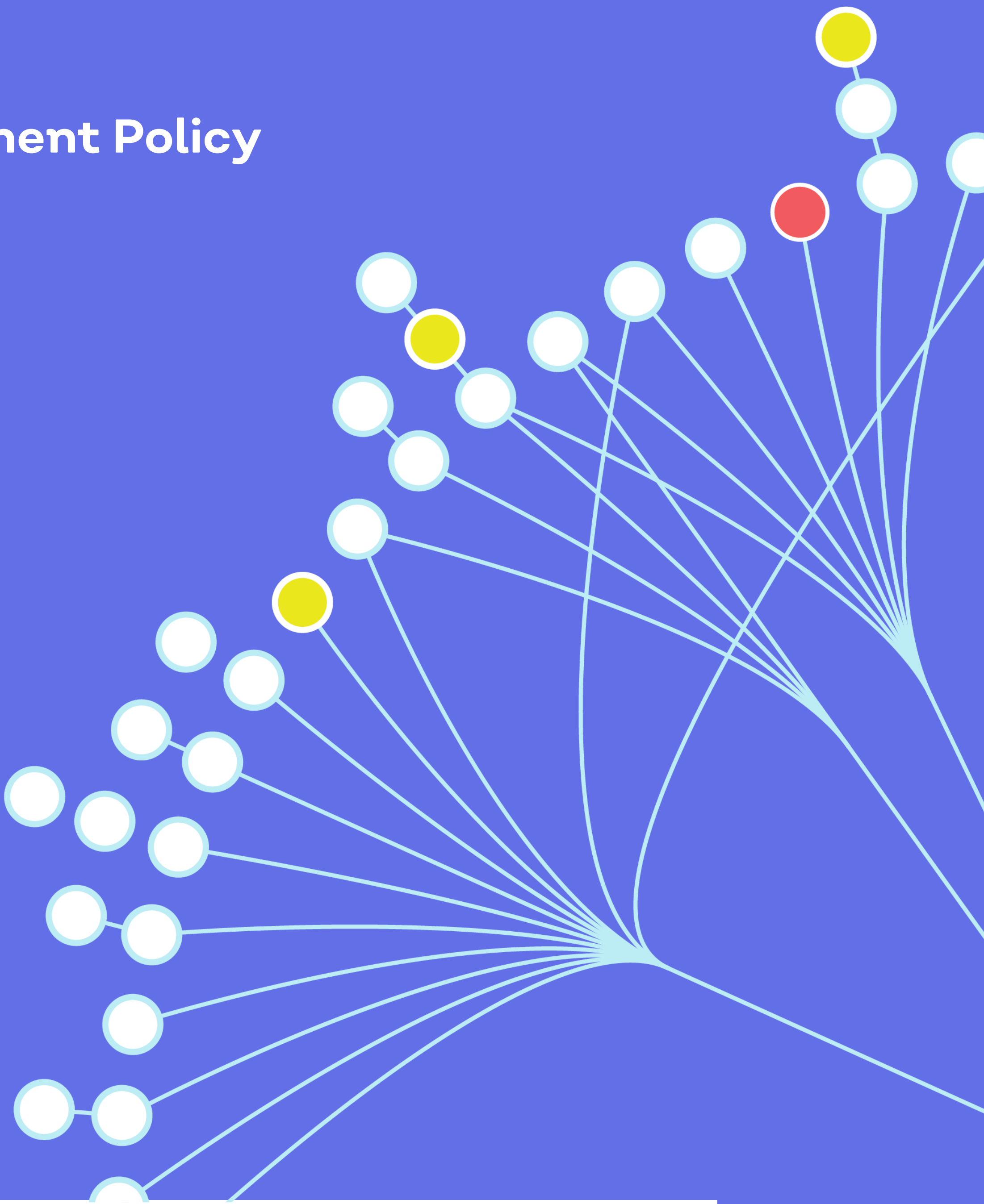
Qualsys

Risk Management Policy
Qualsys Ltd



Our software reduces compliance burden associated with regulations and standards:

ISO

GxP QUALITY SYSTEMS

FDA 21 CFR Part 11

MHRA Regulating Medicines and Medical Devices

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

Kate Armitage
Product Quality Assurance Manager
+44(0) 114 282 3338
Kate.Armitage@qualsys.co.uk

Brands we work with

YAZAKI | DIAGEO | BUNZL | Accolade Wines | NHS

Honeywell | UNIVERSITY OF LEEDS | Nestlé | BT | sodexo

Welcome to our risk management policy

Kate Armitage

Product Quality Assurance Manager

kate.armitage@qualsys.co.uk

Qualsys provides a best of breed governance risk and compliance software solution to some of the world's largest and most trusted businesses.

It's imperative that Qualsys takes the correct steps to identify and mitigate the risks inherent in our operational environment and within our business, as well as recognising and managing new opportunities.

Qualsys has a robust and systematic process for risk management that supports our proactive, forward-looking approach to risk. We use our electronic quality management system and the module Risk Manager to manage our risk process.

The goal of this document is to provide you with an overview of our risk control policy, our risk management methodology and to highlight the key high-level steps we take.

Risk Manager Module: https://qualsys.co.uk/grc-solutions/modules/risk-management-software/

Contents

1. Scope and context

Our commitment to managing risk, risk appetite and risk tolerance

Every employee is responsible for identifying risk.

A risk is: "Any effect of uncertainty on objectives." Risk is the main cause of uncertainty in an organisation therefore they need to be identified and managed before they can negatively affect the business. Risks should be seen as opportunities for improvement. They are not all negative.

Risk can come from both internal and external sources. Qualsys categorises risks as follows; strategic, operational, change, compliance, people, product, service, financial, health and safety, documentation, supplier, information governance.

Staff are routinely trained in risk-based thinking, and this is encouraged in their daily routine.

A risk-based approach to processes, procedures and change management is also encourage.

It is the responsibility of Qualsys staff to follow the guidance outlined in this document and it is the responsibility of the Qualsys Management team to enforce the guidance.

Qualsys is risk averse. There may be occasions where risks with a higher score have to be accepted. This will be on a case by case basis and will require sign off by the Board before being able to be approved.

A live risk assessment can be found in our internal Risk Manager system.

The risk management system aims to help the business achieve its objectives and goals.

2. Our risk management process

Our approach to managing risk and opportunity

Establishing the Context
This relates to defining the external and internal parameters such as Operational Risk, Product or Service Risk, Financial Risk, Health and Safety, Information Governance etc. to be taken into account when managing risk criteria for the risk management context.

Risk Assessment
This relates to the overall process of Risk Identification, Risk Analysis and Risk Evaluation.

Risk Identification
This refers to the process of finding, recognising and describing risks.

Risk Analysis
This refers to the process by which the nature and level of risk are determined.

Risk Evaluation
This refers to the process of comparing the results of the risk analysis against the risk criteria in order to determine whether the level of risk is acceptable or not.

Risk Treatment
This relates to the process of modifying the risk.

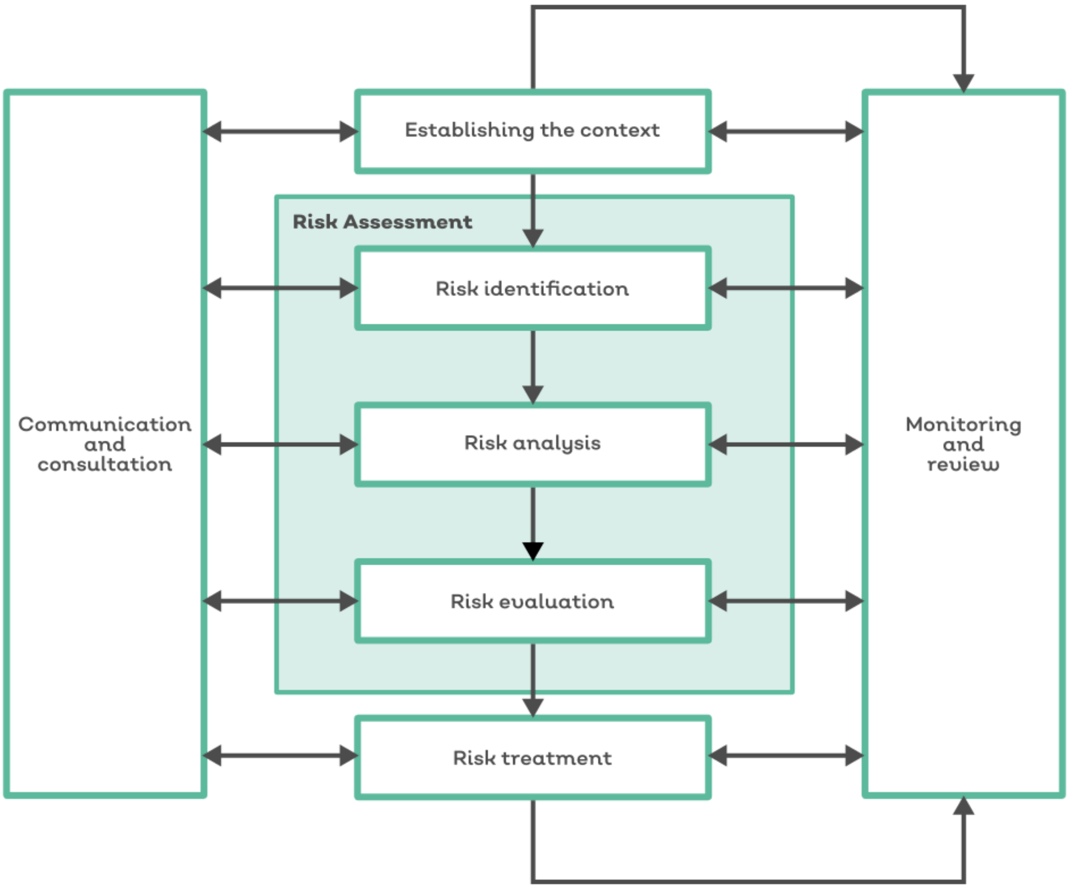
Monitoring and Review
To monitor means to supervise and to continually check and critically observe. It means to determine the current status and to assess whether or not required or expected performance.

A review is an activity. Review activities are carried out in order to determine whether something is a suitable, adequate, and effective way of achieving established objectives.

Communication and Consultation
Communication and consultation is a dialogue between an organisation and its stakeholders. This dialogue is both continual and iterative. It is a two-way process that involves both sharing and receiving information about the management of risk. However, this is not joint decision making.

Once communication and consultation is finished, decisions are made and directions are established by the organisation, not by stakeholders.

Discussions could be about the existence of risks, their nature, form, likelihood, and significance, as well as whether or not risks are acceptable or should be treated, and what treatment options should be considered.



3. How to identify, communicate and manage risk

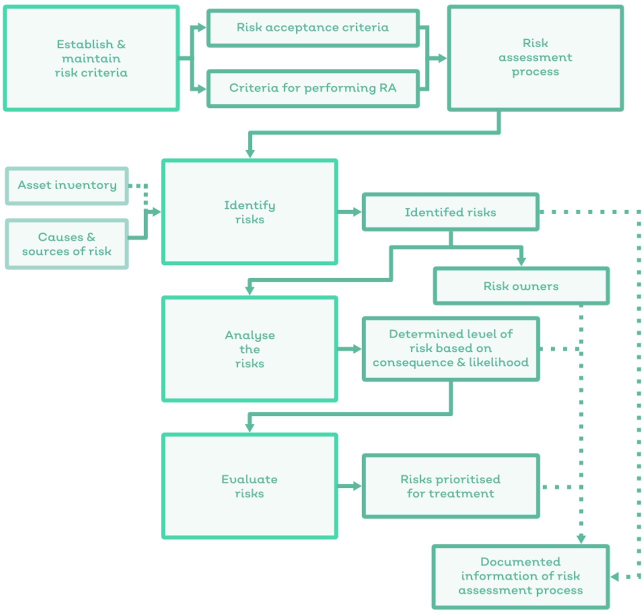
Employee roles and responsibilities to manage risk

Risk Manager is accessible for all employees to identify and manage risks.

A Risk can be identified by anyone; however, only departmental leads and the Quality Manager should complete the entries in the Risk Manager module. The Risk Suggestion functionality is used.

Qualsys will be using the Risk Assessment Types functionality in Risk Manager; i.e. Net, Gross and Target Assessments.

The following fields will need to be completed:
Risk Type – This is the type or 'category of Risk' such as Environmental, Health and Safety or Infrastructure.
Name – This is the risk name; please use the name of the asset at risk and the risk itself. e.g. 'Technical Director – Long term Loss'.
Description – Please provide a description of the risk that is being logged. This is to aid in the understanding of the Risk and its implications. This relates to the Risk column on the Risk Assessment spreadsheet.


Establish & maintain risk criteria
Risk acceptance criteria
Criteria for performing RA
Risk assessment process
Asset inventory
Causes & sources of risk
Identify risks
Identifed risks
Risk owners
Analyse the risks
Determined level of risk based on consequence & likelihood
Evaluate risks
Risks prioritised for treatment
Documented information of risk assessment process

Impact Description – This relates to the impact of the risk if it did occur; e.g. for Slips and Trips the impact may be 'injury', 'time off work' and 'lawsuits'. This relates to the Impact column on the Risk Assessment spreadsheet.

Asset Under Threat – This relates to what assets are at threat from this risk; e.g. Personnel or Staff would be the asset under risk from trips and falls. Multiple assets can be chosen if appropriate.

Owner – This will automatically default to whomever is inputting the Risk, however it can be changed. When transcribing the from the spreadsheet, the Owner should be the Quality Manager. Thereafter the Owner should be the departmental lead that the Risk has been logged by. This may get changed during the Risk Management life cycle to the person applying the mitigating controls for example.

Group Owner – this relates to the permission group that the Risk falls under. This can be left blank for the time being.

Likelihood – This relates to how likely the risk is to occur.

Impact – This relates to the impact of the risk on the asset or the company, if it does indeed occur.

Detectability – This relates to how detectable the risk is before it occurs; would there be any warning of the risk occurring? (currently not used).

The risk should now be saved.

In the ‘Reason for Assessment’ box, enter a reason for the assessment and the proposed Controls. E.g. Target assessment as if we applied the following controls…’.

Complete the assessment - Add the controls under the Controls Tab and add a Journal entry to summarise what has been done, who has been passed what Controls to action and proposed time frames.

As the Controls are received back, new Net Assessments should be undertaken (ensuring the Controls are added under the Controls Tab and Journal entries added) until the Risk Score is of an acceptable level. Please note that this may mean that not all of the Controls are needed.

However, after all of the proposed Controls have been received and are in place, the Net Assessment may still not of an acceptable level. In this instance a new Target Assessment should be carried out, proposed Controls detailed and the process above repeated.

Once the Level of Risk is Green then the Risk can be ‘Approved’.

When it comes to review the ‘Approved’ Risk a new version should be created, and Assessments carried out. Initially this would be a Net Assessment and then Target and further Net Assessments as necessary. The year should be added to the Risk Name.

As with our other software modules, any relevant documents and asc. items can be added to the Risk record.

4. How we analyse and evaluate risk

Our approach to addressing, controlling and treating risk

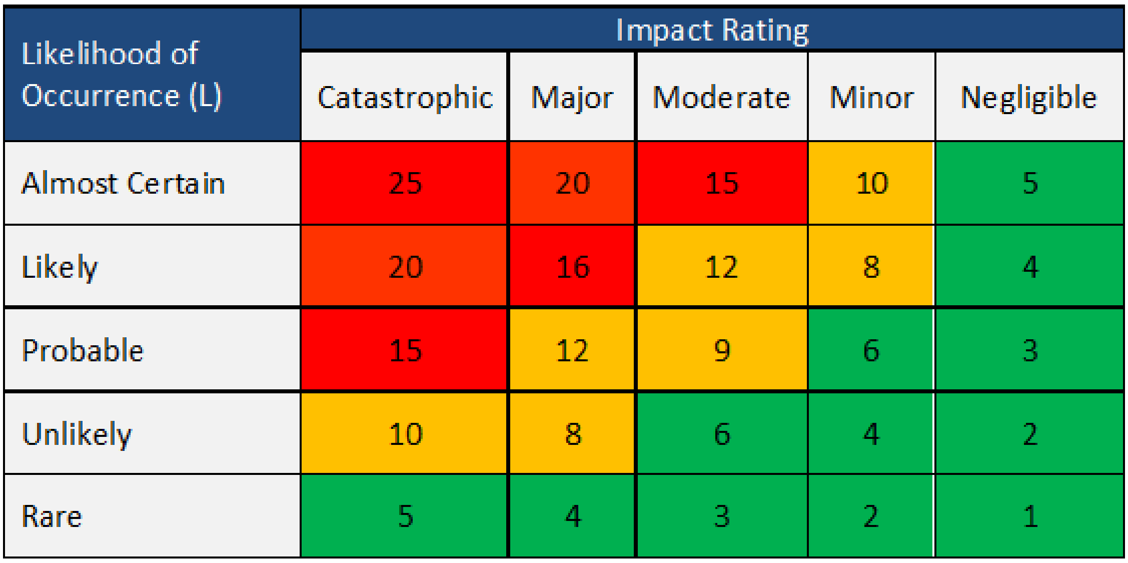
The following tables are intended to provide guidance on the likelihoods, impacts and treatments relevant to Qualsys Risk Assessments.

The aim is to bring the Risk Level to an acceptable level. Those values in Green are considered to be acceptable levels of Risk.

Qualsys is Risk averse There may be occasions where risks with a higher score have to be accepted. This will be on a case by case basis and will require sign off by the Board before being able to be approved.

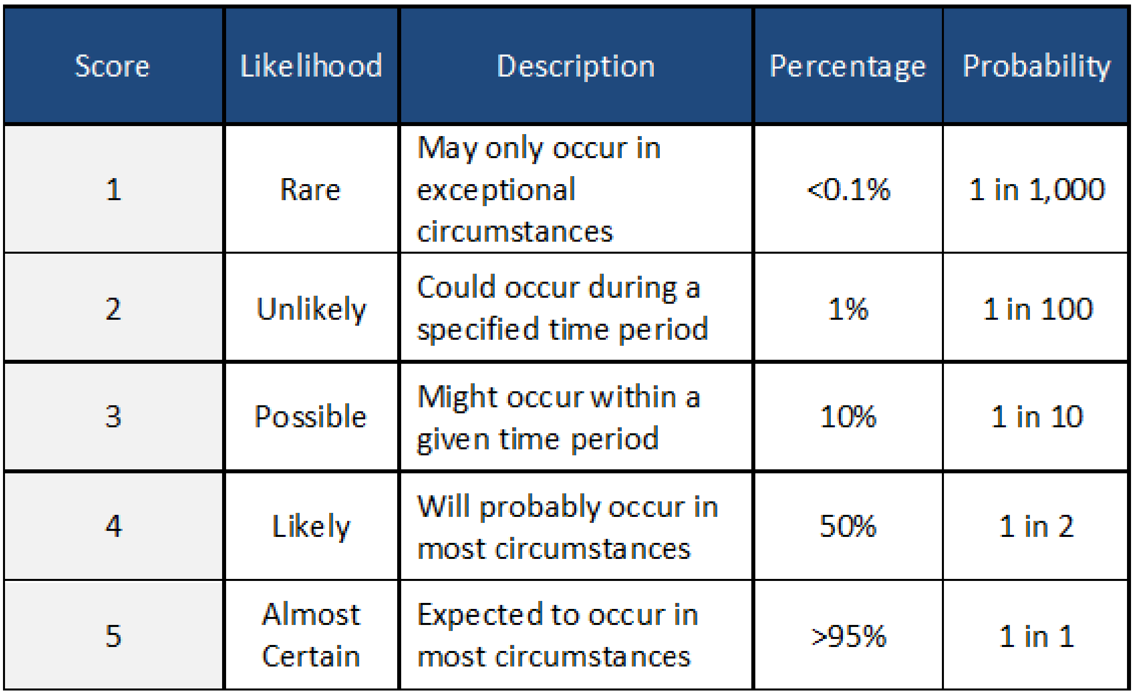
In general, Qualsys is Risk averse. The scores below are reflected in QF125 and QQMS Risk Manager.

Risk Scores and Tolerance:



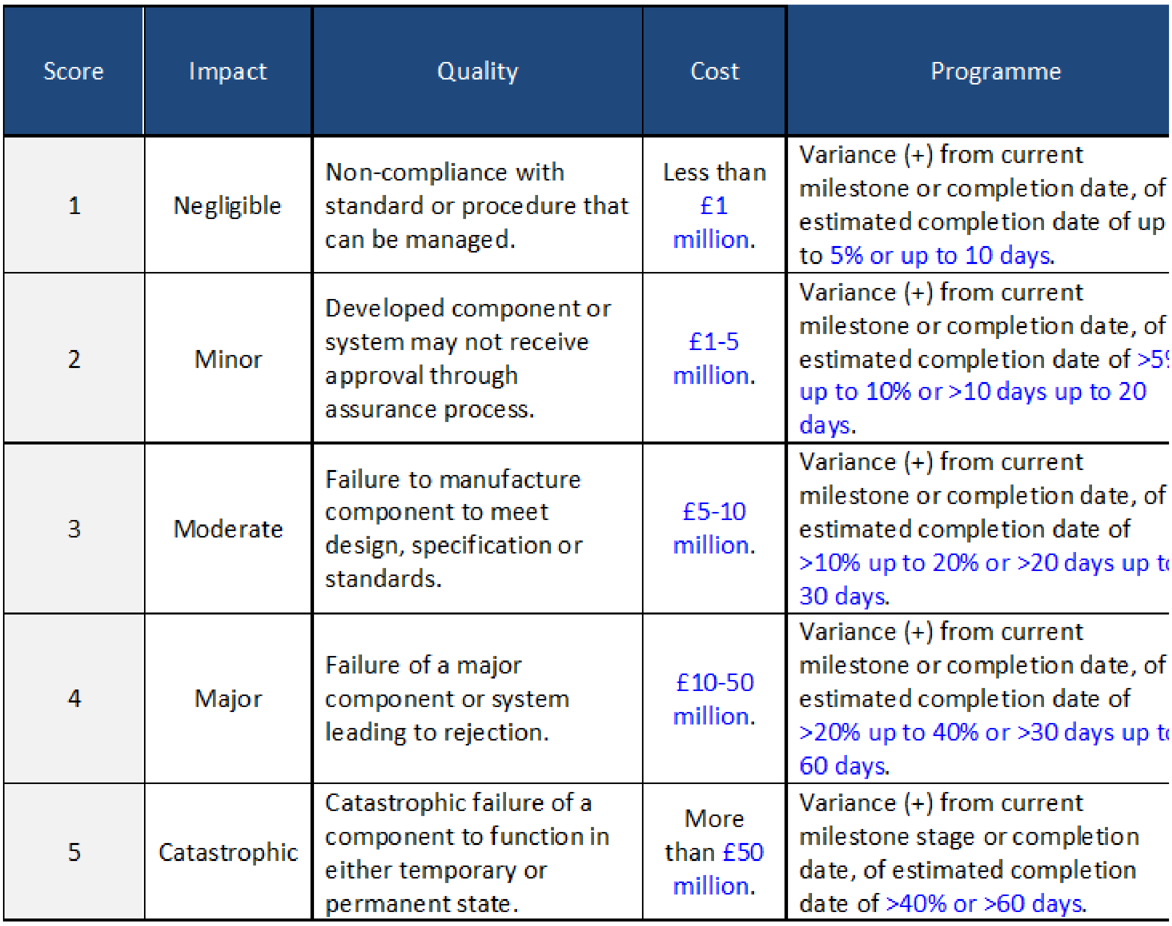
Likelihood of Occurrence (L)	Impact Rating				
	Catastrophic	Major	Moderate	Minor	Negligible
Almost Certain	25	20	15	10	5
Likely	20	16	12	8	4
Probable	15	12	9	6	3
Unlikely	10	8	6	4	2
Rare	5	4	3	2	1

Likelihood

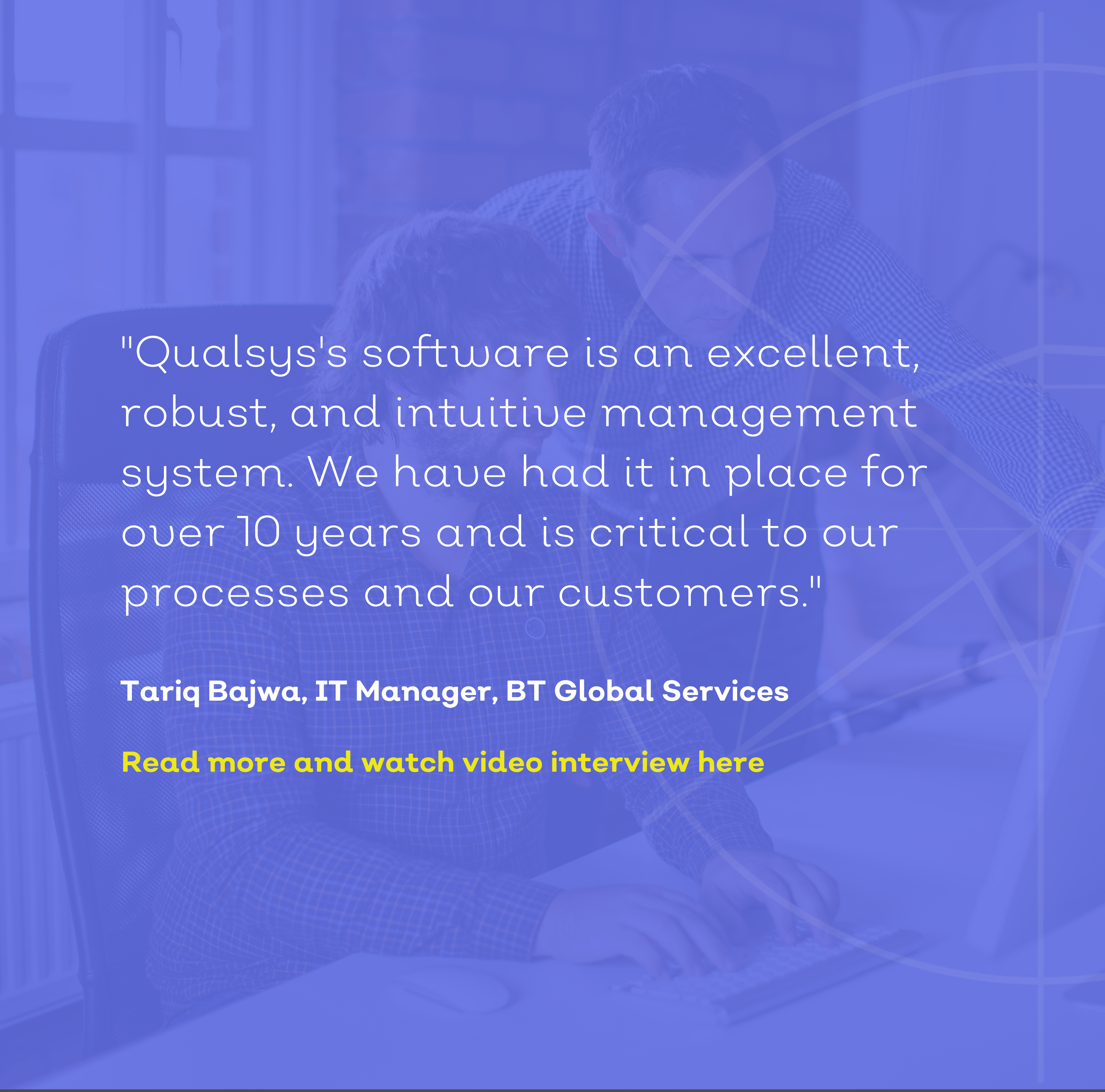


Score	Likelihood	Description	Percentage	Probability
1	Rare	May only occur in exceptional circumstances	<0.1%	1 in 1,000
2	Unlikely	Could occur during a specified time period	1%	1 in 100
3	Possible	Might occur within a given time period	10%	1 in 10
4	Likely	Will probably occur in most circumstances	50%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

Impact assessment:



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 t 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 t 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.



"Qualsys's software is an excellent, robust, and intuitive management system. We have had it in place for over 10 years and is critical to our processes and our customers."

Tariq Bajwa, IT Manager, BT Global Services

Read more and watch video interview here

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

Questions about our risk management policy? Talk to us today.

Qualsys