Risk Management Governance

Main Title:	Risk Management Governance		
Date:	23/07/2016	**Release Maturity:**	Draft/Live/Final
Author:	Allen Woods		
Owner:	Allen Woods		
Client:			
Version:	2,00		
CADMID	Through Life		
Line of Development	Doctrine		
Organisation			
Release Classification	U		
Visibility	All		
Access	All		
Archive Life	5 Years		
Document ID/Number			

Note: This document is only valid on the day it was printed

Revision History

Date of next revision:

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
29/01/2019	N/A	Include risk velocity and three point estimation	

Approvals

This document requires the following approvals. A signed copy should be placed in the project files.

Name	Signature	Title	Date of Issue	Version

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version

References

Internal

Ser	Description	Location
1	On line risk register	Left click here
2	Privacy Policy	Left click here
3	Document Management Policy	Left click here
4	Product Portfolio	Left click here
5	Risk Management High Level Process	Left click here
6	Risk Management Portal Page	Left click here
7	The Company Policy and Governance Framework	Left click here
8	Risk Management and Reporting Slide Deck	Left click here
9	Risk a bit of an explanation MP4 video	Left click here

External

Ser	Description	Location
1	HM Treasury Orange Book	Left click here
2	ISO 310000	Left click here
3	US DoD CMMC	Left click here

Location Details

Original Path on Development
C:\tlmpDocuments\tlmp\02 Mission and Objectives\20 Risk Management\
TLMP Folder Location
C:\tlmpDocuments\tlmp\02 Mission and Objectives\20 Risk Management\

Statement of Copyright

The Old Geeks Shed

9Wahtley Drive, Pewsey, Wiltshire. SN5 AR

Tel: 07780 568449

Email: woodsa200@gmail.com

Skype: apw808

Contents

About the Author

In order to decide for yourselves the experience of the author in respect of whether or not to take this document seriously, the

- *Allen Woods, recently retired.*
- *Ex British Army (1971 – 1995) Taught Arctic Warfare, Several Years On Operations, Funded Himself through College to Study IT*
- *Chartered Member of the British Computer Society for 20 years*
- *Member of the Chartered Status Interview Panel for BCS*
- *In 2010, Finalist of UK "Developer Of The Year" Competition for HSIS*
- *Primarily Employed in UK Defence Supply Chain and Logistics IT since 1995 until 2019*
- *Credits: MoD Health and Safety Information System, Various Internal to Defence P&G Portals, CATMIS, IQB Oversight to Defence Voyager Programme IM Transformation*
- *In respect of contract examination, as part of a major due diligence exercise the author was part of a team, the aim of which was to examine the licence terms, as a matter of contract validation, of 20 major systems, each with an annual maintenance fee in the high 6 low seven figure expenditure range.*

It is a wide and varied range of work experience covering some 30 years in total. In many ways the author was lucky in that he started working in IT when the PC's were beginning to proliferate and along the way was given the chance to work on a wide variety of tasks. A common theme through them all was legal compliance in one form or another.

His by line is "How the hell did that happen" which is appropriate not least because along the way he has made more than his fair share of mistakes and one of the sub plots of the pack that this document forms part, is that it seems to the author that much is having to be relearned. Above all, this document and the pack is an attempt to help. Particularly non-technical people understand some of the technical complexity they are using almost without thought it seems.

None of this is simple. Even writing this document was a complex task.

This page can be removed as it does not form part of the template

Read This First

One of the problems with risk management is knowing how to define the concept of risk. This document and associated supporting material is based on the definition set out below:

"Risk is emergent and therefore unpredictable in terms of final impact (whether it is detrimental or beneficial), it is a key change driver in that risks must be monitored in order to plan mitigation to compensate for any potential risk. Planning mitigation implies the need to identify capability shortfalls and to address them. Risk is also therefore a key performance indicator.

Risk remains emergent until it becomes an event that ***must*** *be dealt with if the event has an impact on the viability of the organisation as a system"*

Risk is lifed.

This document is about risk monitoring and the policy and governance required to manage risk expectations.

Risk is also multi-dimensional and multi-perspective (see figure 3 on page 11) as, risk in one area of activity in the organisation may well impact other areas as part of any event fall out. Risk management and monitoring crosses organisation form function and purpose and may influence multiple lines of development.

Risk and its monitoring is also a key performance indicator.

This document should be treated as a pathfinder, its structure being key rather than the content as content must be tailored to your organisation's specific situation, nevertheless the content contained here is a viable framework for planning risk management.

Its origins lie in the authors experience providing an online risk register for the first UK MoD FLIS Project Management Office which was responsible for the co-ordinated planning of the information management architecture of an £800m programme of work stretching over many years. The risk register presented here was used in the first few years of the programme and was written entirely by the author.

This document is designed to "fit" into the vocabulary and structure of an ISO 27k regime which forms part of the concept of "through life acquisition".

All text in red can be reviewed and removed if desired, the key is the document structure. This document should be treated as "pathfinder not gospel" and be tailored to fit your own organisations needs.

Purpose of this Document

This document sets out the risk management policy of The Performance Organisers (TPO).

Mandate

This document is mandated by the Risk Management Board and sets out the terms and conditions under which risk monitoring, seen as key to the maintenance of the organisation and its viability, is executed.

The Chairman of the Risk Management Board is directly responsible for ensuring that the risk management and monitoring regime set out here is both understood and followed by the organisation.

Sensitivity

Risk monitoring and mitigation is a strategic issue that impacts directly on the ability of the organisation to maintain its viability. Risk reporting is therefore highly sensitive and while the promotion of risk management is seen as an essential planning activity, it should be noted that the results of risk monitoring and mitigation may themselves be commercially sensitive.

Background

Risk is present throughout an organisation, in its buildings, equipment, policies, systems, processes, staff, and visitors. The company recognises that the management of risk is vital to good management practice. It must be an integral part of all the functions and activities of an organisation.

The purpose of the company's Risk Policy is to develop a consistent approach towards the management pf risk across the company and outline processes for recognising, analysing and dealing with risks as well as assuring the effectiveness of the identified processes.

This Risk Policy is designed to enable the company to minimise the frequency and effect of adverse incidents arising from risks and to identify improvements in procedures and service delivery in order to ensure the efficient and effective use of the company's assets.

The management of risks includes the culture, processes and organisational structures, which contribute to the effective management of potential opportunities, threats and adverse incidents.

Definition of Risk

For the purpose of this document the definition of risk is set out below:

Risk is a possible event, both internal and external that may have an impact on the viability of the organisation as a system that may be detrimental and put the viability of the organisation in danger. However, risk may be beneficial in that ignoring something that may be useful to the organisation and failing to adopt it, may also be detrimental to the organisation's viability.

The nature of risk impact cannot be accurately determined until something identified as a risk becomes an event that directly impacts on the organisation.

As a consequence, risk management consists of four core activities:

- *The monitoring of risk maturity, taking into account that maturity has velocity that tend to increase as a predicted risk approaches its "event horizon".*
- *The planning of any mitigation effort to offset or take advantage of any potential risk.*
- *The planned acquisition of new or additional capabilities (skills and resources) required to offset risk impact.*

- *The co-ordination of risk mitigation effort given that each part of the organisation will have its own perception of what is “risky” and it is the case that quite often there will be a balance to be struck in respect of the effective form of risk mitigation to be applied.*

The definition of risk set out above is organisation policy and will guide all risk planning and mitigation efforts.

Risk management is both a strategic issue and one of day to day operational significance and should be treated as such.

Risk Management Statement of Intent

The company accepts that total elimination of risk while desirable is not achievable. Nevertheless, the expects all staff to take all reasonable steps identify and report risk issues and where possible suggest a mitigation approach. The level of risk accepted should be commensurate with any expected reward balanced by costs and effort involved in mitigation efforts. In overall terms the company is looking to achieve a balanced risk portfolio at the company level with net risk averaging out at “medium” using the scoring system illustrated within section 5.

The following key principles outline the company’s approach to risk and internal control:

The Board of Directors has responsibility for overseeing risk management within the Company as a whole;

The approach adopted to identifying and mitigating risk is an open one, receptive to input from all Directors and staff at all levels;

The Risk Management Board supports, advises and implements policies approved by the Board of Directors

The company makes conservative and prudent recognition and disclosure of the financial and non-financial implications of risk;

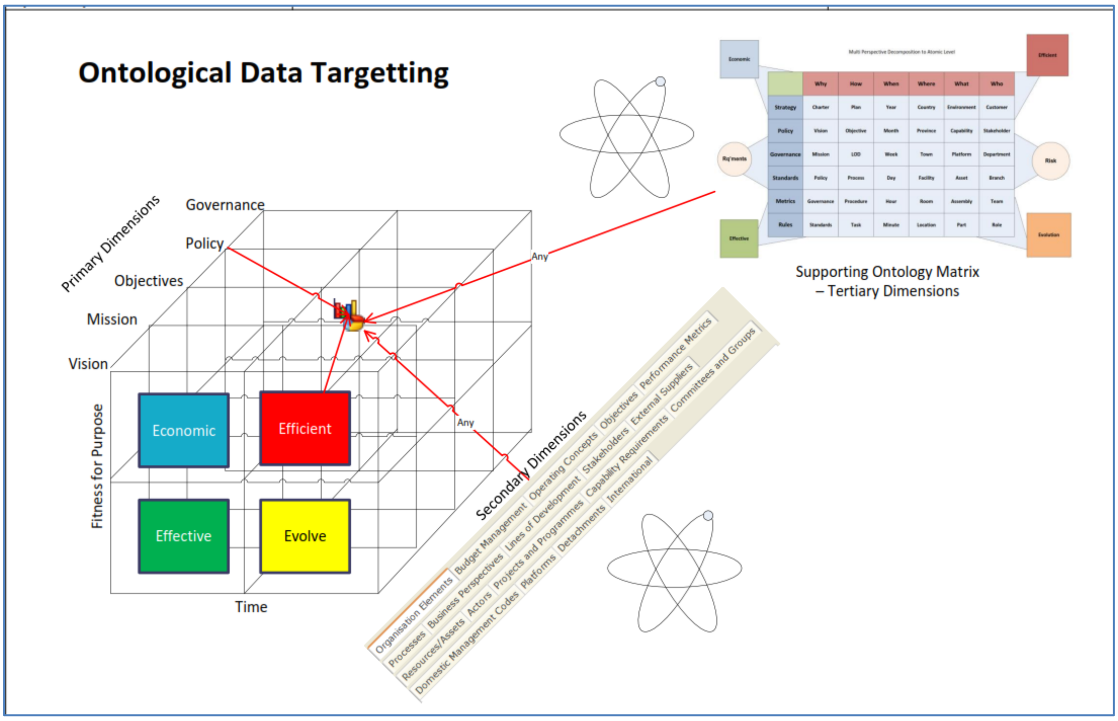
Significant risks will be identified and monitored on a regular basis using the company risk register;

Risks will be identified through the management and executive Governance structures and will be managed at a variety of different levels of the Company;

The company will adopt standard reporting processes and frameworks.

Ser	**Description**	**Location**
1	On line risk register	Left click here
2	Privacy Policy	Left click here
3	Document Management Policy	Left click here
4	Product Portfolio	Left click here
5	Risk Management High Level Process	Left click here
6	Risk Management Portal Page	Left click here
7	The Company Policy and Governance Framework	Left click here
8	Risk Management and Reporting Slide Deck	Left click here
9	Risk a bit of an explanation MP4 video	Left click here

The table above lists the organisations key risk management documents.



	Why	How	When	Where	What	Who
Strategy	Charter	Plan	Year	Country	Environment	Customer
Policy	Vision	Objective	Month	Province	Capability	Stakeholder
Governance	Mission	LOD	Week	Town	Platform	Department
Standards	Policy	Process	Day	Facility	Asset	Branch
Metrics	Governance	Procedure	Hour	Room	Assembly	Team
Rules	Standards	Task	Minute	Location	Part	Role

Figure 1 - Multi dimensional Muti Perspective Risk Reporting and Analysis

Scope

Categorising risks as either Preventable, Strategic and External risks helps managers consider why the risk is occurring and what can feasibly done to mitigate the risk. The definition of the categories as well as mitigation tactics are set out below:

Preventable risks represent the majority of risks faced by the company; they originate internally from failure ensure or prevent particular behaviours. There is rarely, if ever, a benefit to the Company of tolerating a preventable risk. Preventable risks should be mitigated against using a rules or process approach to promote or prohibit behaviours. Failure to manage these risks might feasibly lead to loss of reputation or even prosecution. Examples of preventable risk include fraud or failure to follow process.

Strategic risks are more acceptable and recognise that pursuing one strategic direction over another incurs risks (including opportunity risks). These risks should be managed through reducing the probability of the risk materialising or managing or containing the impact should it occur. In order to test the assumptions strategy risks they require greater levels of discussion and challenge than preventable risks.

External Risks Refers to those risks that are foreseeable by the Company, but are outside of its control in that the company can plan mitigation but cannot prevent. For example, legislative changes which can be monitored, will have some impact, but cannot be prevented from happening.

These risks should be managed though identifying and assessing the foreseeable risks and planning how the impact could be mitigated should they occur. They can be difficult to spot and as a result often fall into the "black swan" category and encompass natural or economic disasters, geopolitical or environmental changes or strong moves by competitor organisations. Scenario planning based on the outcomes of a PESTLE analysis or even assigning staff to consider the Company’s vulnerability to disruptive technologies or competitors can also help to identify external risks. An example of an external risk would be a change to legislation on, or regulation of, student visas.

Key Legislation

Risk management is not a formally regulated activity, it is however referred to in major legislation (the UK DP 2018 Bill, EU GDPR, Health and Safety at Work Act etc) as a key reporting action to be supported in respect of dealing with emergence and its potential impact on organisation viability.

Key legislation that the organisation must consider is available form the Legislation librarian built into the organisation portal. Accompanying each piece of legislation is a quality assurance review questionnaire which will be used for related quality assurance purposes from which legislative risks can be identified.

The organisation has studied and reviewed a number of risk management approaches and have elected to follow and apply the risk management principles and guidelines set out in the UK HM Treasury “Orange” book (see external reference 1). The Orange book was chosen because, by definition, that would mean the implementation and maintenance of a risk management regime that was consistent with UK Government best practice.

Annex C provides a list of key legislation the organisation is obliged to comply with.

Associated Standards

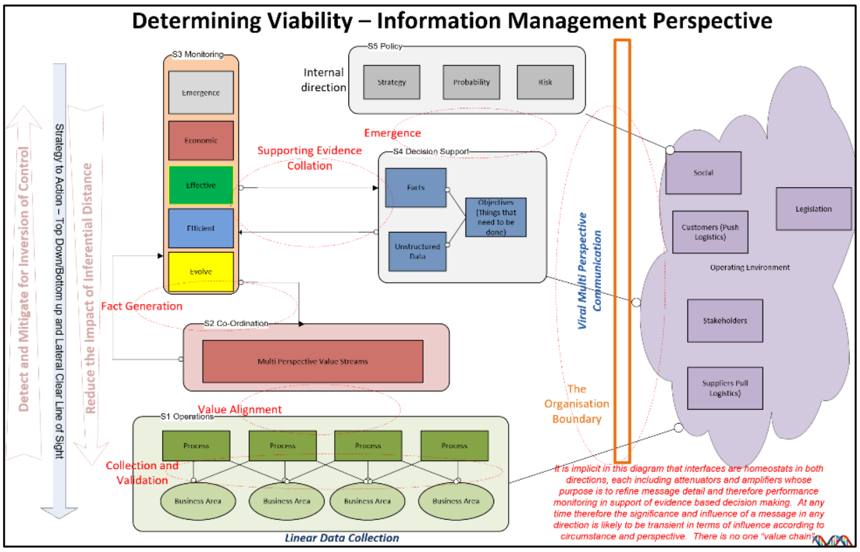

Determining Viability – Information Management Perspective
Detect and Mitigate for Inversion of Control
Strategy to Action – Top Down/Bottom up and Lateral Clear Line of Sight
Reduce the Impact of Inferential Distance
S3 Monitoring
Emergence
Economic
Effective
Efficient
Evolve
Internal direction
S5 Policy
Strategy
Probability
Risk
Emergence
Supporting Evidence Collation
S4 Decision Support
Facts
Unstructured Data
Objectives (Things that need to be done)
Fact Generation
S2 Co-Ordination
Multi Perspective Value Streams
Value Alignment
S1 Operations
Process
Process
Process
Process
Collection and Validation
Business Area
Business Area
Business Area
Business Area
Linear Data Collection
Viral Multi Perspective Communication
The Organisation Boundary
Social
Legislation
Customers (Push Logistics)
Operating Environment
Stakeholders
Suppliers Pull Logistics)
It is implicit in this diagram that interfaces are homeostats in both directions, each including attenuators and amplifiers whose purpose is to refine message detail and therefore performance monitoring in support of evidence based decision making. At any time therefore the significance and influence of a message in any direction is likely to be transient in terms of influence according to circumstance and perspective. There is no one "value chain"

Figure 2 - Risk and Emergence

The risk governance regime presented here is based on the core risk management standards set out below. These standards have been chosen by dint of the authority and reputation of those organisations promoting them. They are to be followed by all members of the organisation who are looking for appropriate guidance,

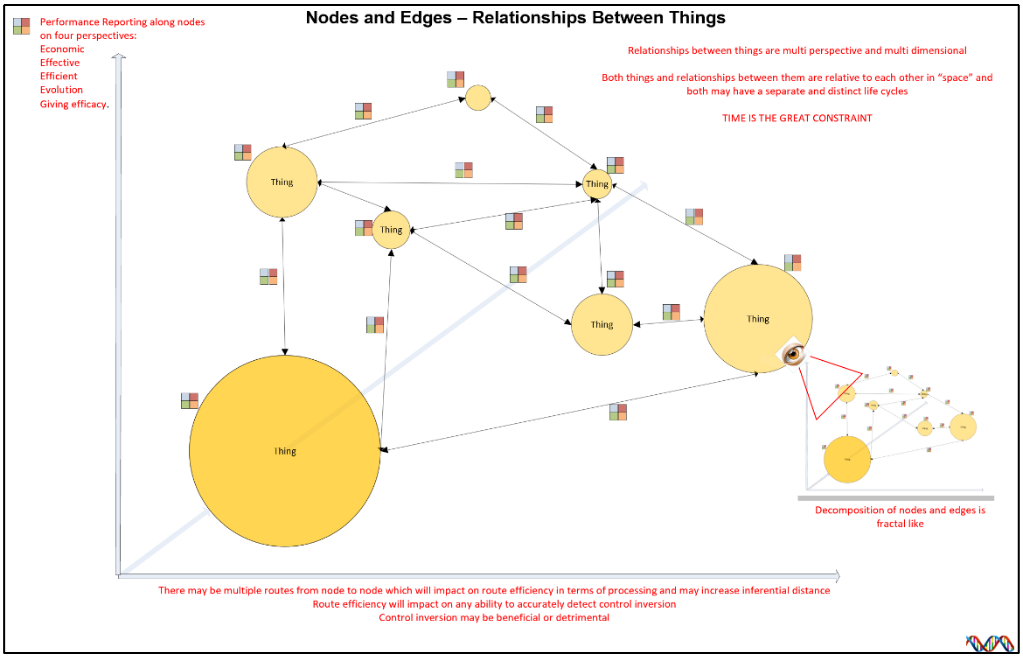
The Risk Manager will promote these standards below where the opportunity arises

Ser	***Description***	***Location***
1	*HM Treasury Orange Book*	*Left click here*
2	*ISO 310000*	*Left click here*
3	*US DoD CMMC*	*Left click here*

Business Intelligence Gathering

Key to successful risk management is the ability to gather accurate and reliable business intelligence both internal (an accurate description of how the organisation works and any anomalies therein), external (market assessments, legislation and more). The organisation recognises the importance of business intelligence gathers and has at its disposal, the following information gathering capabilities as features of its internal information management portal:

- *A digital mpa of the organisation containing an organogram, objective catalogue, process catalogue and more, integrated on the basis of the application of "graph theory"*
- *An online risk register.*
- *An online legislation librarian which contains a searchable copy of all primary legislation that impacts the organisation.*
- *An online internal compliance audit system used as part of the organisations quality assurance programme.*
- *An online performance metric catalogue, which is underpinned by various scoring techniques.*
- *An on line document management library that also contains a corporate dictionary/lexicon.*
- *An active copy of the UK Company register used to monitor performance of competitors in our organisation SIC code grouping.*
- *Copies of all relevant UK Government statistics incorporated into the information management portal as appropriate.*
- *Digital maps of the UK (and elsewhere) accurate to within 30ft.*



Nodes and Edges – Relationships Between Things

Performance Reporting along nodes on four perspectives:
Economic
Effective
Efficient
Evolution
Giving efficacy.

Relationships between things are multi perspective and multi dimensional

Both things and relationships between them are relative to each other in "space" and both may have a separate and distinct life cycles

TIME IS THE GREAT CONSTRAINT

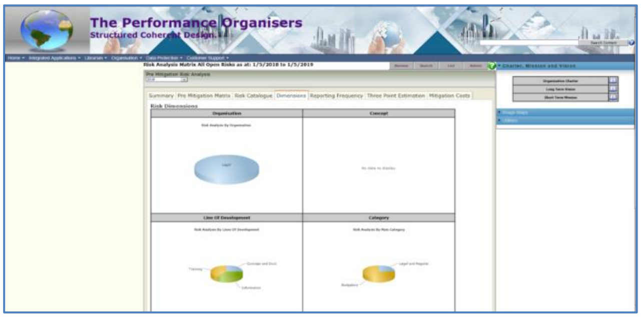
Decomposition of nodes and edges is fractal like

There may be multiple routes from node to node which will impact on route efficiency in terms of processing and may increase inferential distance
Route efficiency will impact on any ability to accurately detect control inversion
Control inversion may be beneficial or detrimental

Figure 3 – Time and Relative dimensions in space

All of which are designed, as a matter of architectural principle, to be capable of being cross referenced with each other. A full list of the information management facilities the organisation has at its disposal can be viewed here. Those involved in risk monitoring across the organisation are invited to make use of them all as a matter of routine confirmation of their research.

Muti Perspective Risk Analysis



Risk Analysis Matrix All Open Risks as at: 1/5/2018 to 1/5/2019

Figure 4 - Multi perspective analysis

The business intelligence tools referred to above support multi perspective risk analysis. For example, the use of the quality assurance audit toolkit can give the means to identify assurance shortcomings on the basis of a report, or series of reports on a given organisation element, or on the basis of common scoring issues across individual questions in any given QA audit question bank. The same multi perspective analysis capability is offered by the Performance Metric library which forms an integral part of the organisation portal.

Those managing risk in the organisation are encouraged to take advantage of the capabilities on offer, the Risk Manager will provide training and guidance to those interested in such matters.

Key Appointments and Roles

Overall responsibility for risk management within the company lies with the Chairman of the Board, with responsibility for implementation delegated to the Chair of the Risk Management Committee. Annex B of this document contains a schematic illustrating the positioning of risk management as an activity in the company management structure.

The company's Charter Statement requires Risk Management Committee to take reasonable steps to ensure that there are "sound arrangements for risk management, control and governance, and for economy, efficiency and effectiveness (value for money), within the company".

The appointment of a Risk Manager is mandated by the risk management policy document available here. The risk manager will be employed by the Vice President of Assurance as part of the company assurance programme. The Risk Manager will liaise and co-ordinate his or her activities with other VP Assurance subject matter experts with the aim of providing an assurance regime that follows best practice but avoids any conflict of interest.

The risk manager will manage the risk management departmental portal page which can be accessed by left clicking here. Annex B contains a schematic illustrating the managerial positioning of the risk manager.

The company's external ISO 9000 auditors have responsibility for assessing the effectiveness of risk management. The company's ISO 9000 Auditors report on the arrangements for risk management to the Board of Directors as part of its annual audit effort.

Corporate Governance

The Risk Management Committee is responsible for reviewing the effectiveness of internal control of the institution, based on information provided by auditors, senior management and the Director of Finance.

For each significant risk identified, the Risk Management Committee will:

Review the risk register and examine the institution's track record on risk management and internal control;

Consider the internal and external risk profile of the coming year and consider if current internal control arrangements are likely to be effective.

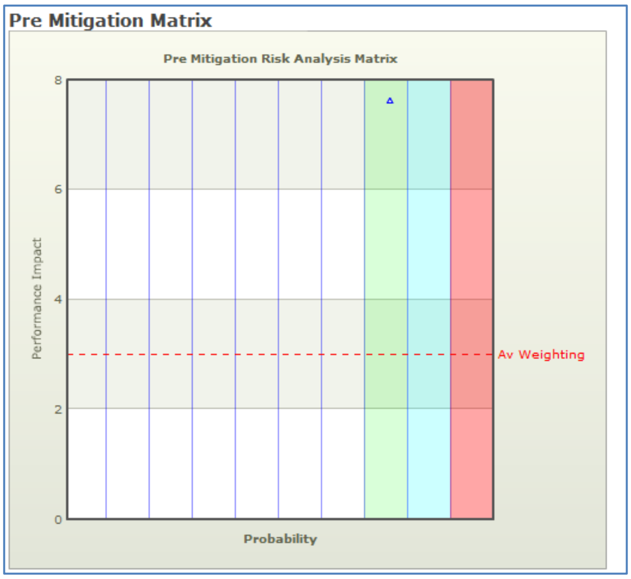


Figure 5 - Sample Risk Matrix

In so doing, the Risk Management Committee will consider:

Control Environment:

- the company's objectives and its financial and non-financial targets;
- organisational structure and calibre of the Senior Management Team;
- culture, approach and resources with respect to the management of risk;
- delegation of authority;
- public reporting.

On-going identification and evaluation of significant risks:

- timely identification and assessment of significant risks;
- prioritisation of risks and the allocation of resources to address areas of high exposure.

Information and communication:

- quality and timeliness of information on significant risks;
- time it takes for control breakdowns to be recognised or new risks to be identified.

Monitoring and corrective action:

- ability of the institution to learn from its problems.
- commitment and speed with which corrective actions are implemented.
- Monitor risk velocity and capability gaps

The Risk Manager will prepare an annual report of its review of the effectiveness of the internal control system annually for consideration by the Risk Management Committee, normally as part of the returns submitted to the shareholders as part of the company's annual statutory report portfolio. Additionally, the Rik Manager will prepare a briefing pack for delivery and presentation at each meeting of the risk management committee. The risk management committee will meet quarterly or, in exceptional circumstances, when the need arises.

Associated Policy

Annex A provides an illustration of the risk policy in respect of its position in the policy hierarchy. This risk policy document is mandated by the Chief Executive Officer to be applied across the organisation. The Risk Policy is, in terms of managerial significance, on a par with the company Privacy, Security, Assurance, Privacy and Document Management policies.

The need to comply with this policy will be written into task terms of reference of key employees.

Infrastructure Support

The company maintains a single on line risk register. The register records all business risks. Annex F provides an illustration of its architectural position and provides an indication that the risk log has an ethical assessment capability that stretches across core perspective boundaries.

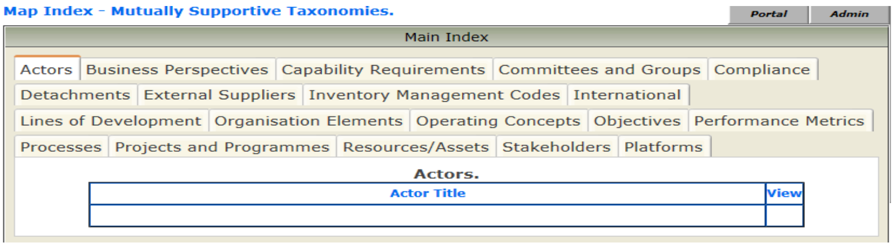
Each Department is required on a monthly basis to detail what they consider to be key risks, their gross score (pre mitigation), mitigating actions and the net risk score (post mitigation) on the risk register.

All risks must be specific (i.e. what it is a risk in relation to) and provide mitigating actions, and a date by which they will be implemented (or become embedded within core activities) and who is responsible for managing the risk. They must also indicate lead indicators, a change to which might signal a positive or negative moment in the Company's exposure to a particular risk.

Where the risk, mitigating actions or the assurance of mitigating actions has not changed, departments are required to indicate that they have reviewed the risk by entering the date of review. When reviewing risks they are responsible for. A commentary should be provided on the level of assurance that can be taken in the mitigating actions clearly stating that they are being implemented and are also effective.

Department Heads are responsible for the departmental section of the risk register but may delegate the maintenance of the register to another member of their staff.

Where appropriate, risks identified by Departments should be mapped to the lines of development and enablers supporting the organisation Strategy or the Business Plan.


Map Index - Mutually Supportive Taxonomies.

Actors.

Actor Title	View

Figure 6 - Risk Dimensions

Risk Scoring and Assessment

The risk register is an integral part of the company Quality Management System the aim of which is to deliver a consistent and coherent reporting capability across multiple perspectives and dimensions or views of the organisation form, function and purpose..

The on line risk register supports the alignment of risk log entries with the dimensions or perspectives of the company listed in Figure 3. this gives the added advantage of providing the means to filter and localise risk analysis effort across the organisation and at the same but do so in a way that avoids the “your numbers are not my numbers issue that often bedevils management reporting.

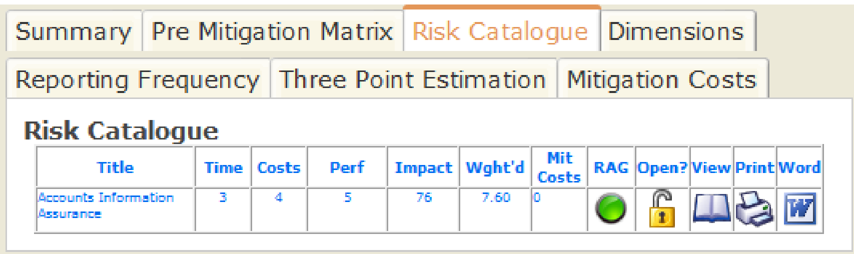
Members of the company Risk Management Committee and Project Sponsors are responsible for determining the impact of all risks for which they are responsible for, using the framework provided in 5.4 as a guide.

The assessment of the probability of a risk occurring is standard across the company:

Probability Score	**All Risks**
1	Highly unlikely to occur (< 20% probability)
2	Unlikely to occur (20% - <40% probability)
3	Likely to occur (40% - <60% probability)
4	Very likely to occur (60% - <80% probability)
5	Extremely to occur (> 80% probability)

Risks will be scored before and after mitigating actions and at each point of coring the total risk will be the multiple of the two elemental scores:

	Impact				
Probability	**1**	**2**	**3**	**4**	**5**
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5



Risk Catalogue

Title	Time	Costs	Perf	Impact	Wght'd	Mit Costs	RAG	Open?	View	Print	Word
Accounts Information Assurance	3	4	5	76	7.60	0	🟢	🔓	📖	🖨	W

Figure 7 - Sample Risk Catalogue

The online risk register provides a variety of means of displaying risk log entries. The simplest is the catalogue itself illustrated in figure 4 which is tabular in and sortable based on the final scoring systems set out above.

Determining Risk Velocity

key aspect of risk management is determining the nature of risk “velocity” by that it is meant the time it will take from a risk to mature to the point it becomes an issue that needs to be dealt with and that the A time period may increase or decrease depending on measurable factors and dimensions that will influence risk maturity.

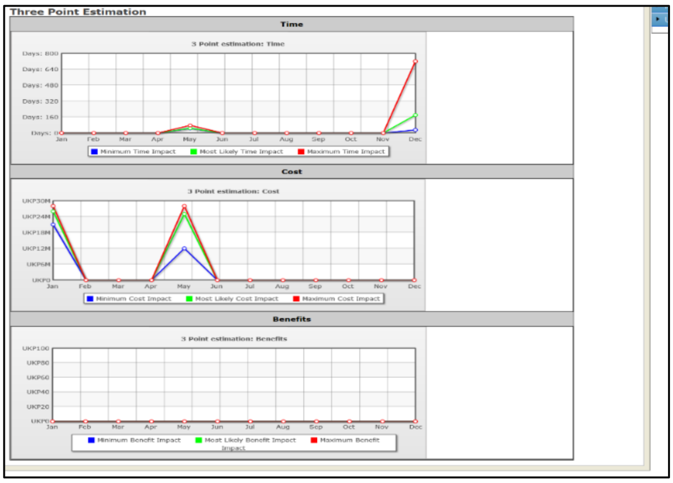


Figure 8 - Determining Risk Velocity

Recognising that, the company will use a “three point” estimation approach based on time, mitigation cost and mitigation benefits to measure changes in velocity in respect of when a risk matures to become an issue or event

In addition to the “three point” estimation technique set out here, an adaptation of the concept of engineering tolerances will be applied based on tracking of minimum, achievable mean and maximum values of the impact of mitigation efforts. The concept of tolerances providing the means to execute a gap analysis approach across all three measurement dimensions

It should be understood that the “three point” estimation and tolerances will be applied to each risk profile and updated as part of normal editing of each risk log entry The risk register therefore provides an historical record of risk maturity that can be accessed by any and all interested parties subject to the company security policy related to access control with each being given a summary score according to objective assessment of velocity with a reporting status of “1” indicating immediate impact as per the table below.

Impact	Financial	Quality	Time
1	Financial implications of the risk are **very low** and are comfortably within the ability of the risk owner to manage locally.	The impact on quality is **very low.** Risk occurring would represent a minor revision to planned outcomes.	The impact is **very low**. It will have little effect on timescales.
2	Financial implications of the risk are **low** (<10% of the budget or company turnover). It remains within any contingencies set.	The impact on quality is **low.** Risk occurring would may detract slightly from the desired quality of the outcomes.	The impact is **low**, It may delay one or more elements of the activity but not the overall timescale.
3	Financial implications of the risk are **medium** (10% - <25% of the budget or company turnover). It may exhaust or be larger than contingencies made but can be managed without additional funds.	The impact on quality is **medium.** Risk occurring would detract from the desired quality of the outcomes but not detract from the overall purpose of the activity.	The impact is **medium**. Overall timescale slightly extend but it is unlikely to materially affect desired outcomes.
4	Financial implications of the risk are **high** (25% - <50% of the budget or company turnover). It is not possible to meet the cost within the approved budget and further funding would be required.	The impact on quality is **high.** Risk occurring would significantly detract from the original desired quality of the outcomes and may reduce the viability of the activity as outcomes require revision.	The impact is **high.** Timescales greatly extended. Outcomes may be later than required in order to obtain maximum benefit.
5	The impact on finance is **critical** (>50%of the budget or company turnover). Increased cost would negate benefits of activity and may destabilise the reporting unit.	The impact on quality is **critical.** Risk occurring would reduce quality of desired outcomes to such an extent that it negates benefits of activity.	The impact is **critical.** Extended timescales mean that outcomes would be too late and negate benefits of activity

Risk Mitigation Planning and Monitoring

Mitigating actions are controls and actions taken to reduce the likelihood of a risk occurring, or to limit the impact of the risk. Risk exposure is the net risk after all mitigating actions or factors have been taken into account. The primary means of measuring risk mitigation is to make an estimate of the financial cost of any required mitigation efforts.

The risk register also captures:

The deadline for mitigating actions to be implemented (or embedded) by;

Leading edge indicators which may signal that a risk is increasing or decreasing in response to mitigating actions;

Assurance mapping so that Managers can demonstrate that mitigating actions are both being implemented as designed and delivering the desired effect. The assurance mapping can be used to further test the assumptions of risk owners.

The online risk register is also multi-dimensional and multi perspective in nature. Furthermore, each risk register entry can be referenced from any other application that supports hyperlinks and is connected to the company network. Finally, risk register entries can be downloaded, individually, into the company office automation software as fully formed risk reports.

The mix of mitigation reporting formats and views giving the means to assess mitigation impact on a multi dimensional basis.

Internal Control

The system of internal control is designed to manage and mitigate rather than eliminate the risk of failure to achieve policies, aims and objectives. It is based on an ongoing process to identify the principal risks to their achievement, to evaluate the nature and extent of those risks and to manage them efficiently, effectively and economically.

Related to significant risks are policies that among other things form part of the internal control processes of other parts of the organisation, particularly process owners.. The policies are approved by the Board of Directors and implemented by the Risk Management Committee.

Risk Management is addressed on a company-wide basis but individual Departments, and staff have an essential role in the identification, assessment, on-going monitoring and mitigation of risks. Departmental and professional planning documents should identify mitigating actions that will be taken to reduce significant risks.   In some cases, individual risks will be formally owned by a Departmental Senior Manager or Project Team Lead where the function concerned lies wholly or mainly within its remit.

Reporting arrangements through senior line management are designed to monitor key risks and their controls. Decisions to rectify problems are made by the member Director with responsibility for the risk, with reference to other staff and company committees and the Board of Directors as and where appropriate to do so.

The strategic planning and annual budgeting process is used to set key objectives in support of the 2020 work streams and enablers, agree action plans and allocate resources. Targets contained in the Departmental and Project Planning documents provide mitigating actions which are explicitly linked to risks faced by the company. The annual estimates (macro budget) presented to the Board of Directors contain an analysis of risks inherent in them and how these are mitigated.

Risks associated with major company projects will be managed through the appropriate project boards adopting project management methodologies such as PRINCE2 and have a distinct section within the risk management procedures document.

The Corporate section of the Risk Register is compiled by the Senior Risk Manager and reported to the Risk Management Committee to help facilitate the identification, assessment and monitoring of risks of significant importance to the company. The document is normally discussed monthly by the Risk Management Committee and presented to each meeting the Risk Management Committee. Emerging risks are added as required, and improvement actions and risk indicators are monitored on an ongoing basis through line management structures.

The Risk Management Committee is required to report to the Board of Directors on internal controls and alert it to any emerging issues. The Risk Management Committee oversees internal audit, external audit and management as required in its review of internal controls. The Risk Management Committee has responsibility delegated by the Board of Directors, for governance oversight of risk assurance, ensuring that the Risk Policy is appropriately applied. It directly monitors the management of the most significant risks to the company, as recorded in the Corporate Section of the Risk Register.

Internal audit is an important element of the internal control process. In addition to its programme of probity and value for money work, internal audit is responsible for aspects of the annual review of the effectiveness of internal control systems. The internal audit plan is guided by, but not limited to, the assessment of risks identified through the company’s risk management procedures.

External Audit provides feedback to the Risk Management Committee on the operation of internal financial controls reviewed as part of the annual audit.

Capability Gap Analysis

As risk velocity increases, so the nature of any capability gaps that may need addressing will require attention. Like risk velocity therefore there will be a need to monitor the performance of any and all parts of the organisation that may be affected if a risk becomes an event that affects operational efficacy. With that in mind, associated with each risk log entry will be a need, for evidence-based decision support purposes, to provide a performance reporting capability to the risk management committee. Each risk record in the register supports the alignment of performance indicators with risk profiles.

Performance Monitoring

Ser	Metric Title	Perspective	Link

As performance is affected either on a beneficial or detrimental basis it may be the case that new requirements may arise that will involve the acquisition of new capabilities which, of necessity, may need to be planned. It should be noted that new requirements may also be subject to development across the acquisition life cycle and may have dependencies across all of the lines of development as described using the acronym TEPIDOIL (LS). As a consequence as part of any capability gap analysis effort, each risk log entry may have associated requirement log entries which must be made available to the risk management board for prioritisation as risk velocity increases.

Requirements Catalogue

Ser	Requirement Title	Sponsor	Link

Quality Management and Compliance

Risk reporting is part of the quality management regime of the company. Specifically, risk management forms part of the regulatory compliance framework of the company for privacy, security and assurance matters. The risk log in particular is database driven and fully auditable with a risk history record being kept automatically by the risk register itself as changes are made to risk log entries.

Risk management is also subject to regular external audit as a part of the company ISO 9000 and ISO 27000 implementations to be carried out by the company external audit partners.

Training

The Risk Manager will be responsible for the development and implementation of a risk awareness and management training programme.

A draft risk management reporting theory slide deck is available and is referred to in the document references, or it can be downloaded here

Future Considerations

Nothing at this time.

Document Review Timetable

This risk policy document will be reviewed annually at least, the next review to take place on or about 23rd July 2019. In the event of the need to change the content of form of this document in the meantime, the Risk Manager will submit any proposals to the chair of the Risk Management Committee as and when circumstances demand.

Sponsorship

This risk policy is sponsored by the Chief Executive Officer and is actioned and maintained by the Vice President of Assurance. It is a mandated policy document and must be followed and applied by all company employees.

Document Sign Off

This document has been reviewed by the Project Manager and approved for inclusion in the project requirements catalogue.

Printed/Typed Name **Signature** **Date**

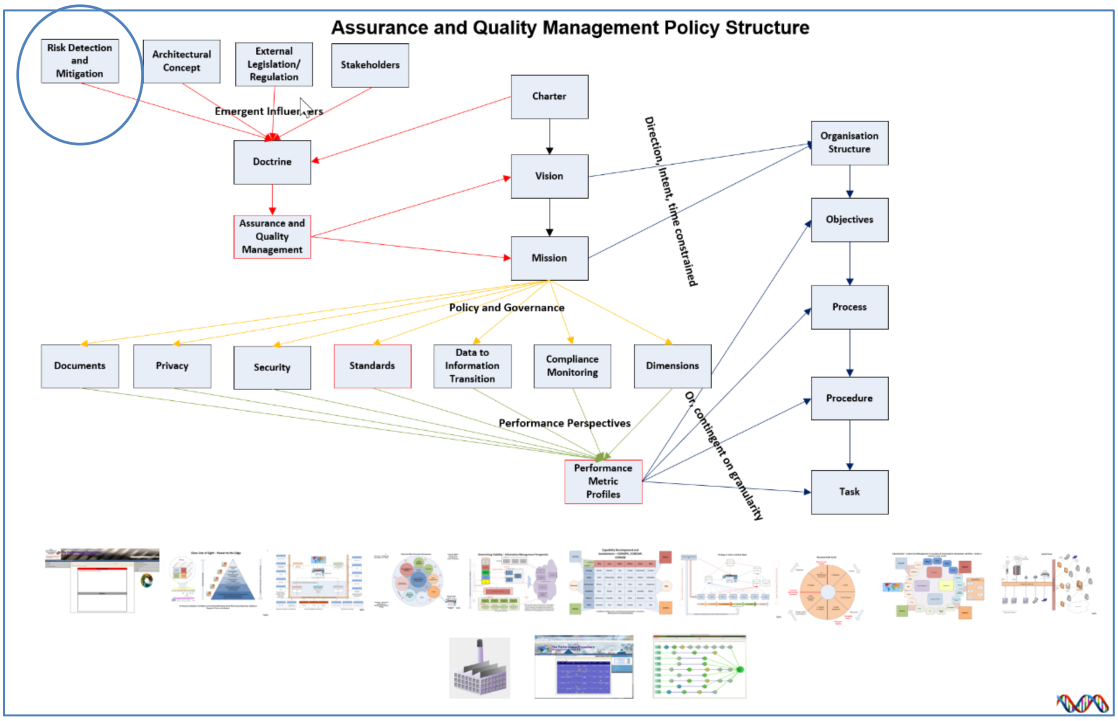
This document has been reviewed by the Quality Assurance Group and approved for use.

Printed/Typed Name **Signature** **Date**

This document has been reviewed by the Supplier Project Manager and approved for use by the Supplier Project Team.

Printed/Typed Name **Signature** **Date**

Annex A – Policy Scope Structural Context



Assurance and Quality Management Policy Structure

Annex B – Managerial Status

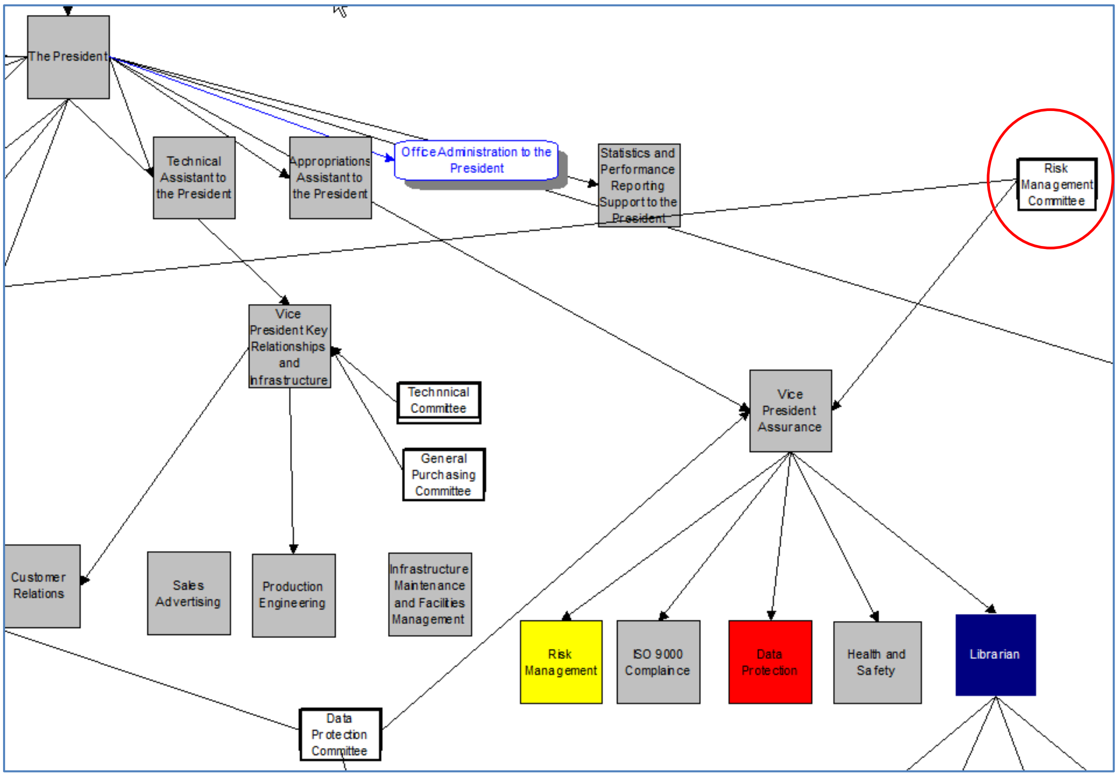

The President
Technical Assistant to the President
Appropriations Assistant to the President
Office Administration to the President
Statistics and Performance Reporting Support to the President
Risk Management Committee
Vice President Key Relationships and Infrastructure
Technnical Committee
General Purchasing Committee
Vice President Assurance
Customer Relations
Sales Advertising
Production Engineering
Infrastructure Maintenance and Facilities Management
Risk Management
ISO 9000 Complaince
Data Protection
Health and Safety
Librarian
Data Protection Committee

Figure 9 - Risk Manager Organogram

Annex C – Key Legislation

This annex provides a list, that is not exhaustive, that is to be used as a guide in respect of other UK legislation that will need interpretation in respect of GDPR compliance. In particular, the view of the Performance Organisers is that much of the defence in respect of the recording, storing and retention of personal data on the grounds of legitimate interest and contract is contained within such legislation.

This list will be subject to regular review by the company DPO and its legal representatives as the circumstances demand and where appropriate, those legislative articles that apply will be incorporated into this policy document.

Ser	Legislation Name
1	The UK Companies Act 2006
2	The UK Consumer Credit Act
4	The UK Sales of Goods Act
5	The Health and Safety at Work Act
6	The Value Added Tax Act
7	International Financial Reporting Standards
7	The UK Bribery Act
8	UK Commercial Law
9	UK Criminal Law

It should be noted that the United Kingdom Information Commissioner is also responsible for the monitoring and policing of the following statutory instruments which may, as a consequence, influence the content of this policy document.

Ser	Legislation/Regulation Title
1	Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)
2	Freedom of Information Act 2000 (FOIA)
3	Environmental Information Regulations 2004 (EIR)
4	Environmental Protection Public Sector Information Regulations 2009
5	Investigatory Powers Act 2016;
6	Re-use of Public Sector Information Regulations 2015
7	Security of Network and Information Systems Directive (NIS Directive);
8	Electronic Identification, Authentication and Trust Services Regulation (eIDAS)
9	Data Protection Act 2018 (DPA);
10	General Data Protection Regulation (GDPR)
11	The UK Data Protection Bill 2018

Annex D – Reading List

TPO is a software development company and as a consequence, the emphasis of risk management in the company is on the software development life cycle. The reading list produced here reflects that, but this list should be considered as part of the company reading list which is provided to support and explain the ethos the company applies.

Ser	Title	ISBN	Author
1	Information Risk Management	978-1-78017-265-1	David Sutton
2	Software Engineering Risk Analysis and Management	0-70-010719-X	Robert N Charette
3	CMMI guidelines for Process Integration and Product Improvement	0321154967	Mary Beth Chrissis, Mike Konrad, Sandy Shrum
4	HM Treasury Orange Book	N/A	Left click here

Annex E – Risk Log Architectural Position

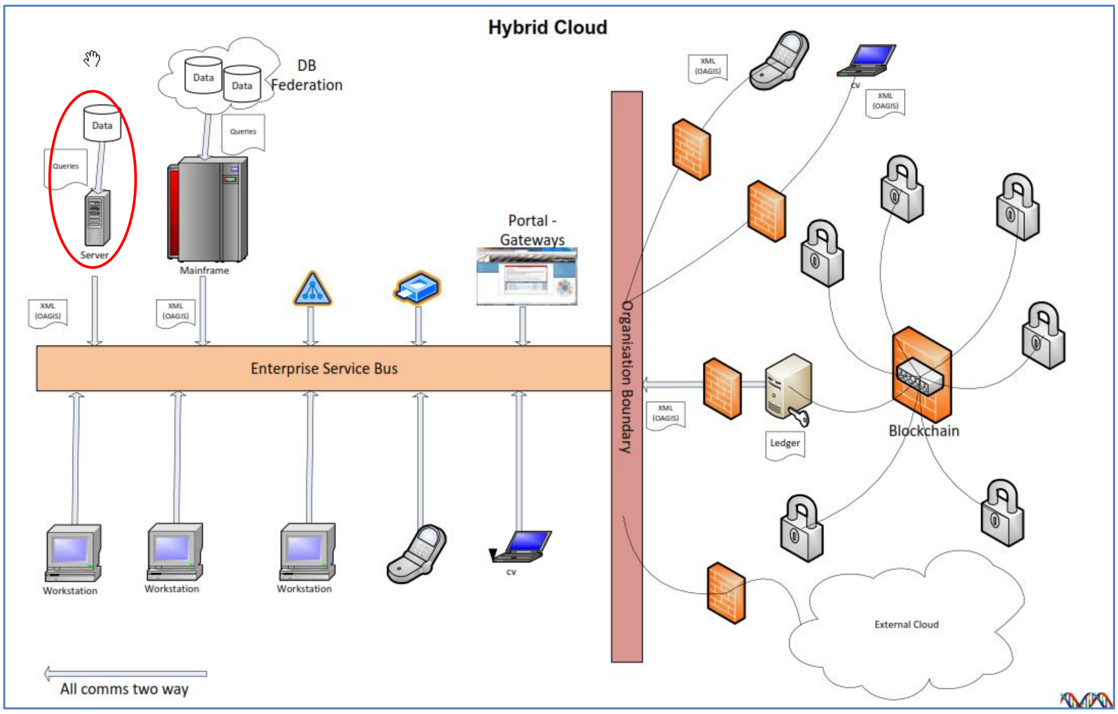


Figure 10 - Risk Log, Architectural Position

The risk log is positioned inside the company boundary. The risk log is a commercially sensitive application and one that has an ethical context in respect of its architectural impact

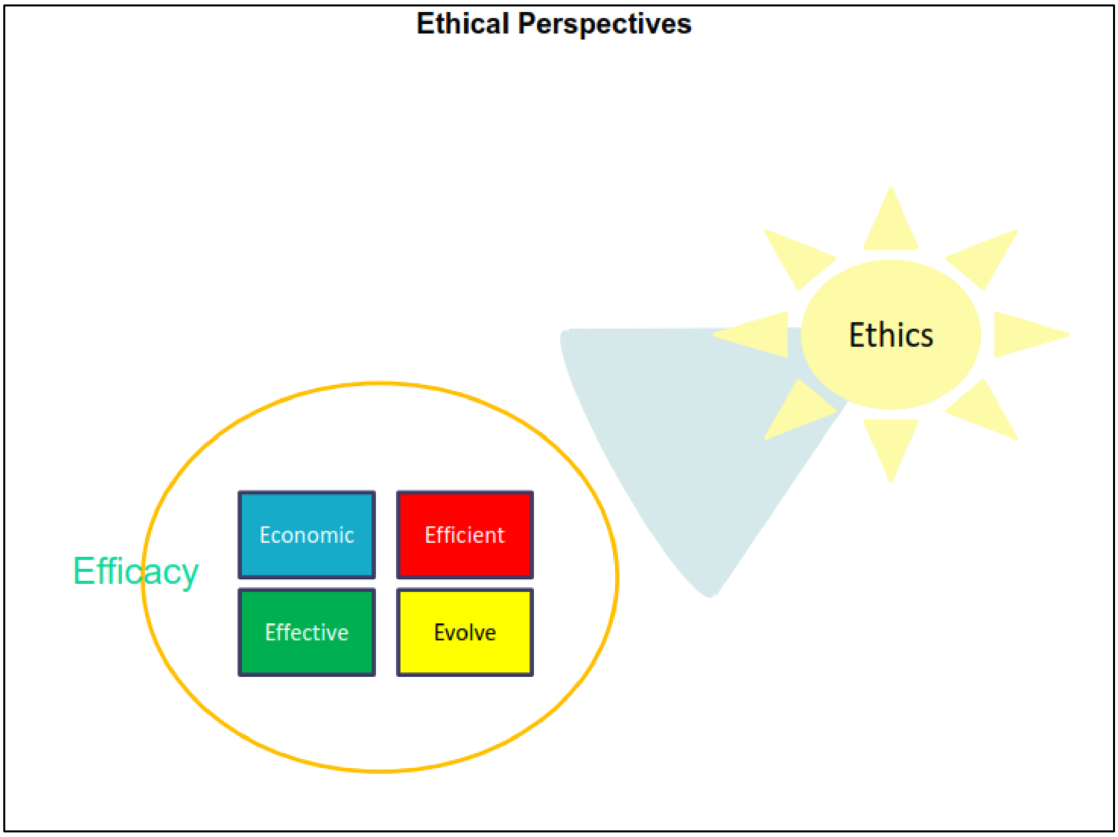


Figure 11 - Risk Log. Ethical impact.

Annex F – Process Catalogue

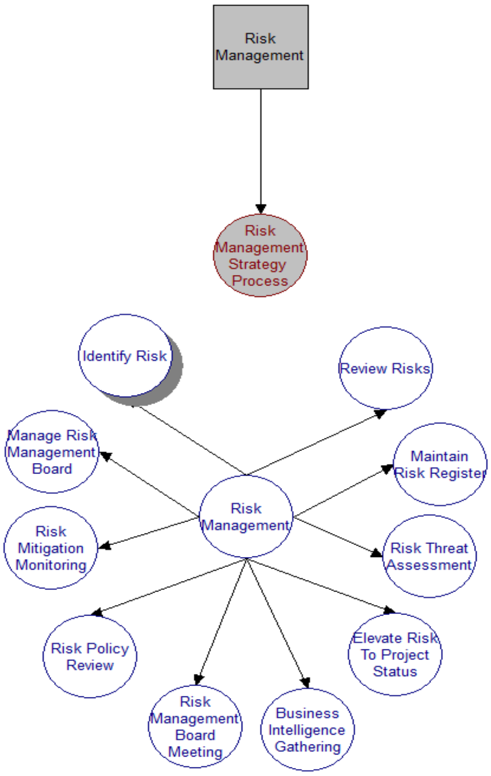

Risk Management
Risk Management Strategy Process
Identify Risk
Review Risks
Manage Risk Management Board
Maintain Risk Register
Risk Management
Risk Mitigation Monitoring
Risk Threat Assessment
Risk Policy Review
Elevate Risk To Project Status
Risk Management Board Meeting
Business Intelligence Gathering

Figure 12 - Risk Register Process Catalogue

The image above is a screen shot of the current risk management process catalogue. The related process profiles are set out below:

Ser	Process Name	Process Profile Link
1	Business Intelligence Gathering	Left click here
2	Elevate Risk to Project Status	Left click here
3	Identify Risk	Left click here
4	Maintain Risk Register	Left click here
5	Manage Risk Management Board	Left click here
6	Review Risks	Left click here
7	Risk Management Process	Left click here
8	Risk Management Strategy Process	Left click here
8	Risk Mitigation	Left click here
10	Risk Policy Review	Left click here
11	Risk Threat Assessment	Left click here