Managing Data in an Evolving World

A guide for good data governance

IIRSM Technical Paper

Ian Dalling SFIIRSM

August 2016

INTERNATIONAL INSTITUTE OF
RISK AND SAFETY MANAGEMENT

Managing data in an evolving world

International Institute of Risk and Safety Management
01-08-2016

Abstract

This paper is primarily aimed at those responsible for establishing governance arrangements and the design and implementation of management systems. It will enable organisations to view data opportunities and threats within the context of the overall management of the organisation and apply pragmatic and proportionate prospect and risk management to equitably satisfy the needs, expectations and aspirations of internal and external stakeholders while making the best use of resources.

Data, together with personnel, commerce, matter and energy, forms the structures and dynamics of an organisation. It is an essential and critical element in the effective and efficient delivery of the organisation's purpose as judged by its various stakeholders. It is therefore a key component of an organisation's potential prospects and risks as it operates under a myriad of uncertainties that is made worse by the ongoing data revolution with information technology at its core.

Why data is a key governance issue and why it cannot be managed in isolation of the organisation as a whole is explained and how organisations should approach its systematic management and conduct integrated holistic prospect and risk management assessments. It is particularly relevant to organisations managing major hazards and threats.

KEY CORPORATE MESSAGE

The ongoing data evolution will create new organisation opportunities and threats presenting new management challenges. Internal and external system interfaces will become more dynamic, complicated and blurred making analysis and prediction much more difficult. This will necessitate prospect and risk management having to be holistically and systematically applied to an organisation's overall business systems and not just to IT systems viewed in isolation. This must address the potential positive and negative impacts on stakeholder requirements, needs and aspirations. The objective should be to achieve an equitable stakeholder balance while making the best use of resources. Organisations must not blindly follow IT fashion and its persuasive marketing but should ensure that its systems, supply chain and delivery chain are resilient and able to deliver its purpose with a high degree of confidence. Governance must be holistic, systematic, comprehensive and delivered via a fully integrated management system recognising no artificial boundaries.

Acknowledgements

The project team thank:

a) The Chartered Quality Institute Integrated Management Special Interest Group for the free use made of universal management definitions and other extracts from MSS 1000:2014.
b) The International Standards Organisation for the ability to hyperlink to descriptions of their standards.
c) Wolfram Alpha for providing a timeline of systematic data and the development of computable knowledge on their web site. Some of this data was used in the creation of Figure 3: Past Evolution of Data.
d) Peer reviewers that kindly provided valuable comments on the drafts of this paper:
   - Anne Mallory, Director of Mallory Health and Safety Consultants Ltd, UK.
   - Dr Gayle Brewer, Senior Lecturer in Psychology at the University of Central Lancashire, UK.
   - Dr Herbert Dlaska, owner of DLC-Integrated Quality Management GmbH, Austria.
   - Dr Shahzeb Malik, Technical and Research Manager, IIRSM, UK
   - Suleiman Shehu, CEO Azinta Systems, UK.

Summary

Directing the management of data is a key corporate responsibility that stands alongside the management of personnel, commercial, matter and energy structures and processes. During the long evolution of data throughout the history of humankind, each data innovation has improved the potential for organisations to deliver their goods and services more effectively and more efficiently. This continual data innovation is ongoing and is presenting many management challenges.

The way that data is held, processed, shared and communicated is becoming increasingly sophisticated through globally advancing technical innovation. It is essential that organisations engage with this ongoing change in the way data is used in their internal and external operating environments in order to exploit the upside, guard against the downside and remain competitive.

Organisations need to be proactive in their strategic data decision making in order to achieve optimal outcomes. It is essential that an integrated approach is taken to managing data opportunities, hazards and threats because data directly or indirectly permeates the whole of an organisation's structures and processes. Not only is it inappropriate to attempt to manage data in isolation of other aspects of the organisation, it is inappropriate to manage everything else in isolation of its data components. Stakeholder satisfaction may result directly from some aspect of data or from a wider aspect where data is only a contributing element.

Organisations currently exist within an ongoing data revolution as significant as the industrial revolution creating new opportunities, hazards and threats. The pace of this ongoing revolution is impossible to predict and whether it will continue indefinitely or at some point end. The introduction of novel applications of data has the potential to assist with solving many problems and adding value but it can also create unintended consequences such that we potentially trade one set of problems for another.

The evolving and increasingly sophisticated use of data will require that organisations continually adapt and evolve in order to remain aligned with their stakeholder needs and expectations, and the organisation's internal and external operating environment. This will involve the redesign of the structures and processes that deliver goods and services and will involve significant changes in the roles of personnel and the nature of work. This will result in economic, social and political effects.

Organisations as they currently exist will inevitably change to varying degrees, those that fail to adapt sufficiently, or quickly enough, may disappear. Many new organisations are likely to emerge to meet the demands of new data innovations and their applications.

Organisations need to be competent at identifying data opportunities, hazards and threats, and in the evaluation of the corresponding prospects and risks that affect customer and other stakeholder needs, expectations and aspirations. Organisations need to be viewed as systems that are only as strong as their weakest component – cyber and non-cyber data prospect and risk controls must be equally robust and as strong as the organisation as a whole.

As well as interfacing with personnel, the management system will increasingly interface with smart machines and things in general. Data will become increasingly intertwined with personnel, commercial, and matter and energy components that deliver the organisation's purpose via its goods and services. In the coming years many aspects of the current human

role in organisations will be subordinated to IT processes and intelligent infrastructure raising many social, economic and political issues no less significant than those associated with the industrial revolution. Legislation and regulation will need to be globally harmonised keep up with the ongoing data revolution.

It is essential that management objectives are delivered via a fully integrated management system addressing the totality of the strategic, tactical and operational management of the organisation – it must nurture fully joined up management thinking processes and be prospect and risk informed with an equitable degree of stakeholder upside and downside balance. Data and other technology are just tools that do not become prospects and risks until their application potentially affects stakeholder needs, expectations or aspirations.

The sophistication of the management system will need to be more than a match for the data induced challenges.

The sophistication of the management system will need to be more than a match for the challenges created by the evolving use of data. It must improve prospects and reduce risks by not only employing both general data management good practices, such as password, document and record control etc., it should implement organisation specific controls informed by effective prospect and risk assessment. Also, in managing change, the organisation should neither lag nor be too far ahead of the wind of data innovation. Failure to achieve this will degrade the effectiveness and efficiency of its structures and processes making it less competitive and more vulnerable to failure.

As explicit knowledge and data as a whole are very valuable organisational assets, it is appropriate that data should be prominent within its governance arrangements. Ultimately, success will depend on every structure and process owner, manager and participant being competent and diligent in their respective duties, and coordinating and cooperating with others. As always, success will critically depend on the awareness, commitment and governance of top management, it's allocation of resources, its cooperation with stakeholders, and its effective coordination of the activities of the organisation as a whole.

As always, success will critically depend on the awareness, commitment and governance of top management, its allocating of resources, its cooperation with stakeholders, and its effective coordination of the activities of the organisation as a whole.

Organisations are often established with primitive governance arrangements and management systems. This leaves them potentially vulnerable to unrevealed risks that may harm performance and unrevealed unexploited prospects that could enhance performance. It is important that organisations become aware of their governance and management system maturity and take appropriate management action to improve it to the highest level within the limitations of what is practicable for the size and type of organisation.

Managing Data in an Evolving World

By Ian Dalling (IIRSM)

Contents

Figures

Tables

1. Introduction

This paper forms part of a package of resources created by the International Risk and Safety Management Institute Technical Committee to assist in effectively managing data within all levels of an organisation from top-level strategic decision making down to day-to-day operational data management. This is becoming critically important to organisations because of the current unprecedented advances in data science and technology which can potentially be employed to improve the delivery of an organisation's purpose but also expose it to new or elevated hazards and threats. These advances in data technology are driving closer integration and automation of systems while creating vulnerabilities to malicious and non-malicious modes of failure.

These new challenges can critically impact internal and external stakeholders in previously unexperienced ways with devastating effects on the organisation. The media continually reports headline grabbing data incidents demonstrating that organisations large and small are failing to effectively manage prospect and risk in the fast evolving technological environment. Such incidents include data loss, unauthorised sharing, spying, corruption, theft, warfare etc. and can affect any structure or process with a data component.

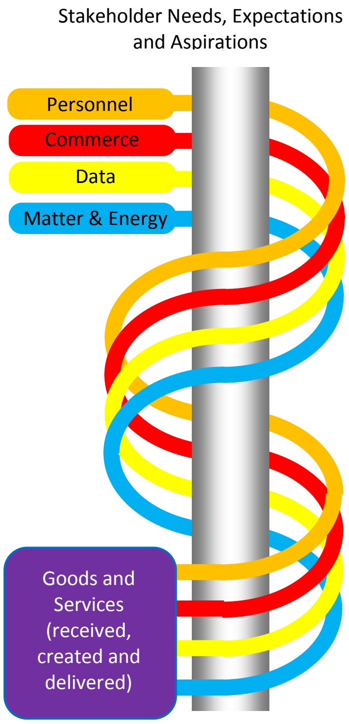

Stakeholder Needs, Expectations and Aspirations
Personnel
Commerce
Data
Matter & Energy
Goods and Services (received, created and delivered)

Figure 1: Context of Data

The intention of this paper is to raise corporate awareness of the principal issues and advise on how to systematically organise resources to exploit data related opportunities while minimising the potential impacts of the associated hazards and threats.

The paper takes a holistic approach to managing structures and processes with a data component by using an integrated prospect and risk management approach. Prospect and risk management is essential because any given data malfunction will have varying effects on different structures and processes within an organisation and indeed across organisations with different purposes. These effects in turn will also not necessarily impact the stakeholders in the same way or to the same degree.

It should be noted that the term 'information' is often used instead of 'data', and 'cyber' is used more restrictively in relation to computers and computer networks.

Prospect and risk management is essential because a given data malfunction will have varying effects on different structures and processes within an organisation and indeed across organisations with different purposes. These effects in turn will not necessarily impact the stakeholders in the same way or to the same degree.

Organisations of all types and sizes deliver their purpose through a combination of personnel, commercial, data, matter and energy structures and processes. These components closely interact and permeate the whole organisation, its projects, its supply chains and its delivery chains in a way that is generally unique to each organisation. It can be very complex even in a small organisation.

Data is used in many ways including informing decision-making, communication, as a receptacle for explicit knowledge, and intelligent control of structures and processes. Data can even be used to control data e.g. programmable computers. It is a valuable capital as important as financial, manufactured structure, human, social and relationship, and natural capitals.

Data is an exploitable asset that has the potential to produce intended value adding outcomes but also unintended negative outcomes such as accidental loss and malicious attack. How this is managed determines the various dimensions of an organisation's performance that in turn determines the level of satisfaction of stakeholders judged against their specific needs, expectations and aspirations.

This requires that data management is understood as a trans-silo issue affecting all aspects of management and performance and not something that may be solely delegated to an IT manager. Not only is it inappropriate to attempt to manage data in isolation of other aspects of the organisation, it is inappropriate to manage product and service delivery processes in isolation of their data components. Failure to effectively and efficiently manage data within a holistic perspective will lead to non-optimal fragmented management. It may negatively affect product, service, health and safety, environmental, regulatory, reputational, financial or any other aspect of an organisation's performance valued by its various stakeholders.

This paper describes how the use of data within organisations has changed historically and continues to change presenting potential opportunities as well as associated hazards and threats. This needs to be managed in a balanced and systematic way and addressed within top-level decision-making and governance and the architecture of its management system.

Not only is it inappropriate to attempt to manage data in isolation of other aspects of the organisation, it is inappropriate to manage product and service delivery processes in isolation of their data components.

The use of technical terms has been minimised as far as practicable but are however critically important to a proper understanding of the content of this paper. A list of important definitions is included at the end of this paper for reference. The terms opportunity, hazard and threat, prospect and risk are critical to the understanding of good governance and management systems and are often misunderstood. They are the foundation concepts for managing the upside and downside of future outcomes and dealing with uncertainty. The first three terms represent the upside and downsides of potential options while ignoring uncertainty, whereas the latter two take uncertainty into account. The definition of these concepts aligns with everyday general and legal usage. Prospect is sometimes referred to as 'negative risk' by some risk practitioners. These concepts are illustrated in Figure 2 and will help in the conceptual understanding of Sections 3 and 4, which deal with opportunity and hazard/threat identification, and prospect and risk assessment and evaluation respectively.

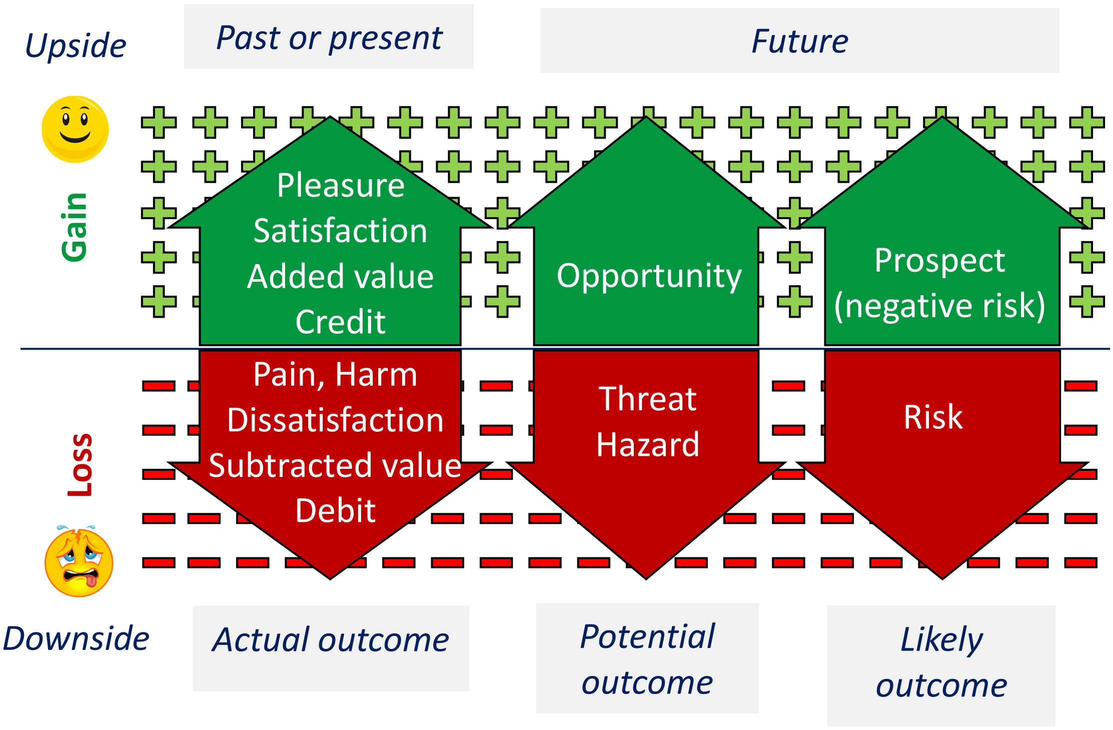


Figure 2: Upside and Downside Terminology

The sections of this paper cover:

a) The general evolution of data and the implications – Section: 2 Evolution of Data.
b) Data opportunities, hazards and threats – Section: 3 Data Opportunities, Hazards and Threats.
c) Managing data under uncertainty in terms of prospect and risk in order to achieve balanced stakeholder satisfaction – Section: 4 Managing Data Under Uncertainty.
d) Embedding prospect and risk control within a fully integrated management system and the selection and adoption of management system standards – Section: 5 Systematic Management of Data.
e) Governance and management system maturity – Section: 6 Governance and Management System Maturity.
f) Overall conclusions that should influence the corporate governance of data – Section: 7 Conclusion.

2. Evolution of data

Data conceptually embraces facts, statistics and other items of information. It may include alphanumeric text, numbers, photographs, video, software etc. Over its lifecycle, it may be created, stored, accessed, processed, communicated, shared, replicated, encrypted, lost, corrupted, stolen or destroyed. It may be tangible or virtual, may be analogue or digital, and hosted by various types of media.

Data is arguably one of the most valuable assets and in its various manifestations forms humankind's explicit knowledge.

Since Homo-sapiens first existed on Earth between 400,000 and 250,000 years ago, they have been continually expanding their understanding of the nature of data and how to use it to help achieve their objectives. Innovation has included: arithmetic and mathematics, written language, systems of notation, numerical time keeping and other measurements linked to the physical world, recording of still and moving images, creation of physical and virtual libraries, the development of statistics, the codifying of human language and being able to use numbers to predict the past, present and future.

The advent of and the increasing number of computer applications, the internet and the world-wide-web etc. has enabled data to be stored in vast amounts, shared and processed with ever increasing effectiveness and efficiency. This has enabled organisations to improve their business processes that deliver their goods and services.

However, as data knowledge innovation has advanced presenting new opportunities for adding value, it has also come with associated hazards and threats where value may be potentially lost requiring the competent application of effective prospect and risk assessment.

20,000 BC: Counting objects using arithmetic.

15,000 BC: Cave Painting - pictures representing stories.

3,500 BC: Knowledge recording using written language.

2,500 BC: Organising time - Sumerian Calendar.

1,700 BC: Mathematical Tables - Babylonians

1,250 BC: Building to store knowledge - Library at Thebes.

1,150 BC: Recording geographic knowledge - Egyptian Maps.

600 BC: Coins representing value - Lydian Coinage.

500 BC: Using arithmetic to predict - Babylonian Astronomy.

500 BC: Relating numbers to nature – Pythagoras.

400 BC: Discovering rules of human language – Panini.

325 BC: Collecting world's knowledge - Library of Alexandria.

300 BC: Organising mathematical truth – Euclid.

250 BC: Computing as a basis for technology – Archimedes.

100 BC: Machine for computing - Antikythera Mechanism.

1453: Mass distribution of knowledge - Johannes Gutenberg.

1595: Notation for symbolic algebra - Franciscus Vieta.

1662: Inventing the idea of statistics - John Graunt.

1687: Mathematics as a basis for natural law - Isaac Newton.

1801: Data controlled machines - Joseph Marie Jacquard.

1837: Capturing images automatically - Louis Daguerre.

1844: Transmitting information by wire - Samuel Morse.

1847: Algebra representing logic - George Boole.

1876: Classifying the world's knowledge - Melvil Dewey.

1877: Recording the sound of anything - Thomas Edison.

1936: Concept of universal computation - Alan Turing.

1940s: Digital Computers - automating computation

1942: Photocopier patented by Chester Carlson.

1950—1960s: Making computers more intelligent using artificial intelligence.

1957: Computer languages for precise task processing.

1960: Connecting and organising information using hypertext.

1966: Government freedom of information act, USA.

1970s: Data relationships become computable via relational databases and queries become easily executable.

1970—1980s: Interactive computing giving immediate results and integrating them with everyday processes.

1970—1980s: Expert logic-based inferential systems.

1974: Products get barcodes UPC Codes

1983: Domain name system for hierarchical Internet addresses.

1989: The Web eventually hosting billions of pages of data.

1994: Yahoo hierarchical web directory – Jerry Yang/David Filo.

1998: Engines to search the web – Google etc.

1999: Advancing connectivity of devices, systems, and services – Internet of things.

2001: Self-organised encyclopaedia – Wikipedia

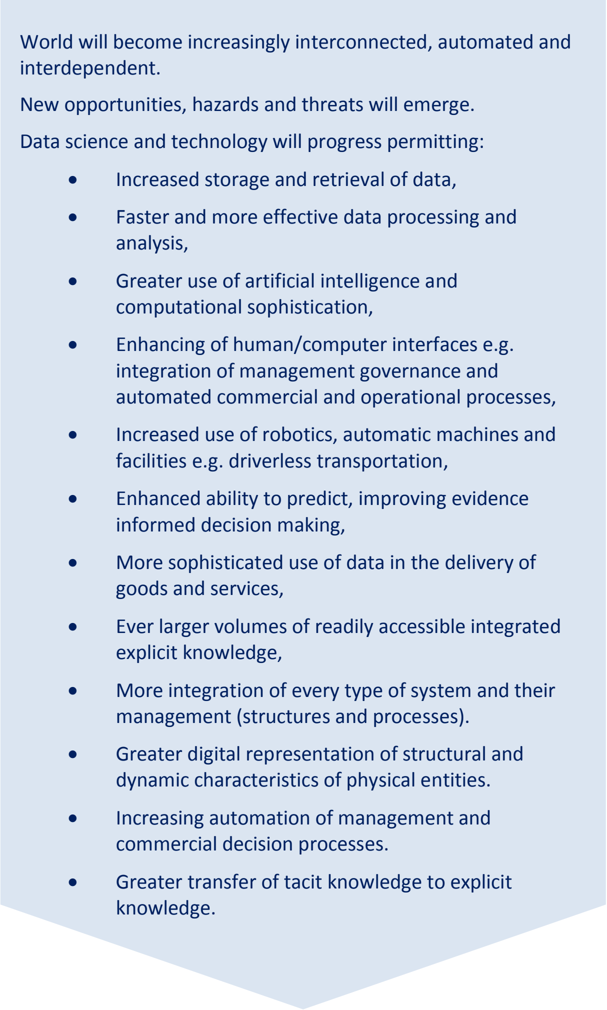
Figure 3: Past Evolution of Data

This is addressed in Section 3.

The nature of data is evolving and becoming more voluminous, self-organising, permeating more and more of human activity and becoming increasingly connected with a growing sophisticated and complex physical and virtual world.

Data communication started just between conscious beings and then extended to include communication with and between machines. Future machines will also routinely communicate between themselves and share data at speeds and in volumes not previously conceived of as possible. Machines such as transport vehicles will be subject to a collective interactive communication and automation.

This increasingly sophisticated use of data will significantly change the nature of work and leisure. Significant societal and political impacts will necessitate re-education and the attainment of new skills. Because of the blurring of boundaries of data control, new challenges are likely to arise with respect to data ownership and human rights.



World will become increasingly interconnected, automated and interdependent.

New opportunities, hazards and threats will emerge.

Data science and technology will progress permitting:

- Increased storage and retrieval of data,
- Faster and more effective data processing and analysis,
- Greater use of artificial intelligence and computational sophistication,
- Enhancing of human/computer interfaces e.g. integration of management governance and automated commercial and operational processes,
- Increased use of robotics, automatic machines and facilities e.g. driverless transportation,
- Enhanced ability to predict, improving evidence informed decision making,
- More sophisticated use of data in the delivery of goods and services,
- Ever larger volumes of readily accessible integrated explicit knowledge,
- More integration of every type of system and their management (structures and processes).
- Greater digital representation of structural and dynamic characteristics of physical entities.
- Increasing automation of management and commercial decision processes.
- Greater transfer of tacit knowledge to explicit knowledge.

Figure 4: Probable Future Evolution of Data

As explained in Section 1, the way that we use data will have a significant impact on the way that we use and manage personnel, conduct commerce, manage energy and matter, and on the way that we interact with customers, our suppliers and other stakeholders. This is the ever-changing domain of the modern organisation that exists in an ongoing data revolution as significant as the industrial revolution. Processes and structures need to continually evolve in order to keep pace with this evolving use of data. It needs to be properly understood and exploited by organisations via creative and intelligent systematic management processes and address a multitude of uncertainties. This requires effective and efficient prospect and risk management addressed in Sections 3, 4.3 and 4.3.

> The data world that we operate in today is very different from that of our ancestors - the future will doubtless be very different again for our successors.

The data world that we operate in today is very different from that of our ancestors and the future will doubtless be very different again for our successors. The introduction of novel applications of data has the potential to assist with solving many of humankind's problems but can also create unintended consequences. Strategic planning needs to recognise this increasingly dynamic environment full of potential prospects and risks that need to be understood evaluated and equitably balanced prior to strategic, tactical and operational decision making. Change needs to be continually managed so that the organisation remains aligned with the evolving needs, expectations and aspirations of its stakeholders while keeping pace with data advancement. The better this is done, the more likely the organisation will be to remain successful, competitive and satisfy its customers and other stakeholders.

3. Data opportunities, hazards and threats

The effective management of systems containing data components depends on effective and appropriate prospect and risk assessment to make sure that stakeholders needs, expectations and aspirations are satisfied equitably while making the best use of resources. An aspects and impacts assessment must first be conducted in order to identify the data opportunities, hazards and threats prior to the conduct of a risk assessment. This section addresses the identification of the data opportunities, hazards and threats leaving Section: 4 Managing data under uncertainty to address the next step which is the full assessment of the associated prospects and risks i.e. taking account of uncertainty. Figure 2: Upside and Downside Terminology in Section: 1 Introduction explains these terms.

Organisations exist in many sizes and types. Each has a purpose, which is the reason it exists. The purpose is delivered through the four principal elements forming its structures and processes, i.e. data, personnel, commerce and 'matter and energy'. The dynamic interactions between these four elements are shown conceptually in Figure 5. This facilitates opportunities to achieve the organisation's and stakeholder's objectives by delivering value through goods and/or services.

Within these dynamics are opportunities, hazards and threats. Any opportunity that may be available has potential associated hazards and/or threats that can subtract from the overall delivered value. This is often referred to as the upside and downside of choices and outcomes – refer to the explanation at the end of Section 1 for more detail. The challenge for management is to maximise gain while minimising losses in all of its forms over the short and long term. It is critically important that the upside and downsides of any use of data in an organisation is properly understood with respect to the performance of the whole organisation and how it affects the various needs, expectations and aspirations of the stakeholders.

Hazards and threats negatively affect an organisation's activities but have different natures requiring them to be treated differently. Hazards are something or circumstances with the potential to cause harm but a threat is something that has the intention of causing harm or behaving in a way that could cause harm.

Hazards may be natural and non-natural. Examples of natural hazards are diseases, flooding, poor air quality, volcanic eruptions, earthquakes, severe weather, wildfires etc. Non-natural hazards are those created through the activities of humankind and many result from organisations' operations, goods and services. They can affect all aspects of performance including finance, goods and service quality, personnel health, safety and welfare, infrastructure safety, environmental, security, commercial integrity, social integrity and reputation. Hazards emanating from humankind may exacerbate natural hazards or combine with them e.g. extreme weather flooding may be made worse because of the features of the built environment.

The way that data is used within the organisation's structures and processes can enhance its opportunities (the upside) and expose it to associated hazards and threats (the downside). It is the exploration and identification of opportunities that generally takes the lead because of the organisation's motivation to deliver value adding goods and services with the objective of sustaining its financial income. However, while it focuses on potential opportunities, it also has to also evaluate the associated hazards and threats in order to see the total upside and downside of the big picture.

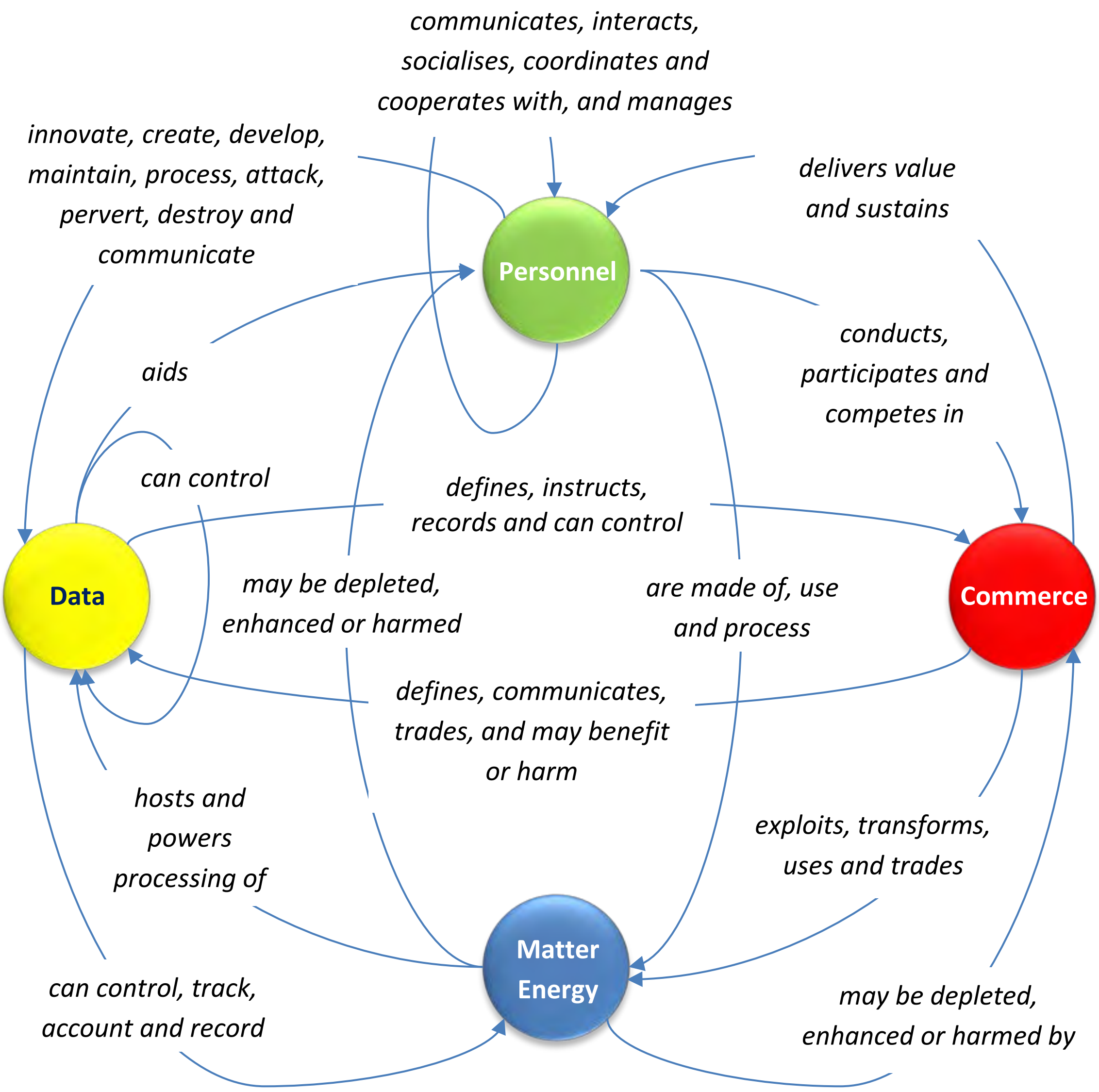

communicates, interacts, socialises, coordinates and cooperates with, and manages
innovate, create, develop, maintain, process, attack, pervert, destroy and communicate
delivers value and sustains
Personnel
aids
conducts, participates and competes in
can control
defines, instructs, records and can control
Data
may be depleted, enhanced or harmed
are made of, use and process
Commerce
defines, communicates, trades, and may benefit or harm
hosts and powers processing of
exploits, transforms, uses and trades
Matter Energy
can control, track, account and record
may be depleted, enhanced or harmed by

Figure 5: Organisation Data Dynamics

3.1 Opportunities

Opportunities typically include the potential to exploit new ways of doing things, new markets, new knowledge, new technology, new customer relationships and contracts, making systems more effective and efficient leading to higher quality goods and services, and reduced costs resulting in improved competitiveness and profitability. Typical data success modes that support opportunity are listed in Table 1.

Table 1: Data Success Modes

Data success modes	Opportunity	Applications
Processing	Improved speed	Complex problem solving
	Greater accuracy	Prospect and risk informed decision-making

Data success modes	Opportunity	Applications
	Greater power Lower cost Exploitation of smart technology. Encryption Higher productivity	Manual and auto control of machines and infrastructure (robotics) Automatic and data assisted management and commercial transactions (trading) Analysing explicit knowledge Intelligent surveillance and defence Design and development of software applications
Storage	Larger Smaller space Improved retrieval and accessibility Lower cost	Holding and accessing explicit knowledge
Communication and interaction	Improved speed Greater accuracy Ability to share and interact Higher productivity Lower cost	World wide web Internet Telephony Global project communication

3.2 Hazards and threats

Hazards and threats expose the organisation to potential losses dissatisfying stakeholder's needs, expectations and aspirations. This negatively affects competiveness, profitability and reputation. Typical data failure modes are listed in Table 2.

Table 2: Data Failure Modes

Data Failure Mode	Hazard	Threat	Example Causes	Defences
a) Loss.	√	√	Human error Human violation Media device failure Losing media device Accidental overwriting	Management system Staff selection and training Personnel risk averse behaviours Duplication and diversity Quality assurance Monitoring and surveillance
b) Corruption.	√	√	Human error Human violation Computer virus Hacking Poor quality product(s)	Management system Staff selection and training Personnel risk averse behaviours Duplication and diversity. System barrier(s) Quality assurance

Data Failure Mode	Hazard	Threat	Example Causes	Defences
				Monitoring and surveillance
c) False (not fit for purpose).	√	√	Human error Human violation Computer virus Hacking Poor quality product(s)	Management system Staff selection and training Quality assurance Monitoring and surveillance
d) Breach of containment – unauthorised access or sharing.	√	√	Human error Human violation Computer virus Hacking Poor quality product(s)	Management system Staff selection and training Personnel risk averse behaviours System barrier(s) Quality assurance Monitoring and surveillance
e) Theft.		√	Hacking Media removal Product/system quality	Management system. Staff selection and training Personnel risk averse behaviours System barrier(s) Monitoring and surveillance
f) Illegitimate access	√		Human error Human violation Hacking Media removal Product quality	Management system Staff selection and training Personnel risk averse behaviours System barrier(s) Quality assurance Monitoring and surveillance
g) Processing malfunction	√	√	Human error Human violation Hacking Product/system quality	Management system Staff selection and training Personnel risk averse behaviours System barrier(s)

Data Failure Mode	Hazard	Threat	Example Causes	Defences
				Quality assurance Monitoring and surveillance

3.3 Malicious threats

An intelligent threat will always seek the weakest part of the organisation or its defences to achieve its objectives. The values and activities of an organisation are a major factor in determining whether it will have enemies and the level of motivation to inflict harm.

An organisation owns or is responsible for a large range of valuable assets that generally increases with the size or the type of organisation. These assets may be threatened by major malicious threats that depend on several factors related to the source of the intention to perpetrate harm and the intended target.

A significant new type of threat that has become prevalent in recent years are malicious threats to computer systems. These threats include a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. The early computer systems which we would now view as rather primitive were always vulnerable to malicious interference but few people understood them or had direct access to them. Today, computers are extremely numerous, readily accessible, are able to process and transfer very large amounts of data and people are widely knowledgeable about computers and how they work. Data science and technology continues to rapidly evolve including malware that can be used maliciously to harm an organisation or individual. The reason that those serving self-interests, choose to do it through a cyber data process rather than some other means such as a non-cyber data process the or via direct access to the infrastructure of an organisation is because it is relatively easier and presents less risk to the wrongdoer as they can generally perpetrate the act remotely and remain anonymous and even undetected. An intelligent threat will always seek the weakest part of the organisation or its defences to achieve its objectives. The values and activities of an organisation are a major factor in determining whether it will have enemies and the level of motivation to inflict harm. A non-exhaustive list of factors influencing these potential threats is listed below in Table 3.

Table 3: Factors Influencing a Malicious Threat

Factor	Issues
a) Malicious person(s) wishing to cause or to show indifference to causing harm.	The principal types of groups or people that may threaten an organisation may be categorised as follows: 1. Criminals motivated by financial or material gain and tend to target financial systems, accounts functions, personal identifiable information, customer orders, and high value assets that can be readily removed. 2. Interest groups who want to create problems for particular organisations because they disagree with the its activities or values or see the organisation as a threat. They tend to take direct action or target information systems or automated processes in order to interrupt production. More extreme groups would include terrorists and tend to focus on organisations who may be a government or defense supplier. 3. Irresponsible self-serving people or groups that may cause harm by being indifferent to the organisation's legitimate operations e.g. a hacker hobbyist. Harm may be inflicted through a general lack of respect for others property. Commercially and socially responsible organisations who intelligently and creatively work to avoid and resolve conflict are less likely to be vulnerable to the second group of attackers.
b) Structure and/or process having the potential to be harmed.	Structures and processes should be hardened so that as far as possible they have little vulnerability presenting an easy target. 'Defence in depth' should be implemented where the potential target is of high value to the organisation or to an attacker or other stakeholder.
c) Capability of attacker to cause harm.	General knowledge of IT, other technology and the industry of the organisation may aid the attacker's ability to inflict harm.
d) Attacker knowledge of organisation's systems, business operations and defences.	Specific knowledge of the functioning of the organisation aids the determination of its vulnerabilities open to attack. Knowledge of the defences that the organisation has implemented aids the attacker in determining the residual vulnerability and creatively innovating methods to penetrate the organisations defences. Threats can act intelligently and creatively to defeat defences unlike hazards that are passive in this respect.
e) Capability of attacker to breach organisation's defences.	The attacker's capability may include resources external and internal to the target organisation. Capability may include skills to persuade individuals to assist them by using coercion such as bribery, intimidation and blackmail.
f) Organisation's threat assessment and development of controls.	A threat assessment should include all factors within this table and be conducted using competent personnel with integrity. The threat assessment should look at the current circumstances of both the target and attacker. It needs to be dynamic and continually reviewed against available intelligence. It should be proactive and not just react to events.
g) Validation of controls	The organisation's arrangements need to be peer reviewed,

Factor	Issues
(defences).	benchmarked, tested and regularly exercised to ensure they are fit for purpose.
h) Implementation and maintenance of controls (defences).	Organisation's should ensure that risk informed physical and administrative security arrangements have been implemented and subjected to appropriate planned and reactive maintenance, inspection, testing.
i) Planned monitoring of management controls (defences).	Inspection and audit and review should be continually conducted to ensure there is confidence in the arrangements, they keep step with current intelligence and technological innovation, and remain aligned with the evolving needs, expectations and aspirations of stakeholders. Continual improvement should drive overt, and where valuable, covert 'plan-do-check-act' management cycles.
j) Intelligence gathering and evaluation.	Governments, industries and organisations, as appropriate, should overtly and covertly gather and share intelligence to inform their prospect and risk assessments, and decision-making.
k) Detection of an attack in progress or being imminent.	Arrangements need to be implemented to detect potential and actual attacks in order to effectively and efficiently trigger risk-mitigating responses.

3.4 Data crime and ethical violations

A potential attacker may consider a number of targets and means of perpetrating harm or achieving self-serving or unethical objectives, data may be just one means to be selected. The attacker may decide that data is the easiest target or means and adopt it individually or in combination with other targets or methods to achieve their objective. The threat may be directed at data within the organisation's computers or computer network or existing generally within the organisation's structures and processes. The perpetrator may potentially come from outside of the organisation or within, at any level including top management and seek the weakest points of the overall system in order to achieve their self-serving objectives.

The same data may exist in cyber and non-cyber form and should receive an equivalent level of management attention and protection proportionate to the associated potential risks to stakeholder needs, expectations and aspirations – refer to section 4. It is therefore advantageous to address threats to cyber and non-cyber data holistically as the same data in different forms is part of the same risk set. Robust defences in one domain may be negated by weaknesses in the other domain e.g. a visitor observing an unprotected document or a 'post-it' label containing a password stuck on a computer screen within an office or a document being openly carried by a person going to a meeting in a public place. Unauthorised observation or recording can be greatly enhanced by high definition cameras and remote listening devices.

3.4.1 Cyber crime

If the threat is directed at the organisation's computers or computer networks, it is generally referred to as a cyber-attack and is becoming more common because of the relative ease with which it can be perpetrated from a location anywhere in the world without the detection of the perpetrator.

Table 4 lists typical potential modes of cyber-crime and defences:

Table 4: Cyber Crime Modes and Defences

Failure Mode	Defences
a) All.	1. Governance arrangements compliant with best practice and legislation. 2. Top management commitment demonstrated by appropriate resourcing and setting of policy. Ensuring cooperation and coordination with relevant stakeholders. 3. Third party certification of management system as appropriate. Refer to section 5. 4. Management controls implemented based on or informed by an appropriately rigorous prospect and risk assessment. 5. Design of systems such that they avoid or minimise the potential for human error and human violation. 6. Data classification system and associated controls proportionate to risk 7. Effective control of personnel recruitment, induction, training, assignment, supervision, surveillance, disciplinary and leaving processes informed by risk assessment. 8. Formal overt and covert management systems informed by risk assessment. 9. System architecture and process design based on prospect and risk assessment, to tried and tested good practices. 10. Prospect and risk informed planned monitoring. Personnel monitoring. Gathering, collation and analysis of intelligence. 11. Contingency arrangements informed by prospect and risk assessment (crisis, emergency, disaster recovery and business continuity plans, insurance and access to legal support following an event).
b) Loss through theft e.g. copying, unauthorised removal of media.	1. Data system architecture barriers. Use of defence in depth employing multiple diverse barriers proportionate to risks. Possible isolation from internet etc. 2. Process administrative controls. 3. Sharing restriction controls. 4. Suppliers and partners vetting, approval and monitoring. 5. Encryption. 6. Fire walls. 7. Location physical barriers and entry control. 8. Backing up of data. 9. Behavioural surveillance conducted by personnel and computer software.
c) Loss through corruption or destruction e.g. malware.	1. Data system architecture barriers. Possible isolation from internet etc. 2. Process administrative controls. 3. Fire walls. 4. Anti-virus software. 5. Backing up of data. 6. Behavioural surveillance conducted by personnel and

Failure Mode	Defences
	computer software
d) Loss of control e.g. trojans permitting an external body or person to make changes to IT structures and processes causing disruption of normal operations and/or stealing of valuable data.	1. Data system architecture barriers. Possible isolation from internet etc. 2. Process administrative controls. 3. Fire walls. 4. Anti-virus software. 5. Behavioural surveillance conducted by personnel and computer software.
e) False data deliberately created to deceive in order to achieve unethical or criminal objectives e.g. false accounting. Can be any type of data including software designed to deceive and the altering of records.	1. Data system architecture barriers. 2. Process administrative controls requiring independent validation of data, approval and change control. 3. Ensure structures and processes discourage and resist corruption and fraud. 4. Collect data to permit data installation and change investigations via an audit trail. 5. Behavioural surveillance conducted by personnel and computer software. 6. Policy of always prosecuting criminals and taking disciplinary action against significant damaging violations of the management system.
f) Degradation of data network or transmission system causing disruption.	1. Data network architecture design, physical barriers and access entry systems. Possible isolation from internet etc. 2. Defence in depth proportionate to risk using redundancy, diversity and/or segregation as appropriate. 3. Interference surveillance.
g) Penetration of data network or transmission system permitting interception of transmitted data and its theft or corruption.	1. Data network architecture design, physical barriers and access entry systems. 2. Defence in depth proportionate to risk using multiple diverse barriers. 3. Interference surveillance. 4. Encryption.

3.4.2 Non-cyber data crime

Non-cyber data crime covers malicious threats to data held or transmitted outside of computers or computer networks. Their impact can be equivalent to cyber threats where the data is the same but in a different form.

Table 5 lists typical potential modes of non-cyber data crime and defences:

Table 5: Non-cyber data crime modes of failure and defences

Failure Mode	Defences
a) All.	1. As per section a) of Table 4: Cyber Crime Modes and Defences.
b) Loss through theft e.g.	1. Infrastructure design, containment and access barriers.

Failure Mode	Defences
copying, unauthorised removal of media.	Use of defence in depth employing multiple diverse barriers proportionate to risks. 2. Process administrative controls. 3. Data item tracking. 4. Data replication at diverse location. 5. Anti-copying or recording measures. 6. Access and sharing restriction controls. 7. Clean desk policies 8. Suppliers and partners vetting, approval and monitoring. 9. Surveillance.
c) Loss through corruption or destruction e.g. vandalism or deliberate damage.	1. Infrastructure design, containment and access barriers. Use of defence in depth employing multiple diverse barriers proportionate to risks. 2. Process administrative controls. 3. Data item tracking. 4. Access and sharing restriction controls. 5. Clean desk policies 6. Suppliers and partners vetting, approval and monitoring. 7. Surveillance. 8. Infrastructure integrity protection measures e.g. fire etc.
d) False data deliberately created to deceive in order to achieve unethical or criminal objectives e.g. false or altered record or counterfeit document. Can be any type of document designed to deceive.	1. Data storage and handling architecture and processes. 2. Process administrative controls requiring independent validation of data, approval and change control. 3. Ensure structures and processes discourage and resist corruption and fraud. 4. Collection and storing of data to permit data life-cycle investigations. 5. Behavioural surveillance conducted by personnel and automated systems. 6. Policy of always prosecuting criminals and taking disciplinary action against significant damaging violations of the management system.

4. Managing data under uncertainty

Prospect and risk assessment is addressed in this section and requires that opportunities and hazards/threats are first identified. This was the objective of the previous section. The distinction between 'opportunity and hazard/threat' and 'prospect and risk' respectively are shown pictorially in Figure 2: Upside and Downside Terminology in Section 1 Introduction.

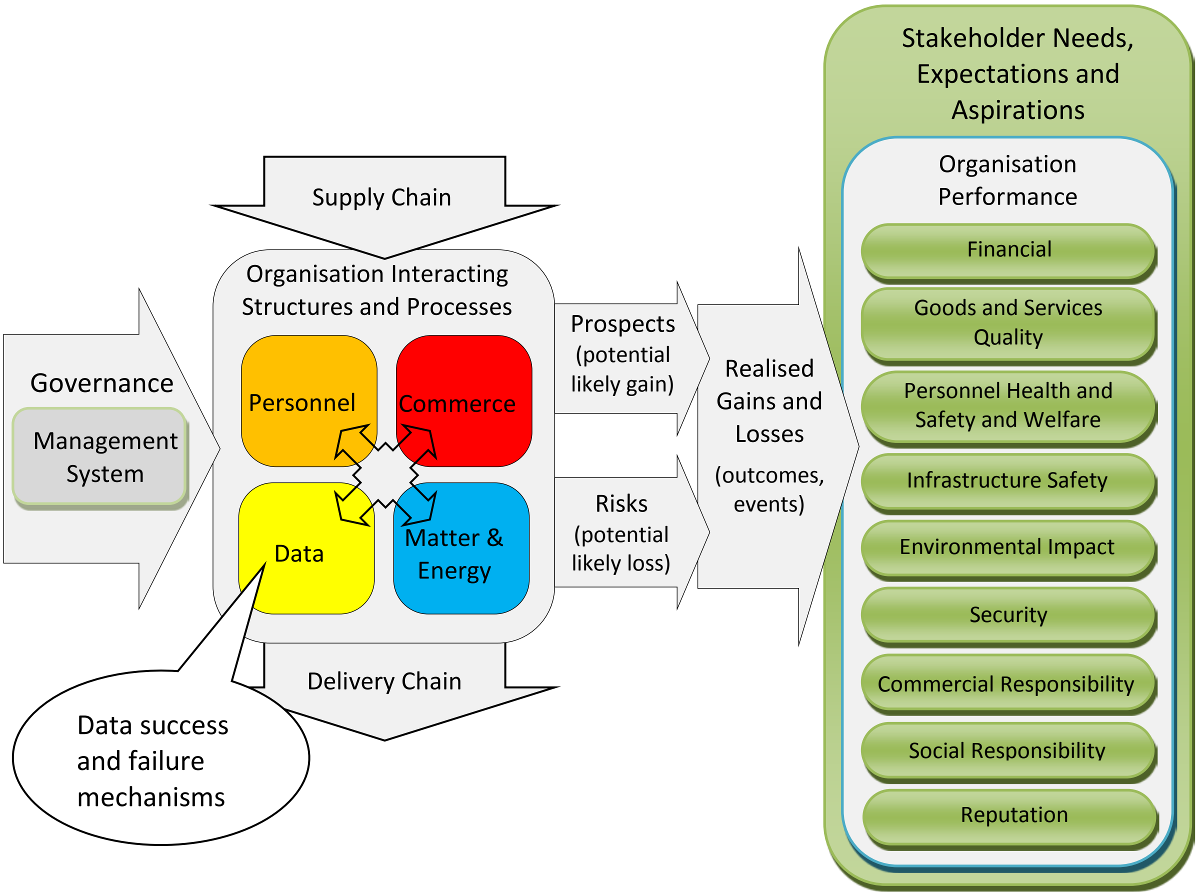

Stakeholder Needs, Expectations and Aspirations
Organisation Performance
Financial
Goods and Services Quality
Personnel Health and Safety and Welfare
Infrastructure Safety
Environmental Impact
Security
Commercial Responsibility
Social Responsibility
Reputation
Supply Chain
Organisation Interacting Structures and Processes
Personnel
Commerce
Data
Matter & Energy
Delivery Chain
Governance
Management System
Prospects (potential likely gain)
Risks (potential likely loss)
Realised Gains and Losses
(outcomes, events)
Data success and failure mechanisms

Figure 6: Governance of Prospect and Risk

Organisations exist to fulfil a purpose and mission but in order to achieve this, the organisation must address uncertainties contained in the prospects and risks of equitably satisfying the needs, expectations and aspirations of its stakeholders, and the uncertainties and variations in its internal structures and processes and in the external operational environment. It should be born in mind that data and other technology are just tools that do not become prospects and risks until their application potentially affects stakeholder needs, expectations or aspirations.

Data and other technology are just tools that do not become prospects and risks until their application potentially affects stakeholder needs, expectations or aspirations.

Prospect and risk pervades structures and processes relating to an organisation's:

- Strategy, tactics and operations,

- Internal and external environment,
- People, commerce, data, matter and energy, and suppliers,
- Stakeholder needs, expectations and aspirations, including conflicts.

Good management requires effective and efficient decision-making and the direction and guidance of the structures and processes that deliver goods and services. This uncertainty must be taken into account in order to make optimal decisions relating to data and satisfying stakeholders – refer to Figure 6. See also Figure 5 on page 13, which illustrate the dynamics between data and the other elements of an organisation. While any potential option may have a prospect of gain, there is invariably the potential for one or more associated losses. The gains and losses may be sudden or occur over a longer period. These gains and losses are not absolute measures and can vary according to the needs, expectations and aspirations of each individual stakeholder or group of stakeholders.

When there is significant uncertainty in potential outcomes, reasoned judgements need to be made informed by evidence and analysis, as far as this is practicable. An optimal decision necessitates the maximising of prospect while minimising the associated risks. This is achieved by using two principal approaches that should both be embedded into the organisation's formal management system addressed in Section 5. The first approach involves the implementation of general prospect and risk controls based on good data management practices e.g. password protection, document and record controls. The second is to implement controls based on prospect and risk assessment performed on the particular circumstances of the organisation. The degree of sophistication that this prospect and risk assessment is conducted should be appropriate to the circumstances and may involve a number of methodologies. Both of these approaches may be mandated by stakeholders via legislation and contractual arrangements. Requirements and guidance on these two approaches may be found in standards, addressed in Section 5.5, and within legislation and associated guidance applicable to the region and type of industry.

Where the uncertainty of potential outcomes is significant, formal prospect and risk management assessment can help facilitate better judgements and decisions. It also makes the processes more transparent to stakeholders and aids independent review and approval where this is applicable. This is the focus of Section 4.1.

4.1 Prospect and risk assessment

Organisations can improve the likelihood of realizing their objectives by the systematic conduct of prospect and risk assessments and developing prospect and risk controls using methodologies with an appropriate degree of sophistication matched to the circumstance. The only justification for using any degree of systematic prospect and risk assessment is where the organisation is likely to be more successful employing it than not, or in order to satisfy a stakeholder requirement. All of an organisation's activity should ideally add optimal value. The organisation or project should not deploy resources in conducting any prospect or risk assessment or with a degree of formality or with a degree of rigour where there is little expectation of adding value, unless it is a stakeholder-mandated requirement.

> The only justification for using any degree of systematic prospect and risk assessment is where the organisation is likely to be more successful employing it than not, or in order to satisfy a stakeholder requirement.

Prospect and risk assessment should consider intended and unintended consequences of all significant structures and processes. It facilitates the definition and implementation of physical and administrative controls to improve the likelihood of the organisation being more successful.

A wide range of management tools and techniques are available to guide prospect and risk assessment processes and training in their use is recommended.

A prospect and risk assessment general approach is shown in Figure 7 following the approach of MSS 1000. The cycle of prospect and risk planning, identification, analysis, assigning of controls and their acceptance should be repeated until an acceptable level of residual prospect and risk is achieved. The stages of the prospect and risk assessment cycle are described in the following subsections.

Intelligent threats present a special challenge for prospect and risk management because the source of the nature of the threat may change when the person(s) gains knowledge of the proposed or implemented prospect and/or risk controls. The source of an intelligent threat could be for example a criminal or a competitor or even a terrorist. The threat can be external or internal to the organisation. Refer to Sections 3.3 and 4.1.5.

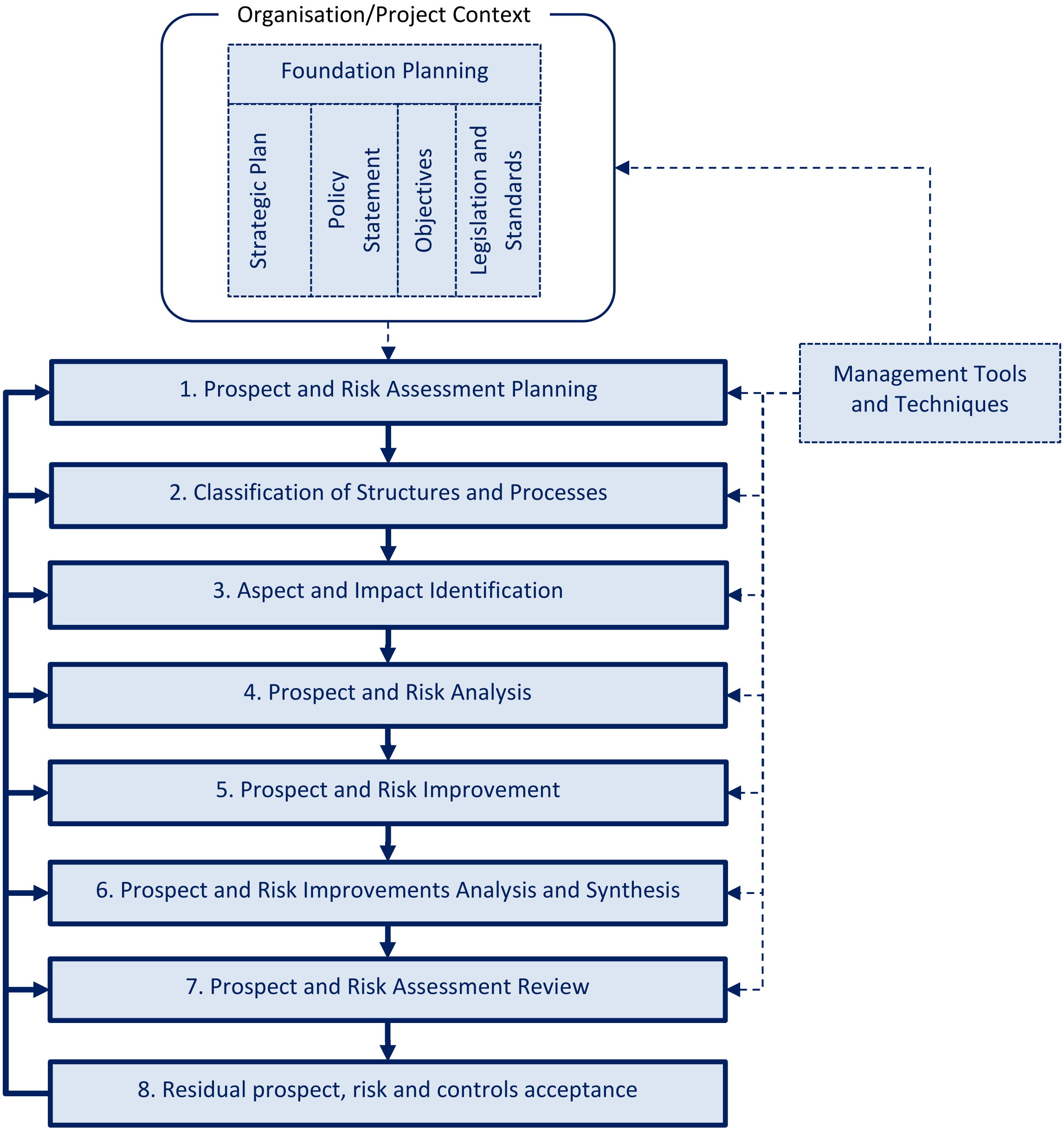

Organisation/Project Context
Foundation Planning
Strategic Plan
Policy Statement
Objectives
Legislation and Standards
Management Tools and Techniques
1. Prospect and Risk Assessment Planning
2. Classification of Structures and Processes
3. Aspect and Impact Identification
4. Prospect and Risk Analysis
5. Prospect and Risk Improvement
6. Prospect and Risk Improvements Analysis and Synthesis
7. Prospect and Risk Assessment Review
8. Residual prospect, risk and controls acceptance

Figure 7: Prospect and Risk Assessment Cycle (MSS 1000)

4.1.1 Prospect and risk assessment planning

Careful planning of the prospect and risk assessments is important to ensure that appropriate methodologies are applied with an appropriate degree of rigour, by competent personnel, for each aspect of the organisation’s structures and processes. This helps achieve the greatest degree of management control for the resource expended.

The degree of application of prospect and risk assessment can only be justified by the degree that it may facilitate improved management control and the adding of value to the various facets of organisation performance. Prospect and risk assessment should therefore not be applied blindly or ritualistically but with good judgement and common sense. In addition to the aspects that the organisation can control directly, it needs to determine whether there are aspects that it can indirectly influence. These may be related to goods and services used by its suppliers, as well as goods and services that it delivers to others external to the organisation. Irrespective, it is the organisation that should ultimately determine the degree of control and influence that it is able to exercise over its aspects and impacts.

Prospect and risk assessments should consider all aspects of performance including personnel, commercial, data, matter, energy, suppliers, normal and contingency structures and processes, change, reputation and security etc., and attempt to equitably balance the needs, expectations and aspirations of customers and other stakeholders while making the best use of resources.

> Technologies or methodologies should not be selected or applied within an organisation or project without considering the prospects and risks of the organisation or project as a whole viewed as a system. A system is only as strong as its weakest link requiring, for example, that cyber and non-cyber data prospect and risk controls should be equally robust.

Technologies or methodologies should not be selected or applied within an organisation or project without considering the prospects and risks of the organisation or project as a whole and its components viewed as a system. A system is only as strong as its weakest link requiring, for example, that cyber and non-cyber data prospect and risk controls should be equally robust.

General and specialist prospect and risk assessments should be selected and used depending on the structures and processes of the organisation.

The conduct of prospect and risk assessments is often influenced by applicable legislation or standards. However, these requirements should be exceeded where necessary to ensure that the organisation's and stakeholder's objectives are optimized.

The organisation should select from the wide range of management tools and techniques that are available to help in guiding prospect and risk assessment processes. Typical management tools are listed in in MSS 1000 and ISO 31010. Prospect and risk assessment methodologies should only be adopted and used to a degree that they add value.

Assessments should cover strategic, tactical and operational structures and processes embracing: personnel including stress, commerce, data, matter and energy including infrastructure and materials, goods and services supply and delivery chains, contingency arrangements, and temporary and permanent change including experiments.

4.1.2 Classification of structures and processes

The classification of physical and non-physical structures and processes according to their potential to impact perceived stakeholder needs and expectations allows controls to be appropriately applied to prospect and risk assessment processes i.e. more sophisticated and rigorous assessments would be applied to structures and processes with a higher perceived potential to impact stakeholder needs and expectations. The process assists in applying graded management control resulting in effective and efficient use of management resources.

4.1.3 Aspect and impact identification

Prospects of fulfilling the purpose of the organisation or project or structure or process while equitably satisfying stakeholder needs and expectations should be identified. This means identifying opportunities and hazards/threats which was addressed in Section 3 Data opportunities, hazards and threats. This should be achieved via creative innovative thinking conducted individually or in teams using appropriate methodologies. The intended and unintended consequences of each prospect should be identified.

4.1.4 Prospect and risk analysis and synthesis

The intended and unintended consequences of existing or proposed structures and processes should be analysed and synthesized using appropriate prospect and risk assessment methodologies. The application of analysis and synthesis ensures that the individual and collective impact of data and other elements are addressed contributing to prospects and hazards. Attempts should always be made to meet stakeholder needs and expectations via creative innovative thinking conducted individually or in teams.

Prospect and risk assessments should be recorded using prospect and risk registers or other suitable database. This may be in the organisations own format or that supplied by a stakeholder which also satisfies the organisation's requirements. A stakeholder format should not be adopted that does not satisfy the organisation's requirements, which can also be required to demonstrate compliance with legislation. An example prospect and risk register is shown in Appendix A: Example Prospect and Risk Log Structure

Expert advice should be sought for the selection and application of numeric prospect and risk assessment tools and methodologies and should only be used by competent personnel.

4.1.5 Prospect and risk improvement

The role of prospect and/or risk improvement within prospect and risk assessment is to increase prospect and/or reduce risk. Prospect and risk controls may be engineered into structures and processes or may be administrative and form part of the management system.

It should be noted that the effectiveness of risk controls associated with an intelligent threat will to a large extent be dependent on the relative effectiveness of risk reduction barriers compared with those of other organisations – the perceived softer target will naturally be selected. A self-serving irresponsible individual or organisation will tend to seek out weaknesses in risk barriers and the organisations with the weaker barriers most vulnerable as they are selected preferentially to organisations with more robust risk barriers. See Section 3.3 that addresses malicious threats.

Considering the assessed uncontrolled prospects and/or risks analysis and synthesis, attempts should be made to improve the prospects and reduce the risks by the application of engineered or administrative controls. Risk should be reduced to a level that is low or otherwise tolerable, and definitely not unacceptable. Prospect and risk controls should be applied that are appropriate and proportionate to the assessed levels and should take account of relevant legislation and codes of good practice. Selection of controls should take account of a prospect enhancement and risk reduction hierarchy such as the following:

- Elimination,
- Substitution,
- Transfer, share, cooperate,
- Engineered controls (includes computer system embedded rules),
- Administrative controls (competence, training, procedures, signage, conventions etc.)
- Personal protective equipment (health and safety),
- Contingency arrangements – refer to Appendix B.

Redundancy, diversity, segregation and limiting the size of inventory may be used to increase prospect and/or reduce risk in the design of structures and processes. Risk of environmental pollution may be prevented or reduced by source reduction or elimination, structure or process change, efficient use of matter and energy including substitution, reuse, recovery, recycling, reclamation and treatment and contingency arrangements.

Risk may be considerably reduced by employing multiple diverse physical or administrative protective barriers known as defence in depth. However, multiple prospect/risk barriers have the potential to fail via common cause failure. Personnel can be a typical source of common cause failure e.g. the same person may operate, maintain or malevolently interfere with the intended independent diverse barriers. This type of risk may be reduced by disallowing a single person to perform critical actions and to minimise the possibility of group conspiracies.

Commercial prospects may be increased or risks may be reduced through redundancy so that for example the organisation is not unduly dependent on a single customer or supplier respectively and also through diversity where for example supply of a good or service would not fail because of a common cause. Regulation is often used to reduce the dominance of large powerful organisations which may inequitably act against stakeholder needs and expectations and may also present an unacceptable risk should they fail because of their size. Governments may also act to stop the failure of large organisations believing them to be of such strategic importance that they are deemed too large to be allowed to fail.

Where significant risk mitigation is practicable following an event, arrangements should be developed through the provision of suitable contingency structures and processes.

Residual prospect and risk must be low or tolerable as judged by stakeholders. Expert advice should be sought if this is in doubt.

4.1.6 Prospect and risk improvements analysis and synthesis

The role of prospect and risk improvements analysis and synthesises is to determine the residual prospects and risks and to provide data to establish the extent of prospect and/or risk improvement through controls. If the prospect and/or risk controls are ineffective or fail, the organisation/project/task may be exposed to the uncontrolled prospect and/or risk.

This data should be used to inform the program of planned proactive monitoring of the organisation.

4.1.7 Prospect and risk assessment review

Prospect and risk assessments require continual review to ensure that that they remain relevant and fit-for-purpose. Changing circumstances should trigger a review but is also prudent to review arrangements periodically because changes in the circumstances may have occurred and have remained unrevealed or not acted upon. New opportunities for prospect and risk controls may also have occurred through technological or other innovation.

4.1.8 Residual prospect, risk and controls acceptance

The role of residual prospect and risk and controls acceptance should be conducted by a designated responsible manager and needs to be confident that the prospect and/or risk assessment has been conducted according to the organisation's approved arrangements, making use of expert advice and support as appropriate.

There is normally limited knowledge when it comes to rare or novel events with serious consequences due to the rarity of the occurrence of such events. In such circumstances, the organisation should apply the precautionary principle to ensure that there is sufficient knowledge of the associated prospect and risk to justify a proposal.

The degree and criticality of the prospect and risk controls should influence the planned monitoring associated with structures and processes.

4.2 What is acceptable prospect and risk?

As explained at the beginning of Section 4, an organisation must attempt to maximise prospect while minimising risk. As a minimum, there should be an aggregate net financial gain that is acceptable to the relevant stakeholders and will sustain the financial viability of the organisation. However, this is only part of what satisfies stakeholders - they may have personal values that are expressed through their needs, expectations and aspirations. Potentially these may span all the facets of an organisation's performance such as finance, goods and service quality, personnel health, safety and welfare, infrastructure safety, environmental, security, commercial integrity, social integrity and reputation – refer to Figure 6 on page 22.

The organisation must ensure that not only the net likely gain is acceptable but also that any individual prospect or risk is acceptable as judged rationally or irrationally by any stakeholder. This is shown conceptually in ###. This is especially important if the stakeholder is able to exert power affecting the operations of the organisation.

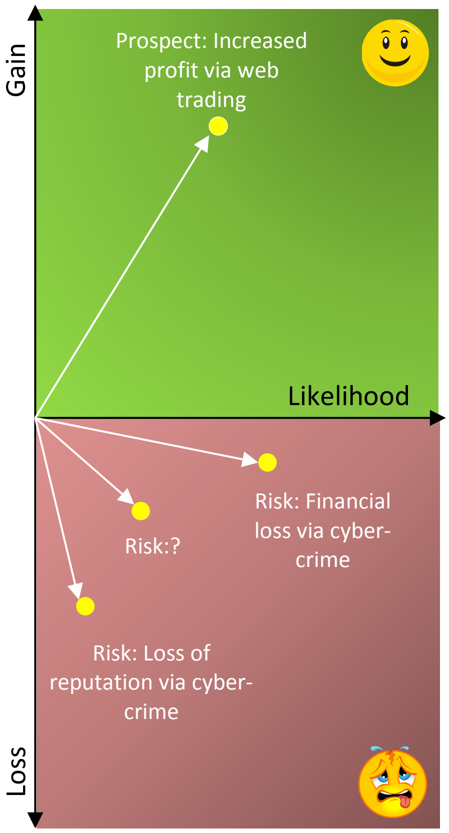

Gain
Prospect: Increased profit via web trading
Likelihood
Risk:?
Risk: Financial loss via cyber-crime
Risk: Loss of reputation via cyber-crime
Loss

Figure 8: Prospect and Risk Plot

This is often a complex analysis beyond the scope of this paper but it is only going to be possible if an organisation properly understands the needs, expectations and aspirations of its stakeholders within the short and longer terms. This is made more complicated because of the ongoing evolution in the way that data is used in delivering goods and services covered in section 2.

Figure 8 shows how prospects and risks can be plotted graphically on a diagram using coordinates representing gain/loss and likelihood of realisation. Curves may be plotted representing prospect or risk functions where the likelihood of various levels of gain/loss needs to be considered. An example of this is the plotting of natural disasters such as earthquakes etc. with different severities.

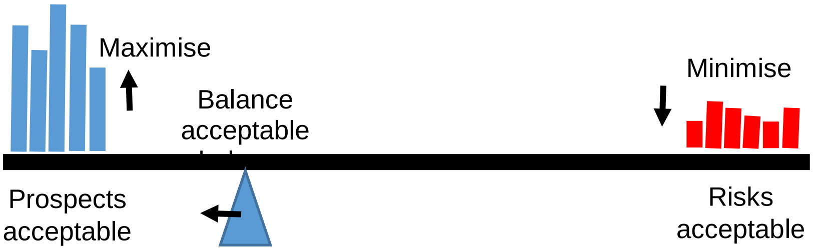


Figure 9: Optimisation of Prospect and Risk

The optimisation of prospect and risk is shown conceptually in Figure 9. Regarding any identified option, the organisation should ensure that:

a) Stakeholder needs, expectations and aspirations and their potential to exercise power over the organisation's activity is sufficiently understood, including that exercised through legislation,
b) That the prospect(s) are sufficiently rewarding to warrant the commitment of resources,
c) Any individual associated risk is acceptable to the relevant stakeholder(s) or may be equitably agreed by stakeholders,
d) Overall, the net prospect is acceptable to the relevant stakeholders and will help sustain the organisation,
e) Unless it is the only option, it is the best overall option when compared with others.

4.3 Performance justification

In some circumstances stakeholders require organisations to produce a structure and/or process justification, e.g. safety cases for major hazard industrial plants, justification of measurement processes in laboratories and submissions to planning or licensing authorities. These generally constitute a structured argument supported by evidence to provide a required level of stakeholder confidence.

Responsibilities and arrangements need to be defined for ensuring that the performance justifications remain current and legitimate.

Performance justifications are often contained in design dossiers, project files, safety cases, planning applications etc. and typically include ‘prospect and risk assessments’, ‘structure and process definitions’, test data and research findings etc. and specific requirements to be demonstrated to a third party such as a regulator, investor or insurer.

5. Systematic management of data

The effective management of data is a critical component of the governance of an organisation. Not only should it not be managed in isolation of other aspects, it must be managed systematically so that the whole organisation follows common good practices that collectively optimally deliver goods and/or services fulfilling the purpose of the organisation. The key is the development and implementation of a fully integrated management system based on universal management principles that subsume quality and risk management best practices. A fully integrated management system not only addresses the management of all the complex and diverse data applications within the organisation, it also helps to manage change as data technology continues to evolve.

A fully integrated management system not only addresses the management of all the complex and diverse data applications within the organisation, it also helps to manage change as data technology continues to evolve.

5.1 What is a management system?

A management system is simply the organisation's overall plan or blueprint for how it is to be managed and operated in order to deliver its purpose, which is the supply of goods and/or services to satisfy customers. Put more formally, a management system is a set of formally defined intentions, principles, rules and guidance used to systematically manage an organisation's structures and processes to achieve its objectives. A management system can be primitive or very sophisticated and can even manage its own evolution based on feedback and analysis of customer and other stakeholder needs and expectations. All organisations, whatever their type and size, can benefit from an appropriate management system. As managing all aspects of change is critical to success, these processes also need to be included in the management system. While the prospect of change may be high there are nearly always associated risks requiring a systematic project based approach.

A management system is simply the organisation's overall plan or blueprint for how it is to be managed and operated in order to deliver its purpose, which is the supply of goods and/or services to satisfy customers.

Everyone's behaviour, within their respective roles with respect to data and the other elements, should be compliant with the management system and made aware during their induction, training and supervision. Some elements such as policy statements are broad-brush principles with a generic focus while others are sharply focused operational instructions.

5.2 Benefits of a management system

Many new organisations created by intelligent and creative people grow to a size where they struggle to manage because they lack a management system and are constantly micro managing every detail such they have no time to develop and grow the organisation let alone get time to play an occasional game of golf. A management system allows senior management to give clear formal direction and guidance on how the organisation is to be managed and operated. It frees up higher management to focus on developing the organisation's vision and strategic planning, rather than constant intervention or 'firefighting' in operational processes. This enables personnel throughout the organisation to perform much better in their respective roles and to interact effectively and efficiently with others internally and externally to the organisation.

A formal management system provides a home for the organisation's explicit management knowledge and a firm basis for review and subsequent improvement initiatives. It is a very significant data structure within an organisation and a powerful and valuable asset contributing to effective and efficient management control.

5.3 Management system architecture

The wisdom contained in an organisation's management system, if it is to be of any value, must be easily accessible to each person who needs direction and guidance. Management system architecture, like building architecture should be functional but also elegant so that employees are comfortable interacting with it, value it and take an active role in its evolution and improvement. Although there are many structures used in practice, management system architecture has tended to be layered, typically three, forming upper, middle and bottom tiers, each with a specific role, as shown in Figure 10.

> Management system architecture, like building architecture should be functional but also elegant so that employees are comfortable interacting with it, value it and take an active role in its evolution and improvement.

The top tier covers the general management arrangements and includes one or more general policy statements communicating the organisation's values and commitments with respect to stakeholder's needs, expectations and aspirations relating to the organisation's performance, such as finance, goods and service quality, personnel health, safety and welfare, infrastructure safety, environmental, security, commercial integrity, social integrity and reputation. It also describes the nature of the organisation, its management philosophy to fulfil its purpose and equitably satisfy its stakeholders' needs, expectations and aspirations while making the best use of resources. The top tier may also include maps that show how the management system links to clauses of adopted management system standards and significant regulations related to management of the organisation. This helps make the management system transparent to other parties.

The middle tier focuses on management control and typically includes management procedures and job descriptions that implement the management system policy and objectives defined in the top tier. It provides direction and guidance to managers.

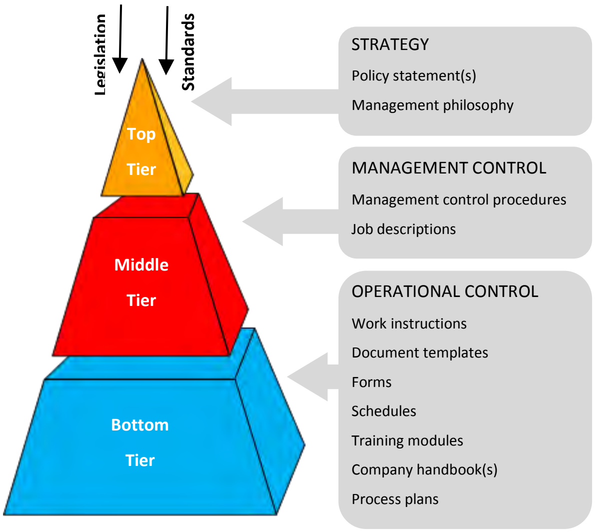


Figure 10: Typical Management System Structure

The bottom tier focuses on operational control and includes a range of documents that control the organisation's day-to-day operations. These documents give direction and guidance to those carrying out operations and many assist in generating operational records e.g. document templates and forms. Company handbooks provide a way of communicating essential information to employees and contractors and often replicate information contained elsewhere in the management system documentation.

5.4 Integrated management systems and data management

As described in Section 1, data tends to be intertwined throughout an organisation's processes that deliver its goods and services. It embraces normal delivery processes, contingency processes and change processes. Process owners and participants span the whole organisation at all levels. Optimal use of data within the processes requires a holistic perspective where every detail is viewed with relation to the whole in an attempt to achieve an overall optimisation of organisation performance equitably satisfying customers and other stakeholders while making the best use of resources. Because of the interconnectedness, a separate management system solely focusing on managing data and ignoring the role of data with respect to the functioning of the organisation as a whole is not the ideal way to maximise the achievement of objectives.

Fortunately for data management, after a long period of operating separate dedicated management systems each focused on a different aspect of an organisation's performance, integrated management systems are becoming the norm. A survey of IIRSM and Chartered Quality Institute members in 2011 showed that 4 out of 5 organisations already had an integrated management system or were intending to implement one <add ref>. While many integrated management systems have only been partial in the past, it is likely that organisations will progress to fully integrated management systems and this is important to effectively and efficiently manage data across the whole organisation throughout all of its structures and processes. Integrated management is elaborated further in the IIRSM paper 'Management Integration: Benefits, Challenges and Solutions - IIRSM' [Ref 2].

5.5 Management standards

There are several management system standards defining good practices that can assist with the effective and efficient management of data. They cover general management, prospect and risk assessment and specialist structure and process requirements related to data management and the organisation as a whole.

Two principal approaches are employed in management standards to enhance the management of prospects and risks within an organisation. One is the adoption of generic prospect and/or risk improvement practices e.g. not assigning personnel to posts, roles, or tasks unless they are competent or appropriately supervised. The other is to conduct appropriate prospect and risk assessments in order to develop proportionate prospect and/or risk improving controls. These two approaches normally operate within a 'plan do check act' management cycle. It should be noted that safety and security are the only two that are concerned with preventing loss by managing risk - all of the others such as commerce, goods/services quality, reputation, health and environment need to address the management of prospect and risk together in a holistic and balanced way.

5.5.1 Non-integrated management standards

Non-integrated management standards focus on a particular facet of the organisation's performance and have a scope that focuses on a subset of the totality of the organisation.

The most commonly used standard for data management systems is: ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements. It specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. ISO 27001 may also be used as a basis for third party certification of the organisation's integrated or non-integrated management system. There are also several supplementary standards providing guidance and detailed elaboration. An abstract of each standard can be read via the following hyperlinks:

- ISO/IEC 27002:2013 - Code of practice for information security controls.
- ISO/IEC 27003:2010 - Information security management system implementation guidance.
- ISO/IEC 27004:2009 - Information security management measurement.
- ISO/IEC 27005:2011 - Information security risk management.
- ISO/IEC 27006:2011 - Requirements for bodies providing audit and certification of information security management systems.
- ISO/IEC 27013:2012 - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-13.
- ISO/IEC TR 27019:2013 - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.
- ISO/IEC TR 27023:2015 - Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 270025.
- ISO/IEC 27031:2011 - Guidelines for information and communication technology readiness for business continuity.
- ISO/IEC 27036-3:2013 - Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security.

Other standards cover additional issues that the management systems must satisfy in order to demonstrate various stakeholder performance requirements. They cover goods and services quality, environmental protection, occupational health and safety and all facilitate third party certification. They each have supplements that are not listed in this document. They are as follows:

- ISO 9001:2008 – Quality management systems – Requirements.
- ISO 14001:2004 – Environmental management systems – Requirements with guidance for use.
- BS OHSAS 18001:2007 Occupational health and safety management systems. Requirements.
- ISO 22301:2012 - Societal security - Business continuity management systems - Requirements.

Social responsibility is covered in ISO 26000:2010 - Guidance on social responsibility but only provides general guidance, is not a specification for a management system and does not facilitate third party certification.

The scope of ISO standards generally covers all sizes of organisation. The ones listed above apply to organisations in general but other standards, not listed, have also been published focusing on particular industries and goods e.g. medical devices.

With respect to the wider management of data, ISO has currently no published management system standards explicitly addressing human resource management or business/commercial/financial management. ISO is currently developing ISO 45001 - Occupational health and safety.

ISO has continued to publish a proliferation of management standards applicable to an organisation's performance and many have not been listed above. This requires organisations to commit increasing resources to management system support and the maintenance of third party certification. While the adoption of an integrated management system makes the organisation's structures and processes more effective and efficient, the fragmented standards and third party certification services have placed an unnecessary burden on organisations. To counter this and aid comparison, ISO has implemented an internal program to align the main headings of its management system standards. This is generally known as alignment to ISO Annex SL. However, while this aids comparison between the standards the content requirements across the standards are not integrated and there is no common ISO set of universal management definitions. This presents a challenge in interpreting requirements for those inexperienced in their application.

5.5.2 Integrated and universal management standards

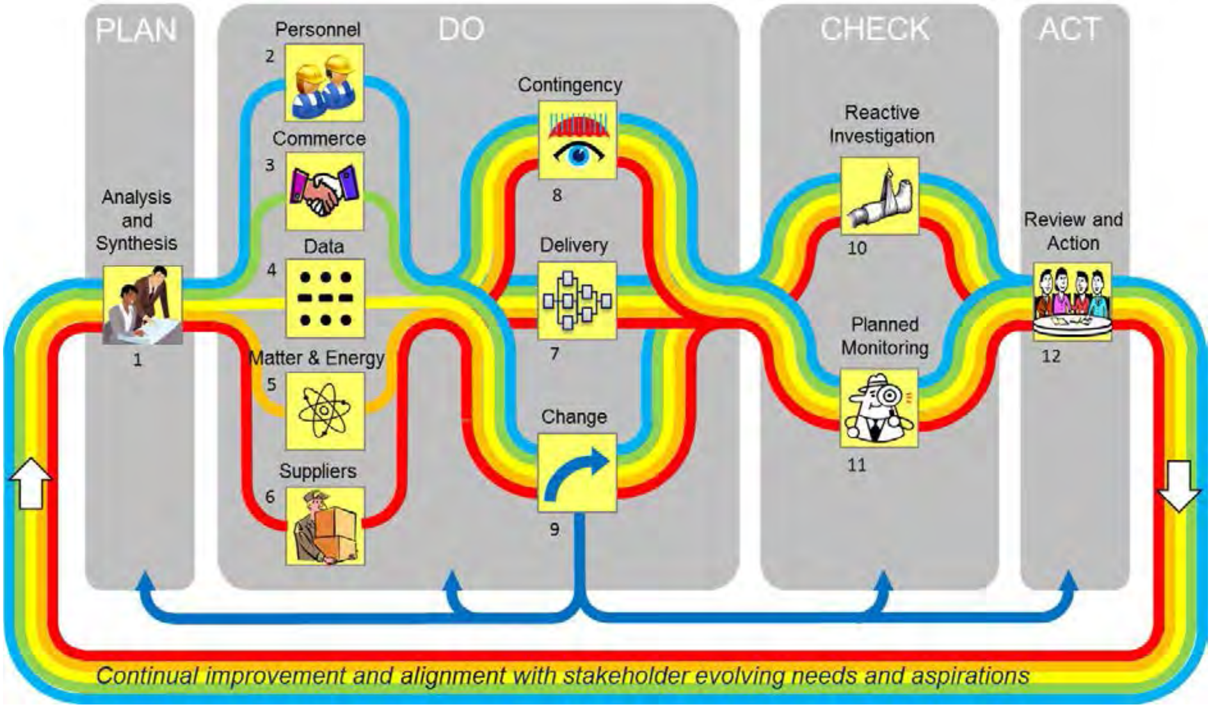


Figure 11: Universal Management Taxonomy

Integrated management standards are designed to address two or more management requirements normally under the control of separate specialist disciplines e.g. quality, environmental and occupational safety practitioners. Universal management standards take this further and facilitate and support full scope management systems addressing the management of the whole organisation and transcending management discipline silos.

The International Atomic Energy Agency merged many of its quality and safety standards taking an integrated approach. This resulted in simplification and removal of replication. However, the Chartered Quality Institute Integrated Management Special Interest Group is believed to be the first to create a fully universal management system standard facilitating full scope integrated management systems. MSS 1000:2014 Management System

Specification is a 300-page document that is free to download via the World-Wide-Web and contains both requirements and guidance. MSS 1000 covers the scope of all the ISO and BSI standards covered in Section 5.5.1 although it may not be so detailed in all areas. It enables an organisation via a single management system standard to create a fully integrated management system addressing the totality of an organisation. MSS 1000 also contains many other novel features meeting the management system needs of organisations and has a section addressing the management of data.

The reason that MSS 1000 is able to subsume the requirements of any management system standard is that it is structured on a universal hierarchical management topic structure (taxonomy) and seventeen universal management principles. This makes MSS 1000 to a large extent futureproof as well as still being open to continual improvement. While normally it is not advisable to align a management system with the sections of a management system standard, it is the opposite with MSS 1000. This is because the requirements structure has been deliberately designed to align with the structure of tried and tested fully integrated management systems that have been subjected to multiple certification processes. The twelve elements of the hierarchical structure and their relationship are shown in Figure 11 and are shown in full in Appendix B: Example Universal Management Topic Structure. It can be used for structuring a management manual or a set of management control procedures using just twelve universal sections or procedures respectively to cover the totality of managing any size or type of organisation. The structure allows the organisation to comprehensively address issues by fully focusing on its structures and processes that deliver its goods and/or services rather than focusing separately on multiple dimensions of performance.

6. Governance and management system maturity

Organisations exist and operate within a corporate world where the adoption of data technology can be heavily influenced by IT industry marketing, management trends and peer pressure from other organisations that it interacts with. Effective governance requires that the organisation is not unduly blinded by these pressures and manages and makes decisions based on or otherwise informed by prospect and risk management that equitably addresses the needs, expectations and aspirations of stakeholders while making the - best use of resources.

Organisations exist and operate within a corporate world where the adoption of data technology can be heavily influenced by IT industry marketing, management trends and peer pressure from other organisations that it interacts with.

The degree that an organisation manages data opportunities and threats/hazards depends on the sophistication of its governance arrangements and its management system or systems. Larger organisations are generally able to draw on internal sources of expert advice and support while smaller organisations may obtain it externally through their trade bodies, government advice and/or consultants. The maturity of the governance arrangements and management system is likely to depend on multiple factors such as:

The degree that an organisation manages data opportunities and threats/hazards depends on the sophistication of its governance arrangements and its management system or systems.

- The size of the organisation,
- Location, whether international and if an exporter and/or importer.
- Stakeholder demands,
- The complexity of relevant legislation and the degree of regulation,
- Range, complexity and risks associated with goods and/or services delivered.
- Complexity and risks associated with the organisation's systems and the degree that it uses advanced technology.
- Time since organisation was first established.

The following levels of maturity, in Table 6, are suggested as being likely to be observed in organisations and influenced by the factors above.

Table 6: Governance and Maturity Levels

Maturity Level	Awareness and Behaviour
1. Primitive.	Unaware of relevant data legislation or basic good practice.
2. Legislation and basic good practice aware.	Data legislation and basic good practice aware but no systematic arrangements in place to identify specific requirements and arrangements for compliance.
3. Legislation and good	Basic management system implemented to direct and guide

Maturity Level	Awareness and Behaviour
practice system.	personnel in basic data management requirements.
4. Data systems assurance.	Formal data management system in place meeting plan-do-check-act principles taking account of relevant data legislation and good practice but not based on formal prospect and risk assessment of the organisation's structures and processes.
5. Data principal modes of failure identified and controlled.	Identification and control of data modes of failure controlled physically and administratively via management system, but not based on risk assessment of the organisation's structures and processes
6. Overall organisation systems involving cyber and non-cyber data subject to prospect and risk analysis, and controlled.	Prospect and risk analysis applied to overall organisation structure and processes where data can be a significant component of stakeholder prospects and risks. Arrangements are embedded within a fully integrated management system embodying assurance principles. Each data centric analysis and synthesis is conducted within the context of the organisation as a whole and taking account of all relevant stakeholders. Have identified relevant standards and endeavour to maintain compliance – see Section 5.5 Management standards.

Each level will potentially add value and improve performance with respect to the management of data but operation at a lower level may leave the organisation exposed to avoidable and unacceptable prospect and risk. However, the higher levels of maturity do require more sophisticated management processes and expertise difficult for many organisations to access or afford.

7. Conclusion

Organisations currently exist within an ongoing data revolution as significant as the industrial revolution creating new opportunities, hazards and threats. The pace of this ongoing revolution is impossible to predict and whether it will continue indefinitely. The introduction of novel applications of data has the potential to assist with solving many problems and adding value but it can also create unintended consequences such that we potentially trade one set of problems for another.

The evolving and increasingly sophisticated use of data will require that organisations continually adapt and evolve in order to remain aligned with their stakeholder needs and expectations, and the organisation's internal and external operating environment. This will involve the redesign of the structures and processes that deliver goods and services with significant changes in the roles of personnel and the nature of work. This will result in economic, social and political effects.

Organisations as they currently exist will inevitably change to varying degrees, those that fail to adapt sufficiently, or quickly enough, may disappear. Many new organisations are likely to emerge to meet the demands of new data innovations and applications.

Organisations need to be competent at identifying data opportunities, hazards and threats and in the evaluation of the corresponding prospects and risks that affect customer and other stakeholder needs, expectations and aspirations. Organisations need to be viewed as systems that are only as strong as their weakest component – cyber and non-cyber data prospect and risk controls must be equally robust and as strong as the organisation as a whole.

As well as interfacing with personnel, the management system will increasingly interface with smart machines and things in general. Data will become increasingly intertwined with personnel, commercial, and matter and energy components that deliver the organisation's purpose via its goods and services. In the coming years many aspects of the current human role in organisations will be subordinated to IT processes and intelligent infrastructure raising many social, economic and political issues no less significant than those associated with the industrial revolution. Legislation and regulation will need to be globally harmonised keep up with the ongoing data revolution.

It is essential that management objectives are delivered via a fully integrated management system addressing the totality of the strategic, tactical and operational management of the organisation – it must nurture fully joined up management thinking processes and be prospect and risk informed with an equitable degree of stakeholder upside and downside balance. Data and other technology are just tools that do not become prospects and risks until their application potentially affects stakeholder needs, expectations or aspirations.

> The sophistication of the management system will need to be more than a match for the data induced challenges.

The sophistication of the management system will need to be more than a match for the challenges created by the evolving use of data. The organisation should neither lag nor be too far ahead of the wind of data innovation. Failure to achieve this will degrade the effectiveness and efficiency of its structures and processes making it less competitive and more vulnerable to failure.

As explicit knowledge and data as a whole are very valuable organisation assets, it is appropriate that data should be prominent within its governance arrangements. Ultimately, success will depend on every structure and process owner, manager and participant being competent and diligent in their respective duty, and coordinating and cooperating with others. As always, success will critically depend on the awareness, commitment and governance of top management, it's allocation of resources, its cooperation with stakeholders, and its effective coordination of the activities of the organisation as a whole.

> Ultimately, success will depend on every structure and process owner, manager and participant being competent and diligent in their respective duty, and coordinating and cooperating with others.

Organisations are often established with primitive governance arrangements and management systems. This leaves them potentially vulnerable to unrevealed risks that may harm performance and unrevealed unexploited prospects that could enhance performance. It is important that organisations become aware of their governance and management system maturity and take appropriate management action to improve it to the highest level within the limitations of what is practicable for the size and type of organisation.

The work in this paper has put the management of data within the overall context of managing an organisation in order to achieve its purpose and equitably satisfy its stakeholders while making the best use of resources. It has shown how to systematically apply prospect and risk assessment via an integrated approach taking account of separate ISO standards or by directly adopting a universal standard such as MSS 1000. It has enabled the management of issues such as cyber threats to be understood within the context of overall organisation security transcending silo disciplines. The content of the paper will therefore aid organisations to improve their strategic, tactical and operational management of cyber and non-cyber data and the systems in which they reside. It will be particularly valuable to organisations managing major hazards and threats. This orderliness of thinking and the ability to take a pragmatic prospect and risk management approach should lead to better decision-making and enhanced performance. Further research to confirm this would be valuable.

Bibliography

1. National Risk Register of Civil Emergencies 2015 edition – UK Cabinet Office.
2. Management Integration: Benefits, Challenges and Solutions - IIRSM.
3. MSS 1000:2014 Management System Specification – Chartered Quality Institute.
4. ISO 9001:2008 - Quality management systems - Requirements.
5. ISO 14001:2004 - Environmental management systems - Requirements with guidance for use.
6. BS OHSAS 18001:2007 Occupational health and safety management systems. Requirements.
7. ISO 22301:2012 - Societal security - Business continuity management systems - Requirements.
8. ISO 22313:2012 - Societal security - Business continuity management systems - Guidance.
9. ISO 26000:2010 - Guidance on social responsibility.
10. ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements.
11. ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls.
12. ISO/IEC 27003:2010 - Information technology - Security techniques - Information security management system implementation guidance.
13. ISO/IEC 27004:2009 - Information technology - Security techniques - Information security management -- Measurement.
14. ISO/IEC 27005:2011 - Information technology - Security techniques - Information security risk management.
15. ISO/IEC 27006:2011 - Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems.
16. ISO/IEC 27013:2012 - Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-13.
17. ISO/IEC TR 27019:2013 - Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.
18. ISO/IEC TR 27023:2015 - Information technology - Security techniques - Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 270025.
19. ISO/IEC 27031:2011 - Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity.
20. ISO/IEC 27036-3:2013 - Information technology - Security techniques - Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security.
21. ISO 28000:2007 - Specification for security management systems for the supply chain.
22. ISO 31000:2009 - Risk management - Principles and guidelines.
23. ISO/TR 31004:2013 - Risk management - Guidance for the implementation of ISO 31000.

24. IEC 31010:2009 - Risk management - Risk assessment techniques.
25. ISO 45001 - Occupational health and safety (under development).
26. ISO Annex SL – management system standard common structure.
27. Wolfram Alpha - timeline of systematic data and the development of computable knowledge.

Definitions

General definitions used in this paper are the universal management definitions contained within MSS 1000:2014. Neither the International Standards Organisation or the British Standards Organisation uses a universal set of management definitions.

Adware

Computer software that automatically displays or downloads advertising material such as banners or pop-ups when a user is online.

Artificial intelligence

Apparent intelligence exhibited by machines or software.

Note 1: It is also the name of the academic field of study focusing on how to create computers and computer software that are capable of intelligent behaviour i.e. the science and engineering of making intelligent machines. This is currently not achievable and thought by many not to be possible.

Aspect

Characteristic of an organization's policy, asset, operation or event that has or may potentially have an impact on something valued by a stakeholder.

NOTE 1: Impacts may occur at local, regional and global scales, while they may also be direct, indirect or cumulative by nature.

NOTE 2: Aspects may include planned and unplanned events.

NOTE 3: The most important aspects of an organization needing to be identified and managed are those significantly impacting the needs and expectations of stakeholders and typically include those with the potential to or actually impact the environment, people and the economy in both the short and long term.

Cryptography

The art of protecting data by processing it (encrypting it) into an unreadable format, called cipher text.

Cyber

Relating to computer systems and networks.

Data

Facts, statistics, or items of information.

NOTE 1: Data may include alphanumeric text, numbers, photographs, video, software etc.

NOTE 2: Data over its life cycle may be created, stored, accessed, processed, communicated, shared, replicated, encrypted, lost, corrupted, stolen or destroyed.

NOTE 3: Data may move in space up to the speed of light and exist in time over its lifecycle.

Encryption
See cryptography.

Firewall (computers)
Technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts.

Information technology
Application of computers and telecommunications equipment to store, retrieve, transmit and process data.

Hardware (computers)
Collection of physical elements that comprise a computer system.

Impact
Positive or negative effect on a person's, an organization's or a stakeholder's objectives, needs, expectations or aspirations resulting from an aspect of the organization.

NOTE 1: It includes effects on the organization's policy, commitments and objectives.

NOTE 2: Objectives, needs and expectations include facets of performance such as those impacting humankind, environment and commerce.

Malware
Malware is short for malicious software and is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It does not include software that causes unintentional harm due to some deficiency. Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

Management system
Set of formally defined intentions, principles, rules and guidance used to systematically manage an organization's structures and processes to achieve its objectives.

NOTE 1: A management system typically comprises elements such as policy statement, descriptions of management approach and philosophy, management procedure, job descriptions, work instructions, document template(s), forms, schedules, training modules, handbooks, contingency plans and process definitions. See also Definition of Document Types.

NOTE 2: A management system is normally formally recorded to facilitate its control and communication. A management system may be recorded and communicated using any suitable communication media or a mixture of them.

NOTE 3: A management system may operate on part or on all of the organization's levels as well as projects and covers management planning, implementation of management controls, Reactive investigation and planned monitoring, and review and action to support continual organizational learning and improvement.

NOTE 4: A management system is used by an organization to control and guide its processes in order to consistently achieve the organization's objectives effectively, efficiently and with agility. It is distinct from other non-management systems within the organization that it may direct or guide.

NOTE 5: A management system may be integrated to various degrees or fully Integrated.

Mode
A way or manner in which something occurs or is experienced, expressed, or done.

NOTE 1: A mode may be associated with the way a structure or process may succeed or fail e.g. success and failure modes analyses.

Prospect
Combination of the potential gain and the likelihood of its realization. It may also be defined as the combination of an opportunity and the associated likelihood of being realized. See also risk, prospect and risk.

NOTE 1: Gain may be financial or any other perceived benefit.

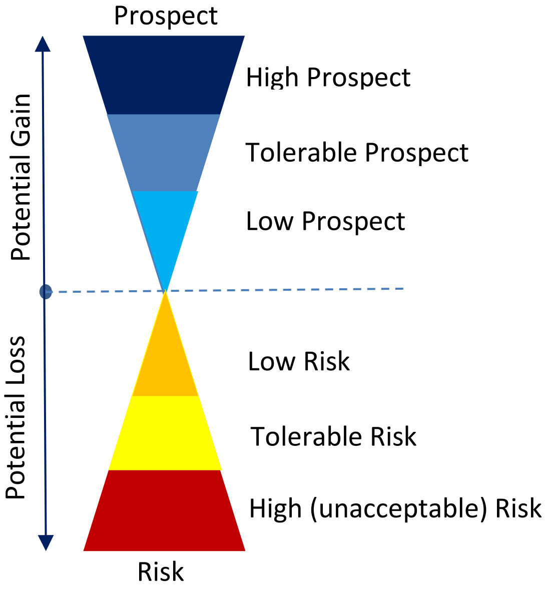
NOTE 2: Prospect is conceptually negative risk. The preferred term is 'prospect'.

Prospect and risk
Respective combinations of positive and negative consequences of a potential event or outcome and the associated likelihood of occurring.

NOTE 1: Prospect and risk are stakeholder judgements or perceptions of whether value is likely to be created or lost and may vary according to the stakeholder and are therefore relativistic and may even conflict with other stakeholders.

NOTE 2: Prospect and risk may be understood conceptually as the mirror of each other.

NOTE 3: Prospect and risk may coexist, may exist in close physical or virtual proximity and may be mutually



dependent.

NOTE 4: Prospect and risk may be space or time dependent e.g. during a scenario or during the changes of the seasons etc.

Figure 12: Prospect and Risk

NOTE 5: Estimates of prospect or risk may be expressed qualitatively or quantitatively.

NOTE 6: The aggregation of prospect and risk is generally not meaningful and should only be done if the respective profiles are similar and expressed in the same units.

NOTE 7: High prospect combined with low risk is the most desirable.

Ransomware
Type of malicious software designed to block access to a computer system until a sum of money is paid.

Risk
Combination of the potential loss and the likelihood of its realization. See also prospect, prospect and risk.

NOTE 1: Negative consequences may include any types of actual or perceived loss or realised threat such as harm to personnel, the environment, commerce, data, suppliers or any other asset structure or process.

NOTE 2: Risk is conceptually negative prospect.

NOTE 3: Loss is that perceived by the stakeholder.

Scareware
Form of malicious computer software that uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying unwanted software.

Software
Programs and other operating data used by a computer.

Spyware
Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

System
Set of elements forming a connected whole.

NOTE 1: A system is structural in nature.

Trojan horse
Any malicious computer program which is used to hack into a computer by misleading users of it's true intent.

Virus
Self-replicating computer programs which install themselves without user consent.

NOTE 1: They are a malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive.

Worm
Standalone malware computer program that replicates itself in order to spread to other computers.

NOTE 1: Worms often use a computer network to spread themselves relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing software program.

NOTE 2: Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Appendix A: Example Prospect and Risk Log Structure

This appendix supports section 4.1.4 Prospect and risk improvements analysis and synthesis. The material is reproduced from MSS 1000:2014 Appendix 3.4.

Figure 13 below provides an example of how a prospect and risk register may be structured for an organisation or project to record uncontrolled and controlled prospect and risk ratings derived from prospect and risk assessments. It acts as a transparent structure to help guide and iterate assessments, facilitate independent peer review, demonstrate compliance with the organisation's prospect and risk criteria, indicate where planned monitoring should be particularly focused, and act as a basis for assessing the impacts of proposed changes within the organisation or project.

The register structure may be adapted to suit the particular needs of the organisation and may be recorded on a spreadsheet or database. Conditional formatting may be employed to promote colour-coded communication (CCC). Absolute prospect and risk estimates may be used instead of prospect and risk ratings.

Typical data entered is as follows:

1. **Reference Number**. This should ideally be an organisation/project universal hierarchical reference to aid identification and traceability.

2. **Structure and/or process**. This defines the focus of the prospect and/or risk assessment.

   An additional column may be added to record the structure and/or process classification e.g. cyber data and non-cyber data storage and processing systems.

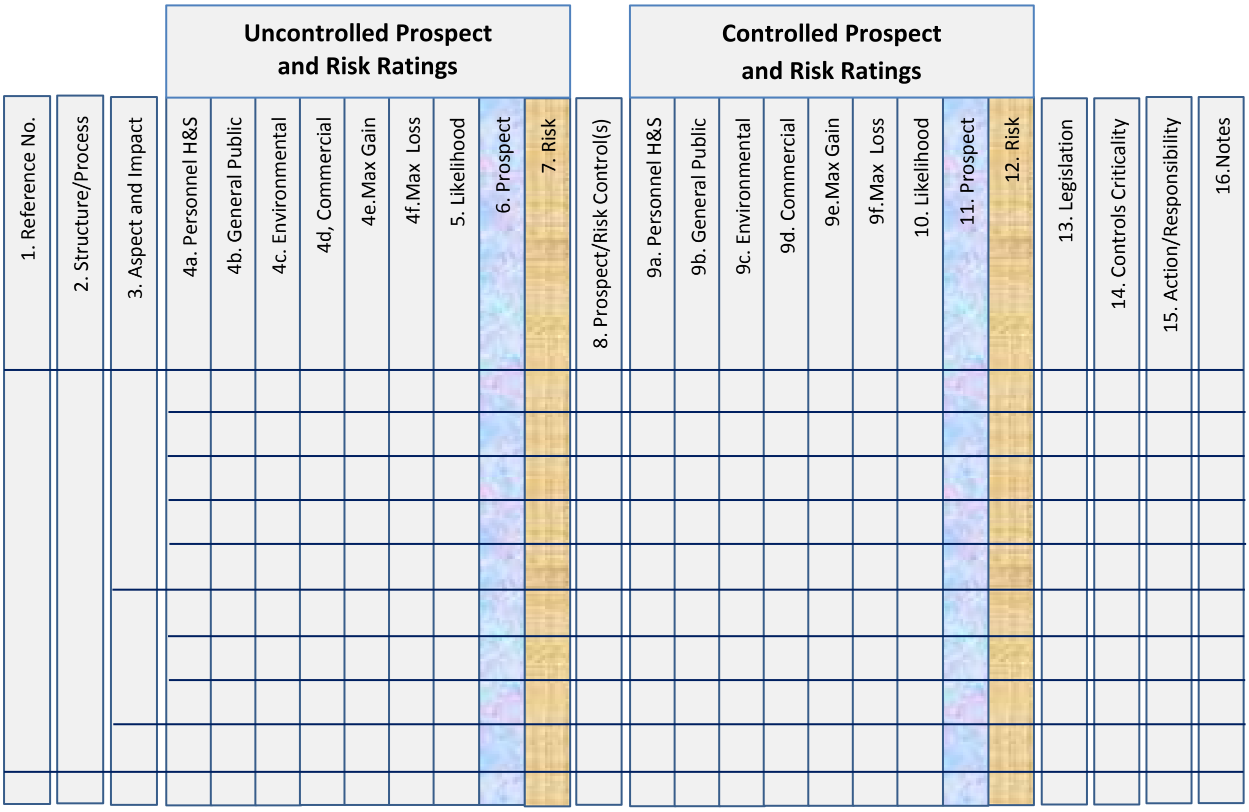
3. **Aspects and Impacts (opportunities, threats, hazards)**. This defines the particular aspects and impacts associated with the structure and/or process that may be viewed positively or negatively by stakeholders e.g. health and safety of people, the environment, commerce and assets etc. These aspects and impacts can be recorded in separate dedicated columns.

4. **Uncontrolled Potential Gain and/or Loss Ratings**. 4a to 4d record the assessed uncontrolled potential gain and loss ratings or computed values. Universal risk ratings are explained in Appendix 3 of MSS 1000:2014. 4e and 4f record the highest gain rating and the lowest risk rating respectively. Gain ratings should be recorded as positive and loss ratings as negative.

5. **Uncontrolled Likelihood**. This is the assessed uncontrolled likelihood rating for the potential event.

6. **Uncontrolled Prospect**. This is the combination of the 4e and 5 ratings and represents the maximum uncontrolled prospect.

7. **Uncontrolled Risk**. This is the combination of the 4f and 5 ratings and represents the highest uncontrolled risk.



			Uncontrolled Prospect and Risk Ratings										Controlled Prospect and Risk Ratings												
1. Reference No.	2. Structure/Process	3. Aspect and Impact	4a. Personnel H&S	4b. General Public	4c. Environmental	4d, Commercial	4e.Max Gain	4f.Max Loss	5. Likelihood	6. Prospect	7. Risk	8. Prospect/Risk Control(s)	9a. Personnel H&S	9b. General Public	9c. Environmental	9d. Commercial	9e.Max Gain	9f.Max Loss	10. Likelihood	11. Prospect	12. Risk	13. Legislation	14. Controls Criticality	15. Action/Responsibility	16.Notes

Figure 13: Example Prospect and Risk Register Structure

8. **Prospect and/or Risk Control(s)**. These are the physical and/or administrative controls applied by management to increase prospect and/or reduce risk and may include contingency structures and contingency processes.

9. **Controlled Potential Gain and/or Loss Ratings**. 9a to 9d record the assessed controlled potential gain and loss ratings corresponding to step 4 above.

10. **Controlled Likelihood**. This is the assessed controlled likelihood rating for the potential event corresponding to step 5 above.

11. **Controlled Prospect**. This is the combination of the 9e and 10 ratings and represents the maximum uncontrolled prospect corresponding to step 6 above.

12. **Controlled Risk**. This is the combination of the 9f and 10 ratings and represents the highest controlled risk corresponding to step 7 above.

Appendix B: Example Universal Management Taxonomy

The following hierarchical structure of management topics may be used to structure fully integrated management systems. It is elaborated in more detail in MSS 1000. Refer to Section 5.5.2.

1. Assessment and Development of Controls

1.1. Foundation planning.

1.2. Strategic plan.

1.3. Policy statement.

1.4. Objectives.

1.5. Legislation and standards.

1.6. Prospect and risk assessment.

1.7. Performance justification.

1.8. Management tools and techniques.

2. Personnel

2.1. Organisation.

2.2. Responsibilities and authorities.

2.3. Provision of expert advice and assistance.

2.4. Employment life cycle - *recruitment, induction, appointment, competence, welfare, work absence and rehabilitation, post or role change, discipline, leaving.*

2.5. Personnel Interactions – *interfaces, communication, consultation, participation and reporting, management of conflict.*

3. Commerce

3.1. Entity maintenance.

3.2. Marketing.

3.3. Contracts - *pre-contract, failure to establish a contract, contract implementation, post contract.*

3.4. Finance – *revenue, payments, banking and cash.*

4. Data

4.1. Management system structure.

4.2. Data control - *databases, internal documents, external documents, library, contract documents and data, infrastructure and goods documentation and data, marketing literature and website, computer software, records, access, loss and corruption.*

4.3. Data Processing – *accounts, indicators.*

4.4. Conventions - *style and colour, nomenclature, dimensions, language.*

5. Matter and Energy

5.1. Selection and combination.

5.2. Handling and use – *receipt, transport, storage.*

5.3. Processing.

5.4. Infrastructure - *facilities, work environment, plant and equipment, configuration, access, egress and protective barriers.*

5.5. Maintenance, inspection, testing and calibration - *proactive and reactive.*

5.6. Waste and emissions.

6. Suppliers

6.1. Classification, vetting and control.

6.2. Specification and ordering.

6.3. Receipt.

6.4. Performance evaluation.

7. Normal Structures and Processes

7.1. Structure and process design and development - *structure and process definition, repetitive and frequently conducted processes, non-repetitive and infrequently conducted processes, significant prospect and risk systems of work, projects, goods and services design and development, measurement and testing.*

7.2. Structure and process implementation.

7.3. Structure and process cessation.

8. Contingency Structures and Processes

8.1. Contingency planning.

8.2. Contingency arrangements implementation – *nonconformities, emergencies, crises and disaster recovery, intentionally halted processes, defect notification and recall, insurance, project contingency arrangements.*

8.3. Contingency arrangements testing.

8.4. Contingency arrangements training.

8.5. Event response.

9. Change

9.1. Change management life cycle.

9.2. Corrective and preventive action.

9.3. Strategic and tactical change.

9.4. Operational structure and process change.

9.5. Project change.

9.6. Management system change.

10. Reactive Investigation

10.1. Internal reactive investigation - *evidence preservation, evidence reporting, investigation and analysis of root causes.*

10.2. External reactive investigation.

11. Planned Monitoring

11.1. Monitoring planning.

11.2. Internal audit.

11.3. External audit.

11.4. Independent audit and surveillance.

11.5. Inspection.

11.6. Survey and benchmarking.

11.7. Self-monitoring and vigilance.

12. Review and Action

12.1. Review scheduling.

12.2. Review.

12.3. Review output and action.

12.4. Action realization.