Risk Management DEMO Training

Implementing Risk Management among NSOs

Intermediate and Advanced Level

Geneva, 27/29 September 2017

Ben Whitestone, UK – ONS

Fabrizio Rotundi, Italy - ISTAT

modernistats

Objectives

- To acquire practical tools for the implementation of a risk management system to align with the characteristics of statistical organizations;

- To share good risk management practices related to the topics covered by the training course.

Agenda

- Establishing the context
- Risk Management Standards
- Development of risk appetite statements
- Integrated Risk Management Frameworks – integrating Quality Management and Agile Delivery with Risk Management
- Wrap-up and close

Up front assumptions

- Attendees understand basic risk management vocabulary.
- Attendees work within organisations who have or are aiming to have a risk management approach.
- Attendees have an appetite to grow their maturity in risk management.

On target expectations

- Exercise – attendees to highlight what they want to gain from the training. Check back at the end.

Risk Management Standards

Management Systems Network

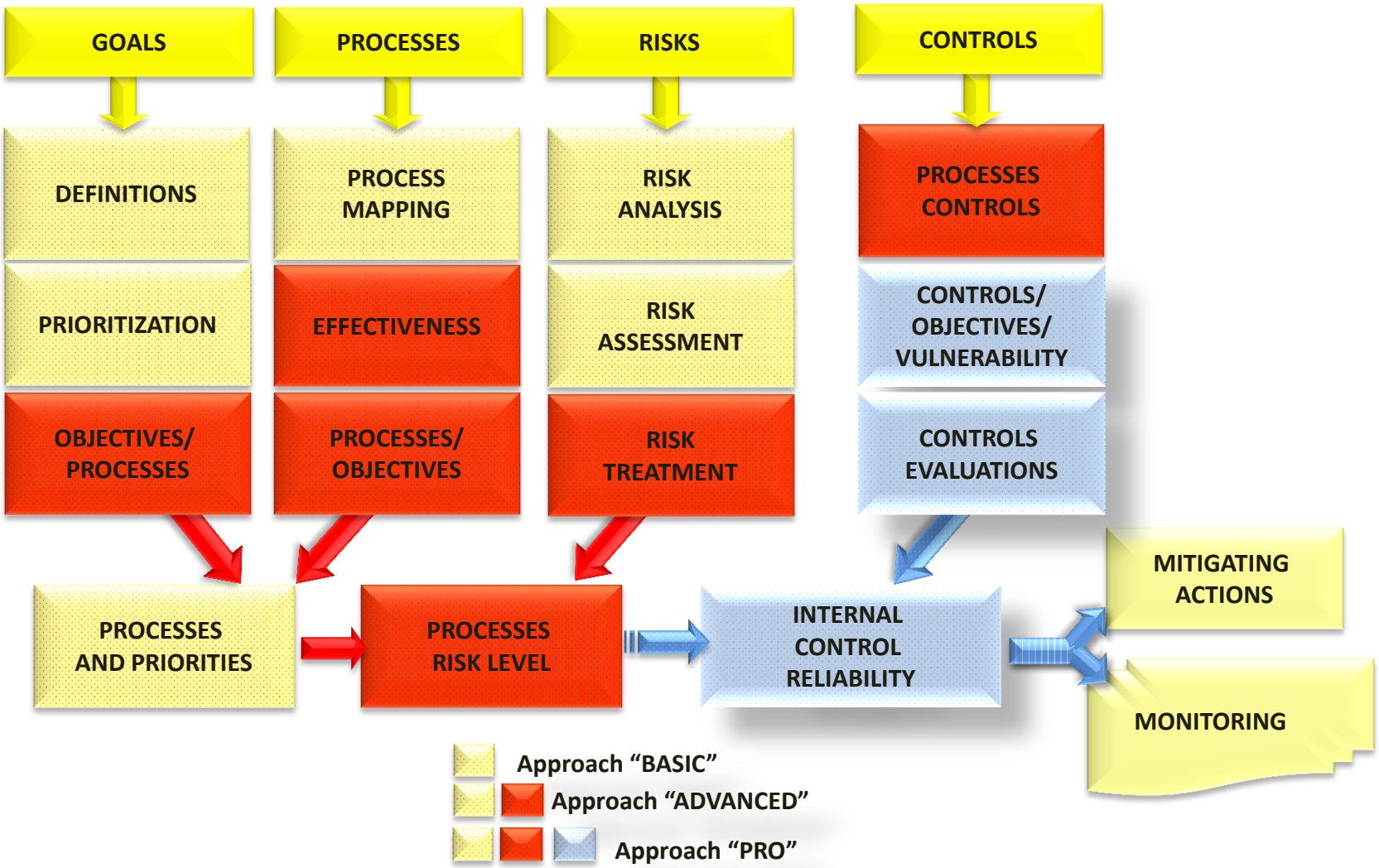
- ☑ *No overlapping !!*
- ☑ *More quality of services and products*
- ☑ *Supporting decision-making processes*
- ☑ *Enhancement of transparency*

- ☒ *Initial investment in resources and training*
- ☒ *Organizational re-thinking of production processes*
- ☒ *High innovation but low experience in P.A.*

Protecting and strengthening:

- *Tangible and intangible assets*
- *Organizational culture*
- *Leadership and relationship*
- *Effectiveness and efficiency*
- *Resources for priorities*
- *Stakeholder's satisfaction*

Risk Management approach



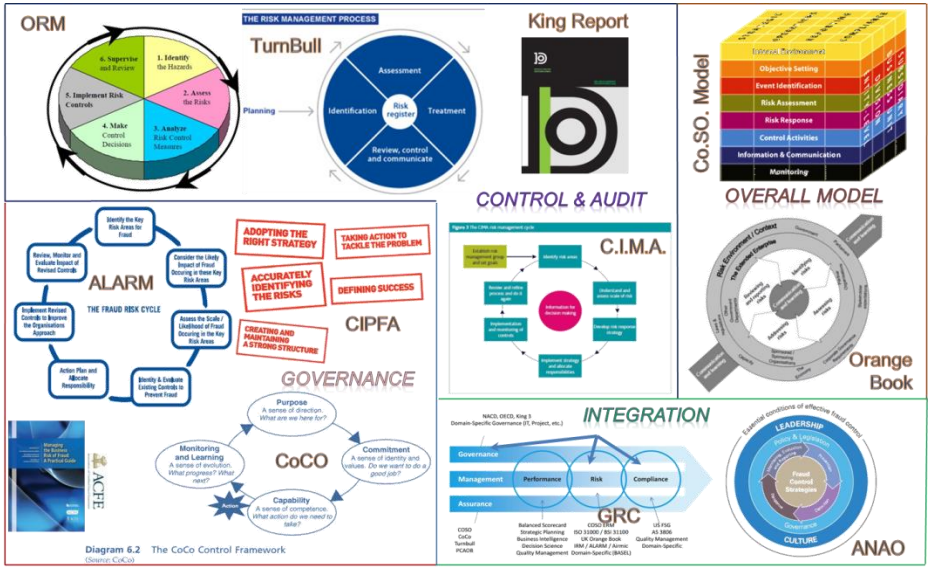
STANDARD - Definition

*The standard is **a method, generally recognized, to create a product, manage a process**, provide services and/or goods; it is a rule coming from the experience of people who, **thanks to their competences, know the needs of the organizations they belong to (producers, sellers, buyers, trade associations, users and regulators).***

Standards:

- have been **developed to help organizations** implement RM systematically and effectively
- seek to **establish a common view on frameworks**, processes and practice, recognized at international level, used by either public and private companies, regularly updated
- reflect the **different motivations and technical focus** of their developers and are appropriate for different organizations and situations
- are **normally voluntary**, although adherence to a standard may be required by regulators or by contract

Risk management standards



Selected standards:

- **ISO 31000:2009** – RM Principles and Guidelines
- **COSO 2004/2013** - ERM- Integrated Framework
- AS/NZS 4360:2004
- IRM/Alarm/AIRMIC 2002 – UK
- ***Especially for managing the Business Risk of Fraud:***
- ANAO - Australian National Audit Office

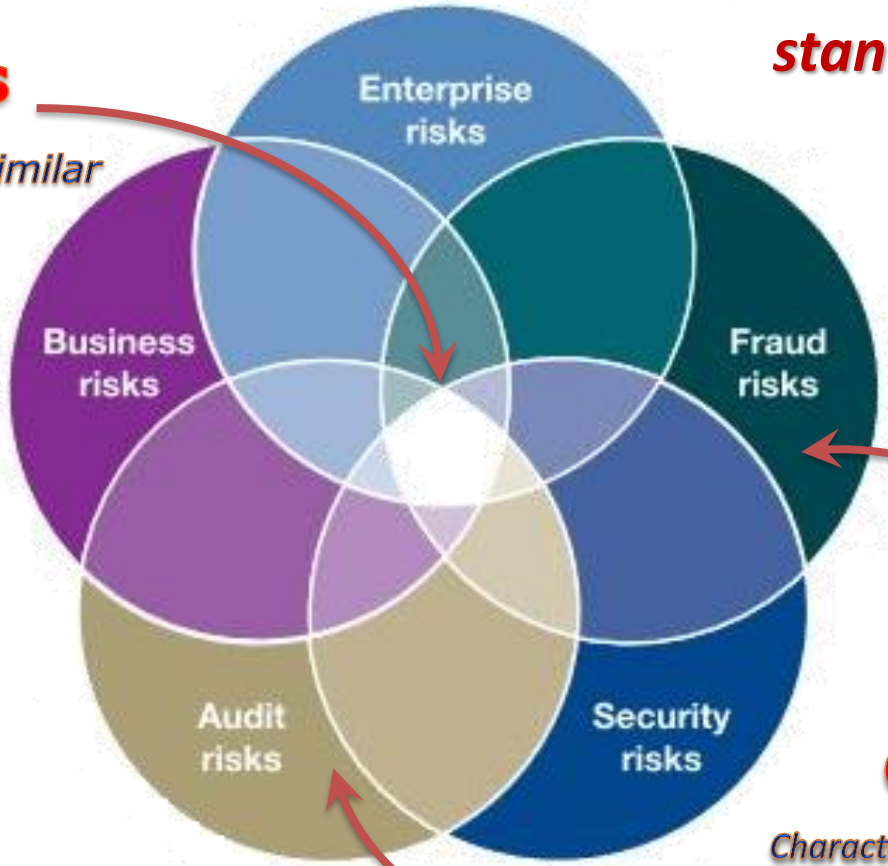
UNI Italian standard by UNI (Italian National Unification body)
EN European standard realized by CEN (European normalization Committee)
UNI EN European standard transposed in Italy
ISO international standard realized by ISO
UNI ISO international standard realized by ISO and adopted in Italy
EN ISO European standard realized by CEN and identical to an ISO standard
UNI EN ISO international standard realized by ISO, adopted by CEN and transposed in Italy
UNI/TS National techinical requirements
UNI CEN/TS European technical requirements transposed in Italy
UNI CEN ISO/TS International technical requirements adopted by CEN and transposed in Italy
UNI/TR National technical report
UNI CEN/TR Italian translation of an European technical report
UNI ISO/TR Italian translation of an International technical report

Risk Management Systems

Differences among standards

RM Process

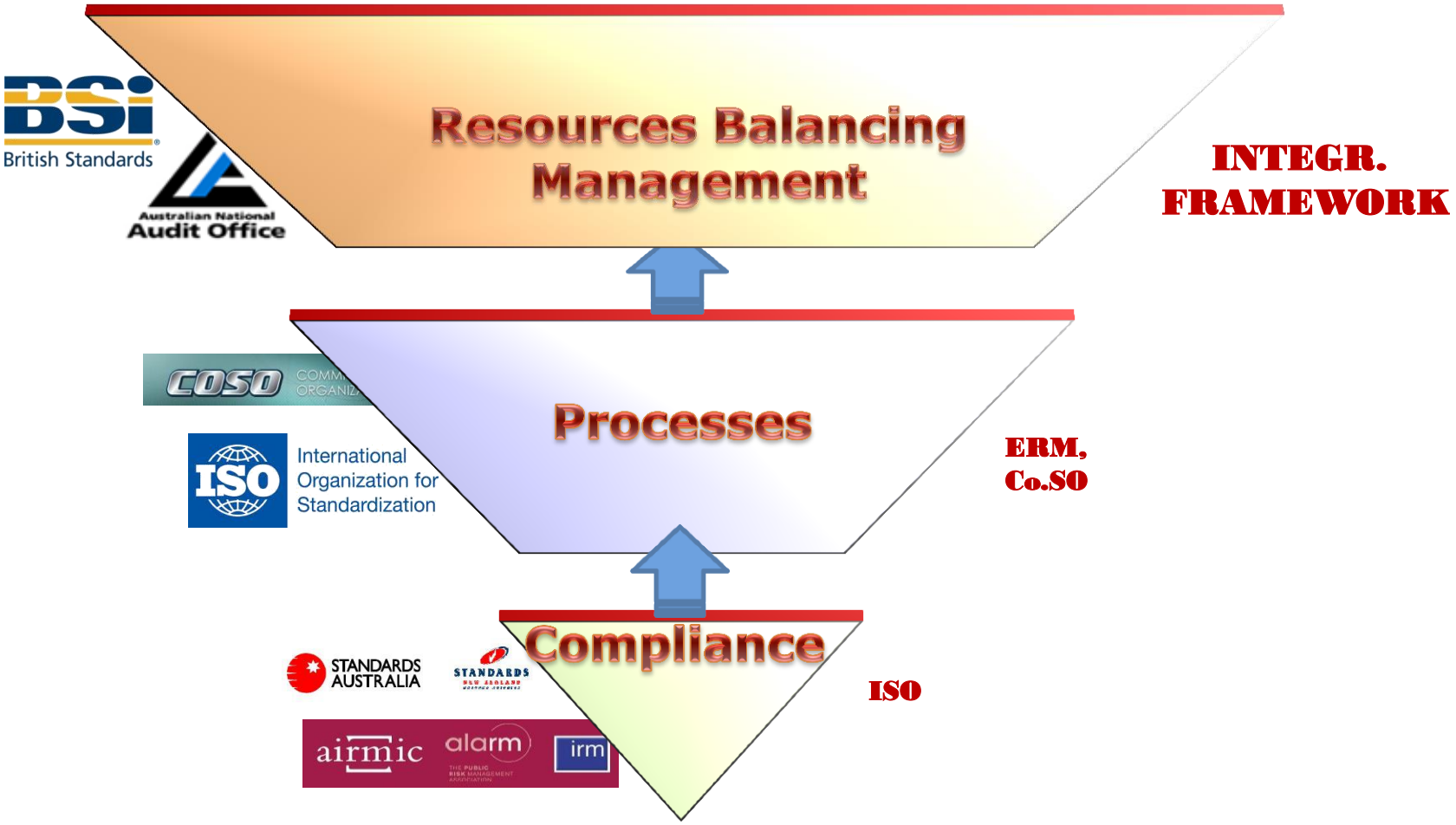
Process phases are very similar



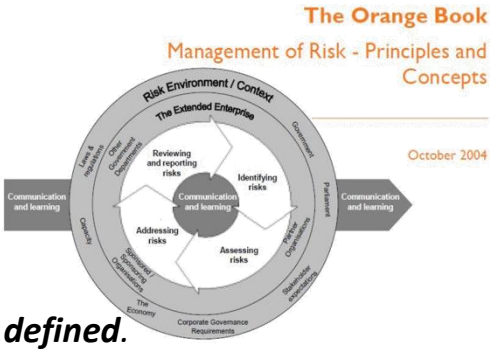
Objects

Characteristics distinguishes approach

Conceptual Framework Map



International Standards



The Orange Book

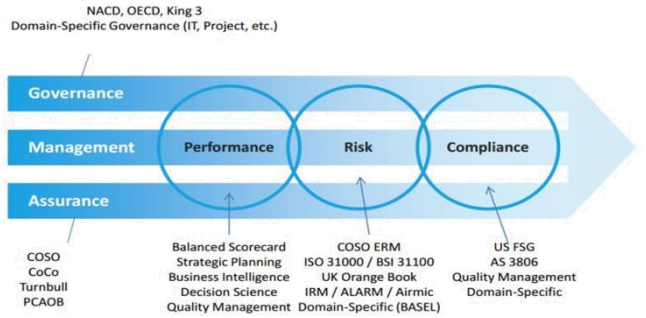
- *The management of **risk has not a linear process**; rather it is the balancing of a number of **interwoven elements which interact** with each other and which **have to be in balance** with each other if risk management is **to be effective**.*
- *The whole model has **to function in an environment** in which **risk appetite has been defined**.*
- *The **particular stage** of the process to manage any particular risk **will not necessarily be the same for all risks**.*

Operational Risk Mangement

- ***Accept no unnecessary** risk that **does not bring adequate returns** in terms of benefits or opportunities*
- ***Make risk decisions at the right level** on allocating resources to reduce or eliminate the risk and implement controls*
- ***Accept risk when benefits outweigh the cost***
- ***Anticipate and manage risk** by planning because **subsequent changes are more expensive** and take more time*

Red Book. *«**Principled Performance**» is an **integrated approach** to business that helps organizations achieve the objectives in a reliable manner, **addressing uncertainty and acting with integrity**.*

*It is based on the selection of the **standards more fitting** to an organization to manage: **Performance, Risk and Compliance***



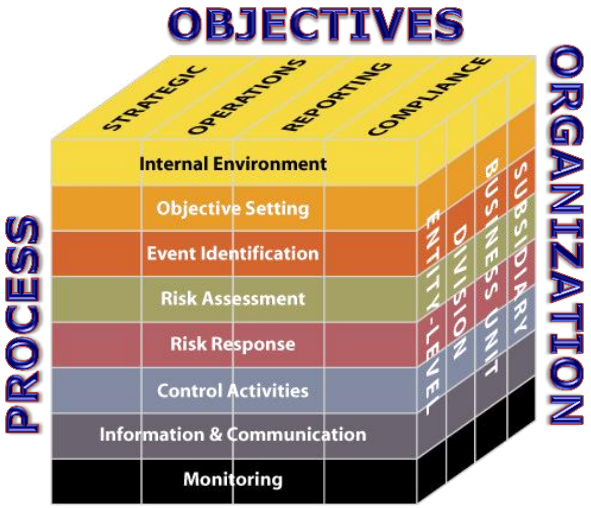
Risk assessment: standards' strengths

Components	ISO 31000 e ss.	ERM	AZ/NZS 4360	ALARM	ANAO
Governance:					
Context analysis,,,,	✔	✔	✔	✔	✔
Actors and responsibilities		✔			
Processes:					
Communication	✔	✔	✔	✔	✔
Context definition	✔	✔	✔	✔	✔
Identification	✔	✔	✔	✔	✔
Analysis	✔	✔	✔	✔	✔
Evaluation of existing controls			✔		
Weighting	✔	✔	✔	✔	✔
Treatment	✔	✔	✔	✔	✔
Monitoring and review	✔	✔	✔	✔	✔
Controls and audits	✔	✔	✔	✔	✔

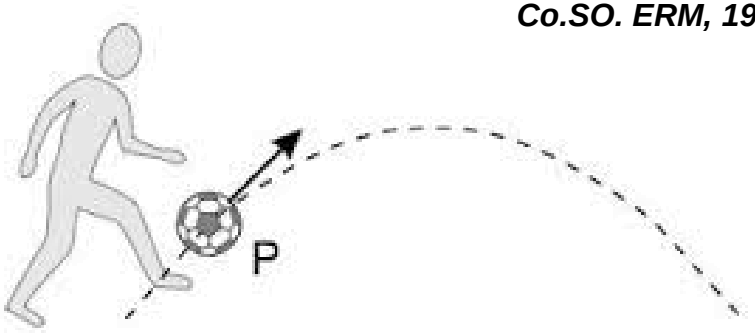
Enterprise Risk Management – ERM

RISK *is the* ***effect of uncertainty on objectives*** *as a deviation from the expected (positive and/or negative) achievements, resulting from the combination of the likelihood and effect of one or more potential events.*

Enterprise Risk Management (ERM) *is " ... a* ***process*** *effected by an entity's board of directors and management, applied* ***in strategy setting and across the enterprise,*** *designed to identify* ***potential events that may affect the entity,*** *and manage risk to be* ***within its risk appetite,*** *to provide* ***reasonable assurance*** *regarding the achievement of entity objectives."*



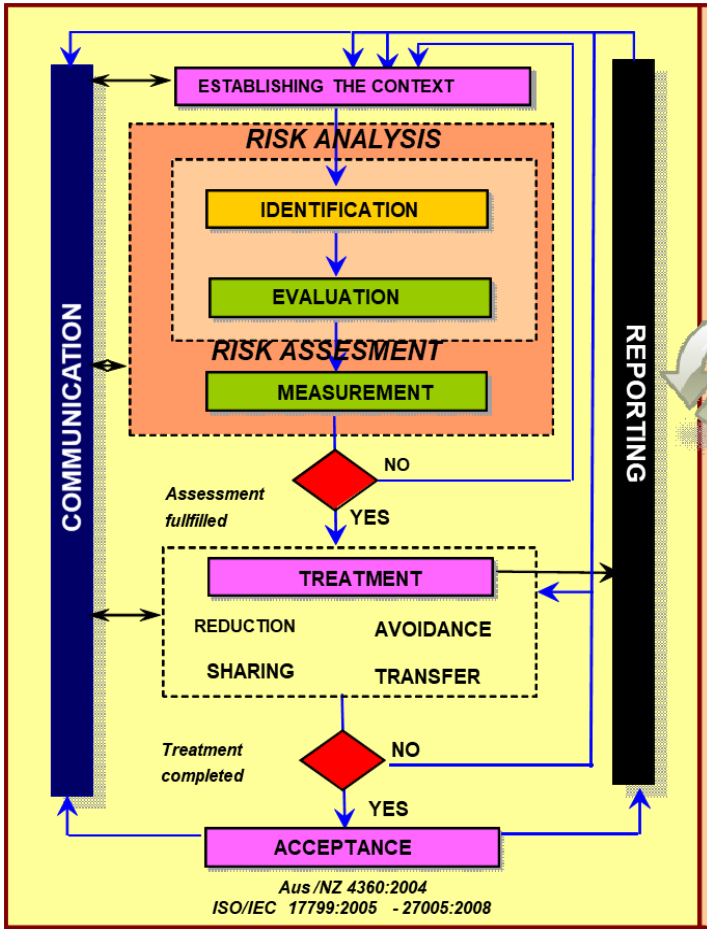
Co.SO. ERM, 1992/2004/2013

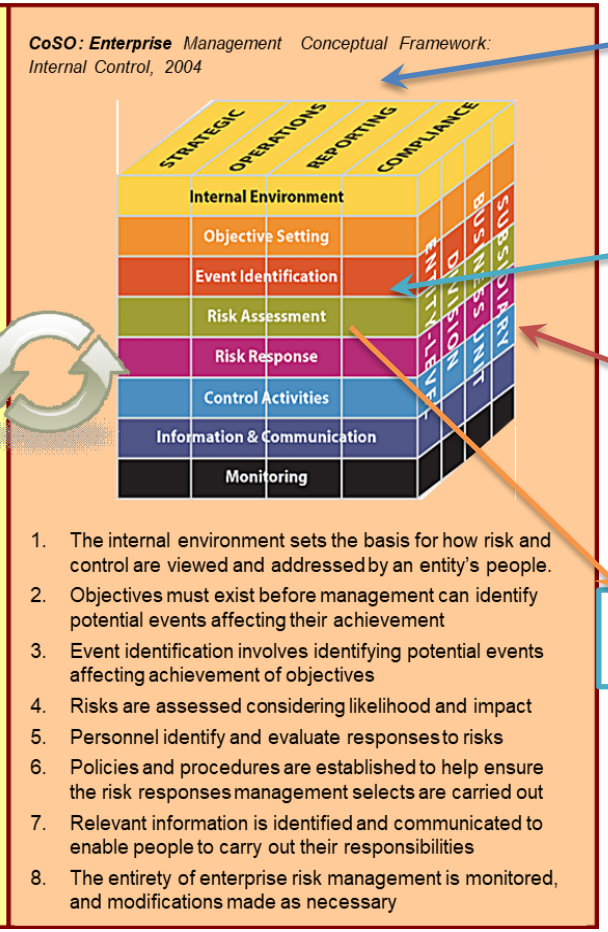


RISK = CIRCUMSTANCES + ACTION

Standards comparison

RISK assessment doesn't only concerns *the* ***combination of Likelihood and Impact*** *but it also entails the analysis of the* ***internal controls*** *as* ***organizational boundaries*** *to* ***risks materialization***





TYPE

PROCESS

ORGANIZATION

$R = L_{ikelihood} * I_{mpact} * O_{rganization}$

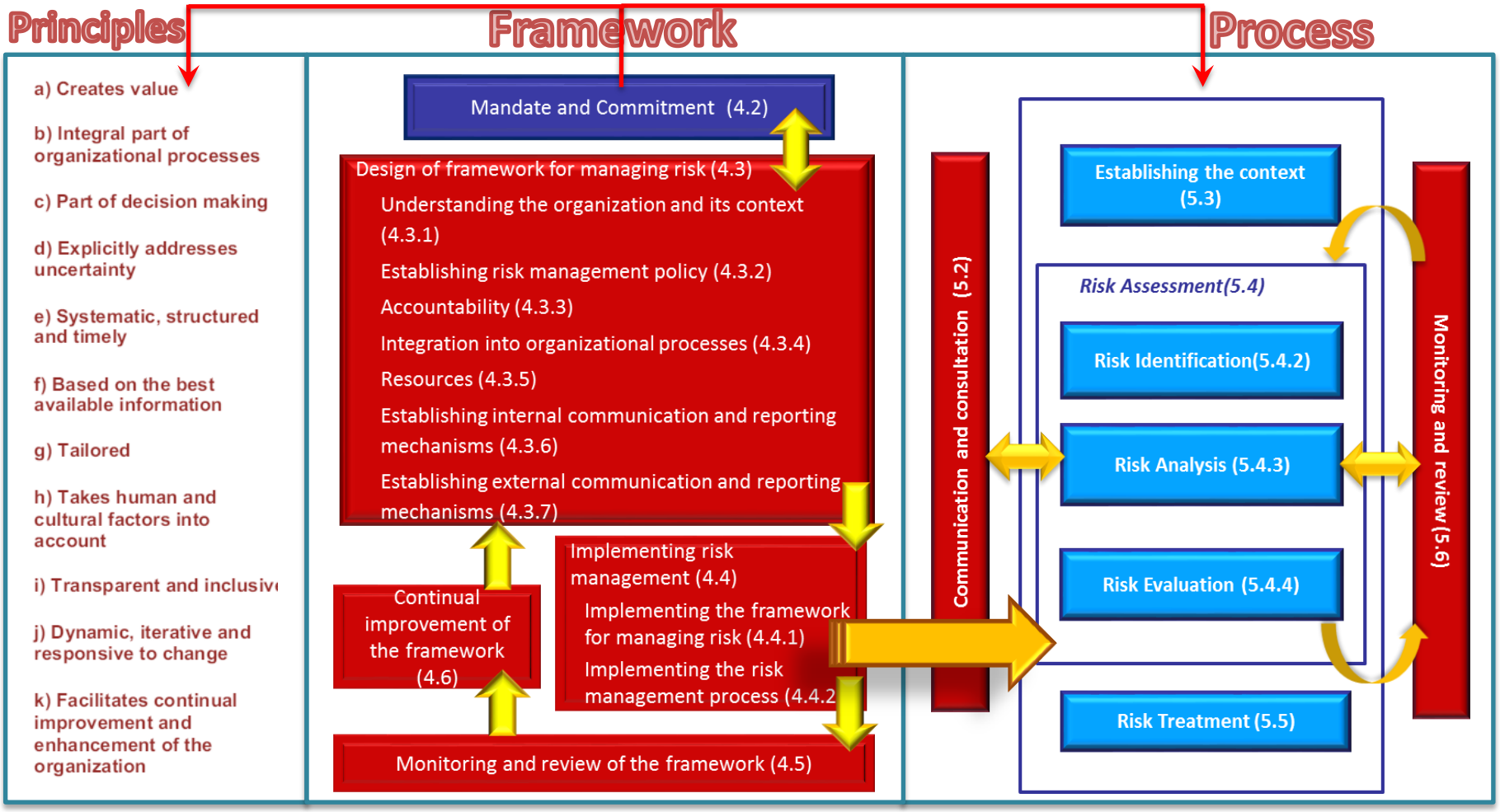
(C_{ontrol})

S_{peed}

$P_{ervasiveness}$

The Risk Management System – ISO 31000:2009 "*family*"

- ***ISO 31000:2009*** *states the Risk Management* ***architecture that includes: Principles, Framework, and Process***
- ***ISO/TR 31004:2013*** *declares how* ***Principles are associated*** *with each phase of the* ***Risk Management process***
- ***ISO 31010:2009*** *describes the* ***techniques*** *for each phase of* ***Risk Assessment*** *(identification, analysis, measurement and weighting)*



The Principles

RISK MANAGEMENT:

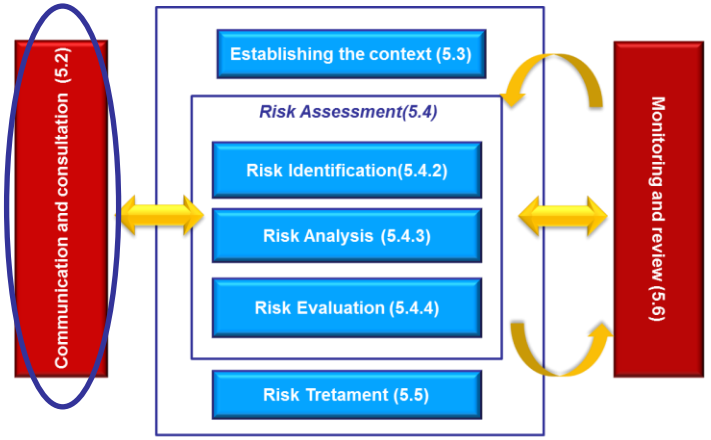
1. *creates and protects value*
2. *is transparent and inclusive*
3. *is tailored*
4. *takes human and cultural factors into account*
5. *facilitates continual improvement of the organization*
6. *is part of decision making*
7. *is based on the best available information*
8. *is systematic, structured and timely*
9. *explicitly addresses uncertainty*
10. *is an integral part of all organizational processes*
11. *is dynamic, iterative and responsive to change*

Risk Process – The Stages 1/4

Communication and Consultation

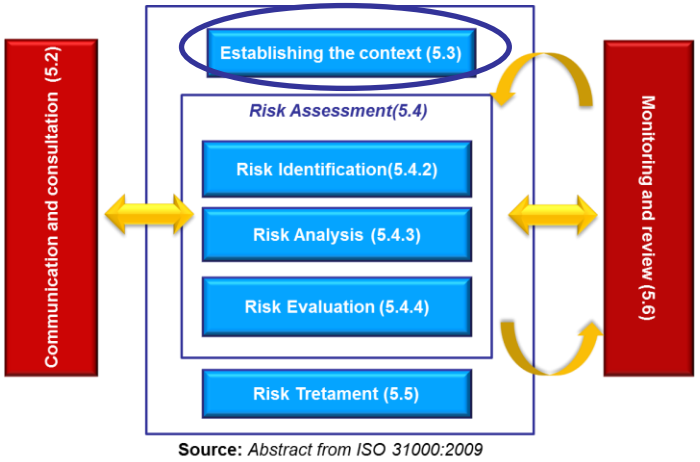
Purposes. To **ensure that stakeholders understand the information** on which decisions are taken and the reasons why those particular actions are required.

Object. Communicating and consulting with internal and external stakeholders **at all stages of the process**, regarding: causes, consequences and treatment measures.



Source: *Abstract from ISO 31000:2009*

- ***Risk management creates and protects value***
- ***Risk management is transparent and inclusive***



Source: *Abstract from ISO 31000:2009*

- ***Risk management is tailored.***
- ***Risk management takes human and cultural factors into account.***

Estabilishing the context

Purposes. To **set goals and define external and internal parameters** for risk management and analysis process criteria.

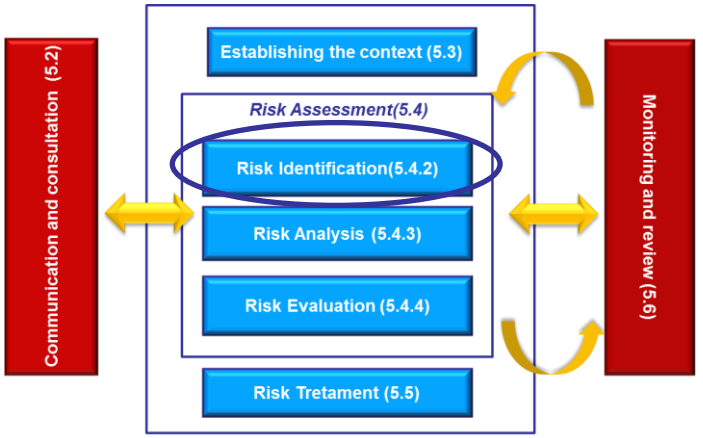
Object. Analysis of the **context in which the organization seeks to achieve the risk management objectives**. Internal: organizational culture, processes, structure and strategies; External: objectives and stakeholders's interests.

Risk Process – The Stages 2/4

Risk Identification

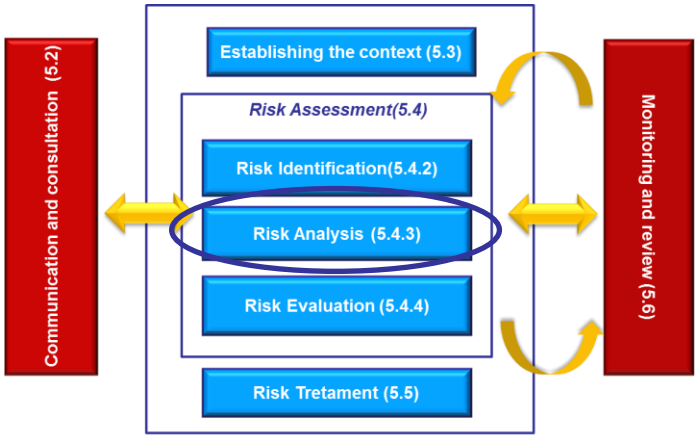
Purposes. To **create a complete list of risks** based on events that may create, enhance, prevent, worsen, accelerate or delay the achievement of the objectives.

Object. Risk identification, i**n order to apply the tools and techniques best suited** to the objectives of Risk Management, using the available expertise.



Source: *Abstract from ISO 31000:2009*

- ***Risk management is based on the best available information***



Source: *Abstract from ISO 31000:2009*

- ***Risk management is systematic, structured and timely***
- ***Risk management explicitly addresses uncertainty***
- ***Risk management is an integral part of all organizational processes***

Risk Analysis

Purposes. To **provide input to risk assessment and decisions** concerning more suitable treatment, especially in cases of options involving different types and levels of risk.

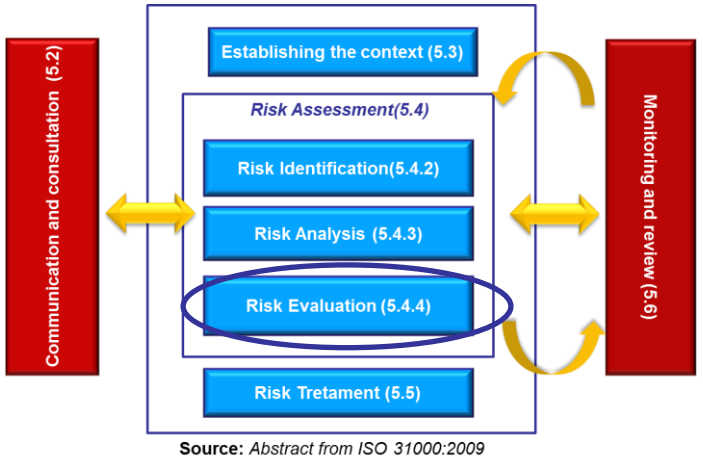
Object. Analyzing **causes/effects and sources of risk**, positive and negative consequences and their probability of occurrence, also based on the efficiency and effectiveness of controls.

Risk Process – The Stages 3/4

Measurement and Weighting

Purpose. To **contribute to decisions on the selection of the risks** that need to be treated and the their implementation priorities; to **evaluate whether to initiate further analysis** or treat the risk maintaining existing controls.

Object. Comparison between the level of risk measured by the analysis, according with the criteria set when establishing the context; consider both the risk tolerance and the duties of compliance



Source: *Abstract from ISO 31000:2009*

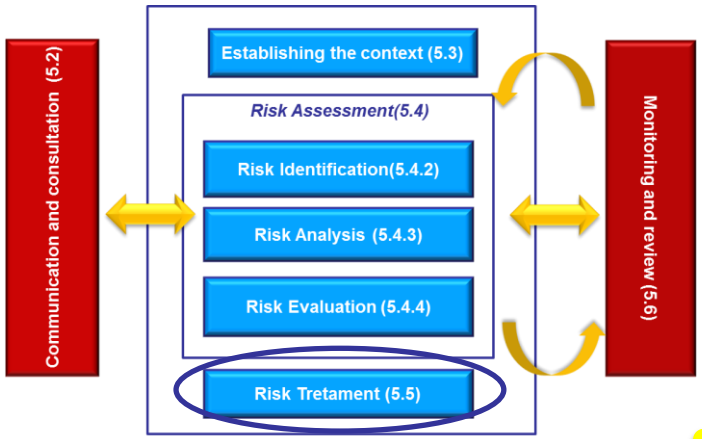
➢ ***Risk management is part of decision making***

Likelihood X ***Impact*** = ***Risk Assessment***

The **Control & Risk Self Assessment (C&RSA), measures the risk's likelihood and impact on the organization**; the multiplication of the 2 factors determines the overall risk value.

A sample of **people representing the critical process, who identified the risks**, qualitatively and quantitatively assesses the risks of the division they belong to.

Risk Process – The Stages 4/4



Source: *Abstract from ISO 31000:2009*

Risk Treatment

Purpose. To **define measures on risk not necessarily exclusive** or fitting to all circumstances: a) avoid; b) take or increase; c) remove the source; d) intervene on probability; e) change the consequences; f) share; g) maintain

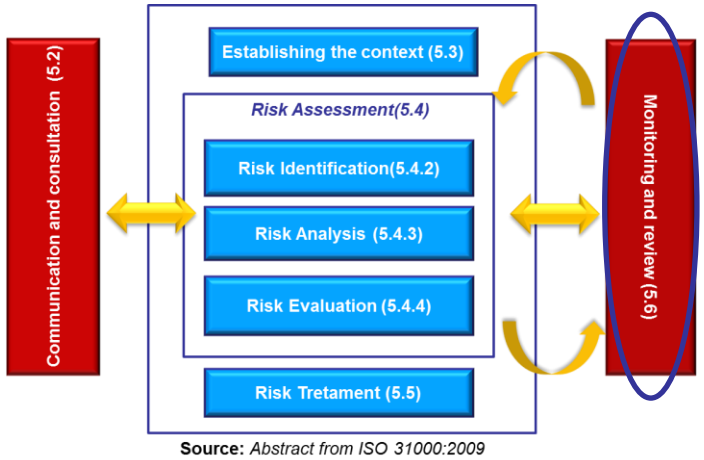
Object. Treatment evaluation; **deciding on the residual risk tolerance**; redefining treatment, if the risk is not tolerable; **evaluation of the action effectiveness**; to provide for the selection of one or more mitigating options

➢ ***Risk management facilitates continual improvement of the organization***

Monitor & Review

Purpose. a) to **check the effectiveness and efficiency of the controls** considered by the system design and by the process; **b)** to **gather information to improve the assessment**; **c) to detect changes of context**, parameters and risks; **d) to review the treatment and priorities**; **e) to identify emerging risks**

Object. a) Analysis of the events, changes, successes and failures; **b) periodically check of the framework**, the process and results; **c) evaluation of the treatment owners's responsibilities,** for the purposes of their appreciation or sanction applications



Source: *Abstract from ISO 31000:2009*

➢ ***Risk management is dynamic, iterative and responsive to change***

Risk Appetite

Development of risk appetite statements

- An organization cannot consider risk as simply resulting from likelihood-per-impact in order to treat it: its management depends on the component variables involved in determining risk appetite, or “the amount of risk that an organization is prepared to accept, tolerate or be exposed to at any point in time”.

- Risk Appetite level mostly depends on the kind of activity performed, the products and services offered, and the regulatory and environmental contexts in which the organization operates.

Development of risk appetite statements

Contents:

- Risk appetite definition
- Risk Appetite components as part of Risk appetite framework (Risk perception, Risk attitude, Risk acceptance, Risk capacity, Risk retention, Risk tolerance)
- Relationships between risk profile and risk appetite

Development of risk appetite statements
(example of practice)

Example: A behavioral approach to risk appetite (ONS-UK)

	Averse	Minimal	Cautious	Open	Actively Seeking
Risk Approach Definition	Avoidance of risk and uncertainty is a key organizational objective	Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have potential for limited reward	Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward	Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward and value for money	Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk)
Risk Type 1			• Behaviors if we were to take less risk • …	• Agreed risk appetite and expected behaviors • …	• Behaviors if we were to take more risk • …
Risk Type 2			• Behaviors if we were to take less risk • …	• Agreed risk appetite and expected behaviors • …	• Behaviors if we were to take more risk • …

Risk Appetite

Risk appetite is the amount of risk an organisation is willing to take

Personal Risk Appetite quiz

Results

Averse	Minimal	Cautious	Open	Actively Seeking
Won't get into car		Consistent Approach		Drive at 120 mph

Development of risk appetite statements

From the risk profile to the risk appetite definition

The variables **expressing risk profile-risk appetite** ratio are as follows:

- **Risk perception**, which describes how people perceive risks according to their values and interests;
- **Risk attitude** (existing risk profile): If an organization is particularly effective in managing certain types of risks, it may be willing to take on more risk in that category, or conversely, it may not have any appetite in that area;
- **Risk acceptance**, which refers to the maximum potential impact of a risk event that an organization could withstand. Often appetite will be well below acceptance;
- **Risk capacity**, which is the maximum level of risk that an organization can assume without violating the regulatory burden;
- **Risk retention**, which considers stakeholders' conservative return expectations and a very low appetite for risk-taking;
- **Risk tolerance**, which is the level of variation that an organization is willing to accept around specific objectives.

Development of risk appetite statements
ONS Example

The approach taken by the **ONS risk management team** was simple, it involved 1) inviting the Executive and Non-Executive Directors of the organization to individually assess risk appetite across risk types (on a matrix, see overleaf), 2) to challenge and explore their views through a series of one-to-one meetings, and 3) to discuss a consolidated view at Board level and to agree the levels of risk appetite with articulated behaviors.

The ONS experience has proven the benefits of this process. Thinking through specifically what risk appetite means for culture/behaviors has been of great benefit, by way of illustration:

- Under a **'Cautious' appetite for 'statistical quality'** risks a potential behavior may be "Formal outputs must be of high quality to maintain reputation and confidence, but development and timeliness needs to be challenged in order to improve quality. Timeliness is recognized as an element of quality therefore we aim for timely statistics whenever possible."
- Under an **'Actively Seeking' appetite for 'innovation'** a potential behavior may be "We recognize the risk of irrelevance without innovation and are relentlessly curious, investing considerable time in new approaches and being prepared to try new things even if many of them do not result in a viable product."

ONS Risk Appetites

Appetite level	Averse	Minimal	Cautious	Open	Actively Seeking
Helpful				Take risk to avoid becoming irrelevant	
Professional - Statistical Quality			Balance quality, value and impact		
Professional - Security		Be vigilant about appropriate access to data			
Innovative					Take risks to innovate
Efficient – Financial Management			Don't over/under-spend		
Efficient - Reform				Take risk to change the Organisation	
Capable - Systems			Focus on new systems		
Capable - People				Take risks to employ the right people/skills	

modernisl

Risk Management is about Appropriate Decision Making

Risk management is not a separate entity to your work/role/job. It is your job

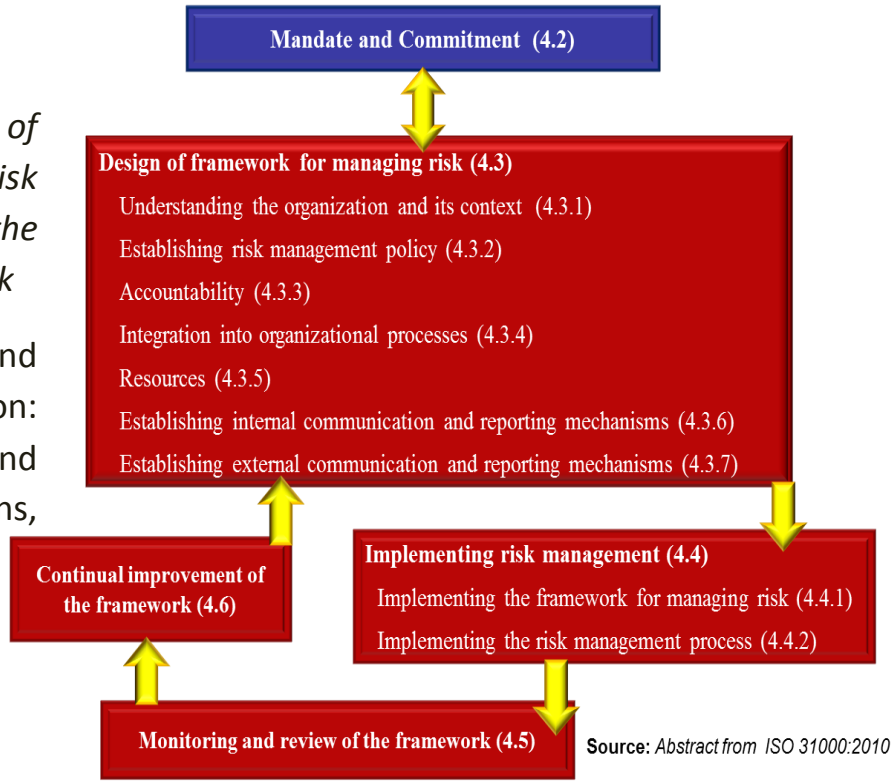
We all undertake risk management daily.

Integrated Frameworks:
Risk and Quality Management

ISO 31000:2009 – *The Framework*

The **Risk Management framework:**

- **Consists of:** ***1.*** *Mandate & Commitment;* ***2.*** *Design of framework for managing risk;* ***3.*** *Implementing Risk Management;* ***4.*** *Monitoring and review of the framework;* ***5.*** *Continual improvement of the framework*
- is a set of **2 types of components** supporting and sustaining risk management throughout an organization: ***a) foundations*** (policy, objectives, mandate, and commitment); ***b) organizational arrangements*** (plans, relationships, accountabilities, resources, processes).
- assists in managing risks effectively through the **application of the RM process** at **varying levels and within specific contexts** of the organization.



Source: *Abstract from ISO 31000:2010*

- ensures that **information about risk** coming from the risk management process is **adequately reported and used as a basis** for decision making and accountability at all relevant levels.
- **complies with the Corporate Risk Profile,** a high-level summary of the most critical risks being managed by the Organization, periodically reviewed, used as a **reference tool** for decision-making.

Integrated risk approach

From a **practical point of view**:

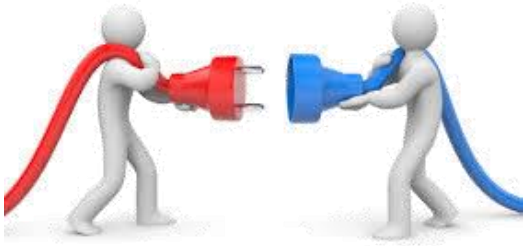
a. **Risk management should not be seen as a separate system**, regardless how the organization manages itself, makes decisions, allocates resources and holds people accountable.
b. **Risk management cannot take place at some levels** if that excludes other ones.
c. **Risk management cannot take place in only a few parts** of the organization.

In models based on an **enterprise-wide perspective of risk**, **internal control are implemented through a risk-based approach**, built on the **following criteria**:

a. **Policy positions reflect the risk appetite** of senior management, and are developed to guide the behavior of empowered staff in managing risks.
b. **Governance** arrangements ensure **transparency and accountability in decision making**, by promoting strong leadership, sound management, and effective planning and review.
c. **Planning and reporting** provide great opportunities to document goals and related risks.
d. **Assurance activities are a part of Internal audit**, aimed at verifying that risk management within an organization is run consistently with international standards and established practice.

Risk Management Integrated Framework

Quality demand comes from the **users' needs**. It encompasses both quality criteria and demands related to risks, but **different objectives** may be in **conflict** with each other. *E.g., accuracy with timeliness.* ***Risk analysis might help assess relations between risks and objectives.***



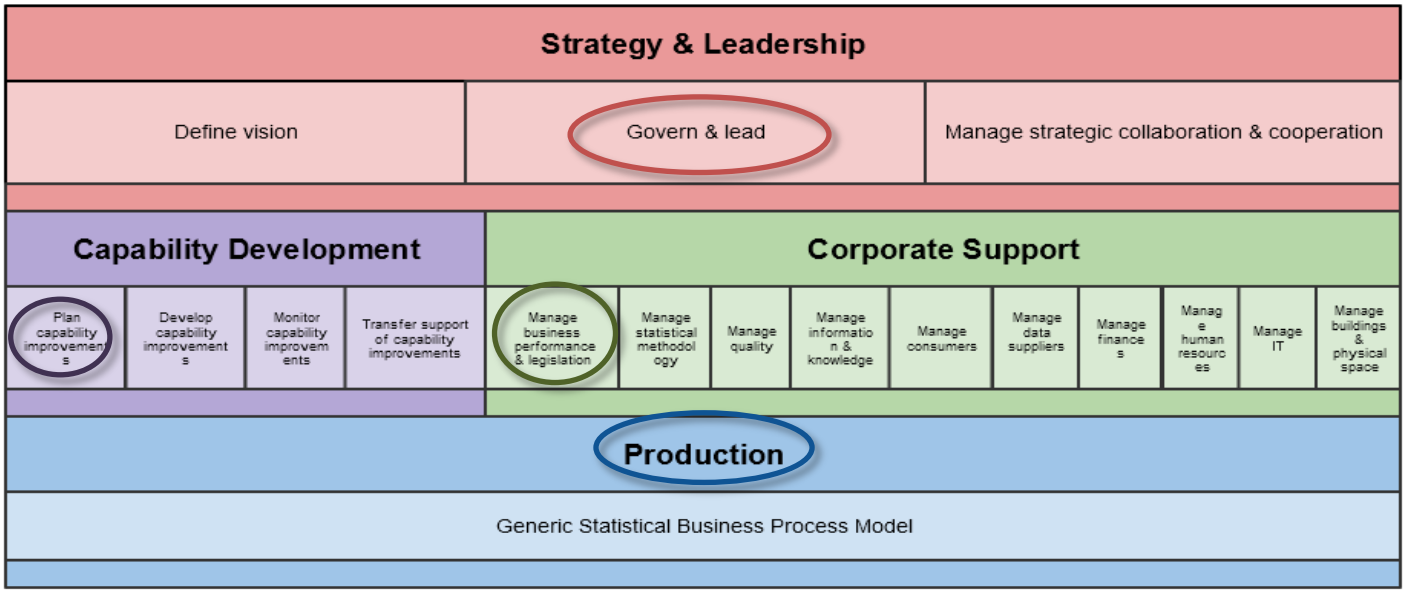
At operational level, **approaches of Quality and Risk management are strictly connected** :

- **Quality is the extent** to which characteristics of an object **meets the requirements** (ISO 9001:2015); if not, corrections and corrective actions are implemented; it's focused on **products, customer satisfaction, processes (input/output)** and the **organization** as a whole;
- **Risk** is defined as the **effect of uncertainty on objectives** (ISO 31000:2009); if the risk level is too high, mitigating measures are implemented.

A process is under control when quality criteria are met and risks are acceptable

Integrated Common Framework

The way to **integrate the Framework in a NSO runs through** to **standardize the interconnections** among: the **Architecture** (GAMSO), **the Process** (GSBPM) and **Risk Management** (ISO 31000)



1. **The RM governance** and the corporate RM (i.e. the overall risks on strategic objectives), could be **placed within the "Strategy and Leadership" activity area, under the "Govern and Lead"**;

2. **The statistical risk management, related to the RM identification and monitoring** phases, **could be placed within the capability management activity area, under "Plan/Monitor capabilities"**;

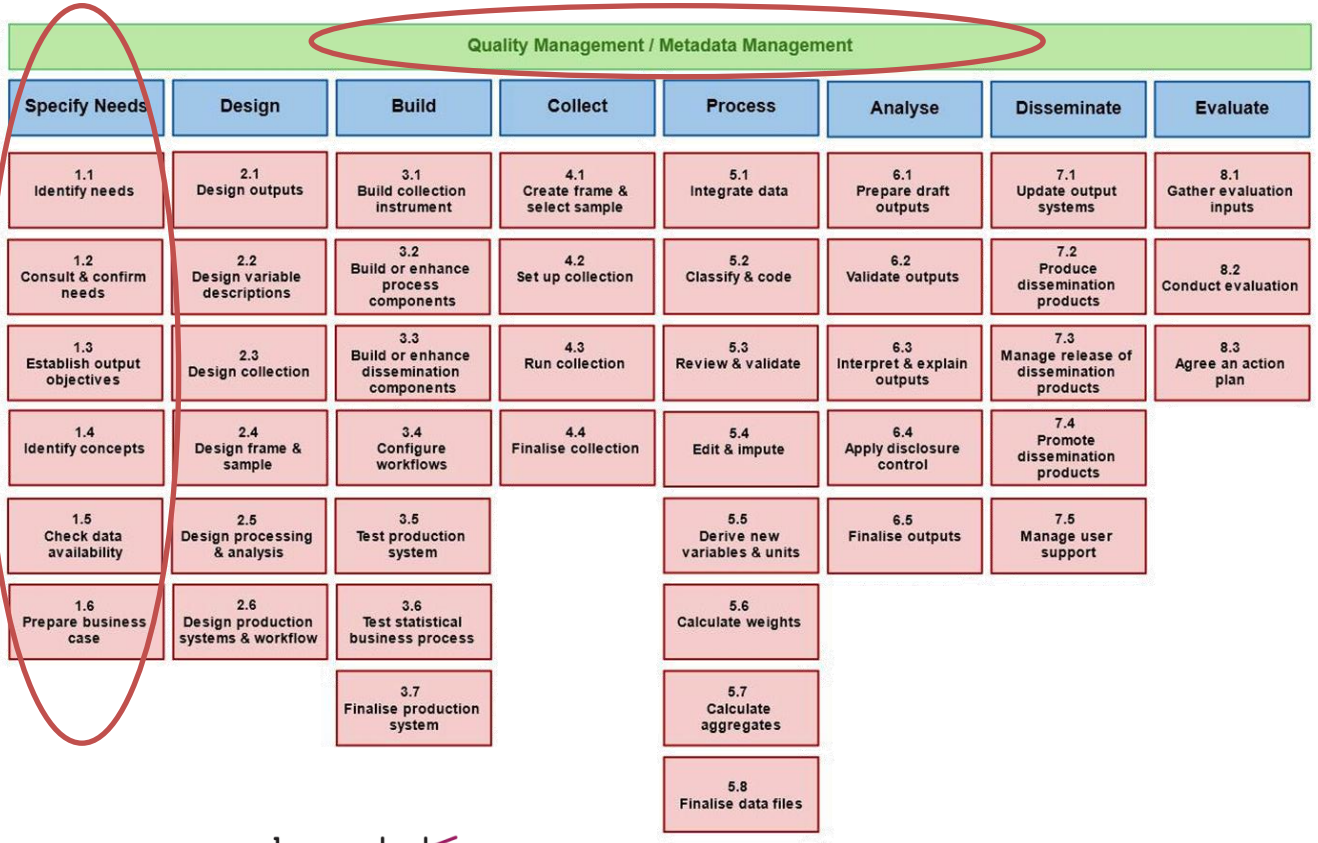
3. **The identification and treatment of organizational risks**, connected to supporting activities, **can be placed in each sub-area of "Corporate support"**, depending on the type of risk (i.e. fraud risks);

4. **The management of operational statistical risks**, is a **routine activity** under the responsibility of the risk owners, within the Production process, especially with regard to the **identification and treatment** phase, in order to **ensure statistical quality and successful delivery**.

Integrated Common Framework

Designing process flow map(s), in order to identify the points where product and **process quality can be measured**, is crucial to implement a quality framework.

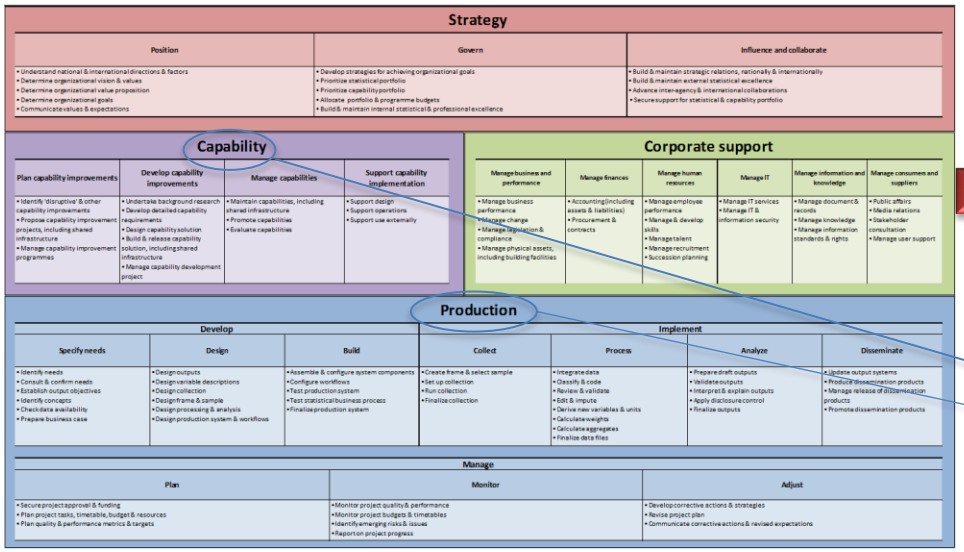
The **Generic Statistical Business Process Model (GSBPM)** is often used by NSIs as a **guide to map the activities of statistical processes** because it ensures that all steps of a statistical process are included for monitoring purposes.



The **GSBPM** recognises **several over-arching processes** that apply **throughout the production phases, and across statistical business processes**, including **quality management**

Quality management, in turn, **involves institutional** and **organisational factors** which are included in other GSBPM over-arching processes (*e.g. Human resources management, **Risk Management***) which can have an impact on quality.

Integrated Common Framework

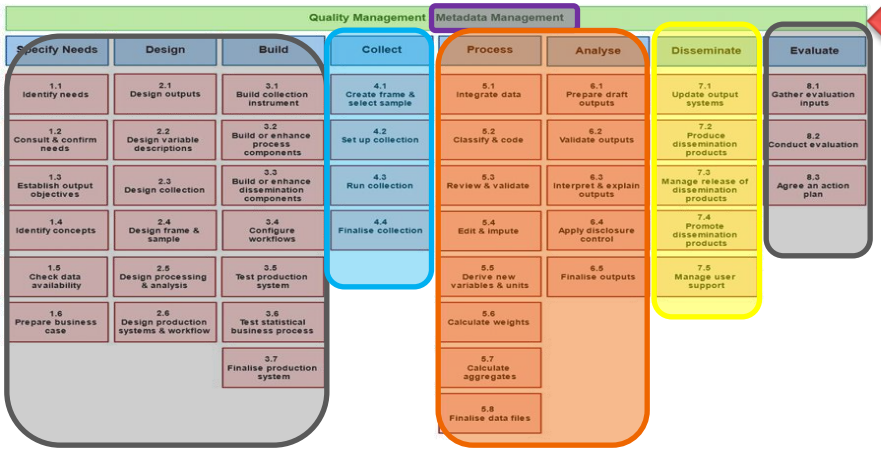


From the Model

By the Tool

Risk Management System

General Overarching Processes



To the Standardized process

*The **organisational Risk Management** encourages practices based on the **early planning of activities**, anticipating possible obstacles in achieving objectives, **instead of the logic of urgency**.*

Risk Management Integrated Framework

- The most advanced **integrated models based on enterprise-wide perspective** of **statistical risk** adopt standardizes **terms** and include in the RM catalog different kind of risks, for example: statistical, fraud, work health and safety, ITC security and transparency.
- They define the **statistical risk** as: **"*the possibility that one or more of the production process components fail to meet the quality standard stated, so that statistical output quality or integrity is affected*".**
- Risk Assessment in **statistical areas** considers the issues that can **affect data quality** in a **statistical processing cycle** as well as *managing stakeholder relationships, the impact of change programs and workforce capability*.
- Risks are managed using the **same framework at a Strategic, Operational and Project level** across the organization. ***Statistical risks can be recognized separately but in any case it should be integrated within the organizational risk framework***.

Risk Management Integrated Framework – Quality gates

Advanced **Quality management model** are **assisted** by the **risk mitigation strategy** based on the **quality gates**, designed to facilitate the detection, discussion and resolution of problems through a collaborative effort to improve the early detection of errors.

Normally, the **6 components** of the quality gates are:

1. ***Placement*** *of quality gates* ***throughout a statistical process***
2. ***Roles,*** ***tasks to people*** *or areas involved in a quality gate*
3. ***Actions,*** *responses to various outcomes for a quality gate*
4. ***Evaluation,*** *a* ***review*** *to examine where improvements* ***can be made***
5. ***Tolerance,*** *an* ***acceptable level*** *of* ***qualitative*** *or* ***quantitative*** *quality*
6. ***Quality Measures,*** *a* ***set of indicators*** *that provide information about* ***potential problems*** *at a given point in the process*

The quality gates are placed by **assessing the key activities** associated with each step of the statistical process**,** according to the ISO 31000:10 methodology.

If a **Statistical Risk Assessment** reveals that the risk rating is **extreme or high** it is recommended that a **quality gate be utilized to mitigate the statistical risk.**

Statistical Risk Register

Examples of **risk register** belonging to **"Statistical Production"**

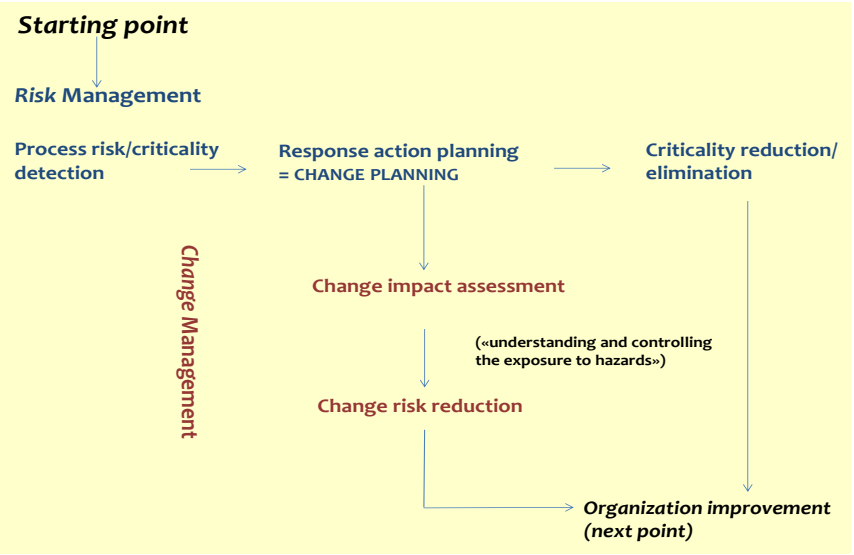
Risk	Treatment
Delay in updating repositories to make balancing data	Mapping and re-engineering the collecting data process for the estimation of a table chart-supply use
Delay in receiving internal / external sources	Risk Analysis aimed at removing obstacles to the data collecting process through internal and inter-institutional agreements
Lack of timeliness in the preparation of data files by the competent departments	Mapping and re-engineering the production process of the national accounts relating to the production and value-added services non-market at current prices
Lack of formalized procedures (supporting documentation, methodological notes, data quality control)	Improving communication and developing information-sharing initiatives
Delay in receiving data concerning financial accounts and investments with regard to both sector and sub-sectors of Public Administrations	Reviewing and monitoring agreements in place
Reduction of the amount of data collected at the local level	Execution and tender's award to provide tablet to municipal detectors of consumer prices
Delay in the computerization of procedures for the acquisition and processing of data	Activating the control system and correcting data through models used by other NSIs
Transmission of questionnaires poorly filled out because of lack of competence	Monitoring procedures of collection data by the local Authorities
Discontinuities in the collection mode and in the data stream	Reviewing organizational process to manage replacements of those involved in data collection
Difficulties in managing archives and data delivery aligned with new tax regulations	Continuous staff training and making up working groups including statistics and informatics

Change, Risk and Project Management

Change management is interconnected with Risk management: Innovation requires risks so every **change strategy comes with its own levels of risk**; changes can be made less risky if they are adequately reviewed, assessed, and coordinated adopting a proper **risk management process**.

The relationship between Risk and Change management is characterized as **having circular** nature:

RM is **a part of the wider cycle of CM** as well as **CM** is a **component** of the **RM's cycle.**

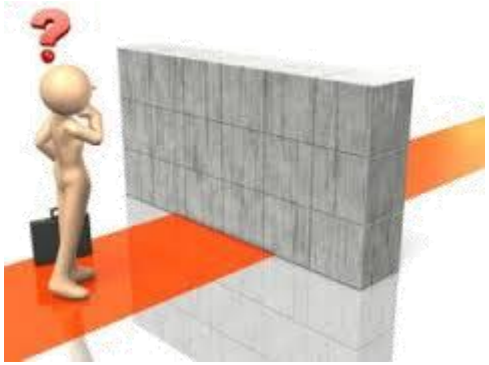


- **Risk Management** identifies **criticalities** in **changing** processes and plans fitting response activities to minimize risk of failure both during and post implementation phases.

- **Change Management** acts **as a subsystem** of **Risk Management**; the actions aiming at reducing the likelihood of incoming risky events are themselves changes.

Project management aligns the organization's components through the implementation of: **Portfolio management** that **optimizes, oversees and selects concurrent organizational initiatives** and **Program management** that defines a set of expected benefits and their transition into the business.

Risks in Change management



Risks in change management could be grouped in:

- **Human resources risks** (e.g., *forms of **resistance to change**, political agendas, competition for power, and **fear of loss of status or job***);
- **Cultural risks** (e.g., ***risk avoidance**, group think, **policies**, or rules (unwritten guides to behavior) that contraindicate the change, control culture, **unclear decision-making** paths, or norms*);
- **Capability development risks** (e.g., ***insufficient training** and learning reinforcement, inability to respond to questions/problems, **low starting capability or capacity**, poor methods for institutionalizing learning, withholding/protecting knowledge, **lack of informal learning***);
- **Process development risks** (e.g., ***insufficient employee involvement** in process definition, processes dominated by single-skilled people, lack of experience with process development tools, work decisions only made at high levels*);
- **Organizational structure/management risks** (e.g., ***weak leadership**, too many layers of management, **dispersed decision-making authority**, matrix management, **unclear role definitions***);
- **Time risks** (e.g., ***unacceptable time frames** for absorption of change, **competing time priorities** of resources needed for the project (training, process design, etc.)*);
- **Environmental risks** (e.g., *market volatility, **changing competition**, **changing technology**, changing leadership, regulatory or **legal uncertainty**, inability to absorb magnitude of change*).

The way forward: the «Risk-Based thinking»

Quality Management (ISO 9001, …)

Change Management (ISO 27000,…)

Operative Objectives
- *Training growth*
- ***Processes reingeneering***

TREATMENT

TRANSITION

Strategic Objectives
- ***Quality improvement***
- *Increase of reputation*
- *Financial Growth*

Barriers to change
- ***Resistance to change***
- *Lack of committment*
- *Lack of Synergy*

TRANSITION

TREATMENT

B

Risk Management (ISO 31000, …)

A

Projects

Current Activities

Strategic Risks
- ***Non-compliance***
- *Communication underrated*
- *Failure to invest*

Portfolio Risks
- ***Poor scopes***
- *Affordability of projects*
- *Poor consideration of value*

As Is
- ***Changes in regulation***
- *Stakeholders' mistrust*
- *Budget constraints*

Risks of Portfolio
- ***Poor synchronisation***
- *Wrong balance of projects*
- *Ineffective cost/benefits analisys*

Operative* Risks
- *Improper business plan*
- *Failure to observe data security*
- *Inadequacy of technology*
- ***Loss of local data***

Areas
- ***Projects and Planning***
- ***Compliance with laws***
- ***ICT***
- ***Data Quality***

Green: Framework
Red: Process

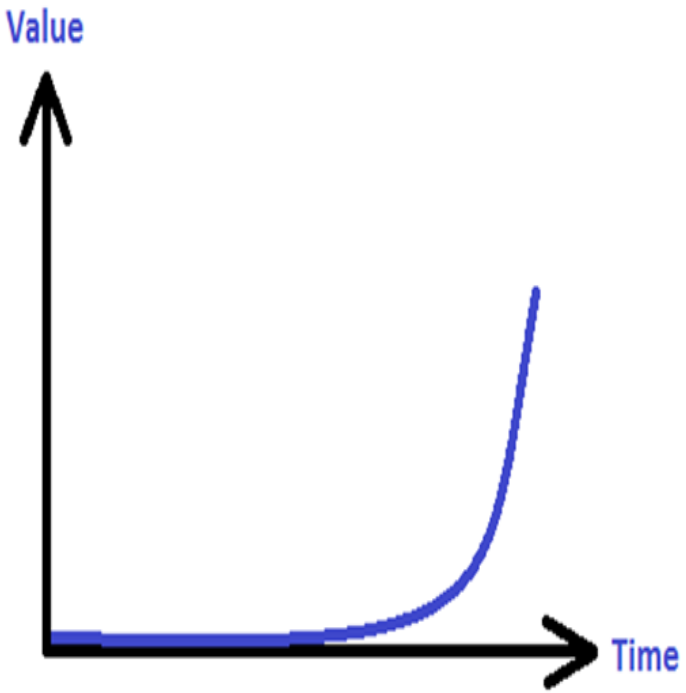
**Risks related to specific projects' and/or activities' objectives*

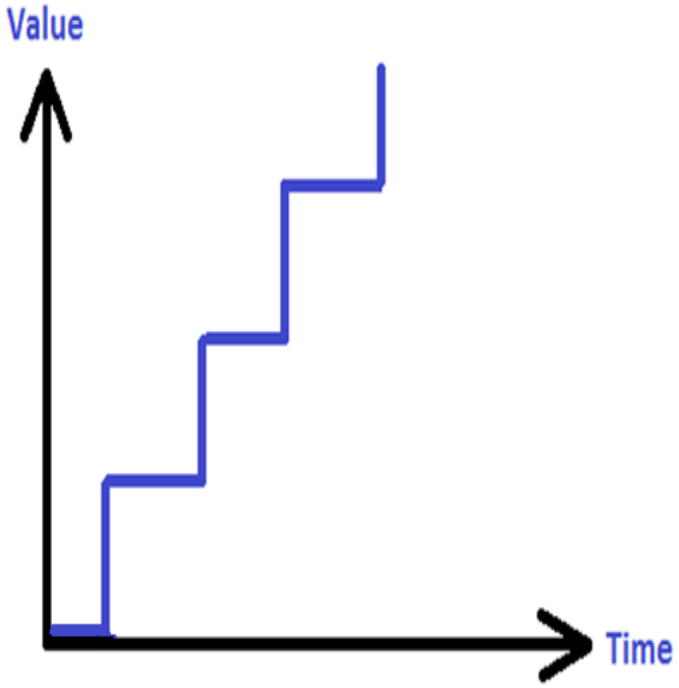
Integrated Frameworks:
Risk and Agile Delivery

Decision Making in an Agile Environment

Agile focuses on the improvement of value, flow and quality, through use of regular feedback loops with users

Development types





An AGILE approach mitigates risk because you're developing & delivering often primarily focusing on delivery and responding to user feedback to improve value for the user

In other words…

Complex rules and regulations give rise to simple and stupid behaviour…

Simple, clear purpose and principles give rise to complex, intelligent behaviour.

DEE HOCK, FOUNDER AND FORMER CEO OF VISA

Risk and Agile: Finding the Sweet Spot

The Agile approach to delivery is being used more and more within NSIs and can prove challenging in some cases.

During times of accelerated change in technology and data we need to find a way through the challenge of embracing Agile delivery while also managing in a risk filled environment and providing assurance and confidence around successful delivery.

Agile should not be seen as being at the expense of risk management but rather as an enabler for the more effective management of risk.

- How can we embrace Agile delivery while still maintaining the right level of assurance and confidence around successful delivery?
- How can risk management and Agile collaborate in order to ensure successful delivery?
- How can NSIs enhance their implementation of risk management best practice in a way which is suited to an Agile culture?

Risk and Agile: Finding the Sweet Spot

PRINCIPLE 1: Define your appetite for risk, and make it real

PRINCIPLE 2: Identify threats and opportunities

PRINCIPLE 3: Deal with threats and exploit opportunities at the most appropriate level but document and escalate if necessary

On target expectations

- Exercise – did we meet all expectations?

Need more information?

- Guidelines on Risk Management
- Enhancing Risk Management with Agile Principles
- UNECE Wiki
- Ask the Community

Thanks for your attention