RISK:
BuildingTrust in Digital Repositories

Seamus Ross, Andrew McHugh,

Raivo Ruusalepp, Hans Hofman & Perla Innocenti

Digital Curation Centre (DCC)

DigitalPreservationEurope (DPE)

HATII at the University of Glasgow & National Archives of the Netherlands

Digital Preservation Today

- Growth in creation of digital information with **scholarly**, **scientific** and **cultural** value continues to accelerate
- Practical approaches aimed at ensuring long-term **authenticity**, **integrity** and **understandability** of digital materials are emerging at a similar pace
- The discipline remains immature though:
  - Are adopted approaches **successful**?
  - What is the **metric** for defining success?
  - Which approaches are **appropriate** for particular digital preservation challenges?
  - Which preservation services and/or service providers can be **trusted**?

Trust, Trustworthiness and Safe Stewardship

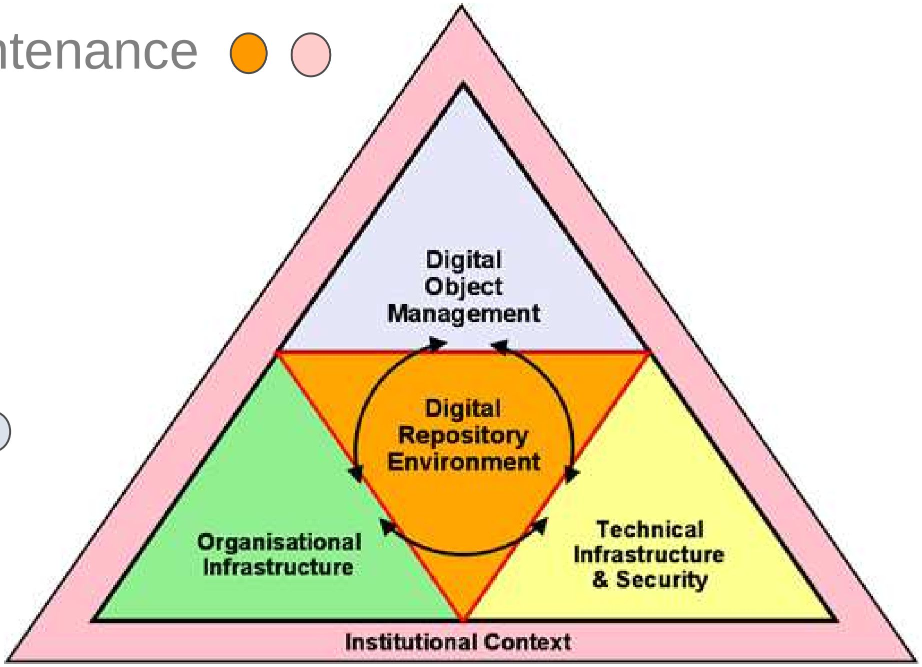
- Evolution of the Digital Preservation (specifically Repository) Landscape:
  - **Defining** the problem
    - *Preserving Digital Information*
    - *Trusted Digital Repositories: Attributes & Responsibilities*
  - **Practical Responses** to the problem
    - repository software [DSPACE, ePrints, Fedora];
    - metadata schema [PREMIS];
    - reference models [OAIS];

- This work focuses on **determining the success of the solutions we propose or have already deployed**

- *“Stewardship is easy and inexpensive to claim; it is expensive and difficult to honor, and perhaps it will prove to be all too easy to later abdicate”* Lynch (2003)

Repository Environments

- Ten principles conceived for Digital Repositories
- An intellectual context for the work:
  - Commitment to digital object maintenance 🟠 ○
  - Organisational fitness 🟢
  - Legal & regulatory legitimacy 🟢
  - Effective & efficient policies 🟠
  - Acquisition & ingest criteria ○
  - Integrity, authenticity & usability ○
  - Provenance ○
  - Dissemination ○
  - Preservation planning & action ○
  - Adequate technical infrastructure 🟡


Digital Object Management
Digital Repository Environment
Organisational Infrastructure
Technical Infrastructure & Security
Institutional Context

Defining Activities and Context

- DCC and DPE collaborations include:
  - Trustworthy Repository Audit and Certification (TRAC) Criteria and Checklist Working Group
    - http://www.crl.edu/PDF/trac.pdf
  - Center for Research Libraries (CRL) Certification of Digital Archives Project
    - http://www.crl.edu/content.asp?l1=13&l2=58&l3=142
  - Network of Expertise in Long-term storage of Digital Resources (nestor)
    - http://edoc.hu-berlin.de/series/nestor-materialien/8/PDF/8.pdf
  - International Audit and Certification Birds of a Feather Group
    - http://www.digitalrepositoryauditandcertification.org

Meeting the shortfall

- Independent measuring of repositories is seen as an essential aim
- It's taken as axiomatic that audit is an appropriate mechanism for establishing repository trustworthiness
- Central to this discussion are issues of:
  - criteria for assessment
  - evidence
  - risk management

} particularly relevant for DRAMBORA

DCC Pilot Audits

- Digital Curation Centre (DCC) engaged in a series of pilot audits in diverse environments
- 6 UK, European and International organisations
- National Libraries, Scientific Data Centers, Cultural and Heritage Archives
- Rationale
  - establish evidence base
  - establish list of key participants
  - refine metrics for assessment
  - contribute to global effort to conceive audit processes
  - establish a methodology and workflow for audit

Filling a Gap

- Existing methods are:
  - too static – ‘one size fits all’ approach
  - too much fixed on the OAIS reference model
  - too little emphasis on evidence in the auditing process
- Audit results should help to manage the repository better continuously, not just give a one-time evaluation

Core Aspects

- The Authentic and Understandable Digital Object
- Based upon established risk management principles
- Bottom-up approach to assessment (in contrast with TRAC and *nestor* methodologies)
- Not about benchmarking, but could be used alongside benchmarking standards or criteria
- Proactive and retroactive applications
- http://www.repositoryaudit.eu/

Objectives

- The purpose of the DRAMBORA toolkit is to facilitate the auditor in:
  - defining the mandate and scope of functions of the repository
  - identifying the activities and assets of the repository
  - identifying the risks and vulnerabilities associated with the mandate, activities and assets
  - assessing and calculating the risks
  - defining risk management measures
  - reporting on the self-audit

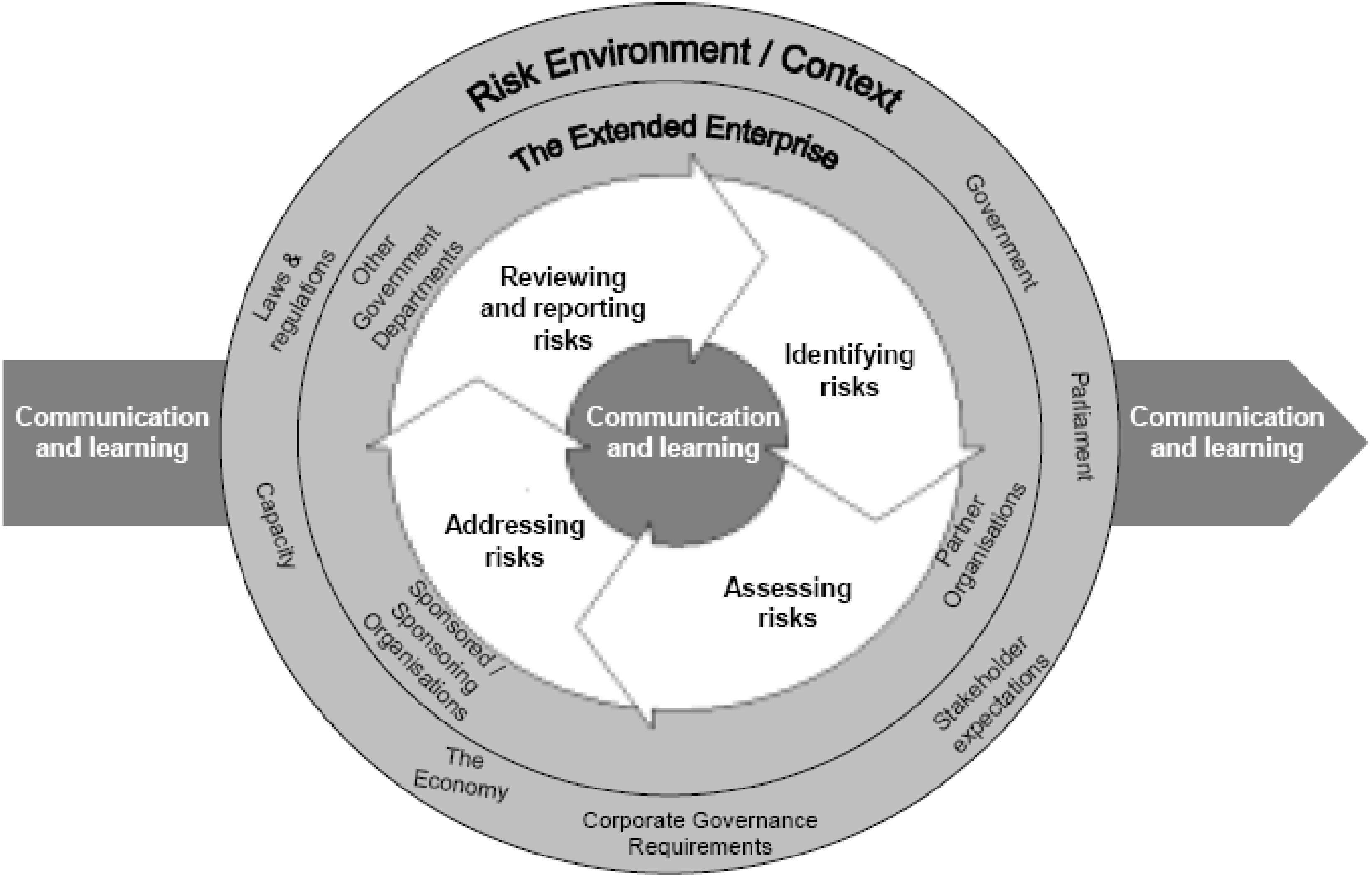
Benefits of DRAMBORA

- Following the successful completion of the self-audit, organisations can expect to have:
  - Established a comprehensive and documented self-awareness of their mission, aims and objectives, and of intrinsic activities and assets
  - Constructed a detailed catalogue of pertinent risks, categorised according to type and inter-risk relationships
  - Created an internal understanding of the successes and shortcomings of the organisation
  - Prepared the organisation for subsequent external audit

What it does not do for you?

- It is not a certifying tool or a OAIS-compliance toolkit, but rather a self-assessment and management tool
- The organization sets the benchmark against which it is assessing itself
- The task of DRAMBORA staff is not to audit or assess anyone’s result, but to provide the tools for them to do it

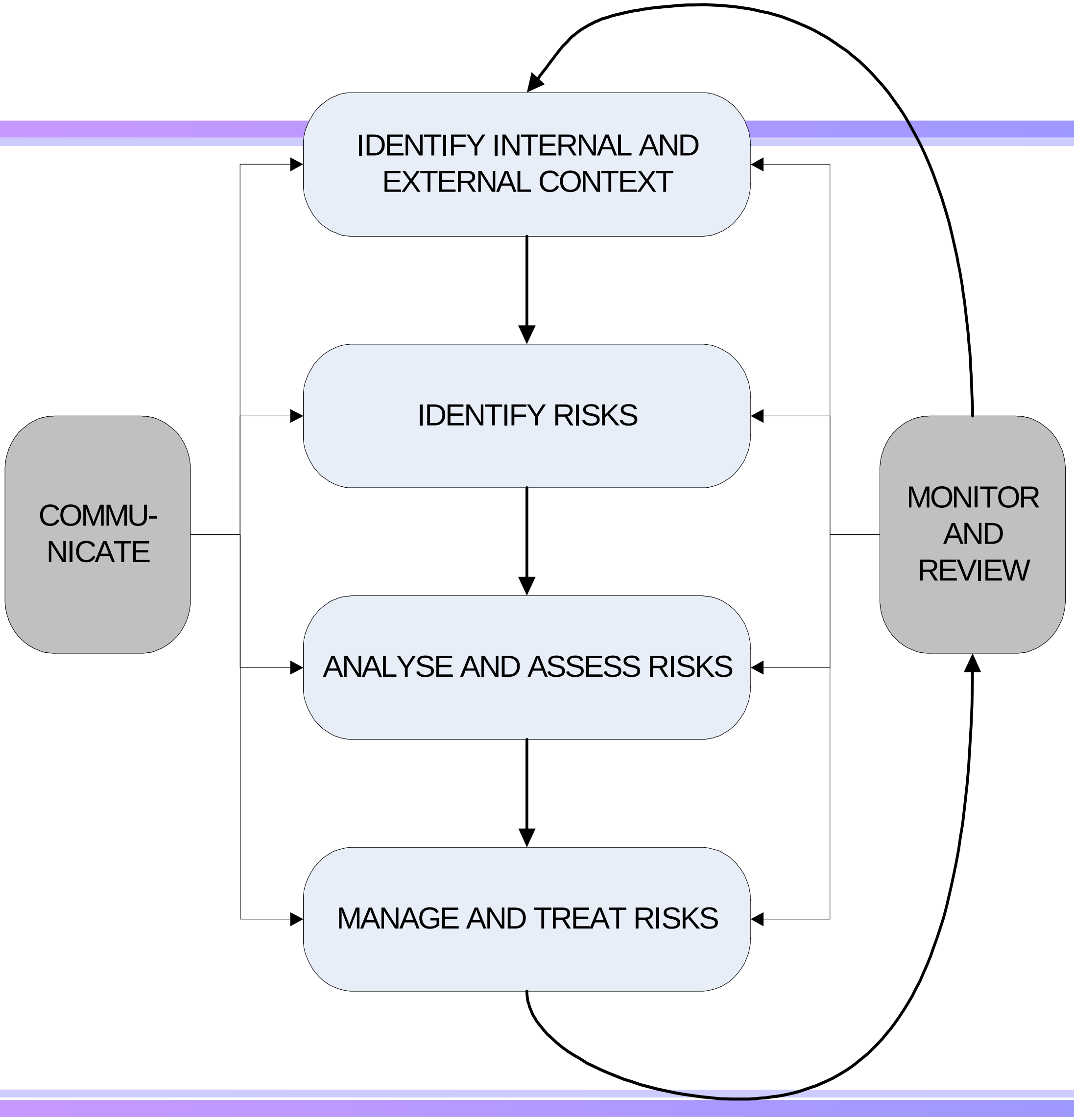
Risk Management Model


Risk Environment / Context
The Extended Enterprise
Communication and learning
Communication and learning
Communication and learning
Reviewing and reporting risks
Identifying risks
Assessing risks
Addressing risks
Laws & regulations
Other Government Departments
Government
Parliament
Partner Organisations
Stakeholder expectations
Corporate Governance Requirements
The Economy
Sponsored / Sponsoring Organisations
Capacity

Anticipated applications

- Validatory: Internal self assessment to confirm suitability of existing policies, procedures and infrastructures
- Preparatory: A precursor to extended, possibly external audit (based on e.g., TRAC)
- Anticipatory: A process preceding the development of the repository or one or more of its aspects

A Recursive Process

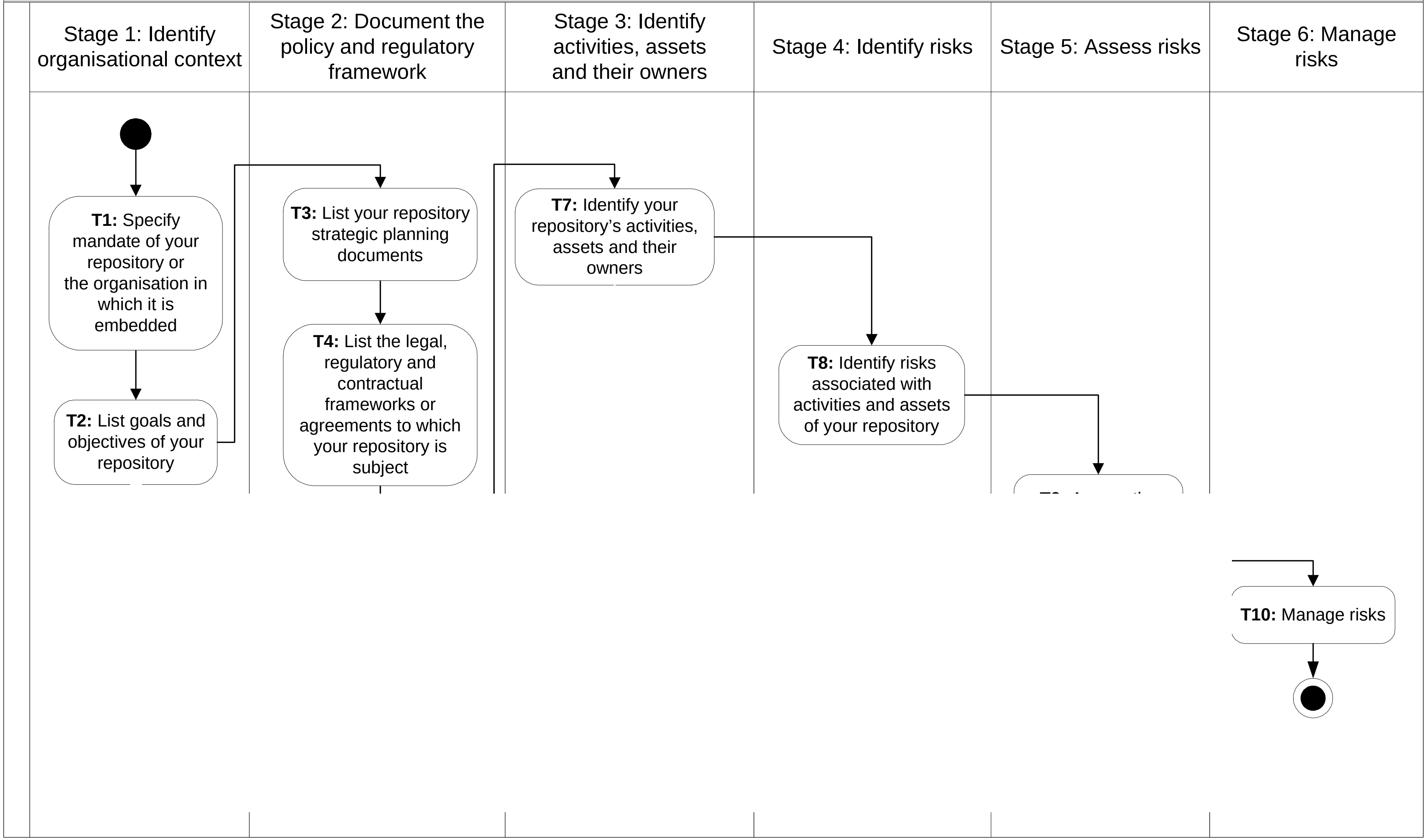


Risk

- Are repositories capable of:
  - identifying and prioritising the risks that impede their activities?
  - managing the risks to mitigate the likelihood of their occurrence?
  - establishing effective contingencies to alleviate the effects of the risks that occur?
- If so, then they are likely to engender a trustworthy status – if they can demonstrate these capabilities

DRAMBORA Workflow

Using the digital repository self-audit toolkit



Stage 1: Identify organisational context

Stage 2: Document the policy and regulatory framework

Stage 3: Identify activities, assets and their owners

Stage 4: Identify risks

Stage 5: Assess risks

Stage 6: Manage risks

T1: Specify mandate of your repository or the organisation in which it is embedded

T2: List goals and objectives of your repository

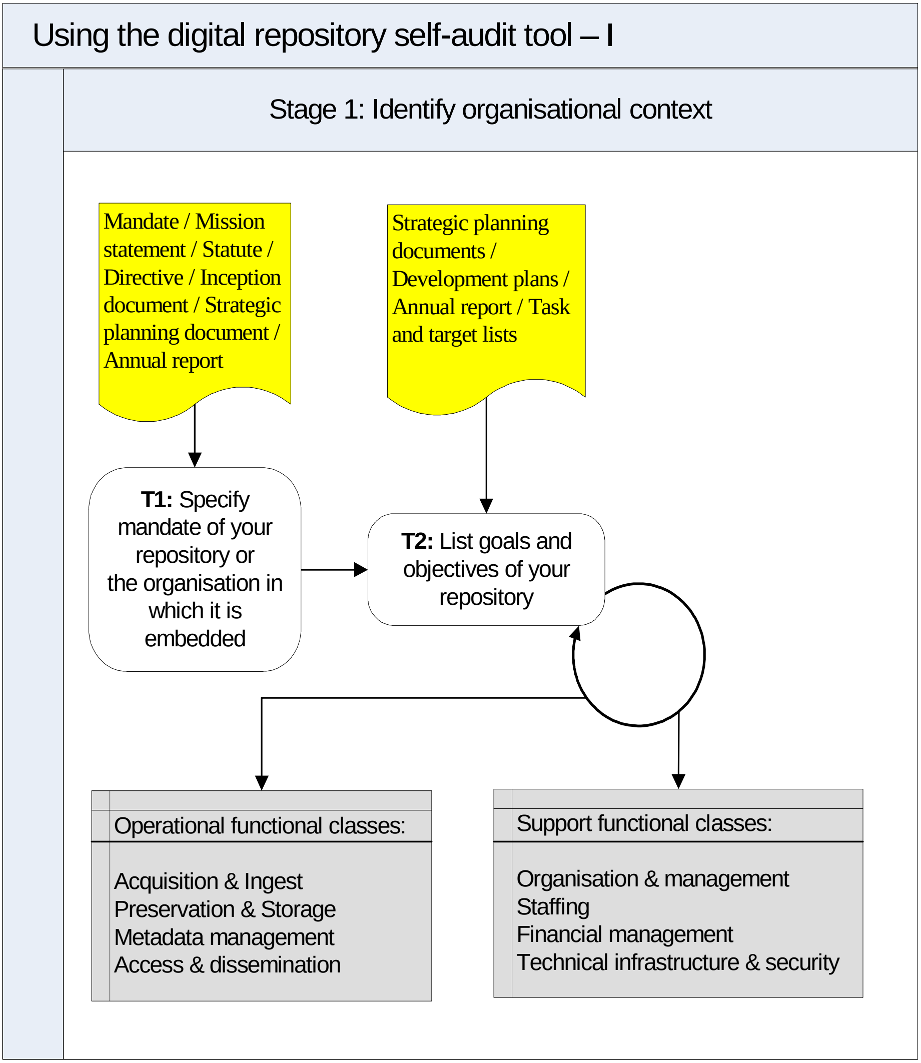
T3: List your repository strategic planning documents

T4: List the legal, regulatory and contractual frameworks or agreements to which your repository is subject

T7: Identify your repository's activities, assets and their owners

T8: Identify risks associated with activities and assets of your repository

T10: Manage risks



Using the digital repository self-audit tool – I

Stage 1: Identify organisational context

Mandate / Mission statement / Statute / Directive / Inception document / Strategic planning document / Annual report

Strategic planning documents / Development plans / Annual report / Task and target lists

T1: Specify mandate of your repository or the organisation in which it is embedded

T2: List goals and objectives of your repository

Operational functional classes:

Acquisition & Ingest
Preservation & Storage
Metadata management
Access & dissemination

Support functional classes:

Organisation & management
Staffing
Financial management
Technical infrastructure & security

Stage 1
Identify organisational context

Organisational Context

- The first stage in developing an organisational profile
- Building a platform to facilitate risk awareness
- Success reflects organisational characteristics and aspirations

Organisational Goals

- Associated with one of 8 functional classes
  - Acquisition & Ingest
  - Preservation & Storage
  - Metadata Management
  - Access & Dissemination

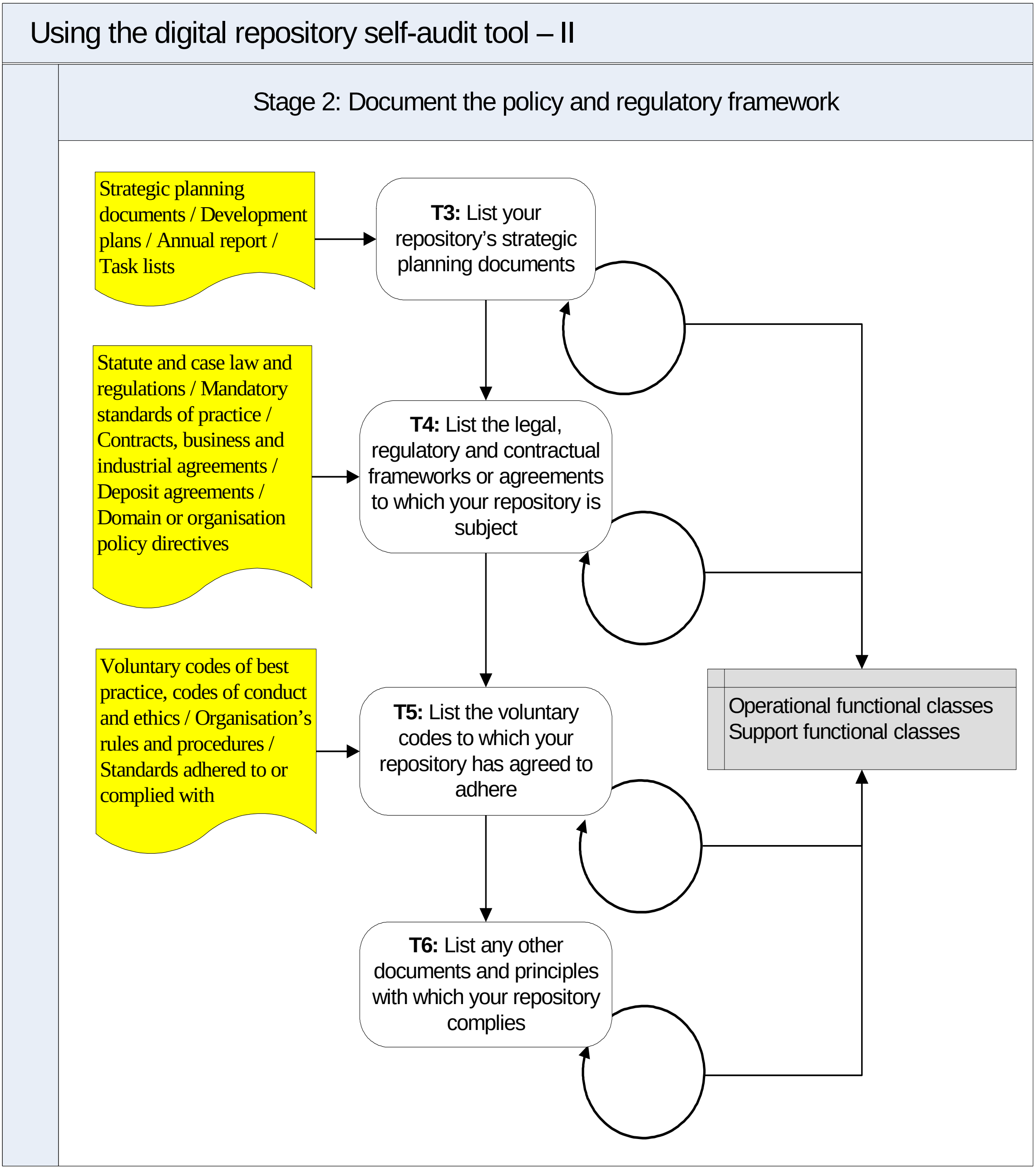
  } operation classes

  - Organisation & Management
  - Staffing
  - Financial Management
  - Technical Infrastructure & Security

  } supporting classes

Stage 2

Document Policy and Regulatory Framework



Using the digital repository self-audit tool – II

Stage 2: Document the policy and regulatory framework

Strategic planning documents / Development plans / Annual report / Task lists

T3: List your repository's strategic planning documents

Statute and case law and regulations / Mandatory standards of practice / Contracts, business and industrial agreements / Deposit agreements / Domain or organisation policy directives

T4: List the legal, regulatory and contractual frameworks or agreements to which your repository is subject

Voluntary codes of best practice, codes of conduct and ethics / Organisation's rules and procedures / Standards adhered to or complied with

T5: List the voluntary codes to which your repository has agreed to adhere

T6: List any other documents and principles with which your repository complies

Operational functional classes
Support functional classes

Document policy and regulatory framework

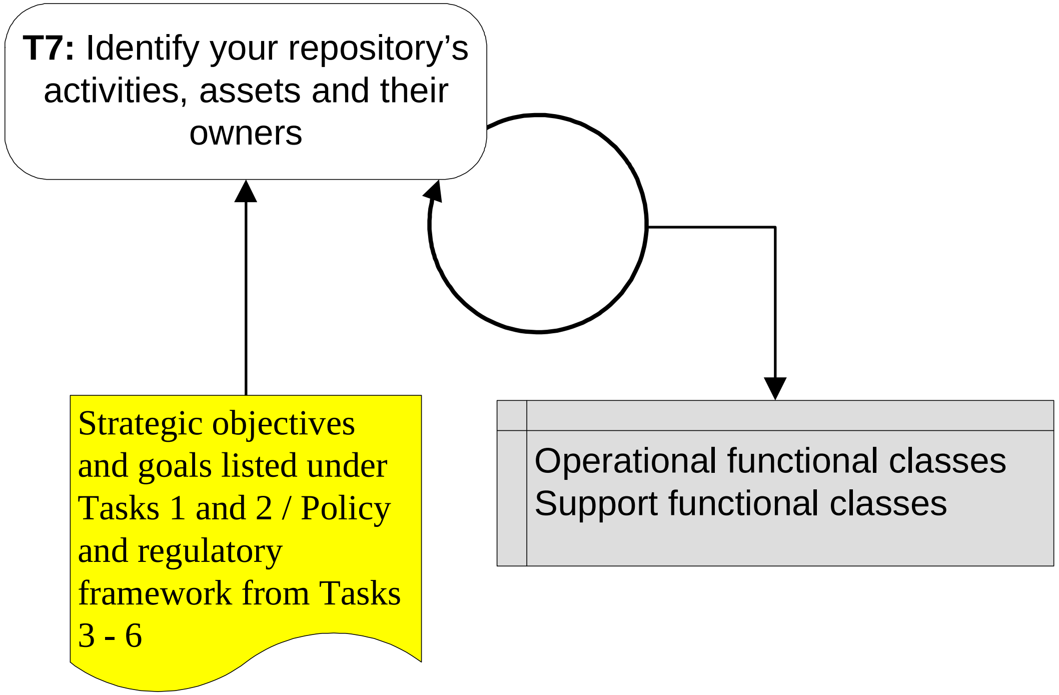
- Aimed at ensuring the repository:
  - operates correctly with respect to regulatory frameworks
  - has an efficient and effective policy framework
  - is aware of societal, ethical, juridical and governance frameworks
  - is aware of legal, contractual and regulatory requirements to which it's subject

Strategic Planning Documents

- Identified within:
  - procedural or operational manuals
  - intranet or shared network storage
  - wikis
- Includes
  - Policies
  - Procedures

Using the digital repository self-audit tool – III

Stage 3: Identify activities, assets and their owners



T7: Identify your repository's activities, assets and their owners

Strategic objectives and goals listed under Tasks 1 and 2 / Policy and regulatory framework from Tasks 3 - 6

Operational functional classes
Support functional classes

Stage 3

Identify Activities, Assets and their Owners

Activities, Assets and Owners

- Building conceptual model of what the repository does
  - split broad level mission and goals into more specific activities or work processes
  - assign to individual responsible actors
  - link to one or more key assets
  - **clues within**: business process re-engineering; imaging & workflow automation; activity-based costing or management; business classification development; quality accreditation; systems implementation

Instructions for this stage

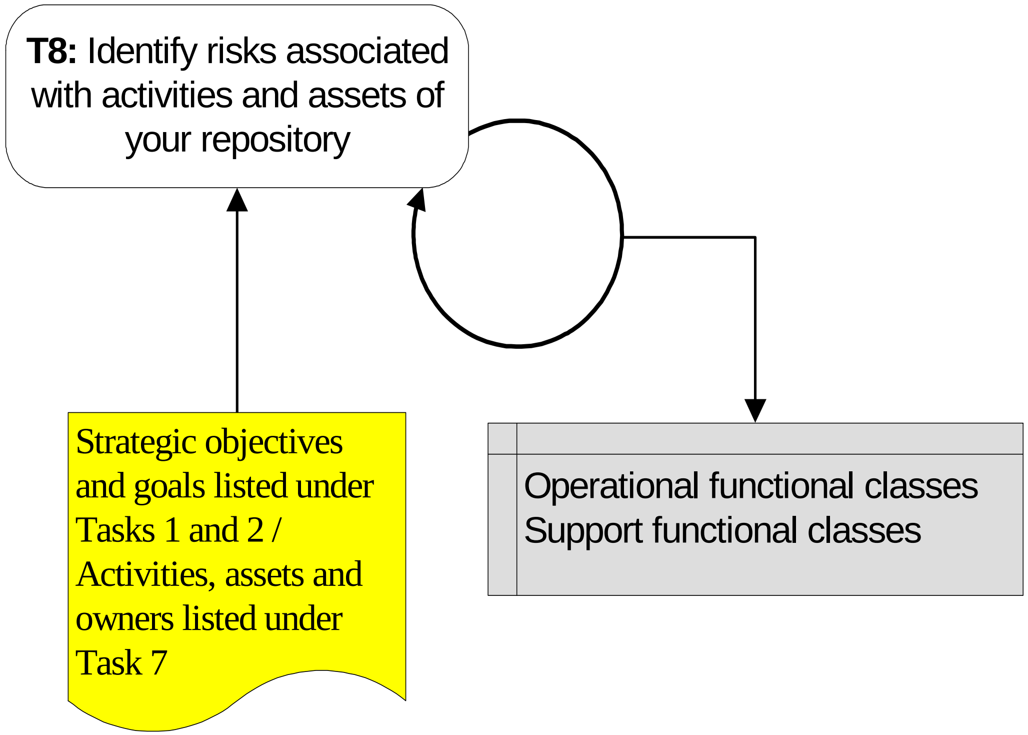
- Hierarchical analysis
  - breaking up organisation's activities into logical parts and sub-parts
    - charter
    - what makes organisation unique?
    - functions and operations
- Process Analysis
  - look in more detail at how repository conducts its business and what is involved

Organisational Assets

- Includes:
  - information (databases, data files, contracts, agreements, documentation, policies and procedures)
  - software assets
  - physical assets
  - services and utilities
  - processes
  - people
  - intangibles, such as reputation

Using the digital repository self-audit tool – IV

Stage 4: Identify risks associated with activities and assets



T8: Identify risks associated with activities and assets of your repository

Strategic objectives and goals listed under Tasks 1 and 2 / Activities, assets and owners listed under Task 7

Operational functional classes
Support functional classes

Stage 4

Identify Risks

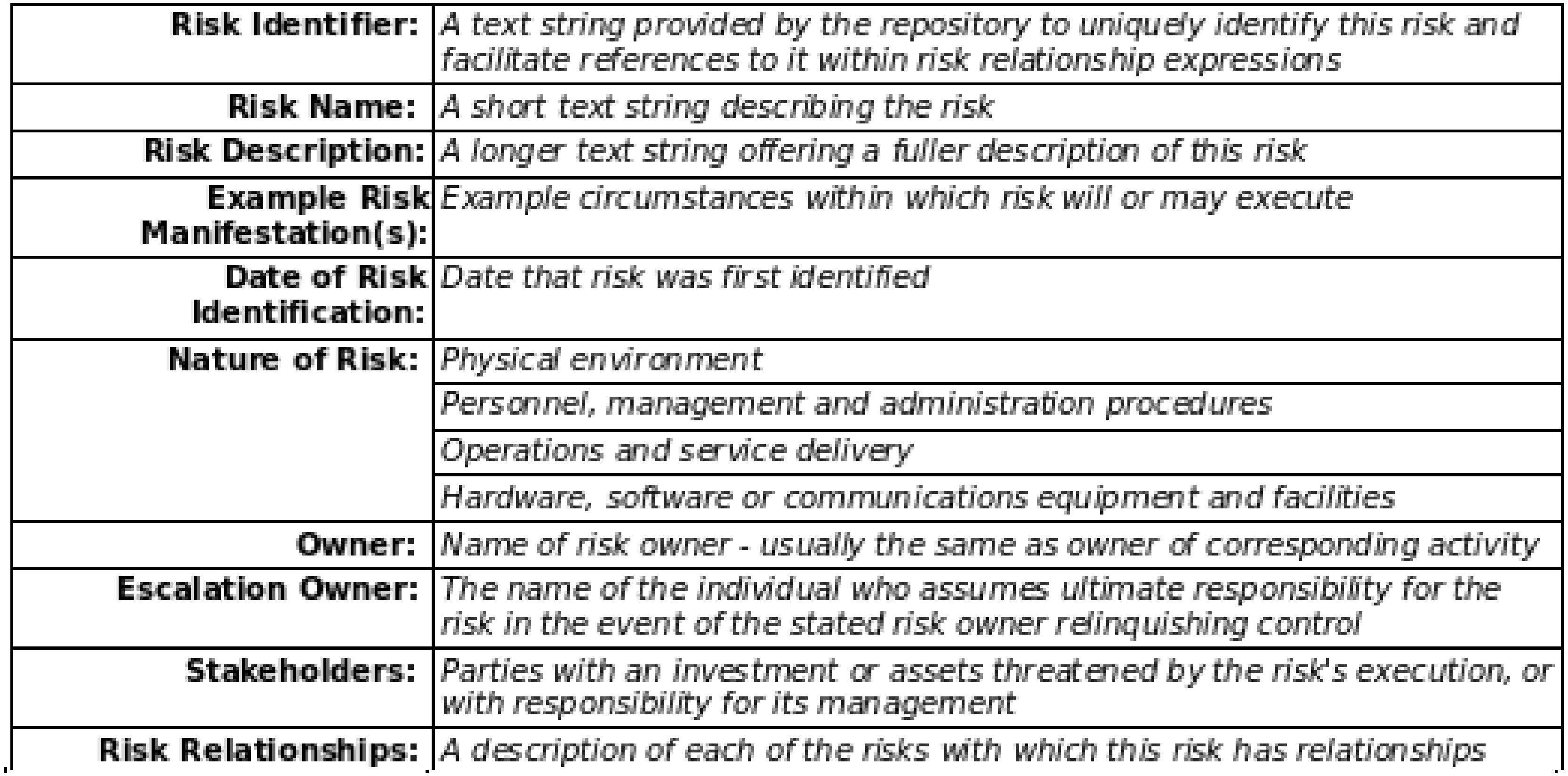
Identifying Risks

- Assets & Activities associated with vulnerabilities – characterised as risks
- Auditors must build structured list of risks, according to associated activities and assets
- No single methodology – brainstorming structured according to activities/assets is effective

Kinds of risk

- Assets or activities fail to achieve or adequately contribute to relevant goals or objectives
- Internal threats pose obstacles to success of one or more activities
- External threats pose obstacles to success of one or more activities
- Threats to organisational assets

Anatomy of a Risk



Risk Identifier:	*A text string provided by the repository to uniquely identify this risk and facilitate references to it within risk relationship expressions*
Risk Name:	*A short text string describing the risk*
Risk Description:	*A longer text string offering a fuller description of this risk*
Example Risk Manifestation(s):	*Example circumstances within which risk will or may execute*
Date of Risk Identification:	*Date that risk was first identified*
Nature of Risk:	*Physical environment*
	Personnel, management and administration procedures
	Operations and service delivery
	Hardware, software or communications equipment and facilities
Owner:	*Name of risk owner - usually the same as owner of corresponding activity*
Escalation Owner:	*The name of the individual who assumes ultimate responsibility for the risk in the event of the stated risk owner relinquishing control*
Stakeholders:	*Parties with an investment or assets threatened by the risk's execution, or with responsibility for its management*
Risk Relationships:	*A description of each of the risks with which this risk has relationships*

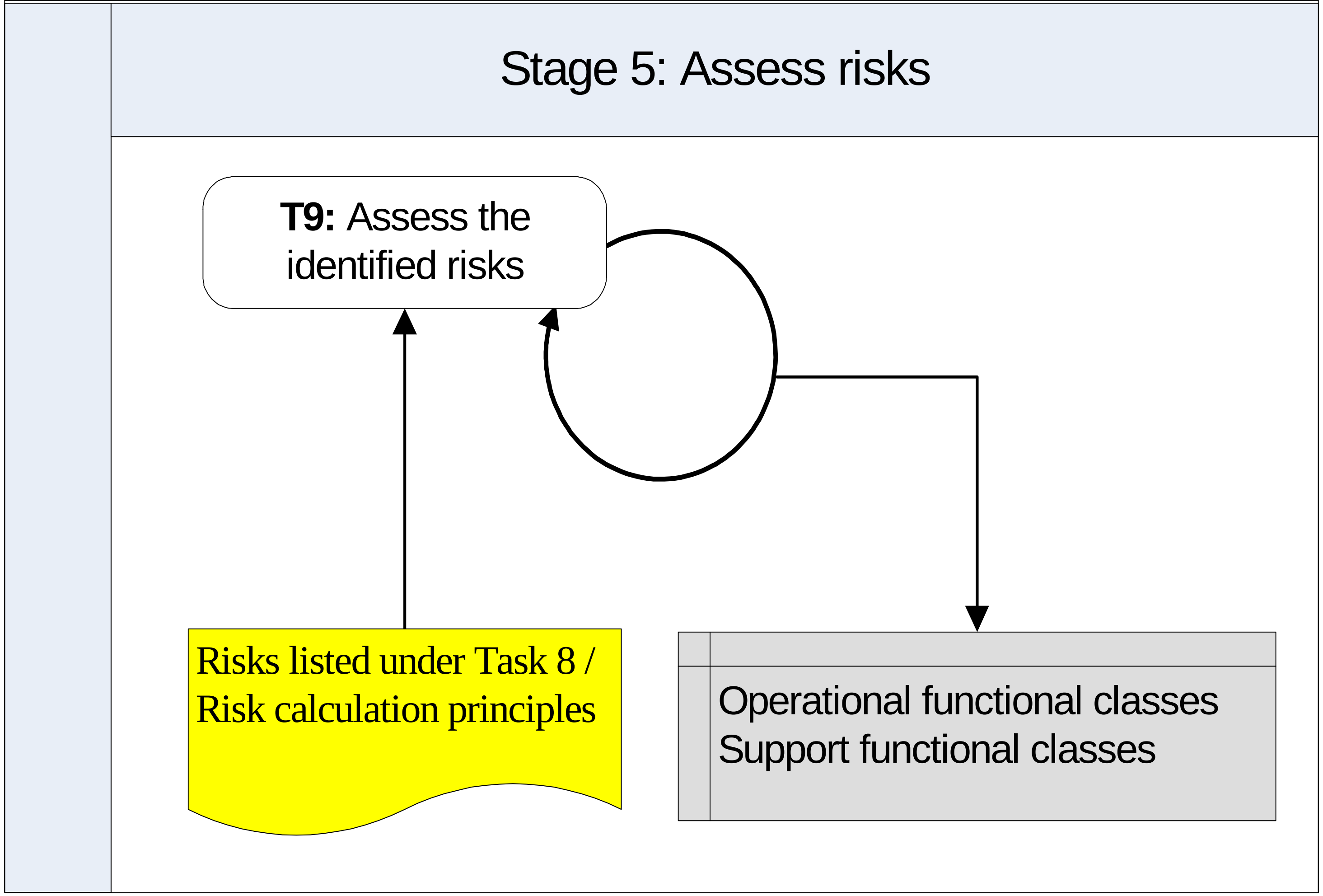
Risk Relationship	*Definition of Risk Relationship*
Explosive	where the simultaneous execution of *n* risks has an impact in excess of the sum of each risk occurring in isolation
Contagious	where a single risk's execution will increase the likelihood of another's
Complementary	where avoidance or treatment mechanisms associated with one risk also benefit the management of another
Contradictory	where avoidance or treatment associated with a single risk renders the avoidance or treatment of another less effective
Atomic	where risks exist in isolation, with no relationships with other risks

Example Risk

- **Loss of Trust or Reputation**
  - One or more stakeholder communities have doubts about the repository's ability to achieve it's business objectives

- **Example manifestation**
  - Irrecoverable loss of digital objects provoke community concerns about competence
  - public statement about cut in funding raises concerns about viability of repository's continued operations

Using the digital repository self-audit tool – V


Stage 5: Assess risks

T9: Assess the identified risks

Risks listed under Task 8 / Risk calculation principles

Operational functional classes
Support functional classes

Stage 5

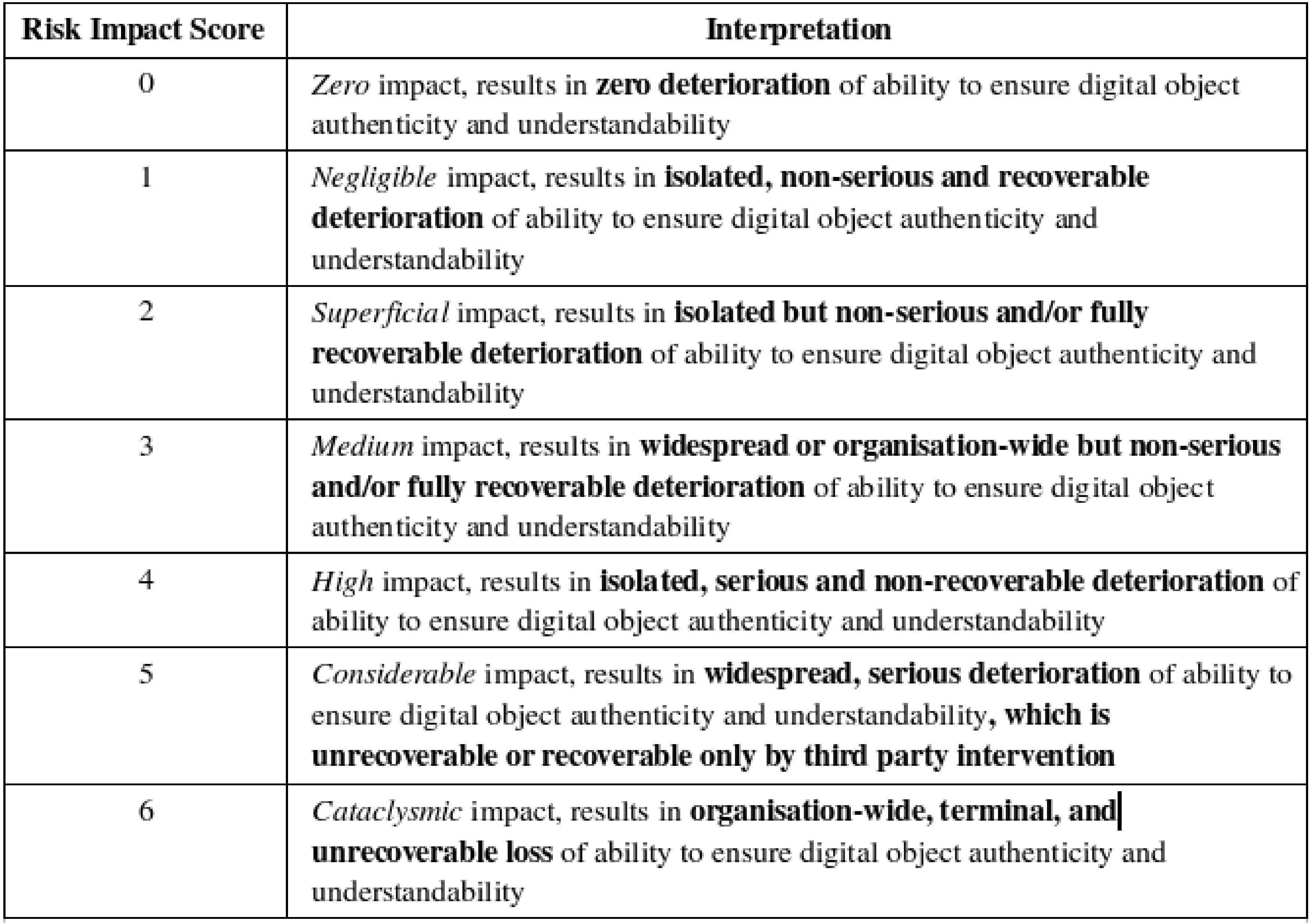
Assess Risks

Assess Risks

- Fundamental issues are:
  - probability of risks
  - potential impact of risks
  - Relationships between / groupings of risks
- A risk assessment must be undertaken for each identified risk

Risk Assessment

- For each risk auditors must record:
  - example manifestations of risk
  - probability of its execution
  - potential impact of its execution
  - relationships with other risks
  - risk escalation owner
  - severity or risk (quantification of seriousness, derived as product of probability and impact)



Risk Impact Score	Interpretation
0	*Zero* impact, results in **zero deterioration** of ability to ensure digital object authenticity and understandability
1	*Negligible* impact, results in **isolated, non-serious and recoverable deterioration** of ability to ensure digital object authenticity and understandability
2	*Superficial* impact, results in **isolated but non-serious and/or fully recoverable deterioration** of ability to ensure digital object authenticity and understandability
3	*Medium* impact, results in **widespread or organisation-wide but non-serious and/or fully recoverable deterioration** of ability to ensure digital object authenticity and understandability
4	*High* impact, results in **isolated, serious and non-recoverable deterioration** of ability to ensure digital object authenticity and understandability
5	*Considerable* impact, results in **widespread, serious deterioration** of ability to ensure digital object authenticity and understandability**, which is unrecoverable or recoverable only by third party intervention**
6	*Cataclysmic* impact, results in **organisation-wide, terminal, and unrecoverable loss** of ability to ensure digital object authenticity and understandability

Risk Impact

- Impact can be considered in terms of:
  - – impact on repository staff or public well-being
  - – impact of damage to or loss of assets
  - – impact of statutory or regulatory breach
  - – damage to reputation
  - – damage to financial viability
  - – deterioration of product or service quality
  - – environmental damage
  - – *loss of ability to ensure digital object authenticity and understandability* is ultimate expression of impact

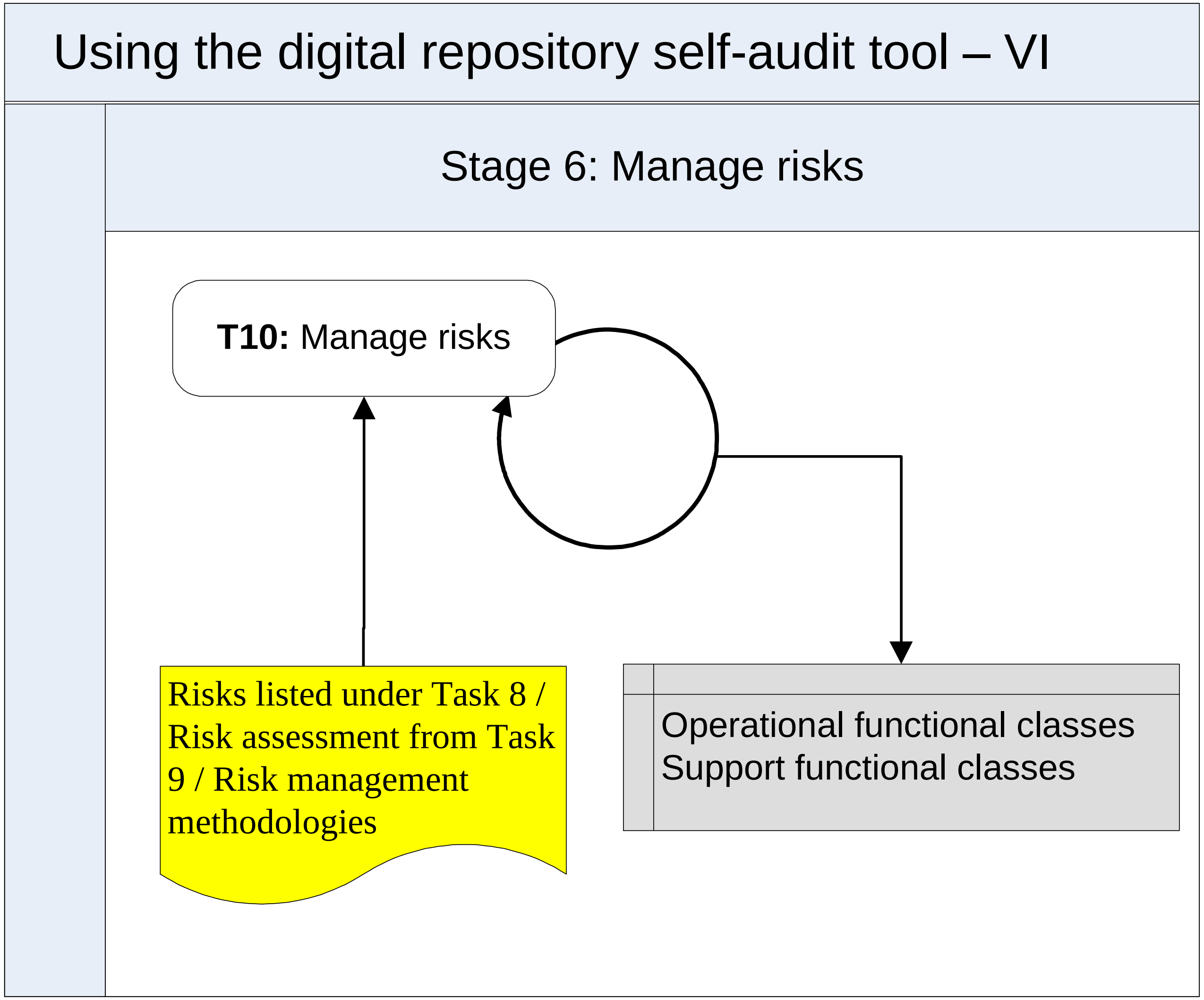
Risk Probability

Risk Probability Score	Interpretation
1	Minimal probability, occurs once every **100 years or more**
2	Very low probability, occurs once every **10 years**
3	Low probability, occurs once every **5 years**
4	Medium probability, occurs once **every year**
5	High probability, occurs once **every month**
6	Very high probability, occurs **more than once every month**

Determining impact and likelihood

- Consider:
  - Historical experiences
  - Mitigation/avoidance measures already in place
  - Experiences beyond repository itself
    - Relevant research
    - Expert opinion (e.g. legal, technical, environmental)
    - Experiences of comparable organisations

Using the digital repository self-audit tool – VI


Stage 6: Manage risks
T10: Manage risks
Risks listed under Task 8 / Risk assessment from Task 9 / Risk management methodologies
Operational functional classes
Support functional classes

Stage 6

Manage Risks

Manage Risks

- Combination of avoidance, tolerance and transfer
  - avoid circumstances in which risk arises
  - limit likelihood of risk
  - reduce potential impact of risk
  - share the risk
  - retain the risk

Risk Management & DRAMBORA

- The toolkit refrains from prescribing specific management policies
- Instead, auditors should:
  - – choose and describe risk management strategy
  - – assign responsibility for adopted measure
  - – define performance and timescale targets
  - – reassess success recursively

Management Risk: Steps

- Auditors should:
  - – identify suitable risk responses
  - – identify practical responses to each risk
  - – identify owners for risk management activities
  - – investigate threats arising from risk management
  - – prioritise risks
  - – update risk register and circulate information
  - – secure approval for planning and allocations

Interpreting the Audit Result

- Composite risk score enables quantification of risks' severity
  - illustrates vulnerabilities
  - facilitates resource investment
- Online tool will feature rich reporting mechanisms
  - what should this consist of?

After the audit

- Improvement requires ongoing activity
  - are risk management strategies working?
  - are risks within a satisfactory tolerance level?
  - risk exposure must be reassessed on an ongoing basis
  - risk management strategies must be re-evaluated
  - management must be informed of developments

DRAMBORA Future

- Test audits and feedback on the methodology – Spring-Summer 2007
- Version 2.0 to be released in September, as an interactive online tool
- Produce a formal audit report at the end of the self-audit
- Version 3.0 in Spring 2008
- Certification of self-auditors in 2008

Your role

We would like you to:

- Use the audit toolkit it in a test-audit on any digital repository (http://www.repositoryaudit.eu/)
- Tell us:
  - What results did you get?
  - What have you learned about your repository following DRAMBORA assessment?
  - What features would you like to see within the toolkit's online version?

Closing Questions?

- If you have any further questions please email us at feedback@repositoryaudit.eu

- We'd be delighted to hear of your own experiences using the DRAMBORA toolkit!