ENTERPRISE CYBER SECURITY

BUSINESS IMPACT ANALYSIS

University of Glasgow

OVERVIEW

- previously concerned with threats, need to understand the impact on the business.
- need to consider the business as whole, beyond the priorities of the technical department.
- understand the difference between disaster recovery and continuity.

BUSINESS IMPACT ANALYSIS

- solid **foundation** for business continuity planning.
- affords identification of **window of recovery**, resources that need to be recovered and mission critical activities.
- benchmark of the **quantitive** and **qualitative** losses that act as justification for contingency plans.
- understand the **dependencies** between business processes and infrastructures.

TIMING

- business impact analysis is a **precursor** to business continuity planning, but is not the motivation for it.
- upper-management should already be **committed** to business continuity planning, rather than waiting for surprises from business impact analysis to spur motivation.
- need an understanding of the level of **risk appetite** of the enterprise.
- establish policy to the limits of **disaster recovery**.

PURPOSE

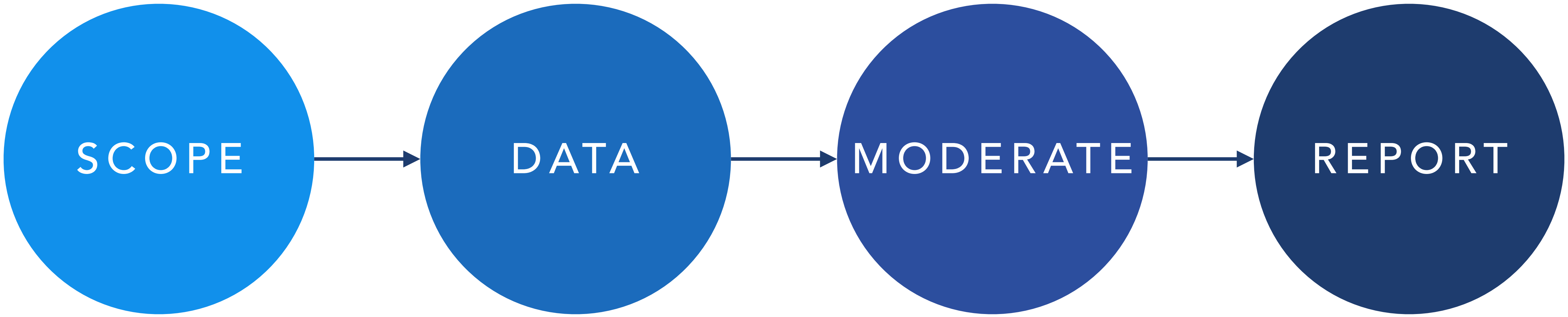
- determine the **qualitative** and **quantitive** impact and loss from possible incidents.

- understand the **tolerance** of business processes, in terms of resources, to possible incidents.

- determine the resources required to **protect** and/or **recover** a process to optimal or tolerable levels.

- focus of the analysis is to understand the **impact**, not the threat itself.

BUSINESS IMPACT ANALYSIS



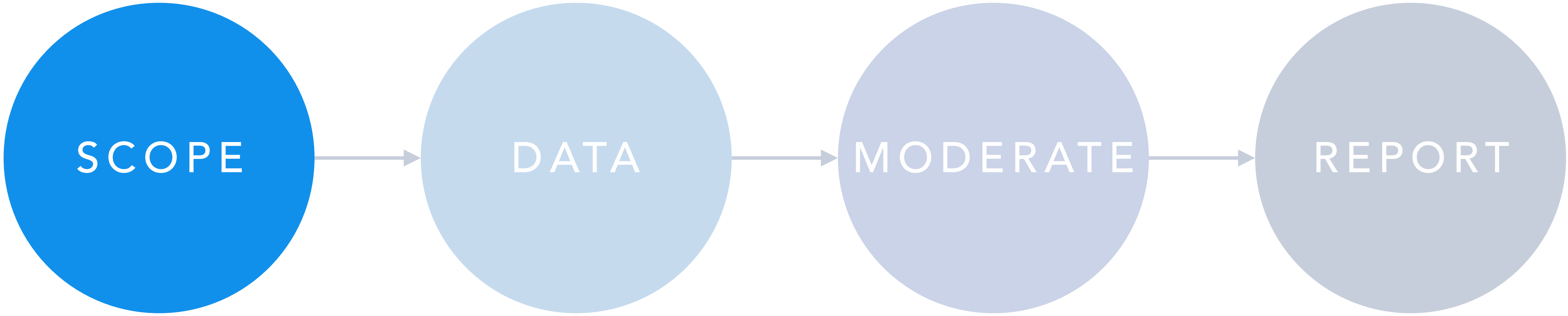
SCOPE

DATA

MODERATE

REPORT

BUSINESS IMPACT ANALYSIS



SCOPE

- determine the **scope** of the business impact analysis and understand the limits.

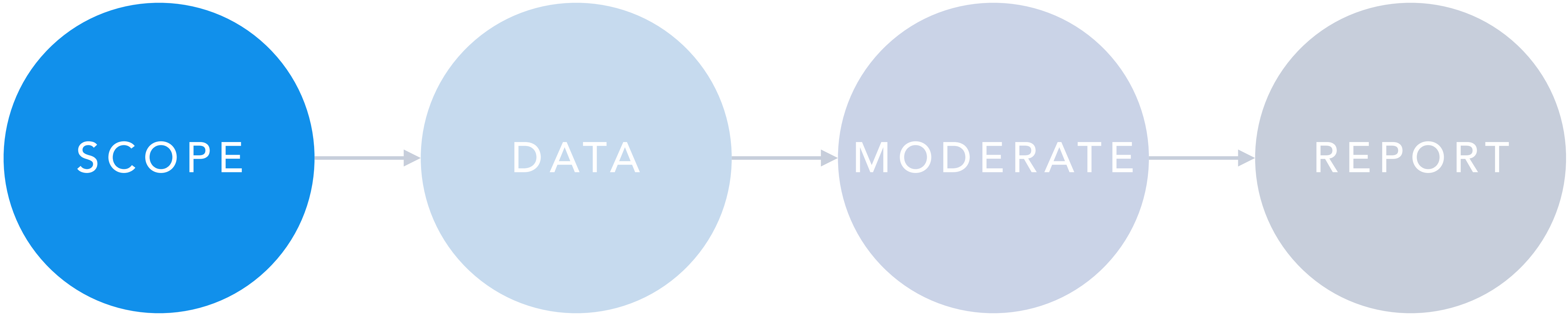
- focus could be the **entire** enterprise or **specific** business units.

- possible to utilise one of the business units as a **pilot** for the process itself.

PLANNING HORIZON

- need to understand the **period of disruption** from potential disasters.
- small business may view it as the time frame it takes to replace the **entire function** of the business
- business units need to consider the impact of their failure on the **larger system**.
- service economy in the UK, consider the example of providing an **alternative call centre** within Glasgow vs Perth.

BUSINESS IMPACT ANALYSIS



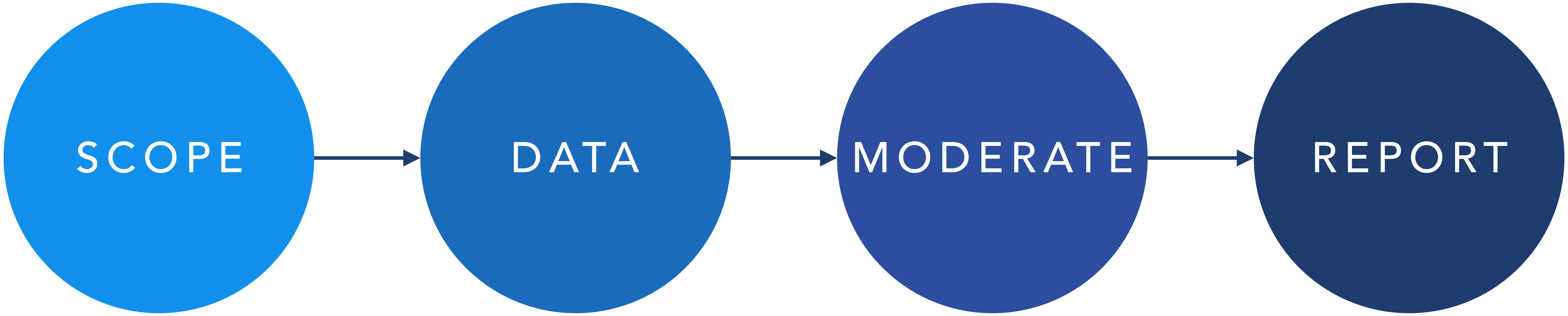
SCOPE

DATA

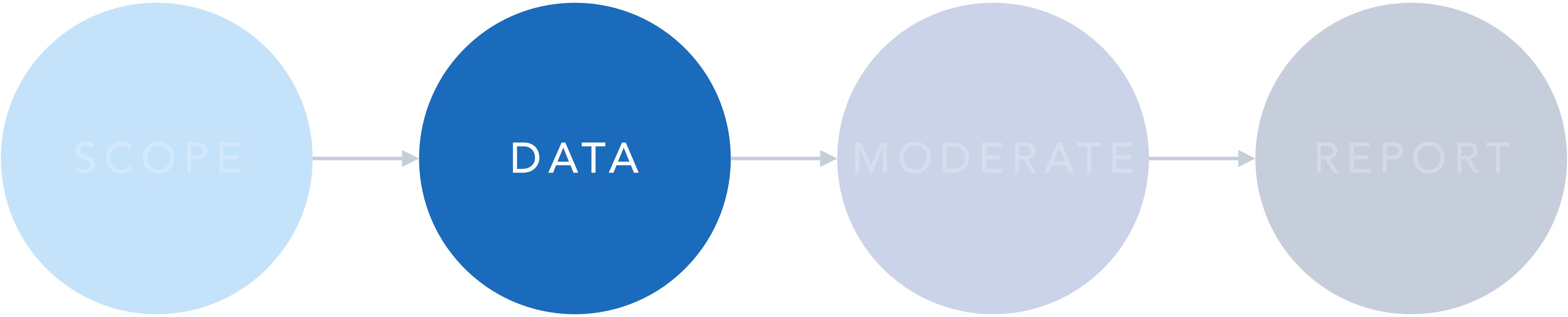
MODERATE

REPORT

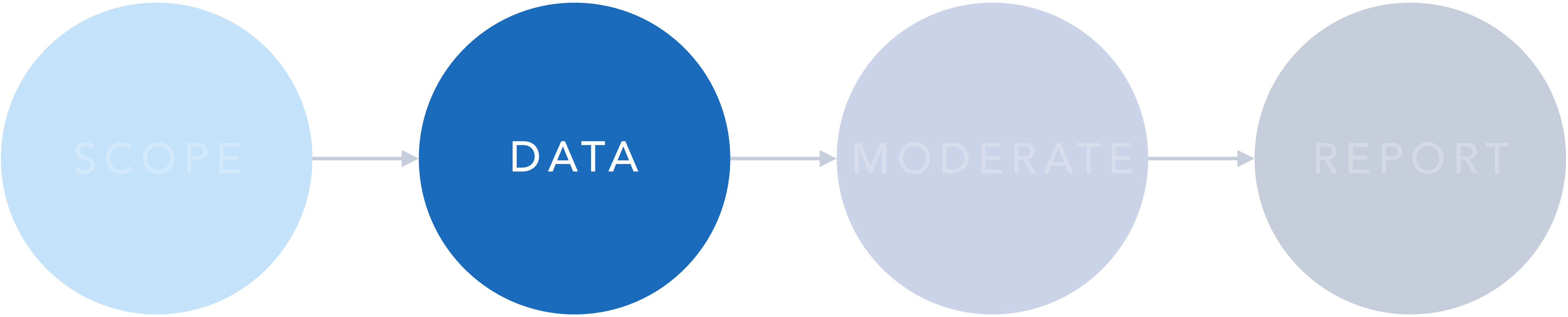
BUSINESS IMPACT ANALYSIS



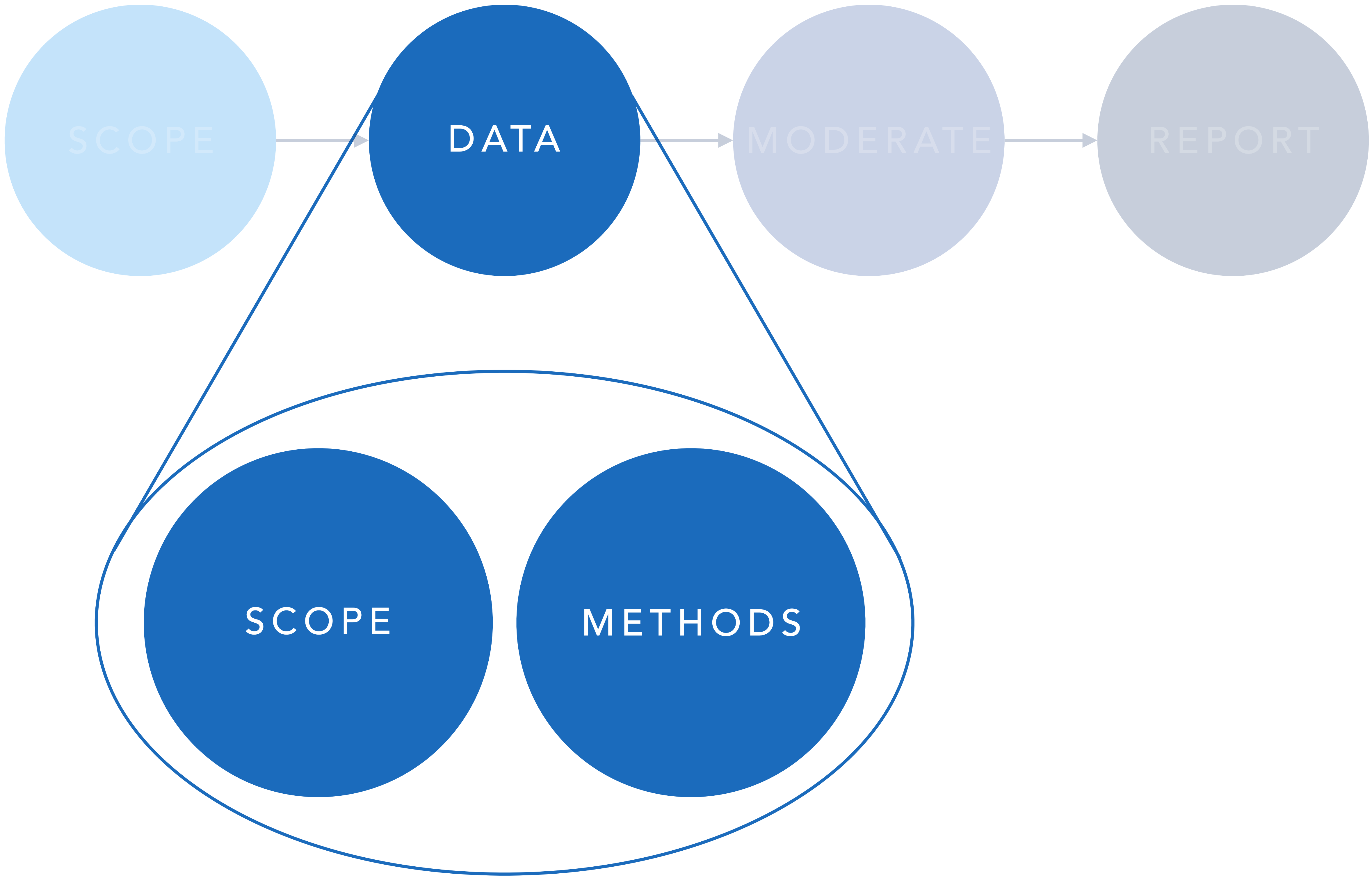
BUSINESS IMPACT ANALYSIS



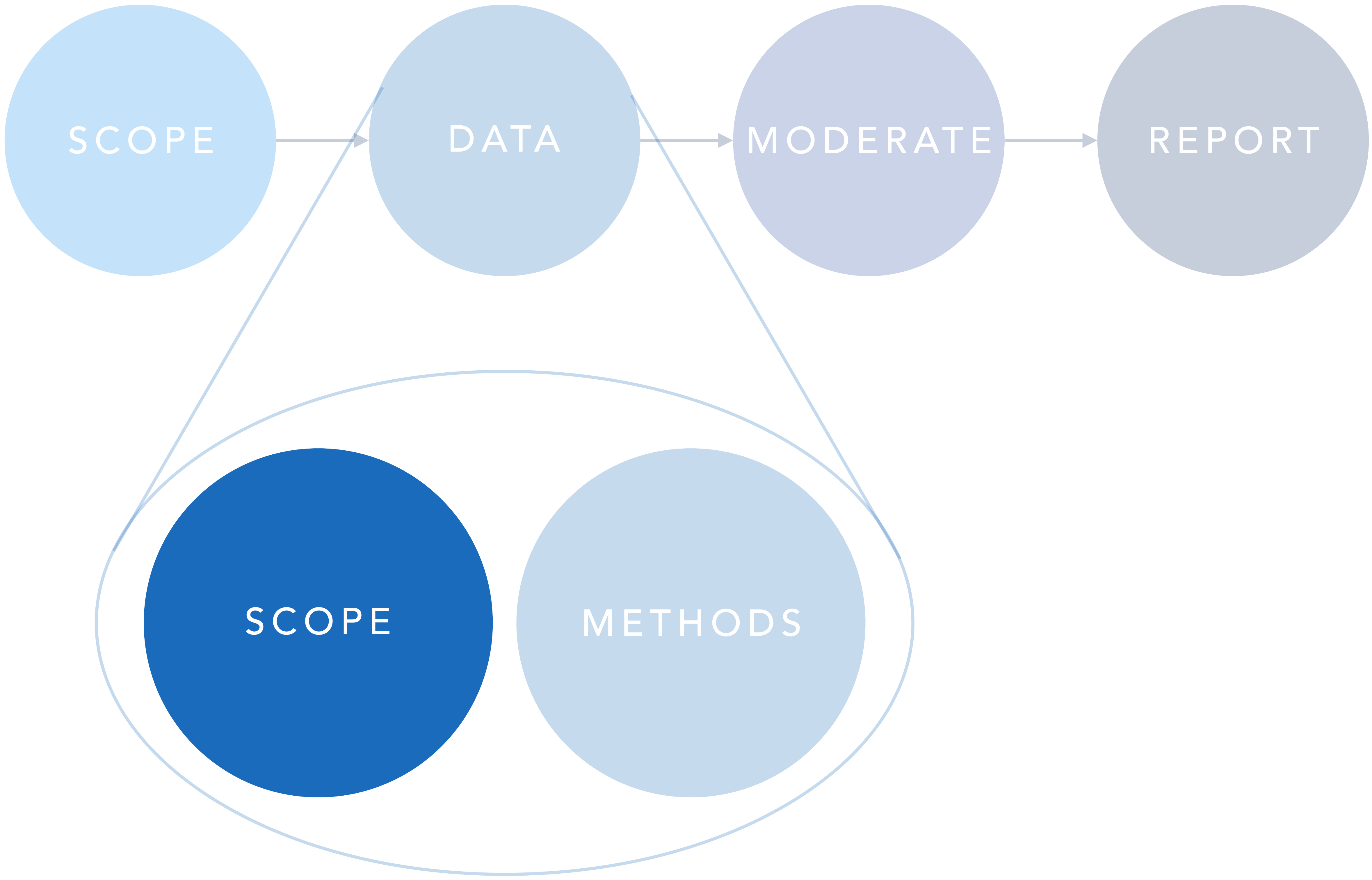
BUSINESS IMPACT ANALYSIS



BUSINESS IMPACT ANALYSIS



BUSINESS IMPACT ANALYSIS



DATA COLLECTION

- enterprises and employees most likely consider every **process** and step as imperative.

- understand the processes that happen will become **critical** within our planning horizon.

- these **critical processes within our planning horizon** need to be throughly considered with other processes left out of the scope.

- develop an approach to **communicate effectively** to all employees to ensure no one is disgruntled from being considered non-critical.

CRITICAL PROCESSES

- business processes considered not as imperative as others, could be **prioritised** to be performed at all costs.
- concerns of market participation, an organisation may view any disruption as incredibly harmful.
- processes that ensure **compliance** and responsibilities could be become prime focus.

CRITICAL PROCESSES

- **prioritised business processes** may be conducted during a period of disruption, but secondary processes will continue to represent a backlog.

- **backlog of processes** could represent another challenge in terms of continuity.

- critical processes may be **dependent on secondary** processes and tasks.

CRITICAL VS CONTINUITY

- **peer-review** to determine the absolutely essential processes for continuity.

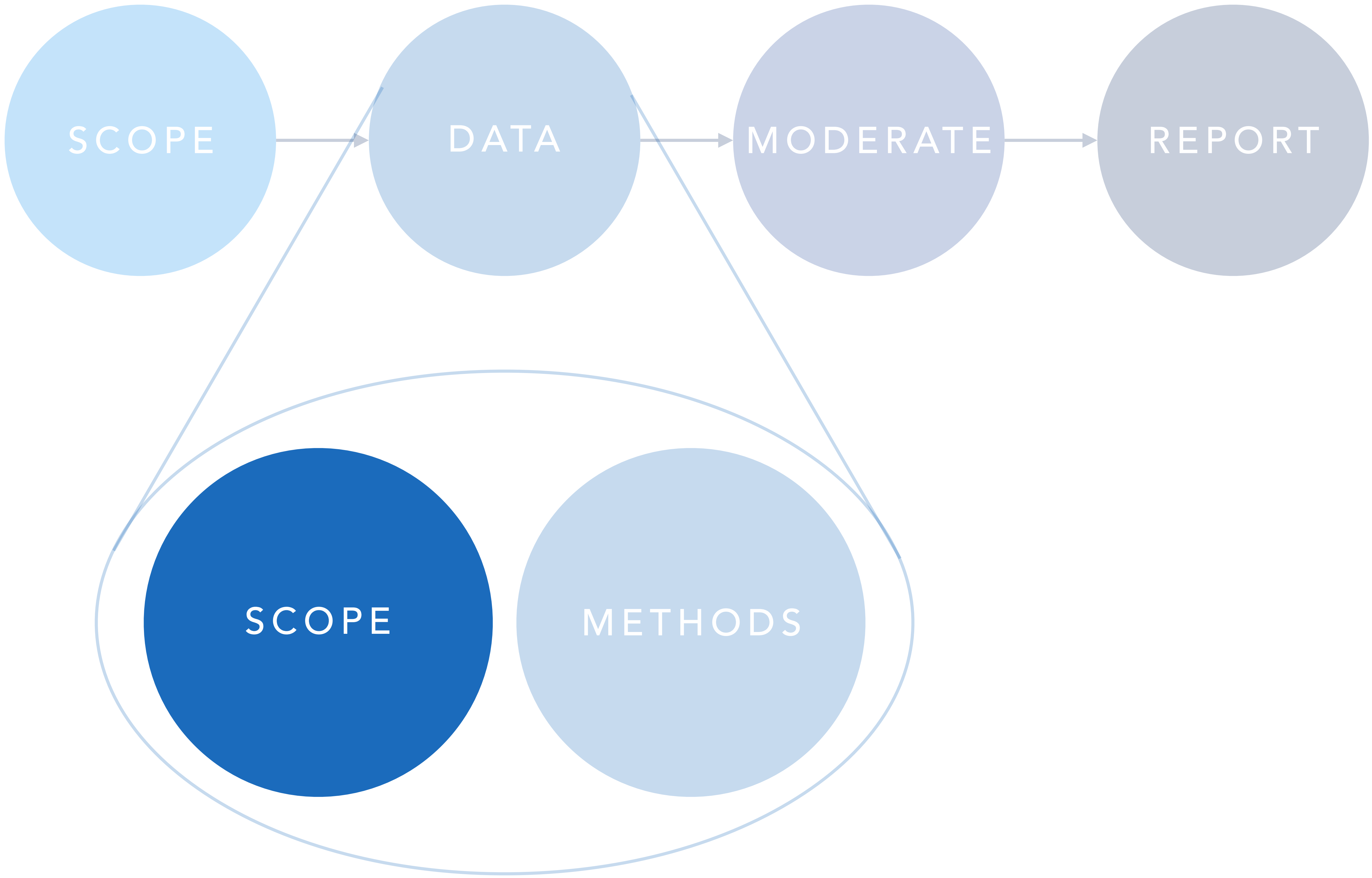
- need to prioritise process to ensure everything is being done to ensure business can continue.

- difficult as some metrics will be **solid and strong**, such as actual cost and breach of law, others will be **softer**, such as customer satisfaction and brand.

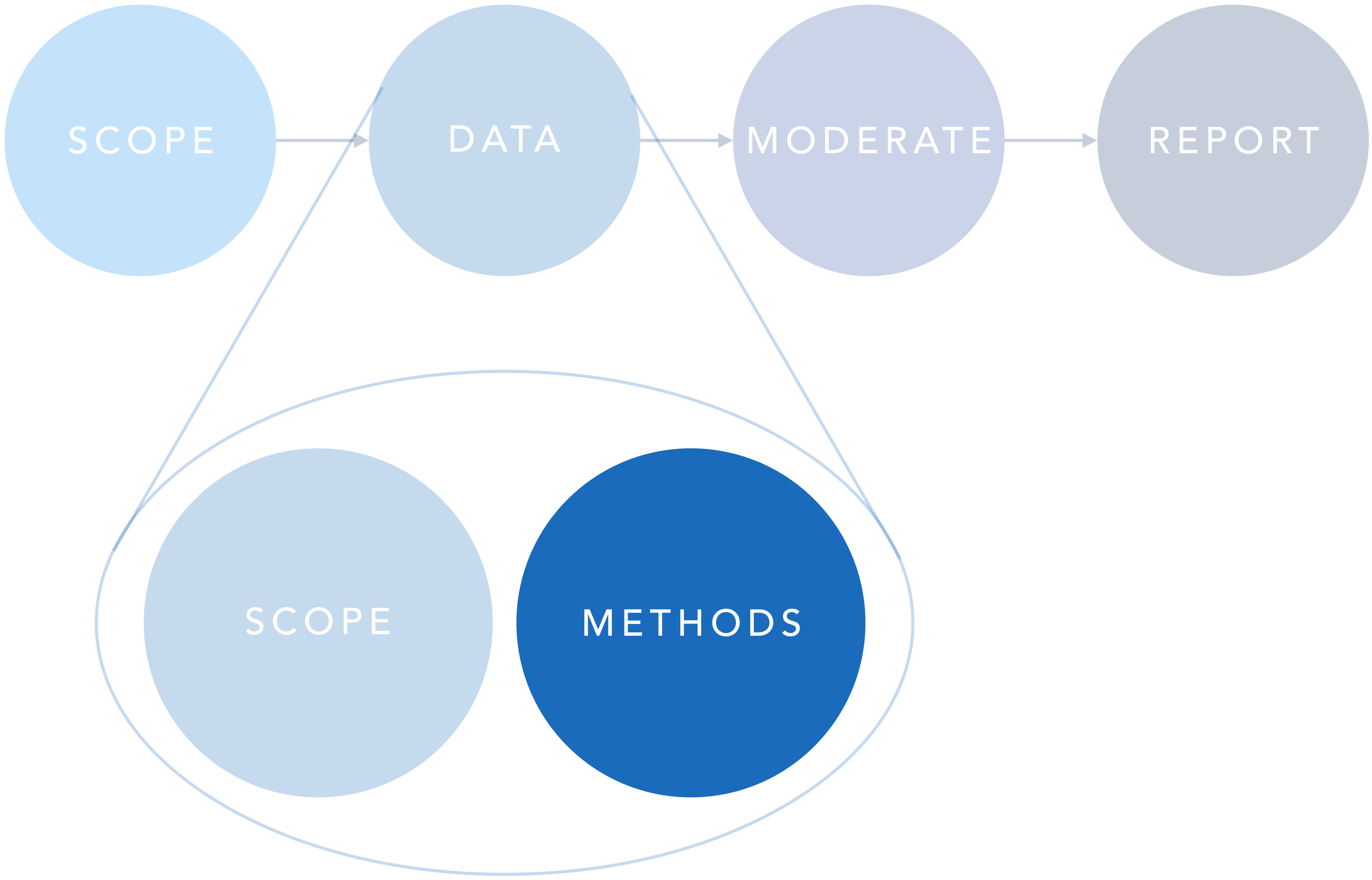
- the reality is that many **processes will rely on measurements** or evidence that is relatively soft.

Waitrose
Cafe
HUMAN VALUES AND THE DESIGN
OF COMPUTER TECHNOLOGY
BATYA
FRIEDMAN
INDSET
CAROL S. DWECK, PH.D

BUSINESS IMPACT ANALYSIS



BUSINESS IMPACT ANALYSIS



SCOPE

DATA

MODERATE

REPORT

SCOPE

METHODS

METHODS

- **questionnaires** issued across the entire enterprise or within individual business units.
- **structured interviews** within employees across the enterprise.
- **workshops** and discussions with various employees from different units and/or backgrounds.
- many aspects of these processes can be **automated** to reduce the overheads of data collection.

APPROACH

- **communicate** purpose and scope of business impact analysis to upper management.
- **presentation** should clearly communicate what is considered an important process and what is the window of interest.
- issue initial questionnaire to **business units** to determine any important business processes.

FIRST WAVE QUESTIONNAIRE

- improved understanding of what is termed as important **business processes** in terms of continuity.

- potential **refinement around the window of interest**, scope may need to be extended or reduced.

- removing business processes at this time that are not important, **spare business units the time on going in deeper**.

DEEPER DIVE

- use more questionnaires, structured interviews and workshops to obtained more detail about critical processes.

- employees involved in business processes must be consulted to ensure a detail and accurate picture of the processes and interdependencies between business units.

DEEPER DIVE

1. determine the actual recover time to bring the business process back online

2. determine the nature of the processes, does it occur annual, perform in a cycle or happen frequently.

3. recovery point for the process, must it restart from failure or can it start from the beginning.

DEEPER DIVE

1. prerequisites of the process, down it need occurs to complete, is there another process it relies upon, external actor?

2. resources requirements for the business process in terms of staff and level of knowledge and experience

3. requirements of the process - do they need an office?

DEEPER DIVE

1. special equipment the team need to bring the process back online.

2. IT requirements of the team

3. What contingency and work arounds are in place and how would these function if something happened.

TIME

- **recovery time objective** (RTO) is the period of time from failure to recovery before business units are considerably impaired.
- **maximum period of downtime** (MTPOD) is the period of time from failure to recovery before an enterprise is enduringly damaged.
- benchmarking with these periods is valuable when discussing, e.g. manager states they have 30-minute MTPOD for a critical process.
- typically more resources will need to be spent if recovery windows are small.

CALENDAR

- understand the calendar itself, in terms of when processes occur.

- business processes could occur and complete continuously.

- some business processes may occur within specific cycles.

- considering computer manufactures and back-to-school shopping season and habits.

RECOVERY POINT

- **recovery point objective** (RPO) is the period of time of permitted loss.

- recovering business processes may require a reasonable window of information and data loss.

- current maintenance process should necessarily inform the creation of the RPO.

- consider preparation time for recording recovery data as this may be expensive.

DEPENDENCIES

- prioritising business processes is expected to ensure energies are focused on critical areas.

- critical business processes could rely on non-critical business processes.

- co- and prerequisite business processes of this nature must be considered to ensure proper recovery.

- otherwise critical processes could be impaired during recovery due outputs from lesser processes not being considered.

UNDERSTANDING RTO, RPO AND MTPOD

RESOURCE REQUIREMENTS

- understand the resource requirements to support critical business processes.

- emphasis is lean critical processes that can function in terms of business continuity.

- duplicate processes can be incredibly expense and need considerable justification.

- short-term lean process may still be expensive, e.g. scaling up staff numbers to manual implementation of process.

EQUIPMENT FACILITIES

- requirements in terms of generic facilities, in terms of hardware, software, offices as well as utilities.
- special facility requirements that include specialist and potentially bespoke equipment.
- emphasis should be placed on lean, minimal resources to support critical processes.
- complexities that can be introduced by maintaining such facilities.

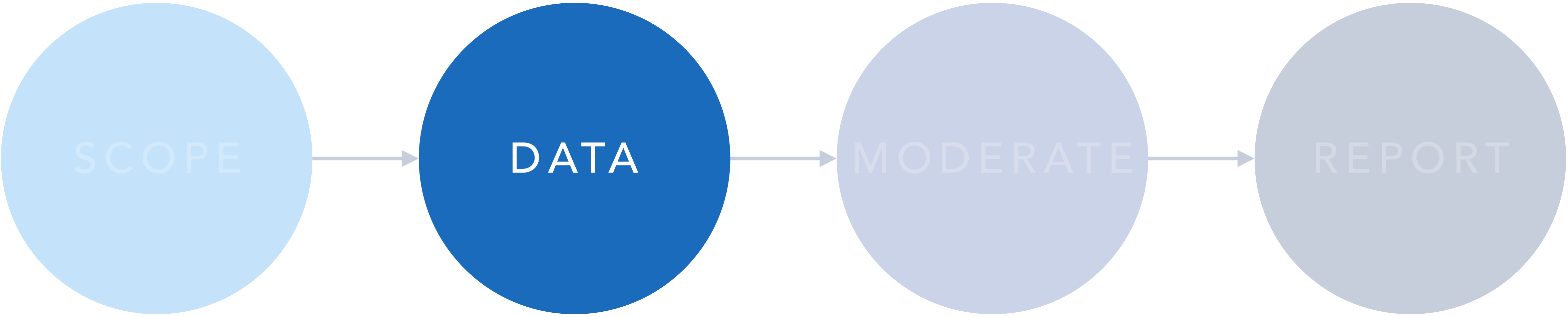
EXISTING SOLUTIONS

- many business solutions may have existing contingency plans as well as workarounds.

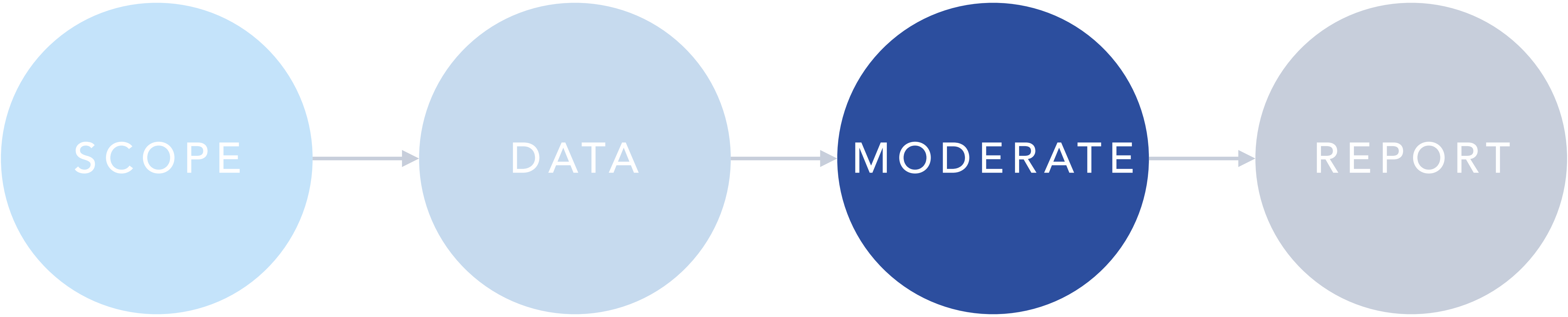
- gathering information about these plans may provide deeper insight into the specific challenges of the business unit and potential dependencies.

- typically such contingency plans have not been throughly assessed or reported, observe caution.

BUSINESS IMPACT ANALYSIS



BUSINESS IMPACT ANALYSIS



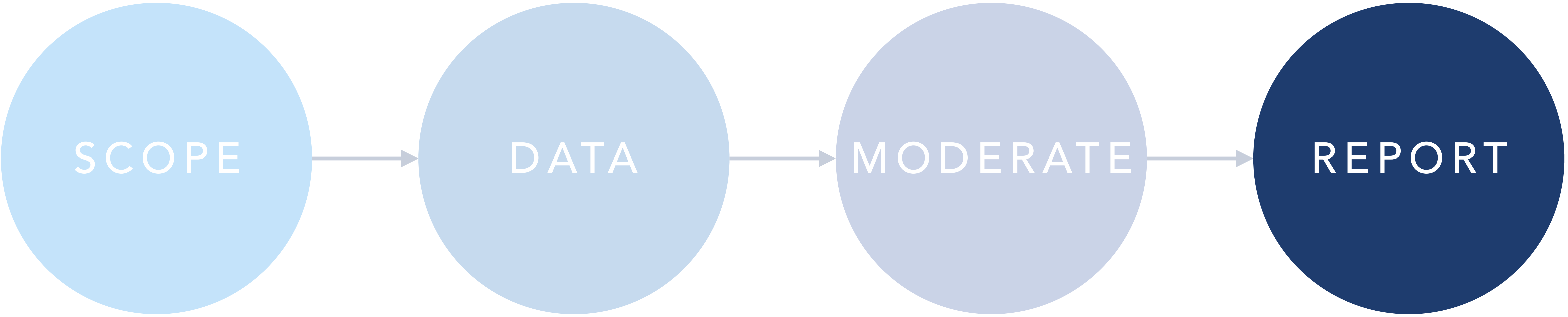
MODERATION

- information gathered needs to be **considered and analysed**.
- determine **validity** of claims made by various business units in terms of operational requirements.
- understand any **gap** between operational necessities and actual continuity capability.
- remember the outcome is an acceptable recommendation, need to have confidence that **appetite exists to address continuity requirements**.

APPROACHES

- compare with **previous business impact analysis** to determine any change.
- compare information gathered across business units to gain insight into **significant difference**.
- **compare** output with other organisations or previous experience.
- **peer-review** with panel to identify any potential questions or areas of improvement before reporting to management.

BUSINESS IMPACT ANALYSIS



REPORT

- output from the business impact analysis is a statement of **operational requirements**.
- the report itself acts as **evidence** for future demonstration of compliance and audits.
- must written formally and adopt a scientific approach, supporting reproducibility.
- the business impact analysis is not to act as strategy.

STRUCTURE

- **motivation** for conducting the analysis as well as the **context** of the organisation.
- underlying **evidence** and assumptions that were made when conducting the business impact analysis.
- detailed **methodology** as well as the process of **validation**.
- statements that either indicate **acceptance or rejection** of the conclusions of the analysis.

REVIEW

REVIEW

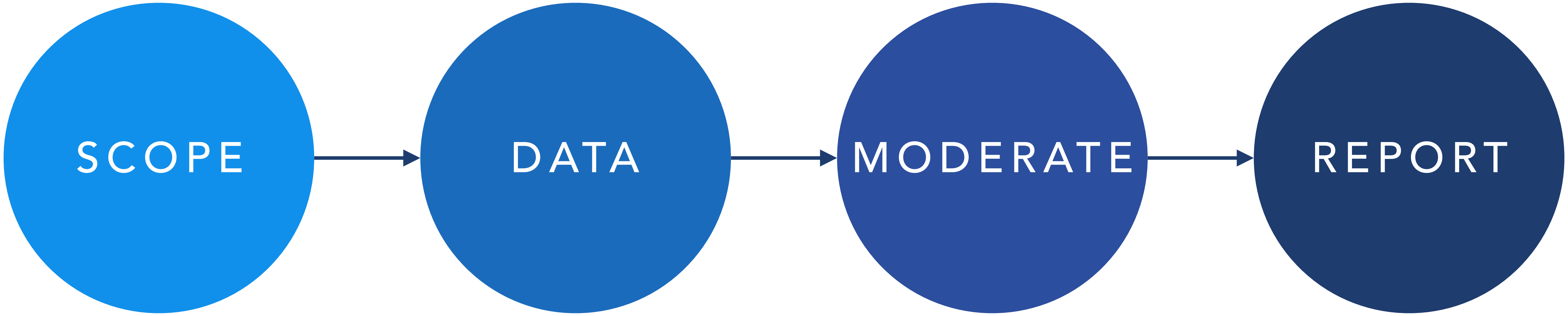
- business impact analysis should be reviewed at least annually or after any major enterprise changes.

- annual review may be unrealistic for many enterprises and unnecessary.

- failure to properly review may result in poor recovery planning.

- tolerances acceptance once may no longer be acceptable and legacy backup procedures may be incompatible with current systems.

BUSINESS IMPACT ANALYSIS



SUMMARY

- business impact analysis should output operational requirements, not strategy.
- strategic planning should be built on the solid foundation of a strong business impact analysis.
- mileage may vary between organisations and may avoid business impact analysis.
- performed properly, business impact analysis can avoid expensive mistakes in continuity planning.

OVERVIEW

- previously concerned with threats, need to understand the impact on the business.
- need to consider the business as whole, beyond the priorities of the technical department.
- understand the difference between disaster recovery and continuity.