Continual process improvement

HP University Electives

Continual Service Improvement (CSI)

Key Concepts

- CSI Model
- The 7 Step Improvement Process

Processes

- Service Measurement
- Service Reporting
- Service Improvement

Continual Service Improvement — Purpose

- to continually align and realign IT services to changing business needs by identifying and implementing improvements to IT services that support business Processes.
- CSI is about looking for ways to improve Process effectiveness and efficiency, as well as cost-effectiveness.

Continual Service Improvement — Objectives

- to review, analyze and make recommendations on improvement opportunities in each Lifecycle phase.
- to review and analyze Service Level Achievement results.
- to identify and implement individual activities to improve IT service quality.
- to improve the efficiency and effectiveness of enabling ITSM processes.
- to improve cost-effectiveness of delivering IT services without sacrificing customer satisfaction.
- to ensure applicable quality management methods are used to support continual improvement activities.

Ownership

The principle of ownership is fundamental to any improvement strategy.

One of the keys to successful implementation is to ensure that a specific manager, a CSI manager, is responsible for ensuring the best practice is adopted and sustained throughout the organization.

The CSI manager becomes:

- the CSI owner
- chief advocate of CSI
- accountable for the success of Continual Service Improvement in the organization.

CSI and Organizational Change

•Successful CSI supports organizational change

•Organizational change presents challenges

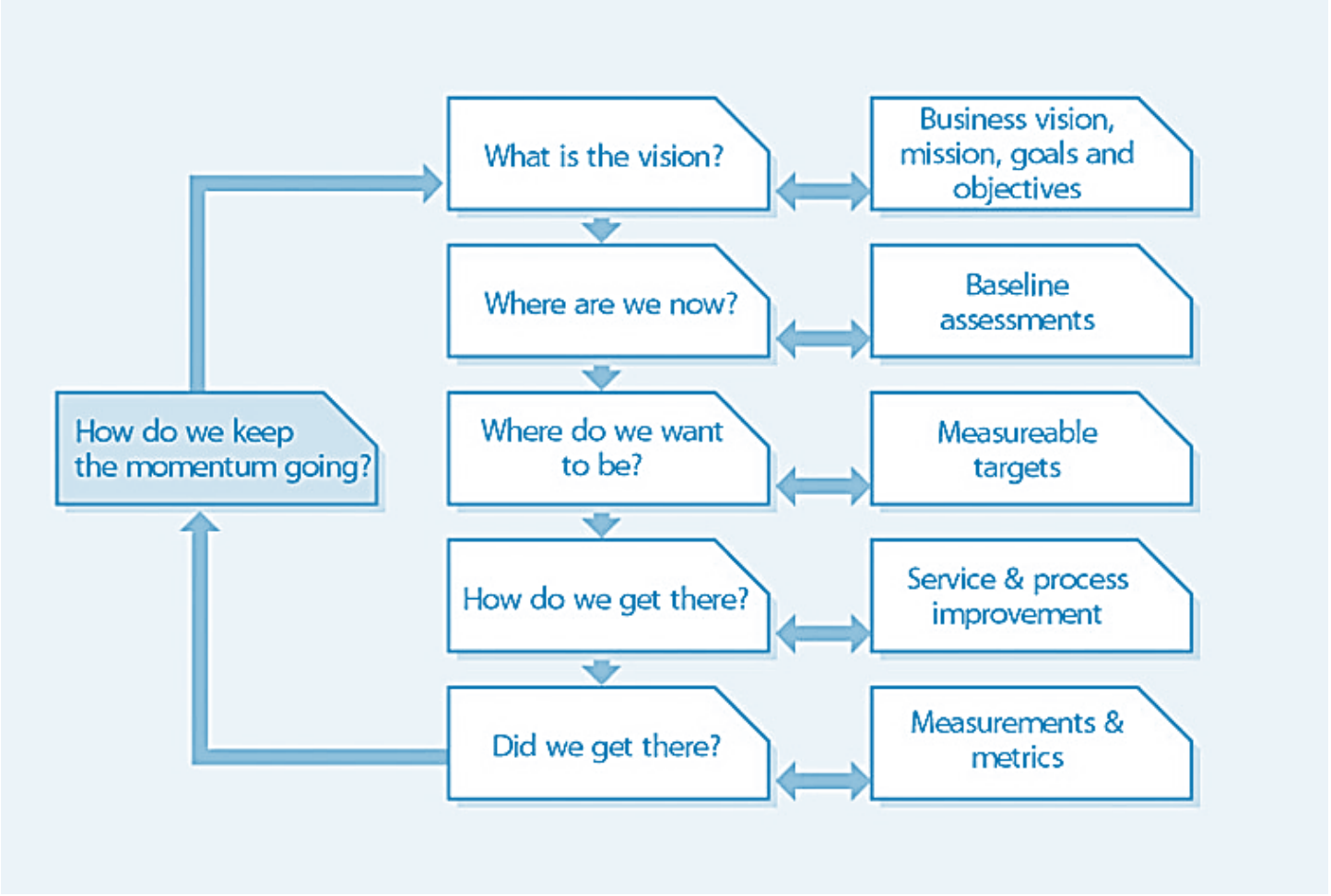
•Use formal approaches to address people-related issues:

- John Kotter's "Eight steps to transforming your organization"

1. Create a sense of urgency
2. Form a guiding coalition
3. Create a vision
4. Communicate the vision
5. Empower others to act on the vision
6. Plan for and create quick wins
7. Consolidate improvements and produce more Changes
8. Institutionalize the Change

- Project Management

Continual Service Improvement Model



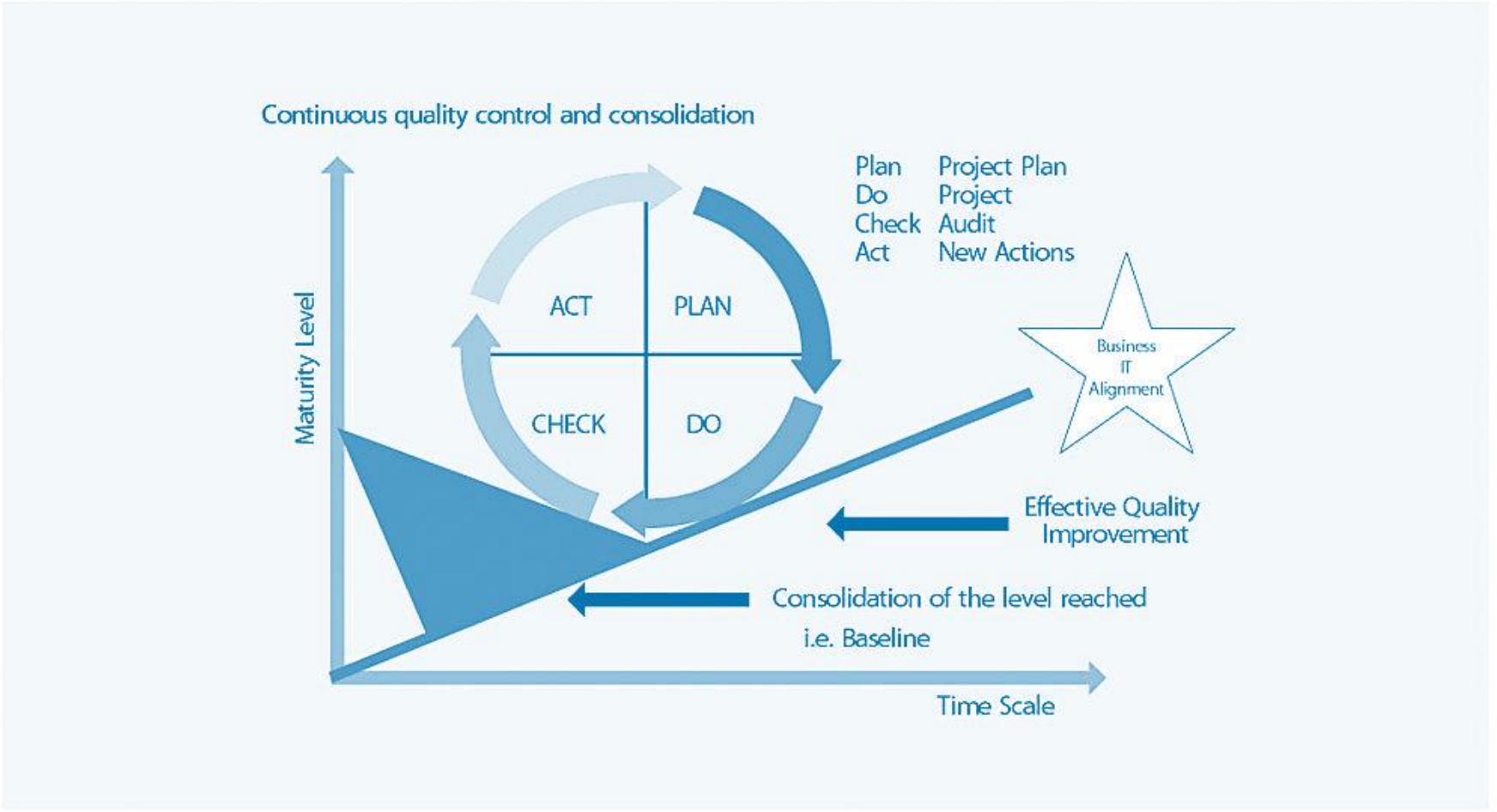
Baseline

An important beginning point for highlighting improvement is to establish baselines as markers or starting points for later comparison.

Baselines are also used to establish an initial data point to determine if a service or process needs to be improved. As a result, it is important that baselines are documented, recognized and accepted throughout the organization. Baselines must be established at each level: strategic goals and objectives, tactical process maturity, and operational metrics and KPIs.

If a baseline is not initially established the first measurement efforts will become the baseline. That is why it is essential to collect data at the outset, even if the integrity of the data is in question. It is better to have data to question than to have no data at all.

The Deming Cycle



CSI Policies

Many of the policies that support CSI activities are often found as a part of Service Level Management, Availability Management and Capacity Management.

Examples of some of these policies are:

- Monitoring requirements must be defined and implemented
- Data must be gathered and analyzed on a consistent basis
- Trend reporting must be provided on a consistent basis
- Service Level Achievement reports must be provided on a consistent basis
- Internal and external service reviews must be completed on a consistent basis (internal is within IT and external is with the business)
- Services must have either clearly defined service levels or service targets that can be used to determine if there are gaps in the services provided
- Service management processes must have critical success factors and key performance indicators to determine if there are gaps between the expected outcome and the real outcome.

CSI Policies

Additional CSI polices that an IT organization should implement:

All improvement initiatives must use the formal Change Management process

All functional groups within IT have a responsibility for CSI activities. This might be only one person in the group, but the intent here is that CSI is not usually a functional group within an organization but that everyone has a hand in supporting CSI activities

Roles and responsibilities will be documented, communicated and filled within IT.

Role — Continual Service Improvement Manager

- Accountable for the success of all improvement activities
- Communicates the CSI vision across the IT organization
- Defines and reports on CSI Critical Success Factors, Key Performance Indicators and CSI activity metrics
- Co-ordinates CSI throughout the service lifecycle
- Builds effective relationships with the business and IT managers
- Ensures monitoring is in place to gather data
- Works with process and service owners to identify improvements and improve quality

Role — Service Manager

- Manages the development, implementation, evaluation and on-going management of new and existing products and services
- Develops business case, product line strategy and architecture
- Develops new service deployment and lifecycle management schedules
- Performs Service Cost Management activities
- Works to instill a market focus
- This role is very similar to the "Product Manager" role in Service Strategy

What is Service Measurement?

- Measuring and reporting performance against targets of an end-to-end service
- Combines component measurements to provide a view of customer experience
- Data can be analyzed over time to produce a trend
- Data can be collected at multiple levels (for example, CIs, processes, services)

Key point: Take baseline(s) before implementing improvements

Purpose/Goals/Objectives

For services there are three basic measurements that most organizations utilize. The Service Design publication covers these measures in more detail.

Availability of the service

Reliability of the service

Performance of the service

It is no longer sufficient to measure and report against the performance of an individual component such as a server or application.

IT must now be able to measure and report against an end-to-end service.

15 HP Confidential

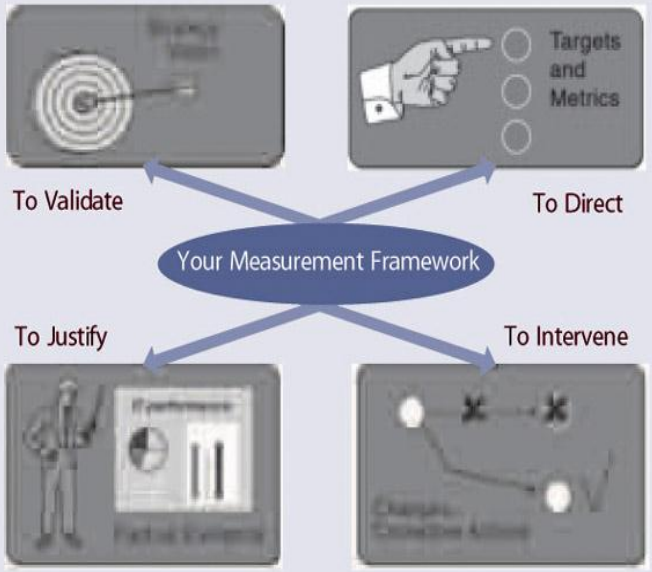
Why do we measure?

To validate

monitoring and measuring to validate previous decisions

To direct

monitoring and measuring to set direction for activities in order to meet set targets. It is the most prevalent reason for monitoring and measuring



To justify

monitoring and measuring to justify, with factual evidence or proof, that a course of action is required

To intervene

monitoring and measuring to identify a point of intervention including subsequent changes and corrective actions.

Basic Concepts

Critical Success Factors (CSF)

Something that must happen if a Process, Project, Plan, or IT Service is to succeed. KPIs are used to measure the achievements of each CCSF.

For example a CSF of “protect IT Services when making Changes” could be measured by KPIs such as “percentage reduction of unsuccessful Changes”, “percentage reduction in Changes causing Incidents” etc.

Key Performance Indicator (KPI)

A Metric that is used to help manage a Process, IT Service or Activity. Many Metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the Process, IT Service or Activity.

KPIs should be selected to ensure that Efficiency, Effectiveness, and Cost Effectiveness are all managed.

17 HP Confidential

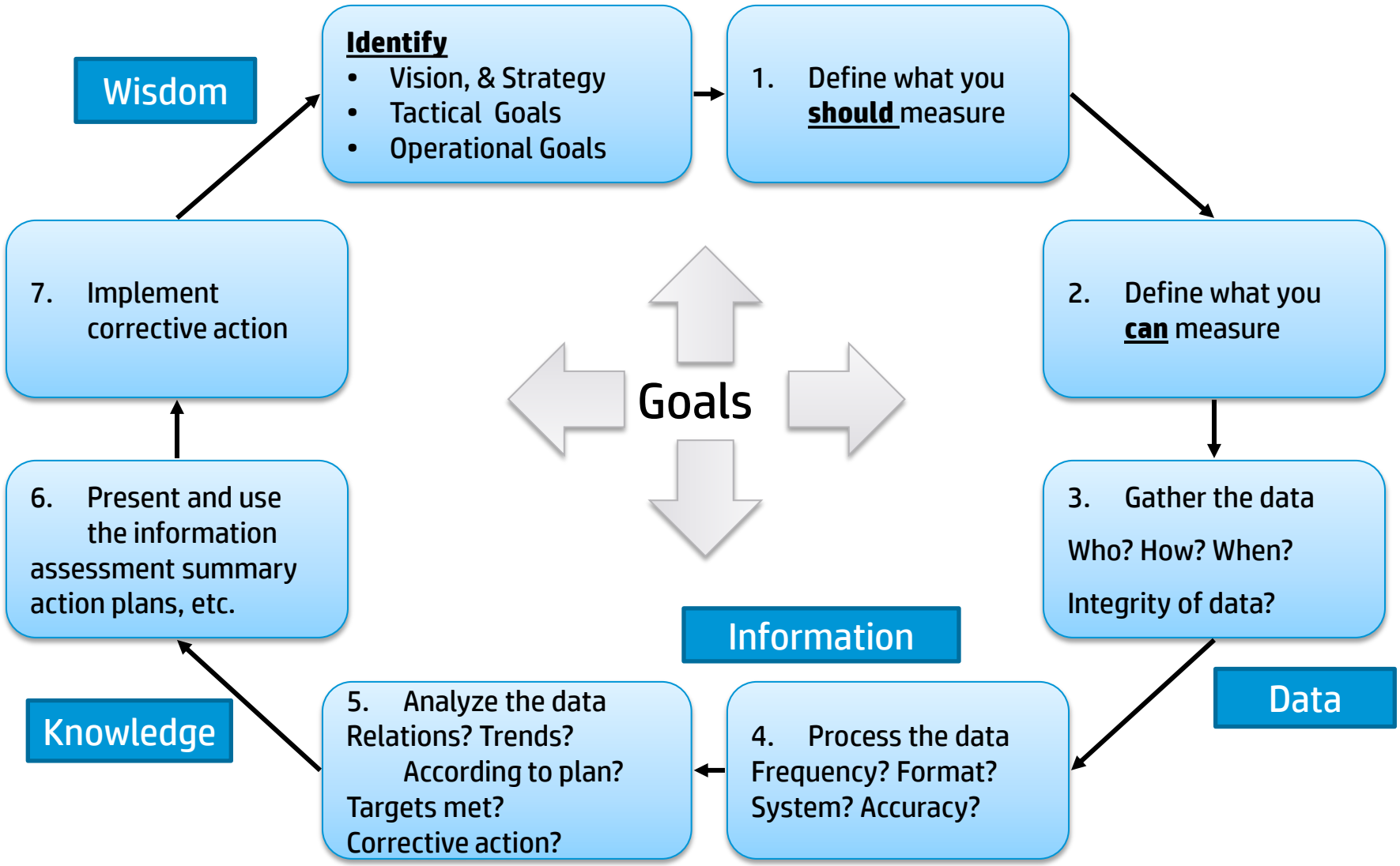
Types of metrics

- Technology metrics: typically components and applications For example
  - Performance
  - Availability
- Process metrics: Critical Success Factors (CSFs), Key Performance Indicators (KPIs), activity metrics for ITSM processes
- Service metrics: end-to-end service metrics

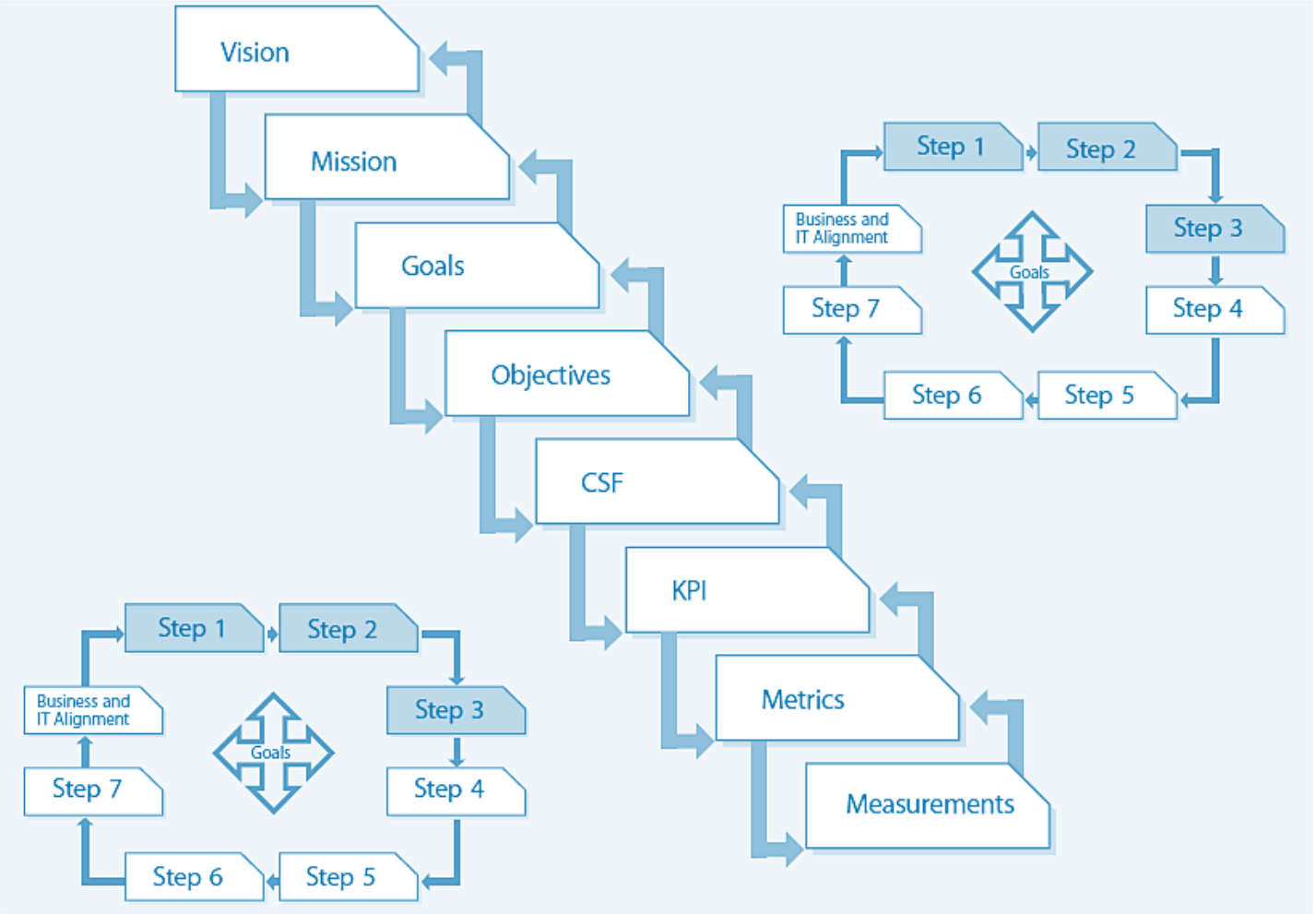
The 7 Step Improvement Process Purpose

- Measurement is essential for Continual Service Improvement
- The 7 Step Improvement Process is designed to provide this measurement

The 7-Step Improvement Process



From Vision to Measure



Service Reporting

Service Reporting

A significant amount of data is collated and monitored by IT in the daily delivery of quality service to the business; however, only a small subset is of real interest and importance to the business. The majority of data and its meaning are more suited to the internal management needs of IT.

The business likes to see a historical representation of the past period's performance that portrays their experience; however, it is more concerned with those historical events that continue to be a threat going forward, and how IT intend to militate against such threats.

It is not satisfactory simply to present reports which depict adherence (or otherwise) to SLAs, which in themselves are prone to statistical ambiguity. IT needs to build an actionable approach to reporting. i.e. this is what happened, this is what we did, this is how we will ensure it doesn't impact you again, and this is how we are working to improve the delivery of IT services generally.

A reporting ethos which focuses on the future as strongly as it focuses on the past also provides the means for IT to market its wares directly aligned to the positive or negative experiences of the business.

Reporting Policy and Rules

An ideal approach to building a business-focused service-reporting framework is to take the time to define and agree the policy and rules with the business and Service Design about how reporting will be implemented and managed.

This includes:

Targeted audience(s) and the related business views on what the service delivered is

Agreement on what to measure and what to report on

Agreed definitions of all terms and boundaries

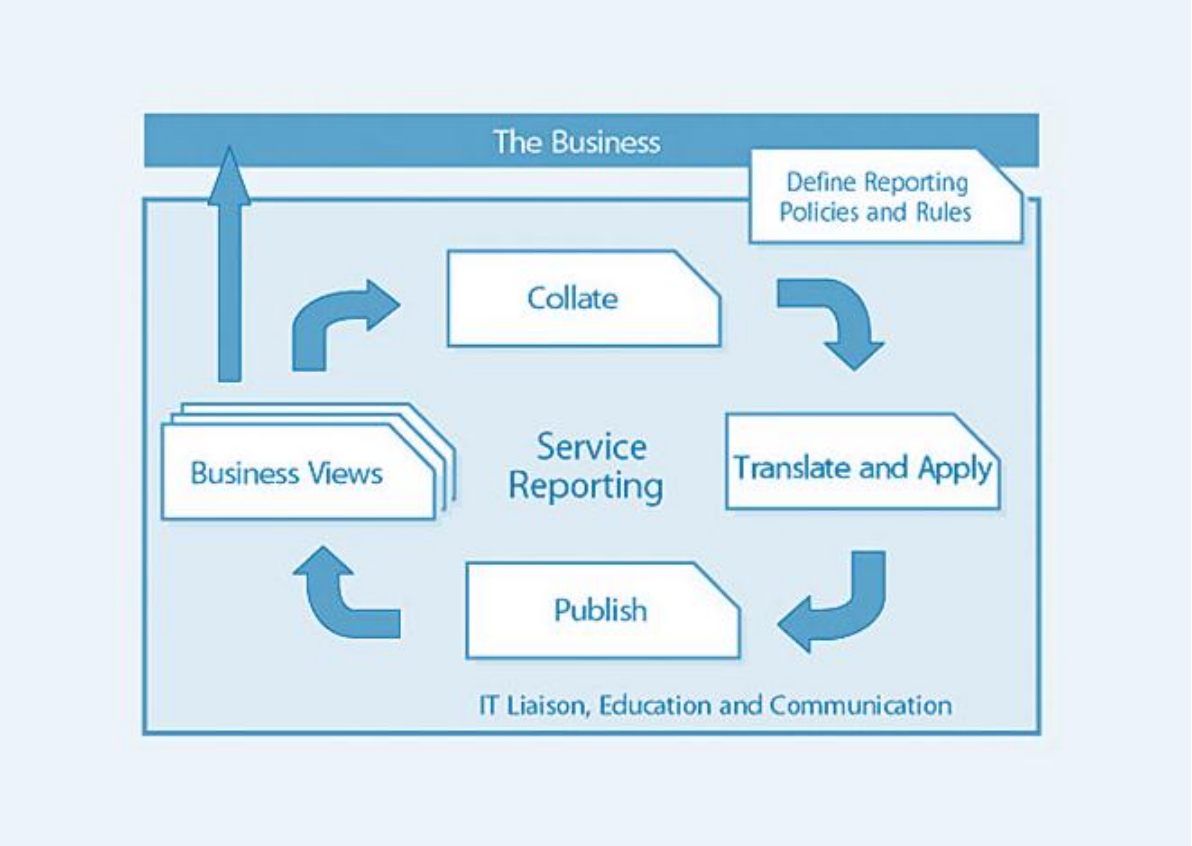
Basis of all calculations

Reporting schedules

Access to reports and medium to be used

Meetings scheduled to review and discuss reports.

Service Reporting Process



Different Levels of Reporting

Before starting the design of any report it is also important to know the following:

What information will be produced, shared or exchanged?

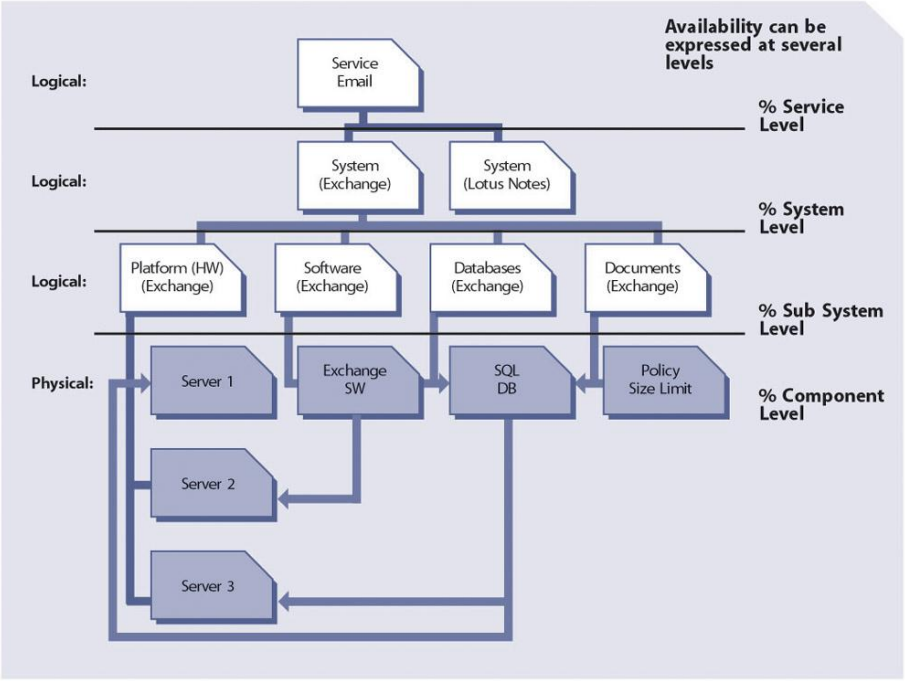
Who is the target audience of the report?

What will the report be used for?

Who is responsible for creating the report?

How will the report be created?

How frequently is the report to be created?



Industry Standards

Industry Standards

Standards exist because a widely recognized governing body, in most cases a governing body with worldwide scope, has agreed on a specific set of principles or protocols and published them for everyone to use.

Standards are usually set by committees working under various trade and international organizations.

ISO – International Standards Organization

IEC – International Electrotechnical Commission

An individual can be accredited as an ISO auditor. Organizations can be audited against an ISO standard. If the audit is passed successfully, that organization is 'ISO xxxxx Certified'.

Industry Standards

The most important standards applying to the world of ITSM are:

- **ISO/IEC 20000: 2005**
- **ISO/IEC 27001: 2005**
- **ISO/IEC 17799: 2005**
- **ISO/IEC 15504**
- **ISO/IEC 19770: 2006**

ISO/IEC 20000: 2005

ISO/IEC 20000: 2005 promotes the adoption of an integrated process approach to effectively deliver managed services to meet business and customer requirements.

ISO/IEC 20000 is based on the ITIL service management processes.

ISO/IEC 27001: 2005

ISO/IEC 27001: 2005 covers all types of organizations and specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks.

It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. It is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

ISO/IEC 17799: 2005

ISO/IEC 17799: 2005 establishes guidelines and general principles for initiating, implementing, maintaining and improving Information Security Management in an organization.

ISO/IEC 17799:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective Security Management practices, and to help build confidence in inter-organizational activities.

ISO/IEC 15504

ISO/IEC 15504 (also known as SPICE – Software Process Improvement and Capability Determination) provides a framework for the assessment of process capability.

This framework can be used by organizations involved in planning, managing, monitoring, controlling and improving the acquisition, supply, development, operation, evolution and support of products and services.

ISO/IEC 19770: 2006

ISO/IEC 19770: 2006 has been developed to enable an organization to prove that it is performing software asset management (SAM) to a standard sufficient to satisfy corporate governance requirements and ensure effective support for IT service management overall.

ISO/IEC 19770:2006 is intended to align closely to, and to support, ISO/IEC 20000.

Service Manager Responsibilities

Which of the following activities does not form part of the Service Manager's responsibilities?

a. Develop new service deployment schedules
b. Assess the ongoing cost of service delivery
c. Develop business case for new or enhanced services
d. Manage service catalog

Types of Metrics

What type of metrics need not be considered when measuring service quality?

a. Technology metrics
b. Process metrics
c. Functional metrics
d. Service metrics