# Very heavy weighting

## 7.1 Explain the following 7 ITIL practices in detail, excluding how they fit within the service value chain: x17

### a) Continual improvement (5.1.2) including: The continual improvement model (4.6, fig 4.3)

Continual improvement is the practice of **identifying and improving** services, service components, or any other element involved in the efficient and effective management of products and services to **align the organization’s practices and services** with changing business needs.

|  |  |
| --- | --- |
| What is the vision? | Business vision, mission, goals, and objectives |
| Where are we now? | Perform baseline assessments |
| Where do we want to be? | Define measurable targets |
| How do we get there? | Define the improvement plan |
| Take action. | Execute improvement actions |
| Did we get there? | Evaluate metrics and KPIs |
| How do we keep the momentum going? | connect back to the 1st step. |

### b) Change control (5.2.4)

The **purpose of the change control** practice is to **maximize** the number of **successful IT changes** by ensuring that risks

* have been properly assessed,
* authorizing changes to proceed, and
* managing a change schedule.

The scope of change control is defined by each organization. It will typically include all IT infrastructure, applications, documentation, processes, supplier relationships and anything else that might directly or indirectly impact a product or service.

It is important to distinguish change control from organizational change management. Organizational change management manages the people aspects of changes to ensure that improvements and organizational transformation initiatives are implemented successfully. Change control is usually focused on changes in products and services.

Change control must balance the need to make beneficial changes that will deliver additional value with the need to protect customers and users from the adverse effect of changes. All changes should be assessed by people who are able to understand the risks and the expected benefits and then authorized before they are deployed. This assessment, however, should not introduce unnecessary delay.

The person or group who authorizes a change is known as a **change authority**. It is essential that the correct change authority is assigned to each type of change to ensure that change control is both efficient and effective. In high velocity organizations, it is a common practice to decentralize change approval, making the peer review a top predictor of high performance.

The **change schedule** is used to help plan changes, assist in communication, avoid conflicts and assign resources. It can also be used after changes have been deployed to provide information needed for incident management, problem management and improvement planning.

Regardless of who the change authority is, they may need to communicate widely across the organization. The risk assessment activity, for instance, may require them to gather input from many people with specialist knowledge. Additionally, there is usually a need to communicate information about the change to ensure people in IT and the business are fully prepared before it is deployed.

The change control practice maximizes successful IT changes by

* confirming measurements of risk
* consenting changes to proceed (towards approval)
* using a change schedule well.

### c) Incident management (5.2.5)

The **purpose of incident management** is to reduce the undesirable impact of incidents by **restoring normal service** operations as soon as possible.

Incident management can have an enormous impact on customer and user satisfaction, and on how they perceive the service provider. Every incident should be logged and managed to ensure that it is resolved in a time that meets the expectations of the customer and user. Target resolution times are agreed, documented and communicated to ensure that expectations are realistic. Incidents are prioritized, based on agreed classification, to ensure that incidents with the highest business impact are resolved first.

Organizations should design their incident management practice to **provide appropriate management and resource allocation to different types of incidents**. Incidents with a low impact must be managed efficiently to ensure that they do not consume too many resources. Incidents with a larger impact may require more resources and more complex management. There are usually separate processes for managing major incidents, and for managing information security incidents.

**Information** about incidents **should be stored** in incident records in a suitable tool. Ideally, this tool should also provide links to related configuration items, changes, problems, known errors and other knowledge to enable quick and efficient diagnosis and recovery. Modern IT service management tools can provide automated matching of incidents to other incidents, problems or known errors, and can even provide intelligent analysis of incident data to generate recommendations for helping with future incidents.

It is important that people working on an incident provide good quality **updates in a timely fashion**. These updates should include information about symptoms, business impact, configuration items affected, actions completed, and actions planned. Each of these should have a timestamp and information about people involved, so that people involved or interested can be kept informed. There may also be a need for good collaboration tools so that people working on an incident can collaborate effectively.

Incidents may be diagnosed and resolved by people in many different groups, depending on the complexity of the issue or the incident type. All of these groups need to understand the incident management process, and how their contribution to this helps to manage the value, outcomes, costs and risks of the services provided:

* Some incidents will be resolved by the user themselves, using self-help. Use of specific self-help records should be captured for use in measurement and improvement activities.
* Some incidents will be resolved by the service desk.
* More complex incidents will usually be escalated to a support team for resolution. Typically, the routing is based on the incident category, which should help to identify the correct team.
* Incidents can be escalated to suppliers or partners, who offer support for the products and services they supply.
* The most complex incidents, and all major incidents, often require a temporary team to work together to identify the resolution. This team may include representatives of many stakeholders, including the service provider, suppliers, users etc.
* In some extreme cases, disaster recovery plans may be invoked to resolve an incident. Disaster recovery is described in the service continuity management practice (section 5.2.12).

Effective incident management often requires a **high level of collaboration** within, and between, teams. These teams may include the service desk, technical support, application support and vendors. Collaboration can facilitate information sharing and learning, as well as helping to solve the incident more efficiently and effectively.

Third party products and services that are used as components of a service require support agreements that align the obligations of the supplier with the commitments made by the service provider to customers. Management of incidents may require frequent interaction with these suppliers, and routine management of this aspect of supplier contracts is often part of the incident management practice. A supplier can also act as a service desk, logging and managing all incidents and escalating to relevant subject matter experts or other parties as required.

There should be a **formal process for logging and managing** incidents. This process does not usually include detailed procedures for how to diagnose, investigate and resolve incidents, but can provide techniques for making investigation and diagnosis more efficient. There may be **scripts** for collecting information from users during initial contact, and this may lead directly to diagnosis and resolution of simple incidents. Investigation of more complicated incidents often requires knowledge and expertise, rather than procedural steps.

### d) Problem management (5.2.8)

The purpose of problem management is to minimize the probability and impact of incidents by analyzing actual and possible causes of incidents and managing workarounds and known errors.

Every service has errors, flaws or vulnerabilities that may cause incidents. They may include errors in any of the four dimensions of service management. Many errors are identified and resolved before a service goes live. However, some remain unidentified, or unresolved, and may be a risk to live services. In ITIL, these errors are called problems and they are addressed by the problem management practice.

Problems are related to incidents, but should be distinguished as they are managed in different ways.

* **Incidents** have an impact on users or business processes, and must be resolved so that normal business activity can take place
* **Problems** are the causes of incidents. They require investigation and analysis to identify the causes, develop workarounds, and recommend longer term resolution. This reduces the number and impact of future incidents.

**Problem identification** activities identify and log problems. This includes:

* Performing trend analysis of incident records
* detection of duplicate and recurring issues by users, service desk and technical support staff
* major incident management identifying a risk that an incident could recur
* analyzing information received from suppliers and partners
* analyzing information received from internal software developers, test teams, and project teams.

Other sources of information can also lead to problems being identified.

**Problem control** activities include problem analysis, and documenting workarounds and known errors.

Problems are prioritized for analysis based on the risk that they pose, and are **managed as risks**, based on their potential impact and probability. It is not essential to analyze every problem; it is more valuable to make significant progress on the highest priority problems than to diagnose every minor problem that the organization is aware of.

Incidents typically have many interrelated causes, and the relationships between them can be complex. Problem control should consider all contributory causes, including causes that contributed to the duration and impact of incidents, as well as those that led to the incidents happening. It is important to analyze problems from the perspective of all four dimensions of service management. For example, an incident that was caused by inaccurate documentation may require not only a correction to that documentation but also training and awareness for support personnel, suppliers and users.

When a problem cannot be resolved quickly, it is often useful to find and to document a **workaround** for future incidents, based on understanding of the problem. Workarounds are documented in problem records. This can be done at any stage, it doesn’t need to wait for analysis to be complete. If a workaround has been documented early in problem control then this should be reviewed and improved after problem analysis is complete.

An effective incident workaround can become a permanent way of dealing with some problems, when resolving the problem is not viable or cost-effective. In this case, the problem remains in the known error status, and the documented workaround is applied should related incidents occur. Every documented workaround should include a clear definition of symptoms it applies to. In some cases, workaround application can be automated.

For other problems, a way to fix the error should be found. This is a part of Error control.

**Error control** activities **manage known errors**. A known error is a problem where initial analysis is complete; it usually means that faulty components have been identified.

Error control includes identification of potential permanent solutions. This may result in a change request for implementation of a solution, but only if this can be justified in terms of cost, risks and benefits.

Error control regularly re-assesses the status of known errors that have not been resolved, including overall impact on customers, availability and cost of permanent resolutions, and effectiveness of workarounds. The effectiveness of workarounds should also be evaluated each time a workaround is used. Workarounds may be improved based on the assessment.

Problem management activities are very closely related to incident management. The practices need to be designed to work together within the value chain. Activities from these two practices may complement each other (for example, identifying the causes of an incident is a problem management activity that may lead to incident resolution), but they may also conflict (for example, investigating the cause of an incident may delay actions needed to restore service).

There are also interfaces between problem management, risk management, change control, knowledge management and continual improvement.

* Problem management activities can be organized as a specific case of risk management: they aim to identify, assess and control risks in any of the four dimensions of service management. It is useful to adopt risk management tools and techniques for problem management.
* Implementation of problem resolution is often outside the scope of problem management. Problem management typically initiates resolution via change control and participates in the post implementation review, however, approving and implementing changes is out of scope for the problem management practice.
* Output from the problem management practice includes information and documentation concerning workarounds and known errors. In addition, problem management may utilize information in a knowledge management system to investigate, diagnose and resolve problems.
* Problem management activities can identify improvement opportunities in all four dimensions of service management. Problem solutions can in some cases be treated as improvement opportunities, so they are included in a continual improvement register and use continual improvement techniques to prioritize and manage them, sometimes as part of a product backlog.

Many problem management activities **rely on the knowledge and experience of staff**, rather than on following detailed procedures. People responsible for diagnosing problems often need the ability to understand complex systems, and to think about how different failures might have occurred. Developing this combination of analytic and creative ability requires mentoring and time, as well as suitable training.

### e) Service request management (5.2.16)

The purpose of the service request management practice is to provide the promised quality of a service by handling all **pre-defined, user-initiated service requests** in an effective and comprehensible manner.

Each service request may include one or more of:

* a request for a service delivery action (for example, providing a report or replacing a toner cartridge)
* a request for information (for example, how to create a document or what the hours of the office are)
* a request for provision of a resource or service (for example, providing a phone or laptop to a user, or providing a virtual server for a development team)
* a request for access to a resource or service (for example, providing access to a file or folder)
* feedback, compliments and complaints (for example, complaints about a new interface or compliments to a support team).

Fulfilment of service requests may include changes to services or their components; usually these are standard changes.

Service requests are a normal part of service delivery and are not a failure or degradation of service, which are handled as incidents. Since **service requests are pre-defined and pre-agreed** as a normal part of service delivery, they can usually be formalized, with a clear, standard procedure for initiation, approval, fulfilment and management. Some service requests have very simple workflows, such as a request for information. Others, such as the setup of a new employee, may be quite complex and require contributions from many teams and systems for fulfilment. Regardless of the complexity, the steps to fulfil the request should be well-known and proven. This allows the service provider to agree times for fulfilment and to provide clear communication of the status of the request to users.

**Some** service requests **require authorization** according to financial, information security or other policies, while others may not need any. To be handled successfully, service request management should follow these guidelines:

* Service requests and their fulfilment should be standardized and automated to the greatest degree possible.
* Policies should be established regarding what service requests will be fulfilled with limited or even no additional approvals so that fulfilment can be streamlined.
* The expectations of users regarding fulfilment times should be clearly set, based on what the organization can realistically deliver.
* Opportunities for improvement should be identified and implemented to produce faster fulfilment times and take additional advantage of automation.
* Policies and workflows should be included for the documenting and redirecting of any requests that are submitted as service requests, but which should actually be managed as incidents or changes.

Some service requests can completely be fulfilled with automation from submission to closure, allowing for a complete **self-service experience**. Examples include client software installation or provision of virtual servers.

Service request management is dependent upon well-designed processes and procedures, which are operationalized through tracking and automation tools, to maximize the efficiency of the practice. Different types of service requests will have different fulfilment workflows, but both efficiency and maintainability will be improved if a limited number of workflow models can be identified. When new service requests need to be added to the service catalogue, existing workflow models should be leveraged whenever possible.

### f) Service desk (5.2.14)

The purpose of the service desk practice is to understand demand for incident resolution and service requests, act as the point of contact for the service provider along with its users and provide a clear path for users to report issues, queries, and requests, and acknowledge, classify, own and act on them.

Service desks provide a clear path for users to report issues, queries and requests, and have them acknowledged, classified, owned and actioned. How this practice is managed and delivered may vary, from a physical team of people on shift work, to a distributed mix of people connected virtually, or automated technology and bots. The function and value remains the same, regardless of the model.

With increased automation and the gradual removal of technical debt, the **focus of the service desk is to provide support for ‘people and business’** rather than simply technical issues. Service desks are increasingly being used to get various matters arranged, explained and coordinated, rather than just to get broken technology fixed, and the service desk has become a vital part of any service operation.

A key point to be understood is that, no matter how efficient the service desk and its people are, there will always be issues that need escalation and underpinning support from other teams. Support and development teams need to work in close collaboration with the service desk to present and deliver a ‘joined up’ approach to users and customers.

The service desk may not need to be highly technical, although some are. However, even if the service desk is fairly simple, it still plays a vital role in the delivery of services and must be actively supported by its peer groups. It is also essential to understand that the service desk has a major influence on user experience and how the service provider is perceived by the users.

Another key aspect of a good service desk is its **practical understanding of the wider organization**, the business processes and the users. Service desks add value not simply through the transactional acts of, for example, incident logging, but also by understanding and acting on the business context of this action. The service desk should be the empathetic and informed link between the service provider and its users.

With increased automation, AI, robotic process automation (RPA) and chatbots, service desks are moving to provide more self-service logging and resolution directly via online portals and mobile applications. The impact on service desks is less phone contact, less low-level work and a greater ability to focus on excellent CX when personal contact is needed.

Service desks provide a variety of channels for access. These include:

* phone calls, which can include specialized technology, such as IVR, conference calls, voice recognition and others
* service portals and mobile applications, supported by service and request catalogues, and knowledge bases
* chat, through live chat and chatbots
* email can be used for logging and updating, and for follow up surveys and confirmations. Unstructured email can be difficult to process, but emerging technologies based on AI and machine learning are starting to address this
* walk-in service desks are becoming more prevalent in some sectors, e.g. higher education, where there are high peaks of activity that demand physical presence
* text and social media messaging, which are useful for notifications in case of major incidents and for contacting specific stakeholder groups but can also be used to allow users to request support.
* public and corporate social media and discussion forums for contacting the service provider and for peer-to-peer support

Some service desks have a limited support window where service cover is available, for instance 08.00 – 20.00, Monday – Friday. Staff are therefore expected to work in shift patterns to provide consistent support levels.

In some cases, the service desk is a tangible team, working in a single location. A centralized service desk requires supporting technologies, such as:

* intelligent telephony systems, incorporating computer-telephony integration, interactive voice response and automatic call distribution.
* workflow systems for routing and escalation
* workforce management and resource planning systems
* knowledge base
* call recording and quality control
* remote access tools
* dashboard and monitoring tools
* configuration management systems.

In other cases, a virtual service desk allows agents to work from multiple geographically dispersed locations. A virtual service desk requires more sophisticated supporting technology, allowing access from multiple locations and more complex routing and escalation. These solutions are often cloud-based.

Service desk staff require training and competency across a number of broad technical and business areas. In particular, they need to demonstrate excellent customer service skills such as empathy, incident analysis and prioritization, effective communications, and emotional intelligence. The key skill they require is to be able to fully understand and diagnose a specific incident in terms of business priority and to take appropriate action to get this resolved, using available skills, knowledge, people and processes.

### g) Service level management (5.2.15 – 5.2.15.1)

The purpose of the service level management practice is to **set clear business-based targets** for service performance, so that the delivery of a **service can be properly assessed, monitored and managed** against these targets.

This practice involves the definition, documentation, and active management of service levels. As services may involve a ‘bundle’ of varied and disparate activities, this means that a number of these activities need to be combined and aggregated together, to reflect a realistic view.

Service level management provides the end to end visibility of the organization’s services. To achieve this, service level management:

* Establishes a shared view of the services and target service levels with customers
* Ensures the organization meets the defined service levels through the collection, analysis, storage and reporting of the relevant metrics for the identified services
* Performs service reviews to ensure the current set of services continues to meet the needs of the organization and its customers
* Captures and reports on service issues including performance against defined service levels.

The skills and competencies for service level management include relationship management, business liaison, business analysis and commercial/supplier management.

The practice requires pragmatic focus on the whole service and not simply its constituent parts, so for example, simple individual metrics (such as % system availability) should not be taken to represent a whole service.

Service level agreements

Service level agreements (SLAs) have long been used as **a tool to measure the performance of services from the customer’s point of view**. It is important that they are agreed in a wider business context. Using SLAs may present many challenges, and often they do not fully reflect wider service performance and the user experience.

Some of the key requirements for successful SLAs include:

* They must be related to a defined ‘service’ in the service catalogue. Otherwise they are simply individual metrics without a purpose, that do not provide adequate visibility or reflect the service perspective
* They should relate to **defined outcomes** and not simply operational metrics. This can be achieved with balanced ‘bundles’ of metrics, such as customer satisfaction and key business outcomes.
* They should reflect an ‘agreement’, that is, engagement and discussion between the service provider and the service consumer. It is important to involve all stakeholders including partners, sponsors, users and customers.
* They must be simply written and easy to understand and use for all parties.

In many cases, using single system-based metrics as targets can result in mis-alignment and a disconnect between service partners as to the success of the service delivery and the user experience. For example, if an SLA is only based on the percentage of uptime of a service, it can be deemed to be successful by the provider, yet still miss out on important business functionality and outcomes which are important to the consumer. This is referred to as the ‘watermelon SLA’ effect.

Service level management identifies metrics and measures that are a truthful reflection of the customer’s actual experience and level of satisfaction with the whole service. This will vary across organizations and the only way to learn what these are is to find out directly from customers.

Service level management requires focus and effort to engage and listen to the requirements, issues, concerns and daily needs of customers:

* **Engagement** is needed to understand and confirm the actual ongoing needs and requirements from customers, not simply what is interpreted by the service provider or has been agreed several years before.
* Listening is important as a relationship building and trust-building activity, to show customers that they are valued and understood. This helps to move the provider away from always being in ‘solution mode’ and to build new more constructive partnerships.

This work is a great opportunity to build improved relationships and to focus on what really needs to be delivered. It also gives service delivery staff an experience-based understanding of the day-to-day work that is done with their technology, enabling them to deliver a more business focused service.

Service level management involves collating and analyzing information from several sources. These sources include:

* **Customer engagement** This involves initial listening, discovery and information capture on which to base metrics, measurement and ongoing progress discussions. Consider asking customers some simple open questions such as:
  + What does your work involve?
  + How does technology help you?
  + What are your key business times, areas, people and activities?
  + What differentiates a good day from a bad day for you?
  + Which of these activities is most important to you?
  + What are your goals, objectives, and measurements for this year?
  + What is the best measure of your success?
  + How do you base your opinion and evaluation of a service, or IT/technology?
  + How can we help you more?
* **Customer feedback** This is ideally gathered from several sources, both formal and informal, including:
  + **Surveys:** Both event-based, from immediate feedback such as follow up questions to specific incidents, and from more reflective periodic surveys that gauge feedback on the overall service experience.
  + **Key business-related measures**: These are measures agreed between the service provider and their customer, based on what the customer values as important. This could be a bundle of SLA metrics, or a very specific business activity such as a sales transaction, project completion or operational function like getting an ambulance to the site of an accident within x minutes.
* **Operational metrics** These are the low-level indicators of various operational activities and may include system availability, incident response and fix times, change and request processing times and system response times.
* **Business metrics** These can be any business activity that is deemed useful or valuable by the customer and used as a means of gauging the success of the service. This can vary from some simple transactional binary measures such as ATM or POS terminal availability during business hours (09:00 – 17:00 daily) or successful completion of business activities, for instance, passenger check-in.

Once this feedback is gathered and collated for ongoing review, it can be used as input to design suitable measurement and reporting models and practices.

# Medium weighting

## 2.2 Explain the use of the guiding principles (4.3): x5

### a) Focus on value (4.3.1 – 4.3.1.4)

This principle aims at creating value for service consumers. To achieve this value, organizations need to tie back the different activities (directly or indirectly) that they do in a logical way.

### b) Start where you are (4.3.2 – 4.3.2.3)

This principle focuses on considering what is already available instead of starting from scratch (or reusability). To achieve this, analyzing the existing state is essential to identify what can be helpful in creating new value.

### c) Progress iteratively with feedback (4.3.3 – 4.3.3.3)

This principle focuses on avoiding doing everything in one batch and gathering the timely feedback. To achieve this, breaking down the work into smaller, manageable components is essential to iteratively accomplish the initiative.

### d) Collaborate and promote visibility (4.3.4 – 4.3.4.4)

This principle focuses on removing silos and building trust. To achieve this, the people of an organization need to work together and share information to the greatest degree possible.

### e) Think and work holistically (4.3.5 – 4.3.5.1)

This principle focuses on working in an integrated way. To achieve this, the various activities of an organization should focus on the delivery of value.

### f) Keep it simple and practical (4.3.6 – 4.3.6.3)

This principle focuses on simplifying the complex work methods. To achieve this, identify and eliminate processes, services, actions, or metrics that do not add any value to the outcome.

### g) Optimize and automate (4.3.7 – 4.3.7.3)

This principle focuses on optimizing the work carried out by its human and technical resources. To achieve this, organizations should automate work to the possible extent that requires minimal human intervention.

## 6.1 Recall the purpose of the following ITIL practices: x5

### Top 7 (x17) – see 7.1

#### i) Continual improvement (5.1.2)

#### j) Change control (5.2.4)

#### k) Incident management (5.2.5)

#### l) Problem management (5.2.8)

#### m) Service request management (5.2.16)

#### n) Service desk (5.2.14)

#### o) Service level management (5.2.15)

### Bottom 8 (x5)

#### a) Information security management (5.1.3)

The purpose of ISM is to

* safeguard information used to run business
* understand and manage risk based on CIA principles
* maintain authentication and non-repudiation

#### b) Relationship management (5.1.9)

The purpose of RM is to

* create and improve communication between the organization and the stakeholders
* identify, analyze and monitor those relationships.

#### c) Supplier management (5.1.13)

The purpose of SM is to

* manage suppliers and their performance
* improve relationships with key suppliers
* find and get new value
* reduce risk of failure

#### d) IT asset management (5.2.6)

Plans and manages the lifecycle of all assets to maximize value, control cost, deal with risk, make purchase decisions, and meet requirements.

#### e) Monitoring and event management (5.2.7)

The purpose of monitoring and event management is to

* analyze service components
* record and report changes (generate events)
* prioritize infrastructure, services, business processes, and information security events

#### f) Release management (5.2.9)

Release management practice makes new and changed services and features available for use.

#### g) Service configuration management (5.2.11)

SCM practice ensures that

* Cis and service configuration is accurate, reliable, and available
* Cis are documented
* Cis have information on interactions, relationships, and dependencies when value is important.

#### h) Deployment management (5.3.1)

The purpose of deployment management is to **move new or changed** hardware, software, documentation, processes, or any other component **to** **live environments**. It may also be involved in deploying components to other environments for **testing or staging**.

# Light weighting

## 1.1 Recall the definition of: (2.0, 2.2.2, 2.3.1, 2.5.4) x2

### a) Service

service – a means of enabling value co-creation by facilitating outcomes that customers want to achieve, without the customer having to manage specific costs and risks.

### b) Utility

utility – the **functionality** offered by a product or service to meet a particular need

What it does. Fit for purpose. Must support performance or remove constraints.

### c) Warranty

warranty – the **assurance** that a product or service will meet agreed requirements

How it performs. Fit for use. Defined and agreed conditions. Typically, availability, capacity, service levels, and continuity.

### d) Customer

customer – a person who defines the requirements for a service and takes responsibility for the outcomes of service consumption.

### e) User

user – a person who uses services

### f) Service management

Service management – a **set of specialized organizational capabilities** for enabling value to customer in the form of services

### g) Sponsor

sponsor – a person who authorizes budget for **service consumption**

## 1.2 Describe the key concepts of creating value with services: x2

2.1, 2.1.1, 2.2 and all subsections of 2.5

### a) Cost

cost – the amount of money spent on a specific activity or resource

Two types – those removed by the service (value proposition) and those imposed on the consumer

### b) Value

value – the perceived benefits, usefulness, and importance of something.

### c) Organization

organization – a person or group of people that has its own functions with responsibilities, authorities and relationships to achieve objectives.

### d) Outcome

outcome – a **result** for a stakeholder **enabled by one or more outputs**

outcome-based thinking – producing practical solutions that deliver valuable outcomes. The thinking focuses on eliminating processes, services, actions, or metrics, that do not contribute to adding any value to the outcome.

### e) Output

output – a tangible or intangible **deliverable** of an activity

### f) Risk

risk – a possible event that could harm or loss, or make it more difficult to achieve objectives

Two types – those removed by the service (value proposition) and those imposed on the consumer

### g) Utility

utility – the **functionality** offered by a product or service to meet a particular need

What it does. Fit for purpose. Must support performance or remove constraints.

### h) Warranty

warranty – the **assurance** that a product or service will meet agreed requirements

How it performs. Fit for use. Defined and agreed conditions. Typically, availability, capacity, service levels, and continuity.

## 3.1 Describe the four dimensions of service management (3): x2

### a) Organizations and people (3.1)

Characteristics for organizational effectiveness for providing a service:

* **well-defined organizational structure** – reporting lines, roles and responsibilities, systems of authority (line, staff, functional), communication model
* **healthy organizational culture** – vision, values, norms, systems, symbols, language, assumptions, beliefs, habits
* **common organizational objective** – must be understood as their contribution to creating value
* **up-to-date organizational skills and competencies** – management and leadership styles (motivation), communication and collaboration model (transparency), skilled people

### b) Information and technology (3.2)

* Information management – define the info
* information exchange – define availability, reliability, accessibility, timeliness, information accuracy, and exchange. Architecture.
* challenges – protection, management, archiving, disposal – security and regulatory compliance

### c) Partners and suppliers (3.3)

Organizational relationships

* goods supply
* service delivery
* service partnership

**SIAM** – Service Integration and Management – an integration middleman who manages with the process

**Factors affecting supplier strategy** – external constraints, subject matter expertise, demand patterns, strategic focus, cost concerns, corporate culture, and resource scarcity.

### d) Value streams and processes (3.4-3.4.2)

value stream – a **series of steps** than an organization takes to **create and deliver products and services** to a consumer.

process – a set of interrelated or interacting **activities that transform inputs into outputs**. They define the sequence of actions and their dependencies and takes one or more defined inputs and turns them into defined outputs.

Value chain = complete map/restaurant layout, value stream = one journey/menu item outcome, process = recipe. [Doug]

Characteristics of value streams – improved performance, better understanding, increased productivity, continual improvement

Every service provider designs and executes value streams that start with demand and end with value co-creation. While there is only one service value chain, each organization may have many different value streams; they might be simple straight-line journeys through the value chain, or they may loop around the value chain in multiple iterations with feedback.

Practices describe something the service provider can do from the perspective of all four dimensions of service management. They are not just about process activities, they also describe the required organization and people, information and technology, and suppliers and partners.

Many practices contribute to each value stream and every practice can contribute to many value streams. Excellent service management combines appropriate practices in the value streams to enable value co-creation. For example, to modify a service, a value stream may include combinations from:

* relationship management to understand the needs and expectations of =customers and other stakeholders
* service financial management to analyze the costs
* risk management to understand the associated risks
* portfolio management to review costs, benefits, risks, and alignment with the strategy, and to decide whether to process
* business analysis to create detailed requirements for the modified service
* service design to design the modified service
* software development and management to create new software features required
* infrastructure and platform management to provide supporting infrastructure
* service validation and testing to ensure that all the new or changed components work together as expected to enable the required value creation
* change enablement to ensure that the service changes happen as and when required
* deployment management to move the new and change components to the live environment
* release management to make the new or changed features available to the users
* continual improvement to ensure that lessons are learned and feedback is incorporated into future work

Other practices may also contribute to this value steam depending on the service being modified and how the organization works. This includes project management, organizational change management, architecture management, service level management, and other practices.

Please not that the involvement of different practices does not imply increasing the number of people and handoffs involved in doing the work. It is quite possible for one person, or a small team, to carry out most or all of the work, using ideas from practices as required.

## 1.3 Describe the key concepts of service relationships: (2.3.2, 2.4, 2.4.1) x1

### a) Service offering

service offering – a description of one or more services, designed to address the needs of a target consumer group. It may include goods, access to resources, and service actions.

### b) Service relationship management

Service relationship management – joint activities performed by a service provider and a service consumer to ensure continual value co-creation based on agreed and available service offerings.

A service relationship.

### c) Service provision

service provision – activities performed by a service provider to provide services

A service relationship.

### d) Service consumption

Service consumption – activities performed by a service consumer to consume services

A service relationship.

## 2.1 Describe the nature, use and interaction of the guiding principles (4.3, 4.3.8 ) x1

## 4.1 Describe the ITIL service value system (4.1) x1

service value system – an explanation of how the components and activities of the organization work together as a system to enable value creation.

The Service Value System is an organizational scope business model based on a **backbone of the service value chain**, triggered by **demand**/opportunity (potential demand), aided by **inputs**, resulting in **value** physically represented by **outputs**. The chain is controlled by **governance** and **practices** and aided through **guiding principles** and **continual improvement**.

## 5.1 Describe the interconnected nature of the service value chain and how this supports value streams (4.5) x1

service value chain – an operating model that defines the **key activities** required to **respond to demand and enable value creation** through the formation and management of **products and services**.

The Service Value Chain is the backbone of the SVS triggered by demand and resulting in value.

## 5.2 Describe the purpose of each value chain activity (4.5.1-4.5.6) : x1

### Generic

#### a) Plan

The plan activity is strategic and ensures a **shared vision and status** for all dimensions, products, and services.

#### b) Improve

The improve activity is about continuous improvement.

### Specific / iterative

#### c) Engage

The engage activity is requirements oriented and provides an **understanding of the stakeholder’s needs**, transparency, and maintaining good **communication**.

#### d) Design & transition

The design and transition activity **ties products and services back to stakeholder expectations** for quality, costs, and time-to-market.

#### e) Obtain/build

The obtain and build activity **ensures components are available when and where needed** and will meet the requirements.

#### f) Deliver & support

The deliver and support activity ensures delivery and support supporting all requirements.

## 6.2 Recall definitions of the following ITIL terms: (5.2.4, 5.2.5, 5.2.6, 5.2.7, 5.2.8, 5.2.11) x2

### a) IT asset

IT asset – any **valuable component** that can contribute to delivery of an IT product or service

### b) Event

event – any change of state that has significance for the management of a configuration item or IT service. Events are typically recognized through notifications created by an IT service, CI, or monitoring tool.

### c) Configuration item

configuration item – any **component that needs to be managed** in order to deliver an IT service

### d) Change

change - an **addition, deletion, or modification** of anything that could have a direct or indirect effect on services.

### e) Incident

incident – an **unplanned interruption** to a service, or reduction in the quality of a service

### f) Problem

problem – a **cause, or potential cause**, or one or ore incidents

### g) Known error

known error – a **problem** that has been **analyzed** and has **not been resolved**