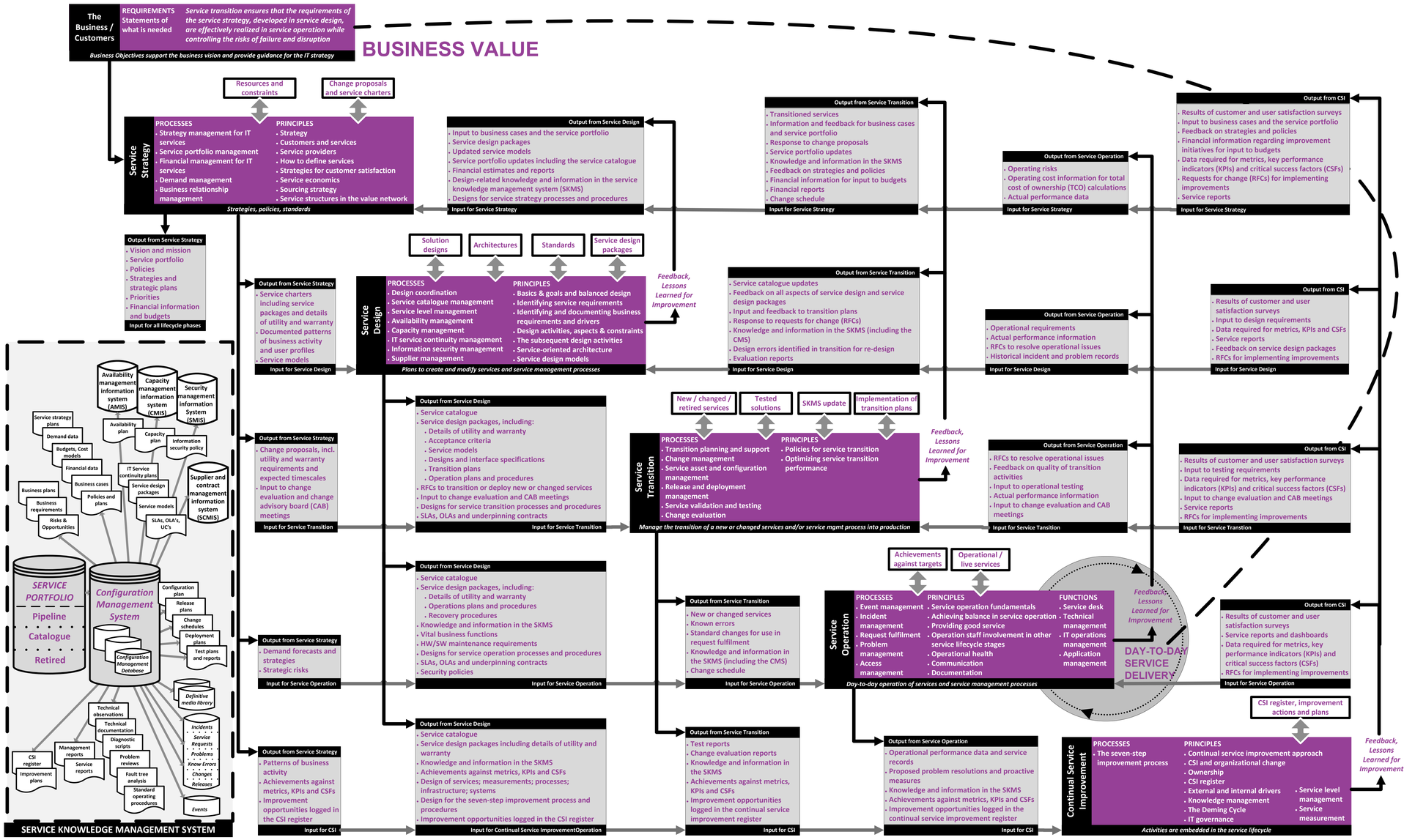
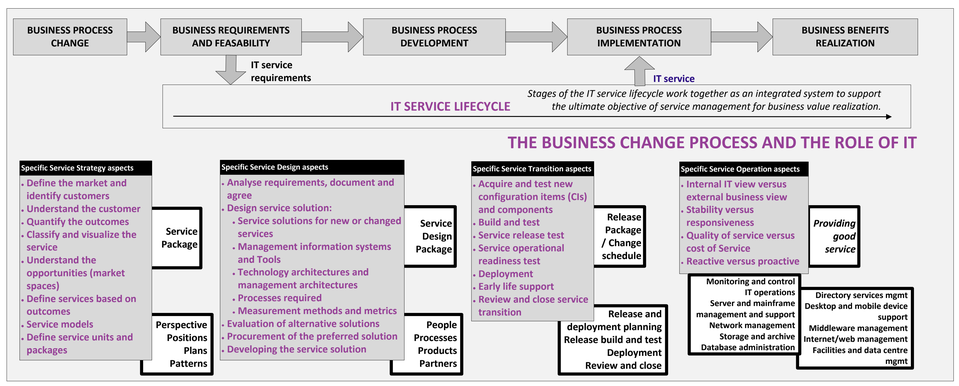
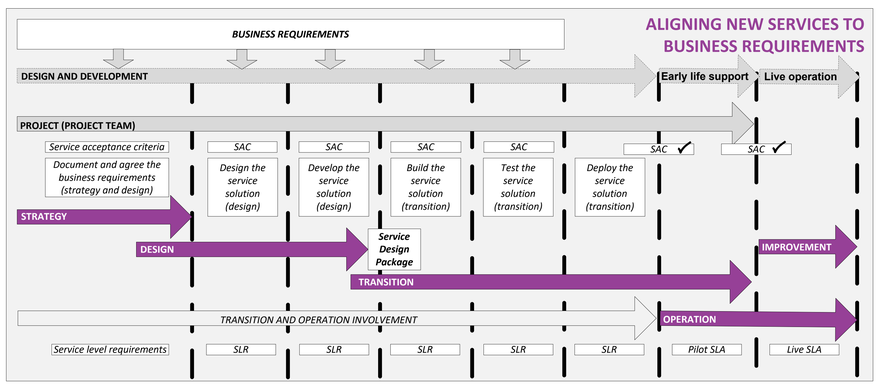
Detailed ITIL® (2011 Edition)
Overall View as a Checklist

Kinkelenburg 18
7339 DL Ugchelen (Apeldoorn)
T: +31 6 47 388 141 **E**: info@m-c-s.nu
I: www.m-c-s.nu







SERVICE STRATEGY

- **Strategy management for IT services**
  Defining and maintaining an organization's perspective, position, plans and patterns with regard to its services and the management of those services.
  Purpose: articulate how a service provider will enable an organization to achieve its business outcomes.
- **Service portfolio management**
  Responsible for managing the service portfolio; the description of a provider's services in terms of business value.
  Purpose: ensure that the service provider has the right mix of services to balance the investment in IT with the ability to meet business outcomes.
- **Financial management for IT services**
  Enables the organization to manage its resources, and to ensure that these resources are being used to achieve the organization's objectives.
  Purpose: secure the appropriate level of funding to design, develop and deliver services that meet the strategy of the organization.
- **Demand management**
  Seeks to understand, anticipate and influence customer demand for services and the provision of capacity to meet these demands.
  Purpose: understand, anticipate and influence customer demand for services and work with capacity management to ensure the service provider has capacity to meet this demand.
- **Business relationship management**
  Enables to provide links between the service provider and customers at the strategic and tactical levels.
  Purpose: establish and maintain a business relationship between the service provider and the customer and identify customer needs and ensure that the service provider is able to meet these needs as business needs change over time and between circumstances.

SERVICE DESIGN

- **Design coordination**
  Through well coordinated activities a service provider creates designs that will support the achievement of the required business outcomes.
  Purpose: ensure that the goals and objectives of the service design stage are met by providing and maintaining a single point of coordination and control for all activities and processes within this stage of the service lifecycle.
- **Service catalogue management**
  Provide the means of devoting that care and attention in a consistent fashion, ensuring that the organization accrues all of the potential benefits of a service catalogue in the most efficient manner possible.
  Purpose: provide and maintain a single source of consistent information on all operational services and those being prepared to be run operationally, and to ensure that it is widely available to those who are authorized to access it.
- **Service level management**
  Responsible for agreeing and documenting service level targets and responsibilities within service level agreements and service level requirements for every service and related activity within IT.
  Purpose: ensure that all current and planned IT services are delivered to agreed achievable targets.
- **Availability management**
  Availability is one of the most critical parts of the warranty of a service. If a service does not deliver the levels of availability required, then the business will not experience the value that has been promised. Without availability the utility of the service cannot be accessed.
  Purpose: ensure that the level of availability delivered in all IT services meets the agreed availability needs and/or service level targets in a cost-effective and timely manner.
- **Capacity management**
  Provides a point of focus and management for all capacity- and performance-related issues, relating to both services and resources. Like availability, capacity is an important part of the warranty of a service.
  Purpose: ensure that the capacity of IT services and the IT infrastructure meets the agreed capacity and performance-related requirements in a cost-effective and timely manner.
- **IT service continuity management**
  Service continuity is an essential part of the warranty of a service. If a service's continuity cannot be maintained and/or restored in accordance with the requirements of the business, then the business will not experience the value that has been promised. Without continuity the utility of the service cannot be accessed.
  Purpose: support the overall business continuity management process by ensuring that, by managing the risks that could seriously affect IT services, the IT service provider can always provide minimum agreed business continuity-related service levels.
- **Information security management**
  Part of the corporate governance framework, which provides the strategic direction for security activities and ensures objectives are achieved. It ensures that the information security risks are appropriately managed and that enterprise information resources are used responsibly
  Purpose: align IT security with business security and ensure that the confidentiality, integrity and availability of the organization's assets, information, data and IT services always matches the agreed needs of the business.
- **Supplier management**
  Ensures that suppliers and the services they provide are managed to support IT service targets and business expectations.
  Purpose: obtain value for money from suppliers and to provide seamless quality of IT service to the business by ensuring that all contracts and agreements with suppliers support the needs of the business and that all suppliers meet their contractual commitments.

SERVICE TRANSITION

- **Transition planning and support**
  Provide overall planning for service transitions and coordinate the resources that they require.
- **Change management**
  Control the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.
- **Service asset and configuration Management**
  Ensure that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed.
- **Release and deployment management**
  Plan, schedule and control the build, test and deployment of releases, and to deliver new functionality required by the business while protecting the integrity of existing services.
- **Service validation and testing**
  Ensure that a new or changed IT service matches its design specification and will meet the needs of the business.
- **Change evaluation**
  Provide a consistent and standardized means of determining the performance of a service change in the context of likely impacts on business outcomes, and on existing and proposed services and IT infrastructure.
- **Knowledge management**
  Share perspectives, ideas, experience and information; to ensure that these are available in the right place at the right time to enable informed decisions; and to improve efficiency by reducing the need to rediscover knowledge.

SERVICE OPERATION

- **Event management**
  Manage events throughout their lifecycle. Detect events, make sense of them and determine the appropriate control action. It is the basis for operational monitoring and control. An 'event' can be defined as any change of state that has significance for the management of a configuration item (CI) or IT service. Events are typically recognized through notifications created by an IT service, CI or monitoring tool.
- **Incident management**
  Restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that agreed levels of service quality are maintained. An 'incident' is defined as an unplanned interruption to an IT service or reduction in the quality of an IT service or a failure of a CI that has not yet impacted an IT service.
- **Request fulfilment**
  Responsible for managing the lifecycle of all service requests from the users. The term 'service request' is used as a generic description for many different types of demands that are placed upon the IT organization by the users.
- **Problem management**
  Manage the lifecycle of all problems from first identification through further investigation, documentation and eventual removal. Responsible for managing the lifecycle of all problems. A 'problem' is defined as the underlying cause of one or more incidents.
- **Access management**
  Provide the right for users to be able to use a service or group of services. It is therefore the execution of policies and actions defined in information security management. Granting authorized users the right to use a service, while preventing access to non-authorized users. It has also been referred to as rights management or identity management in different organizations.
- **Service desk function**
  A service desk is a functional unit made up of a dedicated number of staff responsible for dealing with a variety of service activities, usually made via telephone calls, web interface, or automatically reported infrastructure events.
- **Technical management function**
  Refers to the groups, departments or teams that provide technical expertise and overall management of the IT infrastructure. It is the custodian of technical knowledge and expertise related to managing the IT infrastructure and it provides the actual resources to support the service lifecycle.
- **IT operations management function**
  The department, group or team of people responsible for performing the organization's day-to-day operational activities.
- **Application management**
  Refers tot the department, group or team involved in managing and supporting operational Applications. Responsible for managing applications throughout their lifecycle. It covers the entire ongoing lifecycle of an application, including requirements, design, build, deploy, operate and optimize.

CONTINUAL SERVICE IMPROVEMENT

- **The seven-step improvement process**
  Define and manage the steps needed to identify, define, gather, process, analyse, present and implement improvements.
  Fundamental to CSI is the concept of measurement.
  There is an interaction with the Plan-Do-Check-Act (PDCA) cycle and the Data-to-Information-to-Knowledge-to-Wisdom (DIKW) structure of knowledge management.