Everyday IT Service Management

Partially sourced from ITIL version 2, ITIL version 3 and ITIL ® 4 material

Course objectives

After the course you will

- Have learned about IT Service Management processes and activities and corresponding management roles
- Have learned most everyday IT Service Management terminology
- Have learned about the relations to LEAN, Agile and Devops
- Have insight in the Service Integration and Management (SIAM) model challenges

Agenda and curriculum

Introduction	
- Configuration Management	- Service Level Management
- Service Desk	- Capacity Management
- Incident Management	- Availability Management
- Problem Management	- IT Service Continuity Management
- Knowledge Management	- Information Security Management
- Change Management	- Agile, LEAN, Devops
- Release and deployment Management	-Tools
- Event Management	- Service Integration and Management – SIAM
- Request fulfillment	

About ITIL®

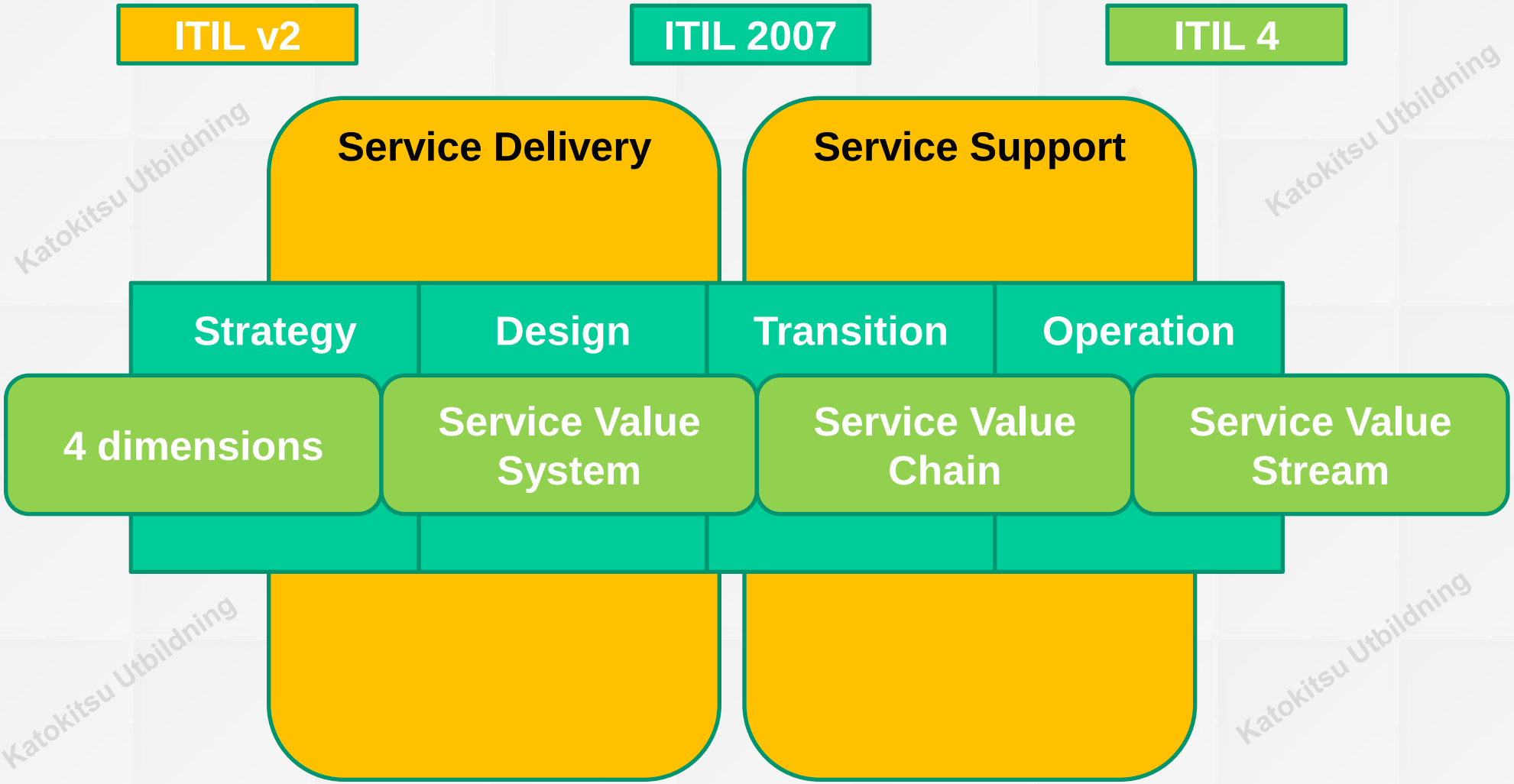
ITIL

It is a guidance for creating value for the IT services consumers.

Used to mean IT Infrastructure Library, today only a trademark

ITIL	Developed by Office of Government Commerce, OGC
ITIL v2	Focused on Service Delivery and Support through defined processes
ITIL 2007 (v3)	Introduces the service lifecycle concept
ITIL 2011	Update of ITIL 2007
ITIL 4	Focusing on value creation through Service Value System and Service Value Chains

About ITIL®



Service Management?

Service Management

- Processes, practices, standardization
- Roles, interfaces, measurements, planning and improving
- Terminology
- Supported by tools

Service Management:
ITIL v2: Is the delivery of customer-focused IT Services, by using a process-oriented approach/method
ITIL v3: A set of specialized organizational capabilities for enabling value for customers in the form of services.
ITIL 4 : IT service management (ITSM) is a concept that enables an organization to maximize business value from the use of information technology.

Service Management

The purpose of services is to help the custoemr achieve its desired outcome.

Everyday Service Management

- Covers the processes and practices associated with the day-to-day delivery, support and maintenance activities for the provision of IT Services.

Service Management

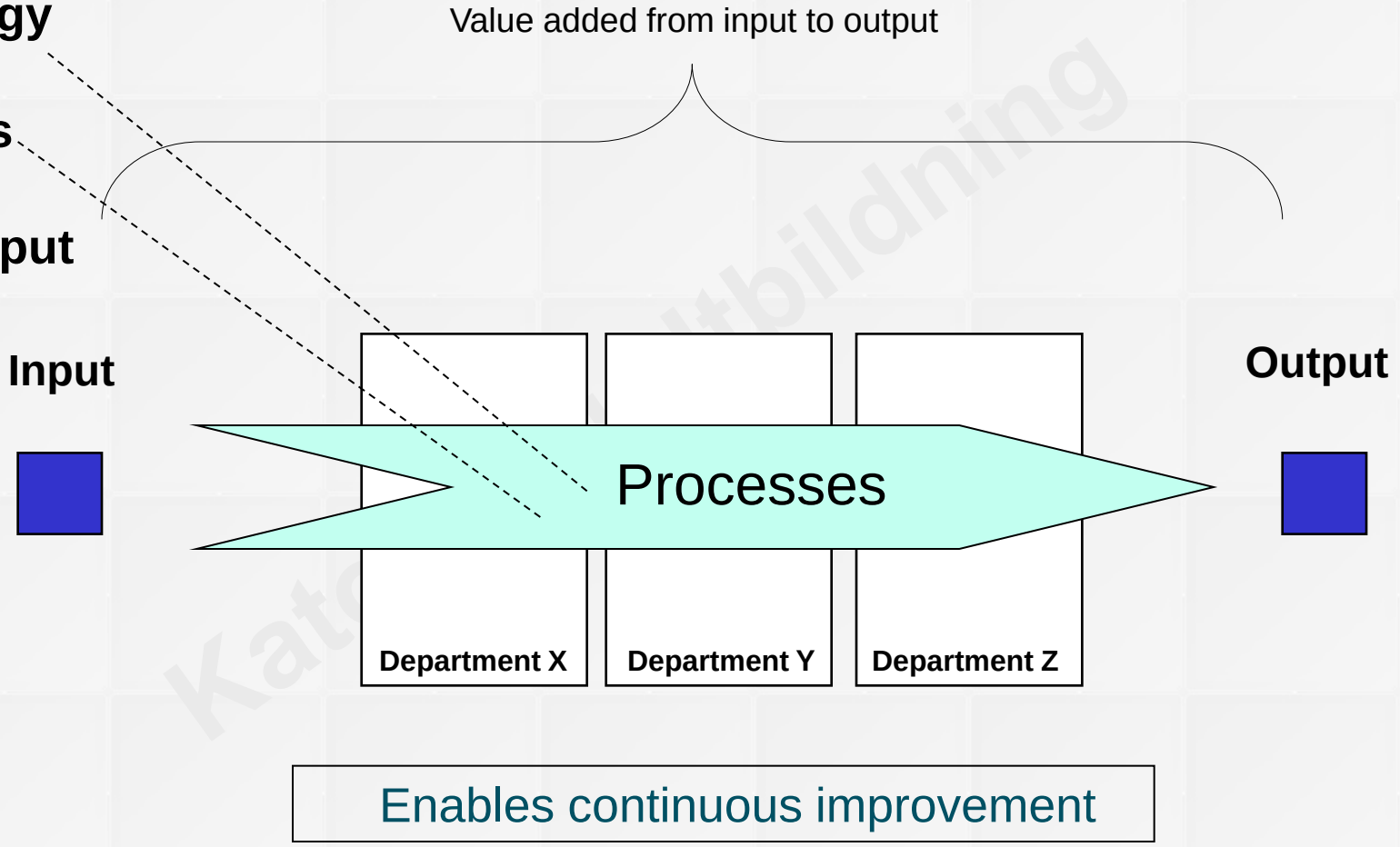
Not covered by this course

Service Strategy, Design, Improvement

- Including Service Portfolio, Finances, Business / Service Relationship Management, Demand Management
- Including planning and designing the services according to the requirements, including Capacity planning, Availability Planning, Information Security Planning, Process and measurements development, UAT planning, project management

Processes thinking

- Objective
- Terminology
- Roles
- Resources
- Rules
- Input / output
- Actions



Enables continuous improvement

Process benefits

- It allows the organization to define its preferred approach to managing the task
- The task will be carried out consistently
- It avoids staff wasting time recreating an approach each time the task is carried out
- New staff can be quickly trained to carry out a process
- It can be measured and assessed
- It can be used as a baseline for improvement

Major challenges in process thinking

- It is seldom that a process goes from input to output uninterrupted by some other process
- Processes can get input from other processes at any stage, not only at the process beginning
- Process inputs are seldom complete at the start
- Processes are not applicable for every scenario as described
- There can be additional activities that are not described in the process documentation
- Processes need to be redefined for Agile, Devops working method
- Processes need to be augmented in a SIAM environment (multiple service providers)

Terminology

Process
A connected series of activities performed with the intent of satisfying a purpose or achieving a goal

Procedure
A set of specific steps that describe how an activity should be carried out and by whom. Can be supported by work instructions

Process owner
Responsible for ensuring the suitability of a process, include sponsorship, design, operation and quality assurance

Process Manager
Responsible for the execution of a process, operation of the defined and agreed process ensuring interfaces, target setting, process audits and managing improvement

Terminology

IT Service
One or more IT systems which enable a business process

IT Infrastructure
All of the components that are needed to deliver IT Services to customers. The IT Infrastructure consists of more than just hardware and software

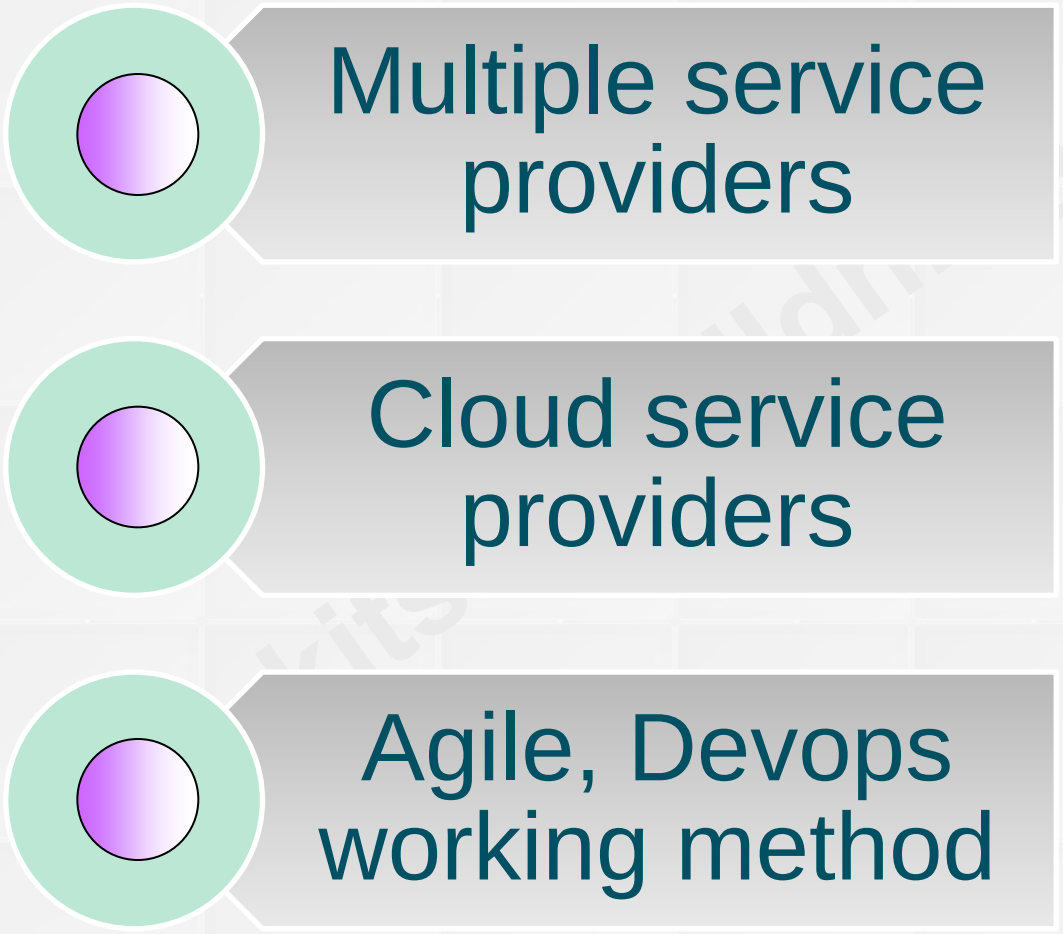
Customer
A business manager authorised to define requirements on service delivery and support

User / Service consumer
The person who uses the services on a day-to-day basis

Triage
focuses on identifying the most urgent work so it can be dealt with first. Low priority work has to wait until high and medium priority work has been completed.

Swarming
Swarming is an alternative to tiered support (1st, 2nd, 3rd line etc.). Swarming creates a single collaborative team who 'swarm' around a piece of work allowing them to share knowledge and identify fast solutions.

Major challenges in Service Management



Value

Definition:

The perceived benefits, usefulness and importance of something.

- Service provision may affect outcomes, introduce costs and risks. In the same time, they support outcomes, remove costs and removes risks. *If the latter is perceived more than the former, then value is created.*

- Output and outcome:

The output is the service (or product) provided. The outcome is what the users achieve with the output.

Value co-creation

Active collaboration between service providers and service consumers

- Delivering extra capacity and availability is not necessarily a value the consumers appreciate
- Delivering services that are not needed is not a value the consumers appreciate

Focus on value

Focus on value

- Who is the service consumer
- What the services help them to do - what are the consumer's needs
- The risks involved for the service consumer
- All improvement work should deliver measurable value for customers and other stakeholders

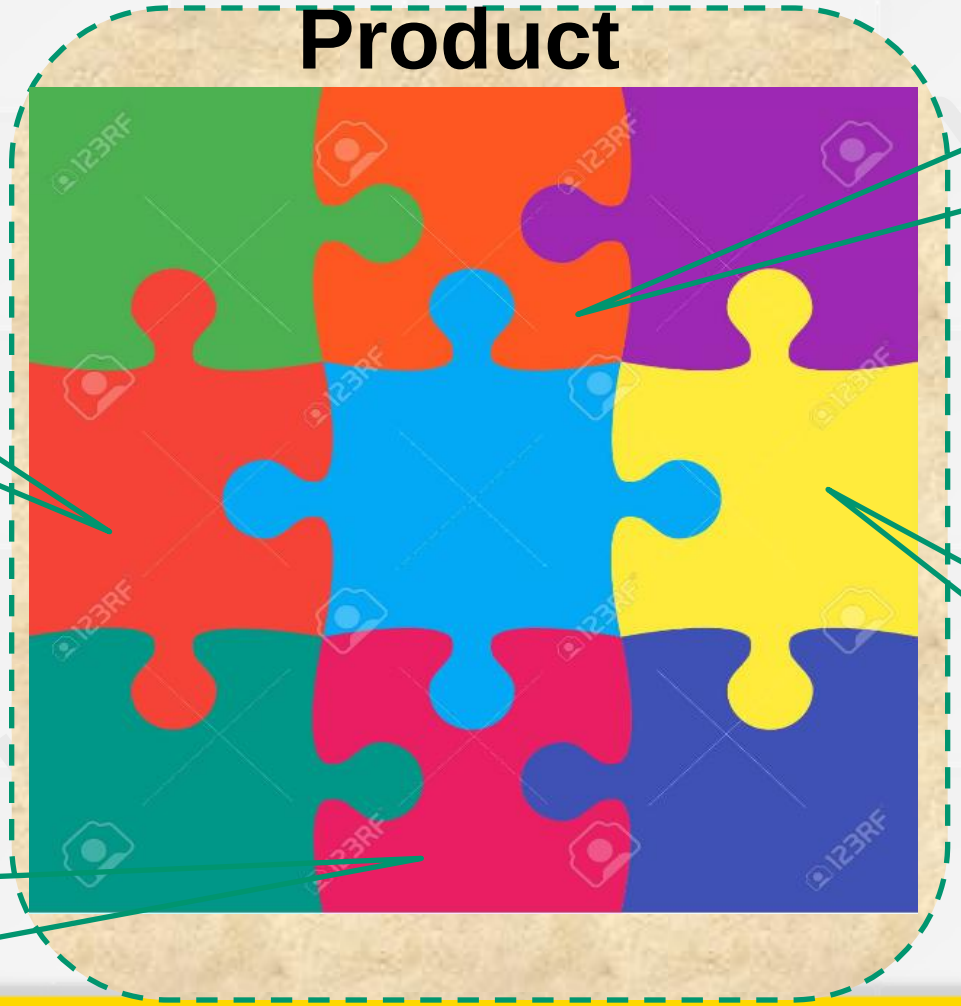
Value can be increased productivity, reduced negative impact, reduced costs, the ability to pursue new markets, better competitive position

Focus on value - outputs

“Outputs are a measure of what your function or organization produced. Output measures are necessary for a function to understand its efficiency, effectiveness and quality; however, it does not measure the value or impact that your services provide for your customers/consumers.

Most process metrics are outputs, as they are one component needed to provide the value that the customer expects. It is the combined outputs of all the processes and activities that create the outcomes.”

Products = configuration of resources



Resource: Organizations and people

Resource: Information and technology

Resource: Partners and suppliers

Resource: Value streams and processes

Keep it simple and practical

Keep it simple and practical

- Do fewer things, but do them better
  - include only activities with value for one or more stakeholders – will allow focus on the quality
- The organization should use the minimum number of steps, and eliminate steps that produce no useful outcome
- A process that is too complicated can be a waste of time
- Easier to understand, more likely to adopt

Easier to achieve quick wins.

Value streams

Value stream:

A series of steps an organization undertakes to create and deliver products and services to consumers.

Value streams should be defined by organizations for *each of their services and products.*

Value streams help the organization to identify wasteful activities and remove obstacles that hinder the organization's productivity (LEAN)

Processes and activities

Configuration Management

Configuration mgt purpose

- To ensure that accurate and reliable information about the configuration of services, and the CIs (configuration items) that support them, is available when and where it is needed.
- Includes information on how CIs are configured and the relationships between them.

Configuration management is a number of activities. Some of these activities are carried out while architecting the solution and others are everyday activities during IT operations.

Configuration Management

Objective (how do we achieve the purpose):

To provide a logical model of the IT Infrastructure by identifying, controlling, maintaining and verifying the versions of all Configuration Items in existence.

Also:

The control of changes that are made to the hardware, software, firmware, and documentation throughout the systems / services life-cycle.

Terminology

Configuration Item (CI)

– *Any component of an IT Infrastructure which is under the control of Configuration Management and therefore subject to formal change control*

Example: Services, Environment, HW/ SW, Relationships, Baseline Models, Documentation (*Procedures, Processes, Contracts, Manuals)*

Configuration Management Database (CMDB)

– *A database that contains all relevant details of each CI and details of the important relationships between CI´s*

Configuration Item

A Configuration Item is (or can be):

- Needed to deliver service
  - Not all components that are needed for the service delivery are regarded as Configuration Items
- Uniquely identifiable
  - Software, hardware, documentation, license
- Subject to change
  - Needs formal change process to authorize the modification of the Configuration Item
- Manageable
  - Only as much details about the service components that can be managed by reasonable resources and is contributing to the successful service management

Creating a CMDB

A **CMDB** should contain all items that influence the IT Infrastructure

Scope – Category

– Part of the IT Infrastructure that Configuration Management controls
– The scope influences the categorization of incidents, Problems and changes

Detail - Level

– What is a CI?
– In how many levels these CI's should be detailed ?
– CI's vary widely in complexity, size and type
  – From an entire system (including all hardware, software and documentation)
  – To a single module or a minor hardware component

Relationships

A relationship within the CMDB describes the dependency or connectivity between CI´s

Examples of relationships:

- Used by
- Part of
- Connected to
- Resides on

Life cycle of a CI

Shows the planned, current and previous states of CI´s

- Planned
- Ordered
- in Test
- in Production
- Broken
- In repair

- Archived

Configuration baseline

What?

A snapshot of the state of a CI or set of CI´s established at a specific point in time, for a particular purpose

Why?

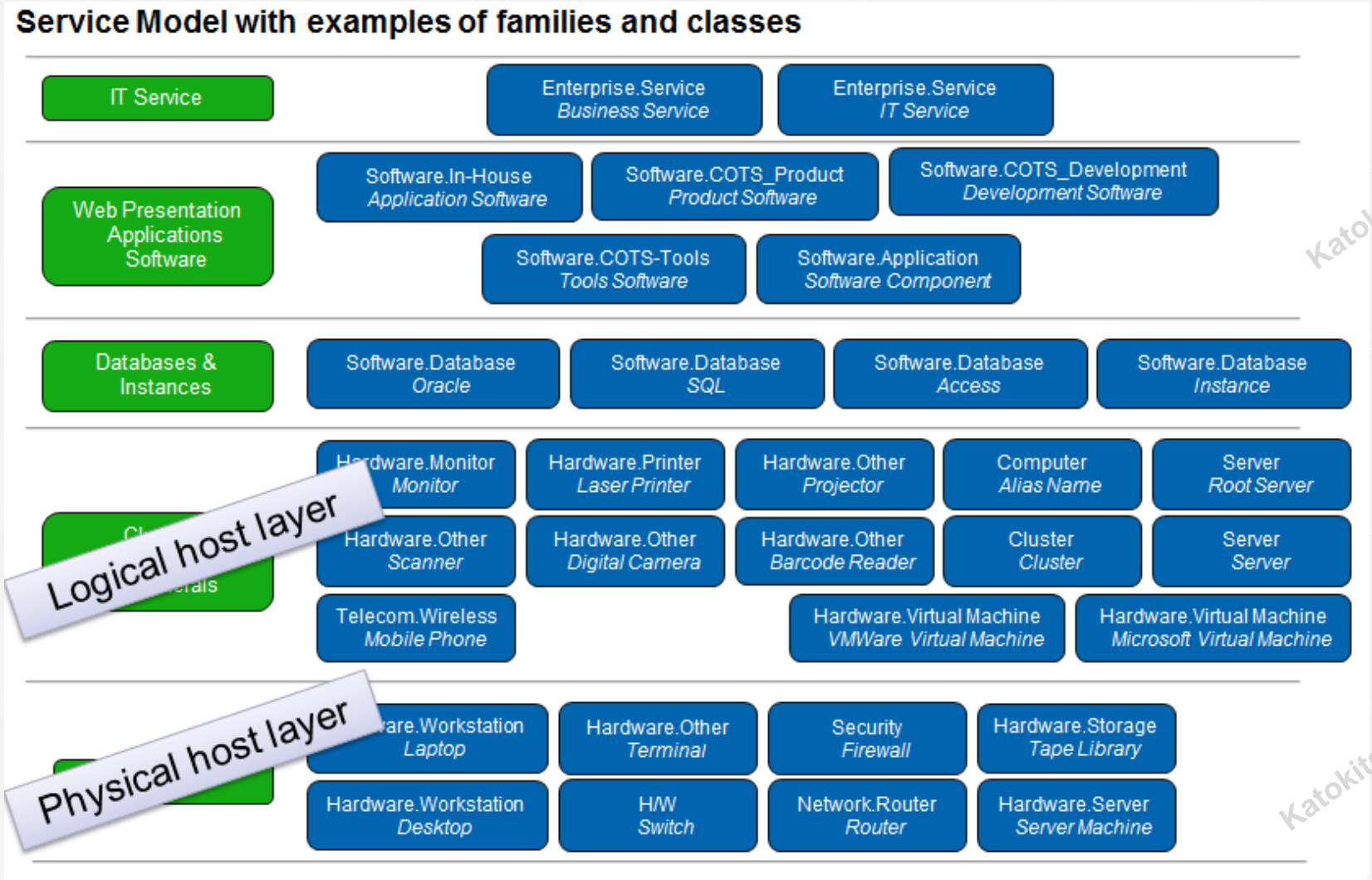
Although the CI record may be updated later, the baseline remains unchanged and available and can be used as:

- Reference of the original state
- Used for the formal control of a configuration

Example

- Desktop computer – all future installations refer to this baseline
- Desktop computer – “last known good configuration”

Configuration service model



Assets

Asset Management

- Element/part of a business / organisation accountancy process
- Assets can include people, accommodation, computer systems, networks, paper records, fax machines etc.
- Asset Management DB maintains details on assets (value, business unit and location)

A CMDB contains
RELATIONSHIPS BETWEEN CI's , DOCUMENTATION
and goes much further than an Asset DB

Configuration Manager's role

- Define the CMDB model
  - Define CI´s at the correct level, optimize model complexity
  - Including relations to services
  - Must be manageable with given resources
- Create and design
  - Process (how to assess and name the CIs physically)
  - Database (who, when and how to populate the database, e.g. discovery tools, relations, interface between CMDB and discovery tool's repository)
  - Define authorities and roles to have access to the CMDB
- Connect with processes:
  - Incident Management
  - Access Management
  - Event Management
  - Change Management
  - Release and Deployment Management
  - Availability Management
  - Capacity Management
- Optimally, automate the process connections for the above
- Perform periodical audits to align CMDB information with 'reality'
- Produce snapshot / baseline extract from CMDB according to requirement

Security aspect of Configuration Management

Configuration information should be shared in a controlled way.

Some information could be sensitive; for example, it could be useful to someone trying to breach security controls, or it could include personal information about users, such as phone numbers and home addresses.

Benefits

Benefits

- Provides information and control of the CIs, supporting other ITIL processes with information
  - Recording incidents on CIs, tracing dependencies for Problem and Change Management - helps with impact and trend analysis
- Describes the current and historical status of our IT Infrastructure
  - Disaster recovery, incident solution
- Security
  - If you don't know what you have, you cannot protect it

Challenges

Challenges

- Needs management commitment for resources
  - human, (often a team)
  - hardware, (may need servers to run the dedicated discovery software)
  - software, (Service Management tool support, discovery tools, license to access protected information, automatic CMDB update of changes, incidents, availability)
  - dependent processes (incident, change, release&deployment)
  - maintain Customer and IT organization foundation data and relations to service CIs and components
- Define the CMDB model
  - Define CI´s at the correct level
  - Including relations to services
  - Must be manageable with given resources
- Align with policy for SIAM model implementation

Risks

An outdated CMDB is totally useless, because people will not trust it, and therefore will not update it – and therefore will not trust it

Letting the discovery tool update the CMDB will not give reliable configuration data and will mask that the Change Management process may not be working properly. Also, lots of unnecessary information will be gathered.

The CMDB can also be used as an Asset Register, used for invoicing the Customer. The discovery tool might give a false picture of what is in use and what has been used during the invoicing period (availability), what is purchased / leased by the Customer.

Risk is therefore, that a separate Asset Register is implemented and this is not aligned with the CMDB.

Service Desk

Objective:

To act as a central point of contact between the User and IT Service Management.

To handle incidents and requests, and provide an interface to other activities (processes).

- SPOC (Single Point of Contact)
- Handles incidents, requests and questions
- Interface for other activities, such as customer change requests, maintenance contracts, software licenses and processes
- Representation of the service provider to the User

Service desk

A Service Desk is a specific organization for a specific purpose

Service desk purpose

- To capture demand for incident resolution and service requests.
- It should also be the entry point and single point of contact for the service provider with all its users

Service desk is the point of communication between the service provider and all its users (SPOC). Needs to understand the organizations and the stakeholders' desired outcome. The service desk *'owns'* all requests.

Service desk

Automation effects:

With increased automation, AI, robotic process automation (RPA), service desks are moving to provide more self-service logging and resolution directly via online portals and mobile applications.

With increased automation the focus of the service desk is to provide support for ‘people and business’ rather than simply technical issues

Responsibilities

Receive and record all calls

- Handle customer complaints and requests

Initial assessment of incidents

- Responsible for supplying first-line support and for assisting in the daily use of IT Services

Monitor and escalate incidents

- Monitor and escalate incidents according to service levels or to Global Service Desk when several service providers may be involved

Inform User / Customer

- Confirmation, status and progress

Produce management reports

Service Desk supporting technologies

✓Intelligent telephony systems, incorporating computer-telephony integration, IVR, and automatic call distribution

✓Workflow systems for routing and escalation

✓Workforce management and resource planning systems

✓A knowledge base

✓Call recording and quality control

✓Remote access tools

✓Dashboard and monitoring tools

✓Configuration management systems

Benefits

Benefits

- **Improved user service, perception and satisfaction**
  - The user knows where to turn to and is clear on expectations on response times
- **Better shared knowledge and communication**
  - Implemented tools to trace user interactions
- **Effective and efficient use of support resources**
  - Many queries addressed to the IT organization are of simpler nature that can be answered without involving technically highly skilled personnel

Challenges

Challenges

- **To find the correct resources and skills**
  - Staff turn-over is high of various reasons
- **Change behaviour of staff and users**
  - Staff that is used to handle more complex issues may feel under-utilized
  - Staff that is used to communicate with the users directly will be assigned tasks from the Service Desk only.
  - Users may want to talk to more technically skilled personnel, trust in Service Desk can be damaged.
  - Users don't want to solve their problem on their own, expecting Service Desk to do that.
- **Costs**
  - Outsourced Service Desk might be more costly than budgeted
  - The users may have a higher hourly rate than the Service Desk staff, therefore, solving an issue might be more expensive with self-help.

Incident Management

Incident Management purpose

- To minimize the negative impact of incidents by restoring normal service operation as quickly as possible.

Focus on resolving the incident ***situation*** -
- which is not necessarily the same as to restore normal service operation.

Fix first, argue later.

Terminology

Incident

– Any event / interruption, which is not part of the standard operation of a Service or causes or may cause a reduction in the quality of that service

If something is not working as it should

Service request

- When the user wants to have something done, e.g. account change, reset password, etc

Work-Around (WA)

– Method / temporary solution of avoiding an Incident, so that the normal standard operation can continue

Incident management

Incident resolution workarounds can also be permanent, if it is not justified to analyse and action the root cause of the incident.

Failure of a configuration item that has not yet impacted service is also an incident, for example failure of one disk from a mirror set.

This raises a number of questions regarding the Service Level Agreement, and also, ‘normal service operation’.

Prioritization of incidents

Impact

- The effect upon the activities of the business

Urgency

- How quickly the Incident needs to be resolved

Priority

Calculated or assigned based on impact and urgency

Prioritization of incidents

- Highest economic benefit, or highest financial impact first
- Techniques based on source or type of demand
- VIP status for some users in incident priority
- Triage based on urgency and impact
- First in. first out or Last in, first out
- Quickest is next or Slowest is next

Categorization of incidents

Categorization is used for:

- Recording incidents – as perceived by User
- Recording the final detected causes – may differ from perception
- Analysing trends to identify specific problem areas
- Escalating incidents to expert groups

Incident manager's role

- Quality
  - Supervise incident data and resolution quality – may use templates for frequent scenarios or categories
  - Supervise number of bouncings and analyse the reasons – input quality, interface to other groups, communication
  - In some cases, incidents are result of changes. If possible, link the incidents to those.
- CMDB verification
  - Make note of incidents that cannot be reported on definitive Configuration Items on right level and verify with Configuration Manager the reasons
  - Report on deviatons between originally set categories against resolution discovered categories and verify with Configuration Manager the reasons
- Escalation to Problem Management
  - Align with Problem Manager prior to creating a Problem Record
  - Link incident to existing Problem Record if any
  - Make note of incidents that were solved based on Problem Workarounds, analyse the possible gains and report
- Escalation to Change / Release & Deployment Management
  - In some cases it is allowed to implement changes to resolve incidents, without prior escalation to Problem Management. E.g. Standard change, emergency change, problem workaround implementation
- Escalation to Global Incident Management
  - If there are several service providers and the incident may depend on other products, the Global Incident Manager will coordinate the resolution process.

Incident manager's role

- Escalation point
  - The incident manager is the natural escalation point for hierarchical escalations
  - Any issues from interfacing processes are also escalated to the incident manager
- Statistics, reports (including options and recommendations)
  - SLA measurements, quality measurements, quantity, knowledge base usage
- GDPR
  - Review what data is needed, how they are stored, how long and how are they disposed of and if there is a GDPR exemption applicable
- Communicate and alert
  - Alert the business and the IT organization about significant incidents
  - During a so called Major Incident, the Major Incident Manager will keep the communication with stakeholders and shield off the technicians from management

Incident manager's role

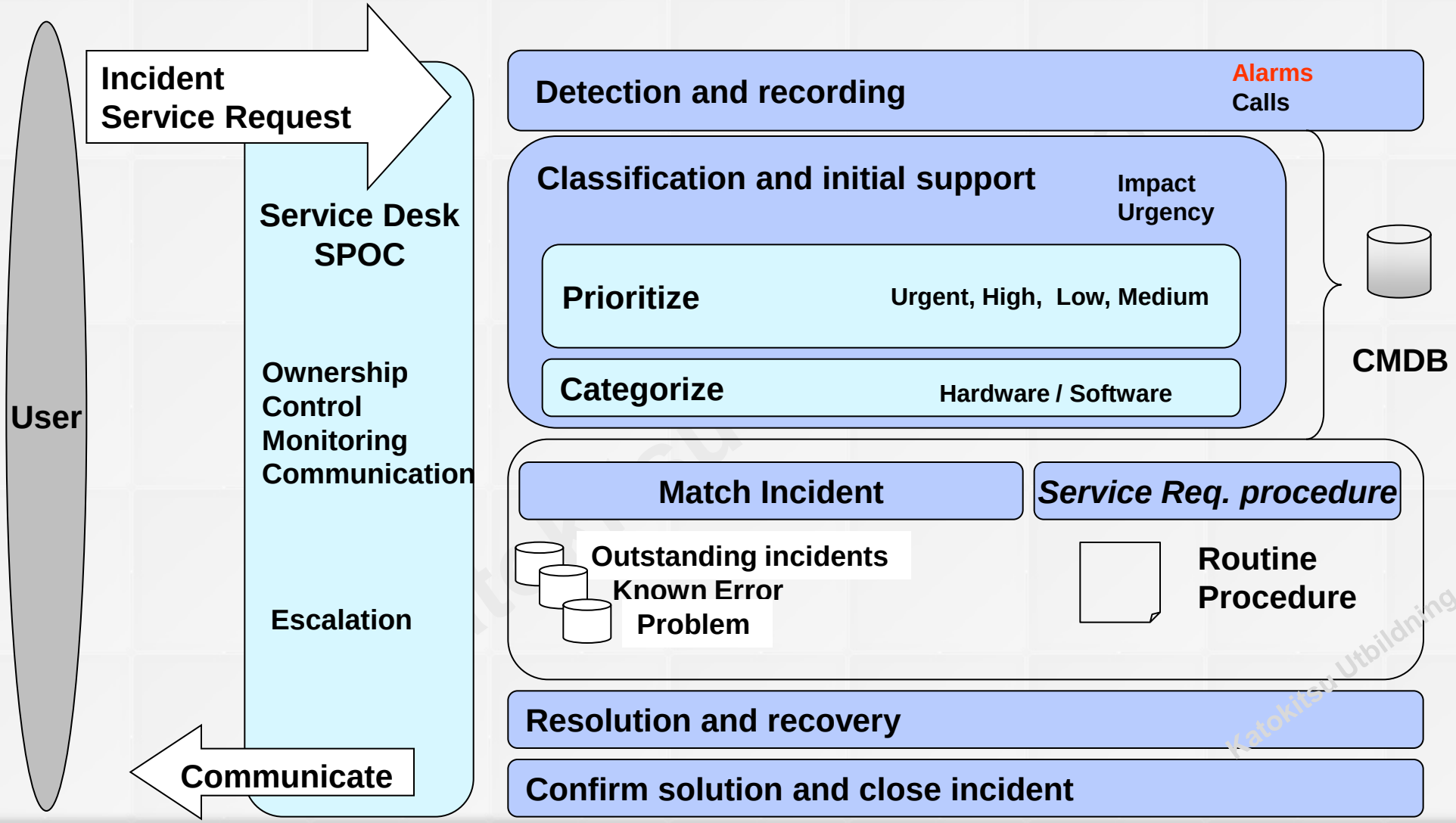
- Backlog
  - If there are unanswered incidents, list and sort them according to age and priority
  - Clear backlog of those that are close to SLA breach
  - Clear low priority incidents, since these are most likely of easier nature
  - Assign experts with responsibility to manage bouncing incidents
  - Some incidents cannot be resolved, clear these off upon user agreement
  - Communicate clearly and loudly the clearing successes
  - Walk through 'on-hold' incidents and activate them.

- Dispatch
  - Dispatch unassigned incidents within group by workload, skills, priority

- Escalate
  - Escalate ASAP to next level, if resolution is not obviously simple or present level lacks skills, tools, authority to resolv

- Daily meetings
  - Put incidents with near-SLA breach on meeting agenda
  - Put incidents with high complexity on meeting agenda
  - Put backlog incidents on meeting agenda

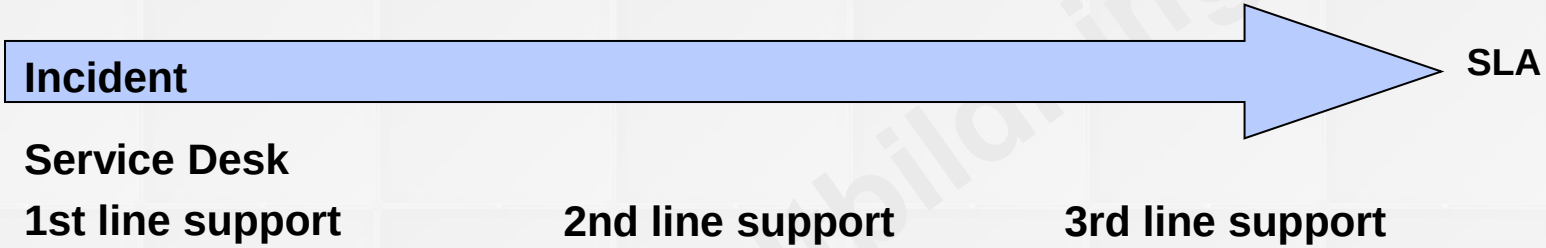
The Incident Life Cycle



Escalation

Functional escalation / Incident routing

- More or other knowledge



Hierarchical escalation / Vertical escalation

– Escalation to a higher hierarchical layer

– Used when SLA will not be met and for major Incident

Benefits / Challenges

Benefits

- Reduced business impact of incidents
- Better staff utilization and therefore greater efficiency
- Elimination of lost or incorrect requests
- User and Customer satisfaction

Challenges

- Empowerment throughout all organizations
- Change work procedures for support staff
- Report and register all incidents and requests
- Keeping SLA leadtimes at the different escalation levels
- Not always possible to confirm the resolution with the user

Problem management

Problem management purpose

- to prevent problems and resulting incidents from happening,
- to eliminate recurring incidents and
- to minimize the impact of incidents that cannot be prevented.

Problem Management involves root-cause analysis (RCA) to determine and resolve the cause of events and incidents, proactive activities to detect and prevent future problems/incidents and Error control to allow quicker diagnosis and resolution if further incidents do occur.

Terminology

Problem

– *When the root cause (=underlying cause) of one or more incidents is not known*

Known Error

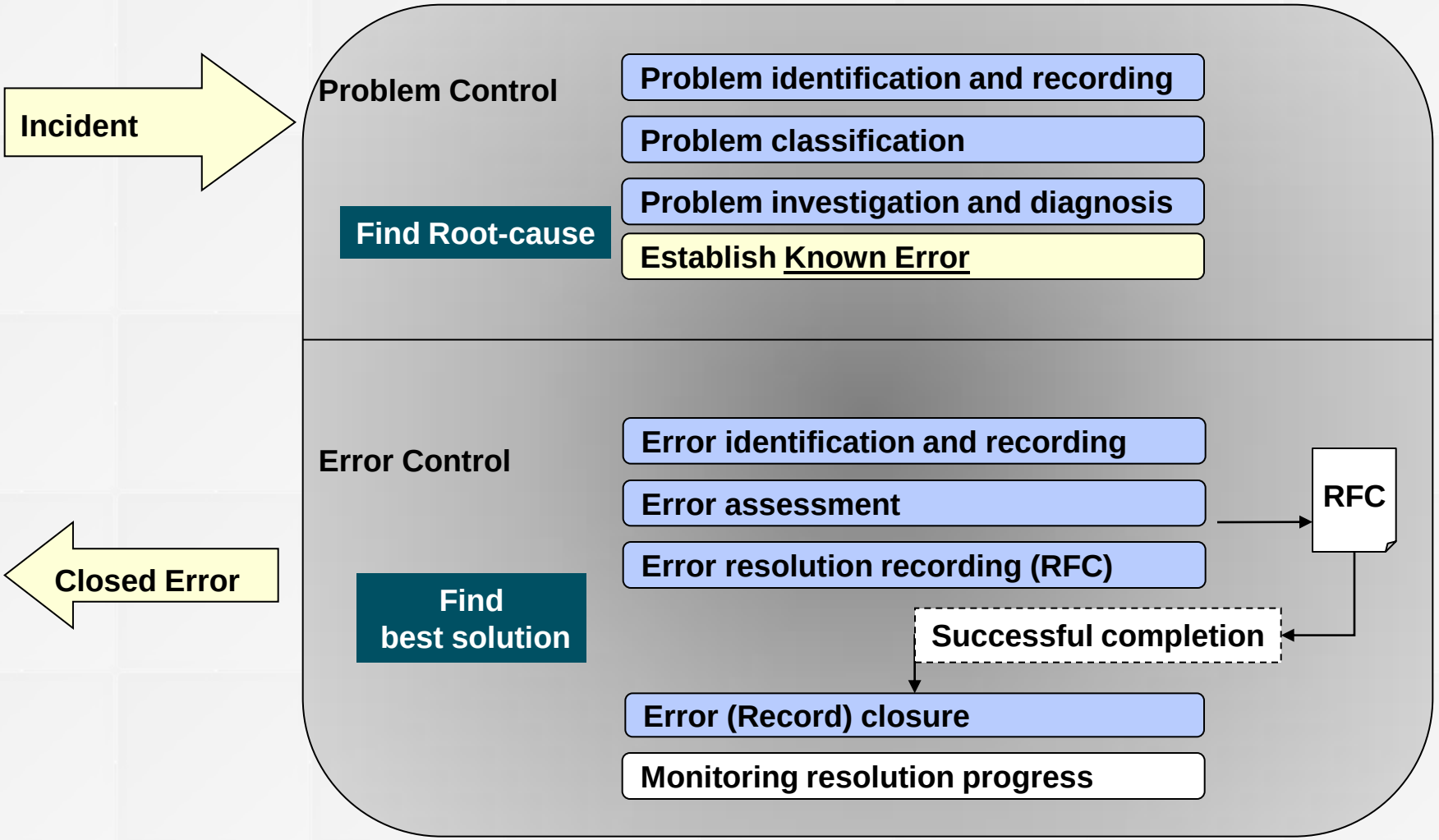
– *An Incident or Problem for which the root cause is known and for which a temporary Work-around or a permanent alternative has been identified.*

Workaround

- A solution that reduces or eliminates the impact of an incident or problem for which a full resolution is not yet available. Some workarounds reduce the likelihood of incidents.

Investigating the root cause of the incidents (**Root Cause Analysis**) can be triggered by incidents or by continual improvement. Implementing the permanent resolution to the root cause may trigger Change management.

Activities



Proactive Problem Management

From reactive	To proactive
Incidents appear and are solved	Identify and resolve problems before an Incident occurs

Why

– Minimise the impact on the service and costs related to business

Proactive work

Trend analysis may identify

- Incidents of a particular type
- Recurring problems with a CI
- The need for more customer training
- The need for better documentation

Results (Output)

- RFC
- Feedback on testing, procedures, training, documentation
- Education and training
- Process or procedural improvement

Problem management

Phases: Problem identification – Problem Control – Error Control

Problem identification	Re-active or pro-active problem detection, logging, filtering (Risk management!), categorizing
Problem Control	Root Cause Analysis (RCA), workarounds, Known Errors logging, options for permanent solution
Error Control	Assessing options for permanent solution and requesting Change if needed.

A Problem Diagnosis and Resolution Example of the 5 why's

Incident	Depreciation value is duplicated	Resolution: remove duplication
Problem investigation – Why 1?	Why was it duplicated?	Double transaction, fault in script
Problem investigation – Why 2?	Why was there fault in script?	3rd party code library faulty
Problem investigation – Why 3?	Why was this not discovered during test?	No test was executed for this use of the function
Problem investigation – Why 4?	Why was no test done?	Test case did not cover
Problem investigation – Why 5?	Why was the case not covered?	……
Change	Work-around	Correct the script
Change	Final solution: Correct the Story or the test case	Close problem record after change implementation

Problem manager's role

- Align with Incident Management about problem candidates
- Analyse and filter problem candidates in regard to cost, complexity, feasibility and applicability
- Authorize (or not) submitting Change Request
- Define and dispatch tasks
- Analyze Event Management alerts for proactive problem investigation
- Extract information from Incident database and other sources to act proactively
- Coordinate activities with Global Problem Manager, if any
- Compile management reports, with options and recommendations

Benefits / Challenges

Benefits

- Improved IT Service quality
- Reduced Incident volume
- Knowledge sharing

Challenges

- Gain Management commitment
- Change work procedures for Support staff
- Create the right categorization/prioritization to make sure that information is co-ordinated
- Defining relevant SLA leadtimes, if at all
- Coordinated work among multiple service providers
- Contract with Customer might not be clear for Problem management
- Selecting which problems are worth investigating (strategy, time, cost, skills, resources, large suppliers dependency, etc)

Request fullfilment – Service Request

Purpose

- To provide a channel for users to request and receive standard services for which a pre-defined approval and qualification process exists.
- To provide information to users and customers about the availability of services and the procedure for obtaining them.

In some cases, a service request is actually reporting an incident or vice versa.

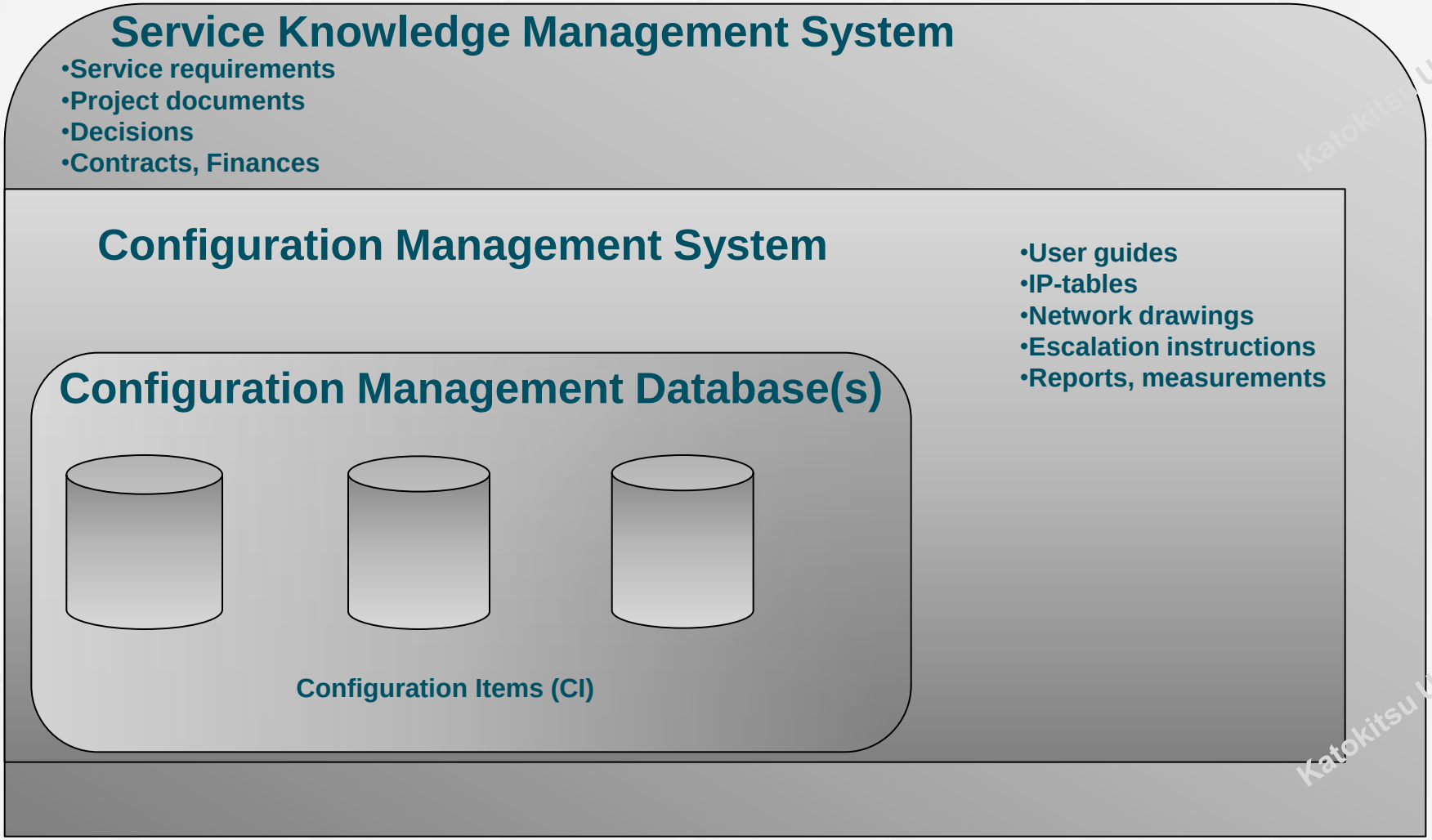
Service Request

A request from a user or a user's authorized representative that includes a service which has been agreed as a normal part of service delivery.

Types, example:

- Request for a service delivery action, e.g. a report, replacing a toner cartridge
- Request for information ('How to....')
- Request for provision of a resource or service (laptop to a user, virtual server for testing) – Service Catalogue on intranet portal
- Request for access to a resource or service (project folder...)
- Standard changes can be implemented as Service Requests

Knowledge Management



Change Management

Change management purpose

- to maximize the number of successful service and product changes by
  - ensuring that risks have been properly assessed,
  - authorizing changes to proceed and
  - managing the change schedule.

Any and every change affects the provided service and its value -> therefore, the Outcome the Customer wants to achieve.

Change Management

Objective:

To minimise the risk for associated incidents when introducing changes to the IT infrastructure.

How:

Through strict control of any changes -
any change needs to be authorized on some level.

e.g. Authorize to proceed with the analysis
-> authorize to proceed with the build ->
authorize to proceed with deployment

Why changes?

Strategic

- *Politics, business development, laws and regulations, environment, economics, partnerships*

Tactical

- *Capacity/Availability/Security/Stability etc improvement*
- *End of life cycle*

Operational

- *Incident / problem solutions, prevention*

Any other

- *Implementation of newest and coolest*

Terminology

Change

– ***The addition of…, the modification of…, or the removal of…, service components***

Request for Change (RFC)

– ***Record of details of a request for a Change to any CI***

Forward Schedule of Changes (FSC)

– ***Schedule that contains details of all the changes authorized for implementation and their proposed implementation dates. It also shows the dependency of each Change.***

Change Management is also sometimes referred to as Change Control or Change Enabler.

Change categorization

Standard

A well known, relatively risk-free Change with predefined procedure

The Change may be executed without contacting the Change Manager, in some cases even by the Service Desk.

Minor

Small business impact on the services

The Change Manager is entitled to authorize this RFC

Significant

Medium business impact on the services

The Change Manager requests advice from the Change Advisory Board (CAB)

Major

Major business impact on the services

Management is involved in the decision process

Priority of a Change

Priority of a Change is based on business impact

Urgent (=emergency)

Change necessary immediately, approval by Emergency Committee (EC) or ECAB

High

Change needed as soon as possible

Medium

Change will solve annoying errors or missing functionalities

Low

Change is necessary and justified, but can wait

Change manager's role

Validation of RFC for:

- Who RAISED the change?
- What is the REASON for the change?
- What is the RETURN required from the change?
- What are the RISKS involved in the change?
- What RESOURCES are required to deliver the change?
- Who is RESPONSIBLE for the build, test and implementation of the change?
- What is the RELATIONSHIP between this change and other changes?
- Are the backup and back-out (restore) plans REALISTIC and proven?
- Is the scheduling according to the change policy?

Understand RFC as a Business Case. Strategic and tactical changes need to be sponsored by the Customer. The Business Case needs to be revisited during assessment, planning and development. Thus, several approval stages might be needed.

Change Advisory Board

A group of representative people responsible for assessing all RFC(s) based on:

- Business impact
- Priority
- Resources (cost, people…)

The CAB gives advice to Change Management

Involve the persons that are needed to asses the Change:
Service Level Manager, User, Customer, Release Manager, Application Manager etc

Change Advisory Board

Input to CAB

- Completed Request for Change (RFC or Change Request)
- Assessment results in the form of Change Proposal, including Costs, risks, resources, etc
- Forward Schedule of Changes (Change Schedule)
- CMDB

Output from CAB

- Approved / rejected RFC
- Change plan
- Updated Change Schedule
- Work order to Release and Deployment

Emergency CAB - ECAB

Urgent (Emergency) Change

- Change approval is still a prerequisite
- Keep the number of urgent Changes low
- Define an urgent Change and communicate roles (based on scenario)
- Test as much as possible

Involve the persons that are needed:
Decide which persons are authorized to approve urgent Change.

At some implementations, defined group of staff will authorize Emergency Changes..

Change Manager's role and activities

- Record / validate / complete RFC
- Get pre-approval from stakeholders
- Submit proposal to CAB
- Formally approve the change
- Update change schedule
- Communicate CAB decisions to stakeholders
- Compile management reports
- Initiate improvement activities
- Update change records
- Update CMDB

- Act for transformation of Normal Changes to Standard Changes.
- Act for minimizing number of Emergency changes.

Post Implementation Review - PIR

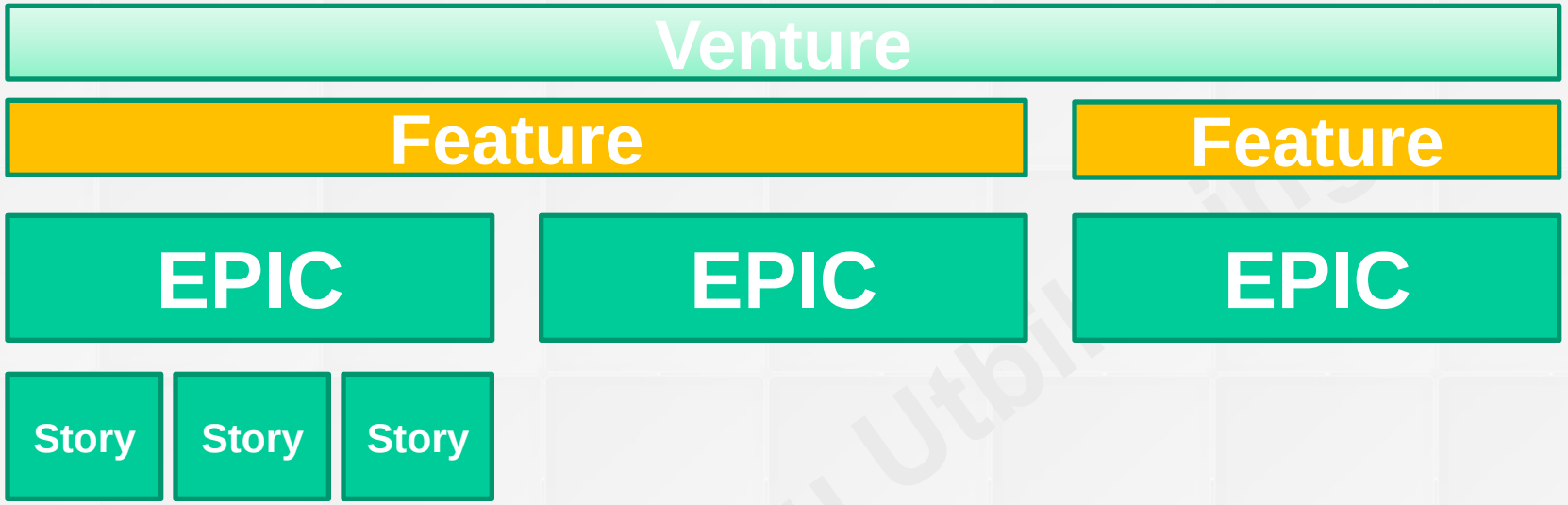
A review held after implementation of a Change to determine if the Change has been implemented successfully.

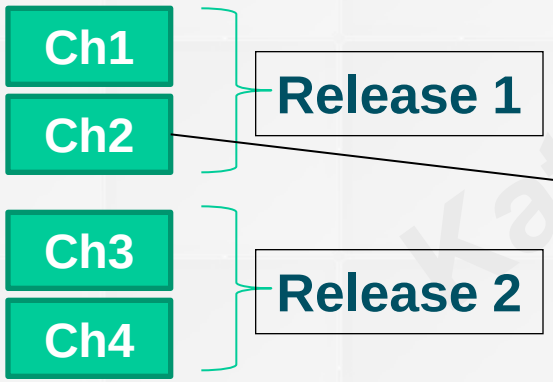
What do we review?

- have we achieved what we wanted?
- customer satisfaction?
- any caused incidents?
- expected benefits obtained?

Lessons learned should be input to future changes

Agile Change Management

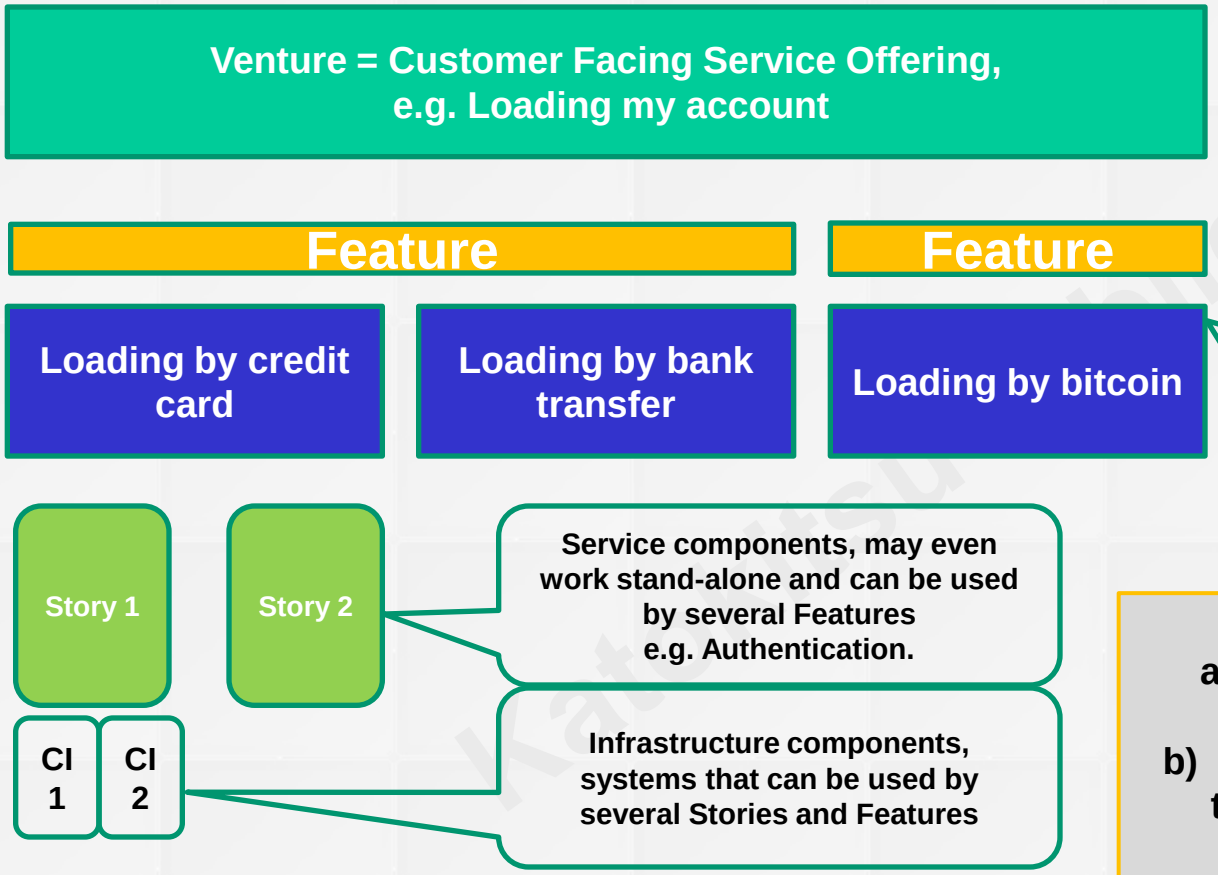




It is up to the operating model what is subject to Change Management:

- EPIC
- Story
- Sprint
- Release

Agile Change Management



If this was not in the original service offering, than this is a Feature requested and the Service Offering (Venture) will be updated too
Any Feature is developed in EPICs, that are broken down to Stories

To measure:

a) Speed of the introduction of the Feature(s)

b) Speed of the design/build/release of the Story – this measurement needs to be presented by corresponding Story

Change in the cloud

- Cloud service providers do not (always) actively notify their customers
- Change Manager needs to check their information, e.g. on their web.
- CMDB update is limited, if at all
- Release Manager can / should / must inform the users about the changes :
  - -When
  - -What
  - -How

Benefits

Benefits

- Improved quality of service and a professional approach
- Documented risk and cost assessment
- Improved productivity of key IT staff, due to better planning and less disruption to repair faulty changes

Challenges

- Maintain control over urgent changes
- Maintain a correct CMDB
- Planning the change without conflicts with other changes, specially in a multi-vendor environment
- Risk assessment needs to analyze both business impact risks and technical risks.
- Back-out (basically restore) procedures are often not proven and the time and resources needed are not calculated and assessed as a risk
- Remediation procedures are not defined. Remediation is when back-out is not possible and the situation is needed to be fixed.
- The same Change manager approves changes for all types of changes – needs skills that not many people have
- Projects tend not to register RFCs in time and with necessary details and quality and thus long-planned changes will need to be implemented as Emergency changes.
- Strategic / political decisions will allow approvals regardless of assessment results

Release and Deployment management

Release mgt purpose

- To make new and changed services and features available for use.

Deployment mgt purpose

- To move new or changed hardware, software, documentation, processes or any other component to live environments.
- May also be involved in deploying components to other environments for testing and staging.

Definitive Media Library (DML)

- A physical storage repository where master copies of software versions are placed, as well as hardware items
- A logical storage, may be one or more physical software libraries or file stores.
- Protection of all authorized software and hardware versions both purchased and developed
- Base for Releases and used for distribution

 Not a good practice to distribute releases from development or test environment...

Terminology

Release

– *A collection of new and/or changed CI's which are tested and introduced into the live environment together*

Release policy

– *Clarifies the roles and responsibilities for Release Management*

– *Describes the normal Release units, normal change content, release frequency, naming conventions, version numbering and scheduling of releases*

Release plan

– *A document that describes all of the activities, resources, responsibilities related to a particular release, and the scheduling of that release*

Activities

1. Create Release policy and plan
2. Design and develop or purchase release tools
3. Build and configure release
4. Test, validate and accept Releases
5. Plan Roll-out
6. Prepare Release and communicate
7. Update CMDB

Deploy: Distribute, install, update CMDB

Test, validate and accept releases

Test if the Release package can be deployed and is working

Validate if the Release works according to the requirements – does what it should

User Acceptance Test – UAT – is done according to predefined Use Cases and acceptance criteria is agreed with the Customer prior to UAT.

Acceptance criteria should not be an ad-hoc decision at the time of the UAT.

Types of Release

Part of the Release Policy

Full release = *all components within a Release unit*

Delta release = *only changed components within a Release unit*

Package release = *individual releases grouped together*

Emergency release

Release unit

The portion of the Infrastructure that is normally released together

How big / small should it be?

It depends...

- Easiness of implementation
- Complexity of interfaces
- Amount of change at each level
- Need of resources and time

Deployment

The change is transferred from the development environment to the production environment (or rather, the DML) in order to subsequently be implemented.

Prior to implementation, a user manual is written and in many cases users receive a training, after which the system is handed over to them.

If there are a large number of users, the implementation period can also be extended over a particular period of time.

Benefits / Challenges

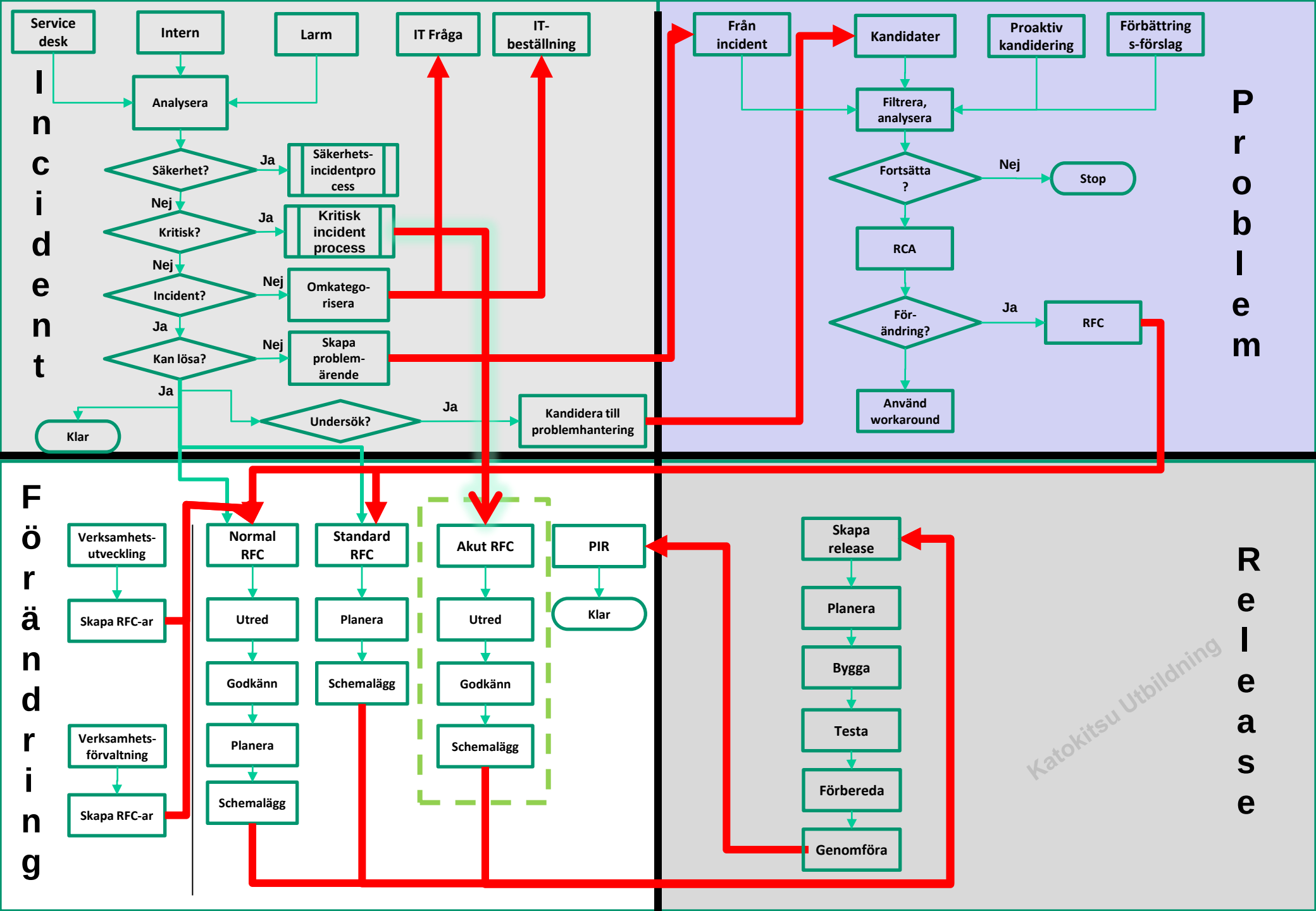
Benefits

- Less disruption of the service to the business
- Schedule releases in advance
- No cost for licenses and support that are not used
- Detection of wrong versions and unauthorised copies of software

Challenges

- Build restricted and representative testing environments and procedures
- Maintaining correct use of urgent procedures
- Coordination of several service providers' releases and deployment

How does it all hang together?


Incident
Service desk
Intern
Larm
IT Fråga
IT-beställning
Analysera
Säkerhet?
Ja
Säkerhets-incidentprocess
Nej
Kritisk?
Ja
Kritisk incident process
Nej
Incident?
Nej
Omkatego-risera
Ja
Kan lösa?
Nej
Skapa problem-ärende
Ja
Undersök?
Ja
Kandidera till problemhantering
Klar
Problem
Från incident
Kandidater
Proaktiv kandidering
Förbättrings-förslag
Filtrera, analysera
Fortsätta ?
Nej
Stop
RCA
För-ändring?
Ja
RFC
Använd workaround
Förändring
Verksamhets-utveckling
Skapa RFC-ar
Verksamhets-förvaltning
Skapa RFC-ar
Normal RFC
Utred
Godkänn
Planera
Schemalägg
Standard RFC
Planera
Schemalägg
Akut RFC
Utred
Godkänn
Schemalägg
PIR
Klar
Release
Skapa release
Planera
Bygga
Testa
Förbereda
Genomföra
Katokitsu Utbildning

Service Level Management

SLM purpose

- Set clear business-based targets for service levels and ensure that delivery of services is properly assessed, monitored and managed against those targets.

Service level

One or more metrics that define expected or achieved service quality.

Terminology

IT Service

– *One or more IT systems which enable a business process*

Service Catalogue

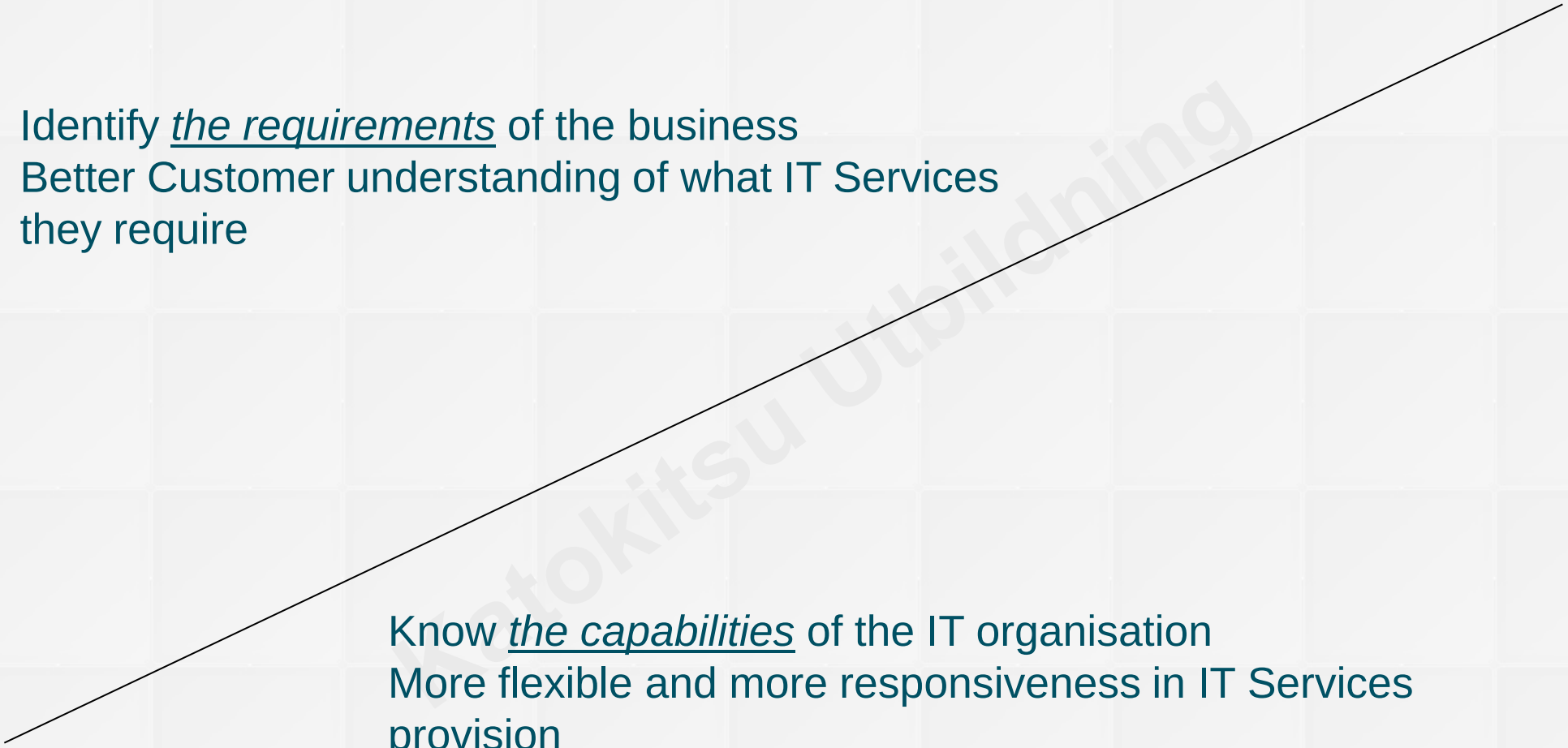
– *An overview of all the IT Services offered by the IT department, containing default levels and options*

Service Level Requirements

– *Customers needs that are used to develop, modify and initiate service*

Service Level Requirements and capabilities

Identify *the requirements* of the business
Better Customer understanding of what IT Services they require



Know *the capabilities* of the IT organisation
More flexible and more responsiveness in IT Services provision

Service Level Management

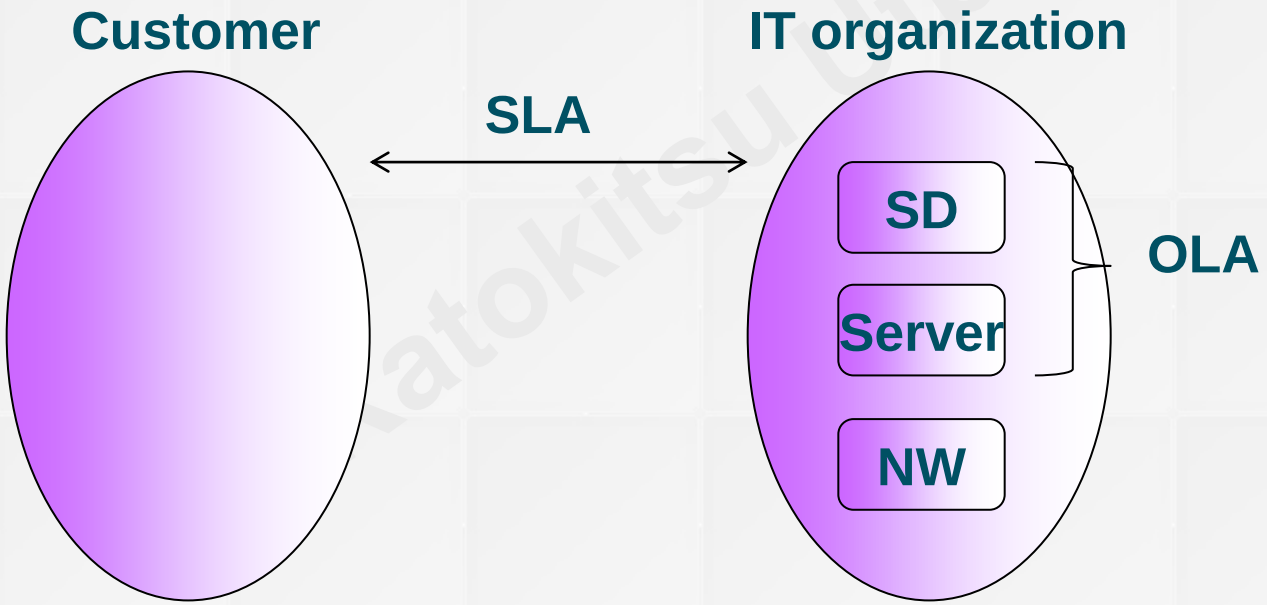
- Design framework for SLA (template, document structure)
- Monitor and produce reports on service performance
- Measure and strive to improve customer satisfaction

Key Performance Indicators (KPIs)

- # or % of service targets being met
- # and severity of service breaches
- # of services with up-to-date SLAs
- Improvements in customer satisfaction (customer experience)

Types of agreements

- SLA – Service Level Agreement – Customer
- OLA – Operational Level Agreement - IT Organization, internal



Structure of agreements

Service based

– SLA covers one service, for all the Customers of that service

Customer based

– An agreement with an individual Customer group, covering all the services they use.

Multi-level SLAs

– Corporate Level - issues on the generic level

– Customer Level - issues regardless of the service being used

– Service Level - issues for the specific service, in relation to this specific Customer group

Parts of an agreement

GENERAL

Introduction

- *Parties*
- *Signatures*
- *Service Description(s)*

Reporting & reviewing

- *Content*
- *Frequencies*

Incentives & Penalties

Change Procedures

SUPPORT

Service Hours

e.g. 24/7

Special Service Hours, e.g.

holidays

Service Calendar

Special support requests

Escalation

DELIVERY

Availability

Reliability

Throughput

Transaction response times

Batch turnaround times

Contingency & Security

Charging

The SLA should not contain anything that is not measurable!

Reporting on SLA

Reporting on delivered services availability, capacity, etc when it is actually ‘in the green’ *DOES* give a bit of indication about the service delivery quality, but…

… it is more important to report on what is NOT working according to the SLA and analyzing the reasons and list options for improvement, along with recommendations out of the listed options.

Service Improvement Program (SIP)

Objective: Controlled improvement of the IT Service provided

Used whenever there is a need:

- Service deviation from agreed levels
- Strategic choice
- Continuous Improvement

The SLM process generates a good starting point for a SIP. SLM works in conjunction with other processes to carry out a SIP. More than one SIP can run simultaneously.

Benefits / Challenges

Benefits

- IT effort is focused on the business key areas
- Improved relationships with Customers due to clarity of IT Service delivery
- Clearer view for both parties of roles and responsibilities
- Service monitoring allows weak areas to be identified, thus allowing for better planning

Challenges

- To create business aligned SLA - not IT-based
- Ensure that targets are achievable before committing to them and verify targets prior to agreement
- Create OLA that supports SLA
- Communicate SLAs properly

More challenges

- Services' components are outsourced to different vendors, e.g.
  - Database
  - Network
  - Storage
  - Communication
  - Application Maintenance

What does the SLA mean in that context?
Who is responsible for the (aggregated) service being able to support the business processes?

More challenges

e.g.

Database availability in SLA = 0.98%

Storage availability in SLA = 0.98%

Network availability in SLA = 0.98%

0.98*0.98*0.98 = 0.94% availability of the service !

Event Management

Purpose

- Monitor and report on services and service components

-Capacity
  -HW usage, response times, concurrent users, bandwidth
-Availability
  -Service / System / component availability
-Security
  -Confidentiality
  -Information integrity

Event Management

Well functioning Event Management can prevent incidents happening and can discover incidents even before the user would experience them.

An overflow of event reports can be contra-productive – difficult to manage

Incident, problem and change records in the service management tool can be initiated

The CMDB records for CIs are flagged for monitoring, depending on the service / component function.

Event Management

Information

Logs events, but does not require any action

Warning

Logs interruptions or breach of capacity / availability thresholds, possible breach of security rules

Exception (Error)

Logs stoppage of service/system/service component, breach of security rules

Capacity management

Business Capacity Management

– *Ensure that the future business requirements for IT Services are considered, planned and implemented*

Service Capacity Management

– *Monitor, analyse, tune, and report on service performance*

Resource Capacity Management

– *Monitor, analyse, run and report on the individual components*

Capacity plans

Management reports

Technical reports

Terminology

Capacity planning

– *Developing a Capacity plan that describes the current (IT Infrastructure) capacity, and expected changes on demands for IT Services*

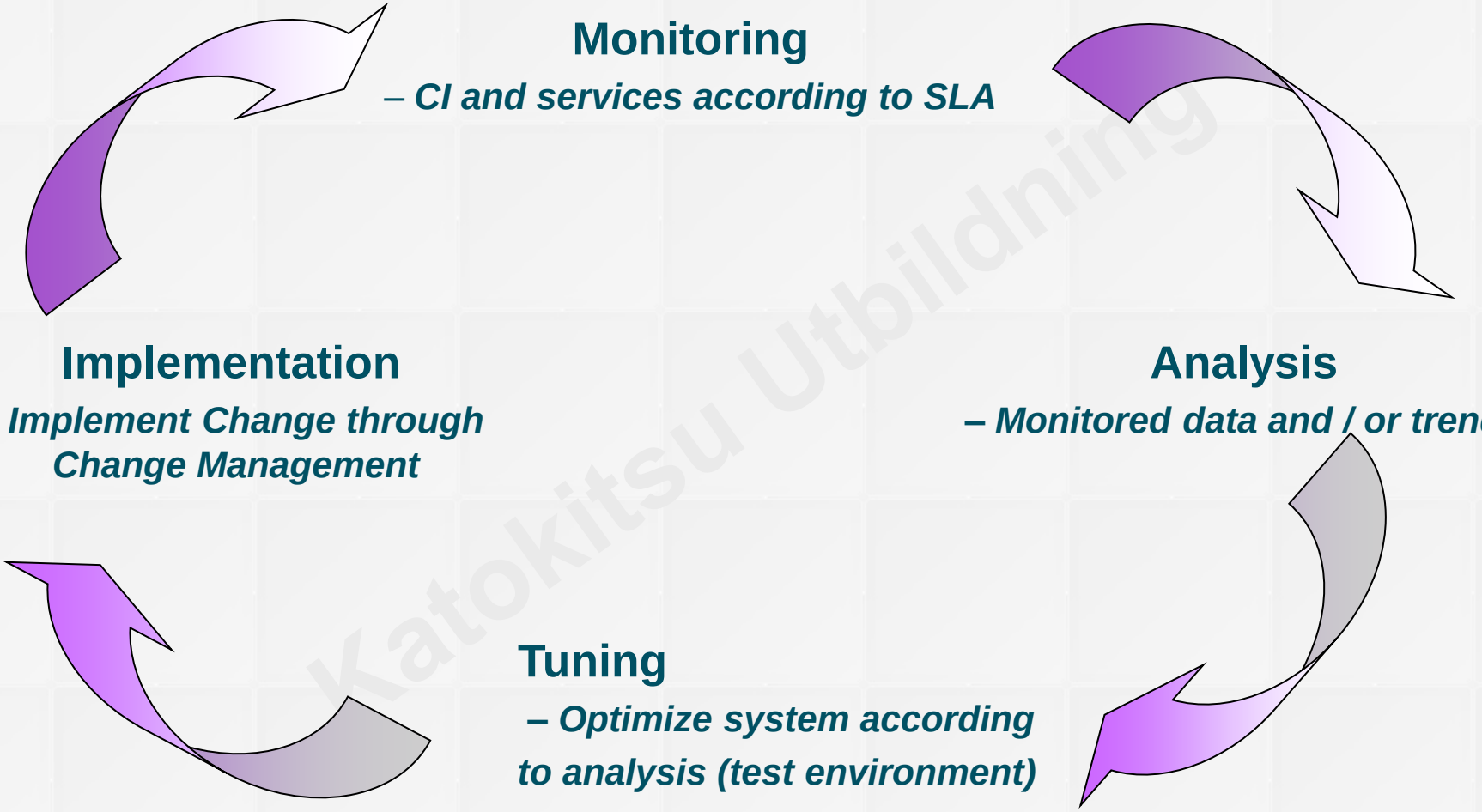
Performance Management

– *Measuring, monitoring and tuning the performance of IT Infrastructure components*

Demand Management

– *Place and manage requirements on capacity*

Operational activities



Benefits / Challenges

Benefits

- Increased efficiency and cost savings resulting in more economic provisioning of IT Services
- Elimination of unnecessary spare capacity and optimizations of equipment
- Reduced risk of performance problems and failure

Challenges

- To create and achieve realistic performance figures for equipment
- To get reliable and accurate business forecasts and information
- Dependence on other service providers' capacity

Availability Management

Purpose

- Make the services available when and where required.

How

- Identify bottlenecks, single-point-of failure elements, opportunities
- Plan and design service availability according to current and future requirements
  e.g.
  - Analysis methods
  - Reduntant solutions
  - Supplier / vendor management
  - Risk management
  - Security management

Terminology

Availability
– *IT Service available to the Customer*

Reliability
– *IT Service is available for an agreed period without interruptions. Involves Resilience and Redundancy*

Maintainability
– *Keep IT Service in operation, maintain and restore*

Serviceability
– *Third part is responsible for support*

Security
– *Confidentiality, Integrity and Availability*

Methods

Component Failure Impact Assessment (CFIA)

– *Using a matrix to identify areas of risk in IT Services looking at the impact of Incident for CI´s*

Fault Tree Analysis (FTA)

– *Using notation to identify a chain of events that causes a disruption to IT Services*

CCTA Risk Analysis and Management Method (CRAMM)

System Outage Analysis (SOA)

– *Analyses down-time to identify improvement in IT Service up time*

CRAMM

Risk analysis	Risk Management
Value of assets	Counter measures
Threats	Planning for potential outage
Vulnerabilities	Managing an outage

CRAMM - CCTA's* Risk Analysis and Management Methodology

Central Computer and Telecommunications Agency

Activities

- Determining availability requirements
- Designing for availability and recovery
- Security issues
- Developing an Availability plan
- Maintenance management

Operational availability

Availability Up Time

MTBF = Mean Time Between Failures

Reliability

MTBSI = Mean Time Between System Incidents

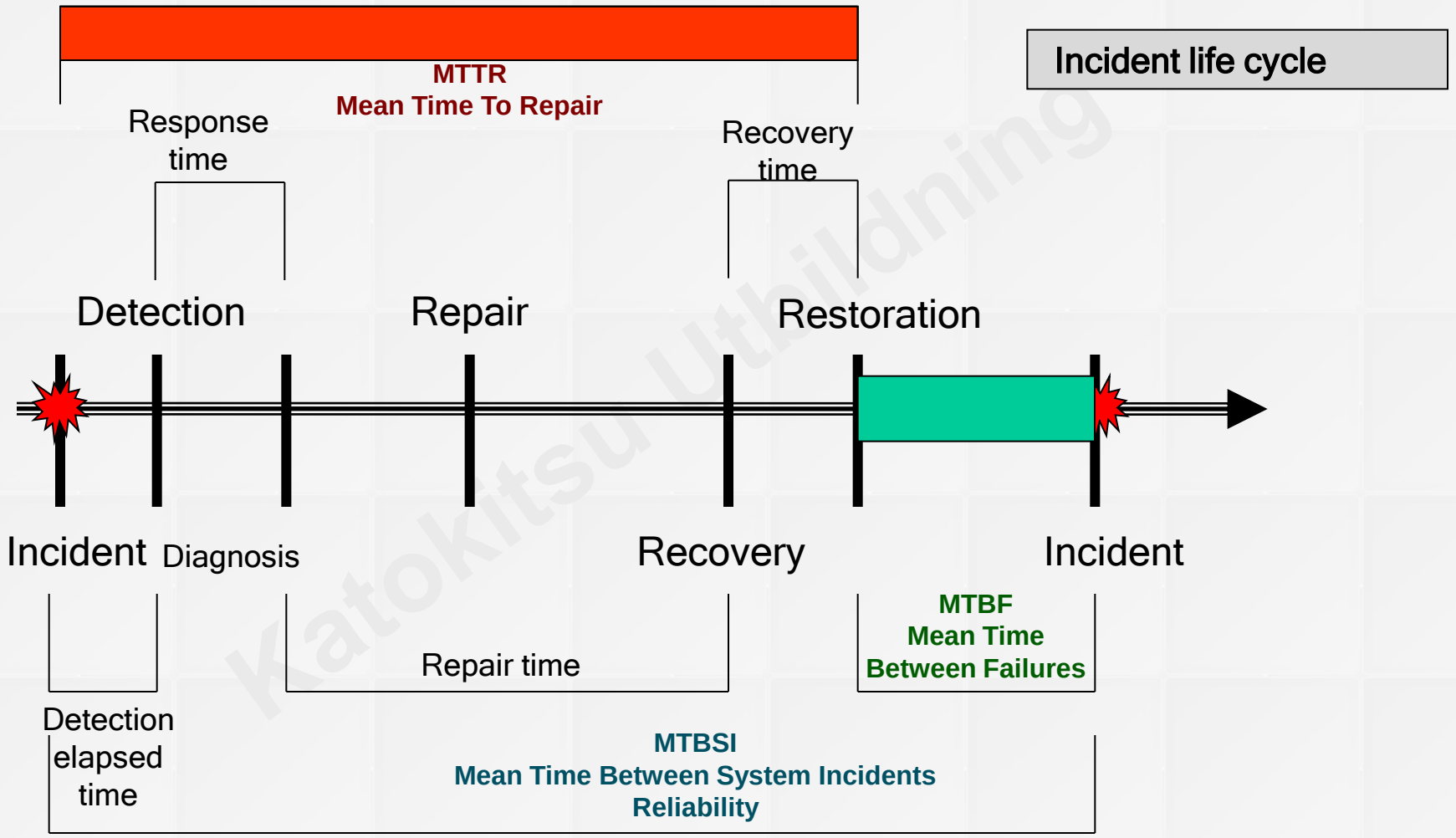
Maintainability Down Time

MTTR = Mean Time To Repair / internal

Serviceability

Availability, Reliability and Maintainability provided by third party

Unavailability - Availability



When is a service available?

"An IT Service is *not available* to a Customer if the function(s) required during *Service Hours* at that particular *Location* can not be used."

$$\text{Availability} = \frac{(\text{AST} - \text{DT})}{\text{AST}} \times 100\%$$

AST = Agreed Service Time
DT = Down Time

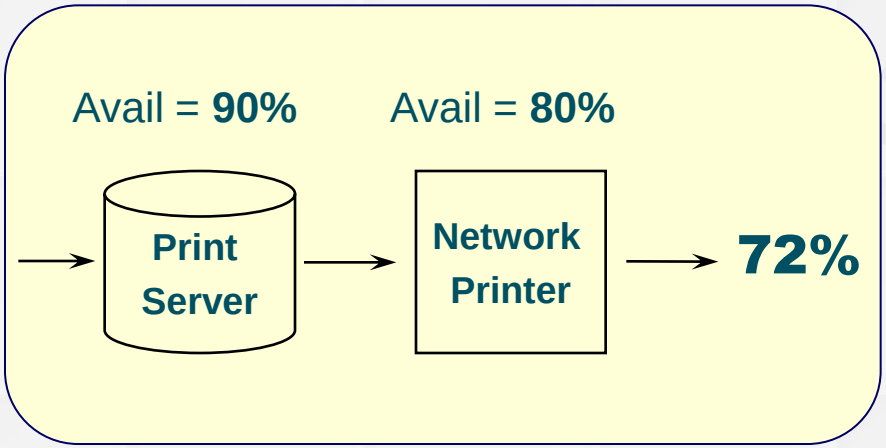
Availability Formula

In Series

Available only if both work =

A x B =

0.90 * 0.80 = 0.72 or 72%



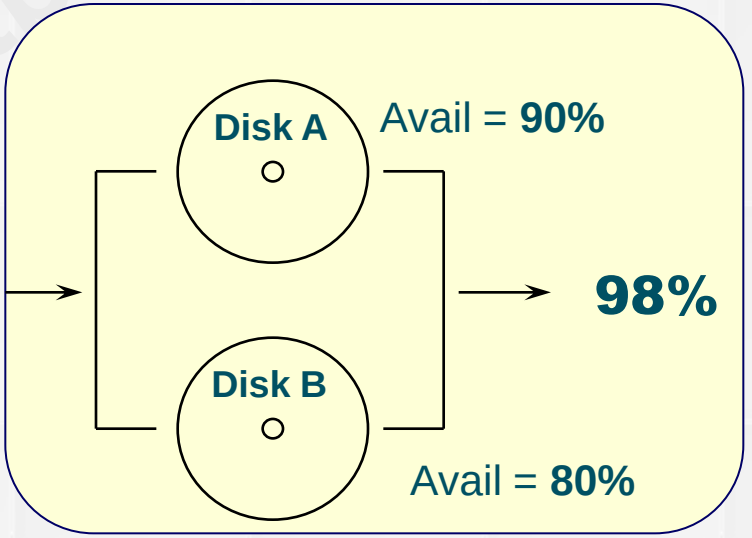
In Parallel

Available = 1 - Not Available =

1 - Both down =

1 - (A Down) x (B Down) =

1- (0.1 * 0.2) = 0.98 or 98%



Benefits / Challenges

Benefits

- Availability levels are measured and controlled
- Predict business changes of availability levels
- Services are designed and managed to cost effectively meet specified business requirements

Challenges

- Define availability levels, and how to measure, together with the customer.
- Find a support tool to measure availability
- Dependence on other service providers' availability

Information Security Management

Purpose	• To protect, control and manage the security on information and IT Services

Information security will be cheaper and more effective
when considered early in design and Change Management

Terminology

Confidentiality
– *Protection of sensitive information*

Integrity
– *Safeguarding of the accuracy and completeness of information*

Availability
– *Ensuring that information and vital IT Services stay available*

Right information to the right people at the right time

Terminology

Security policy

– *Defines Security for the organisation, providing guidance for employees*

Security plan

– *Describes how policy is implemented for IT Services and departments*

Security Measures

Organisational Security Roles, responsibilities, reporting procedures	**Physical Security** Separated facilities on process information and restricted access
Technical Security Control provided within system, network, buildings	**Procedural Security** Who does what , when

Control

Security measures come to play when considering or handling identified threats or real incidents

– Preventions/reduction control
  – E.g. access restrictions
– Detection and repression control
  – E.g. Periodic scanning, quarantine, ‘cut off the environment’
– Correction and recovery control
  – E.g. Cleaning and restoring, service start-up

Benefits / Challenges

Benefits

- Risk assessment is “enforced”
- Management attention is focused on business value
- Creates a security awareness
- Business continuity is supported

Challenges

- Justify the expenses
- Keep procedures, policies up to date
- Maintain security awareness
- Create security rules at the right level

IT Service Continuity Management

Objective:

To support the overall Business Continuity Management process by ensuring that the required IT technical and service facilities can be recovered within required and agreed business time-scales.

Prerequisite: A Business Continuity Plan needs to be in place.

There is no use for IT continuity if the business is closed… 

Planning activities

Initiation

- Initiate BCM

Requirements and Strategy

- Business Impact Analysis
- Risk Assessment
- Business Continuity Strategy

Implementation

- Organisation and Implementation Planning
- Initiate B Implement Stand-by arrangements/ Risk Reduction Measures CM
- Develop Recovery Plans/Procedures
- Initial testing

Requirements and strategy

Determine the requirements based on:

- Business Impact analysis
- Risk assessment
- Business & IT Continuity strategy

Strategy: Determine and agree Risk Reduction measures and recovery options to support the requirements.

Recovery options must be considered for:

- People
- IT Services and their CI´s
- Critical support services (power…)
- Critical assets

Strategy

Manual Standby	
Cold Standby	*Gradual Recovery < 72 h* *Usually consisting of a shell or computer room space with minimum or little equipment already on the floor. Environmentals are usually in place but not activated.*
Warm Standby	*Intermediate Recovery 24h-72h* *Computing facility that has some equipment available although it may not be powered up and running. Some special equipment may need to be procured. Systems and applications have to be setup and installed.*
HOT Standby	*Immediate Recovery e.g. through alternative site* *Computing facility that matches your hardware / software / network requirements and is loaded with your operating system. The equipment is up and running at all times and normally, secondary backup sites are available.*
Reciprocal recovery	Mutual agreement, should be in written form

Read more on: http://www.sorm.state.tx.us/Risk_Management/Business_Continuity/rec_strategy.php

Operational activities

Education, training & awareness	Everybody must know what their role is, and what role to play during a crisis situation
Review & audit	Verify that the ITSCM plan is up to date
Testing	Test the plan under realistic circumstances, every 6 to 12 months
Change Management	Change the ITSCM plan
Assurance	Verify that the ITSCM process and documents meet business needs

Benefits / Challenges

Benefits

- Create risk awareness
- Marketing value - Better customer confidence and business relationship
- Enable business continuity from IT perspective

Challenges

- Gain management commitment
- To review and test the ITSCM plan, regularly
- To make the business decide on recovery options for IT Services
- Create an IT Recovery plan for each service – needs Service Catalog

Tool support

- Multi-vendor capability
- Effective Knowledge search for Incident, Problem and Known Error records
- Effective collision check with changes
- CAB meetings and decisions supported
- Standard integrations with other tools
- CMDB support to all modules
- Predefined measurements and presentations
- Predefined views
- Chat and mail integration
- Breaking down cases to tasks
- Workflow control of activities, approvals
- Service Catalogue on web-surface
- SLA control, warnings and breaches
- Role-based authorities and configurations

LEAN

LEAN

- Increase production effectivity
  - Cost
  - Timeliness
  - Resource

Waste, queue, transport

LEAN

1. ***Delay*** on the part of customers waiting for service, for delivery, in queues, for response, not arriving as promised. The customer's time may seem free to the provider, but when she takes custom elsewhere the pain begins.
2. ***Duplication***. Having to re-enter data, repeat details on forms, copy information across, answer queries from several sources within the same organization.
3. ***Unnecessary Movement***. Queuing several times, lack of one-stop, poor ergonomics in the service encounter.
4. ***Unclear communication***, and the wastes of seeking clarification, confusion over product or service use, wasting time finding a location that may result in misuse or duplication.
5. ***Incorrect inventory***. Being out-of-stock, unable to get exactly what was required, substitute products or services.
6. ***An opportunity lost to retain or win customers***, a failure to establish rapport, ignoring customers, unfriendliness, and rudeness.
7. ***Errors in the service transaction***, product defects in the product-service bundle, lost or damaged goods.
8. ***Service quality errors***, lack of quality in service processes.

LEAN – Value demand

Value Demand is the demand for service from customers, while Failure Demand is the demand caused by a failure to do something right for the customer.

Failure demand is thus demand that only exists because initial demand was not satisfied properly. For example, a large proportion of calls that call centers receive are either chasing down enquiries made earlier, or to correct earlier work that was not done properly.

As one of the key aims of "Lean" is to eliminate waste, Failure Demand represents an obvious type of waste in service organizations.

LEAN – Failure demand

Failure demand can also be defined as "the delivery or production of products and services downstream as a result of defects in the system upstream.

This would include administrative rework, audits, inspections and enquires. This non value-added work can account for the majority of administrative work performed.

By treating failure and value demand alike in statistical analysis, failure demand can give the quite false impression of greater productivity.

This merely reinforces the need to look at what is really going on, and ask why the service is being rendered.

LEAN – Waste

Defects	•Unauthorized system and application changes. •Substandard project execution.
Overproduction (overprovisioning)	•Unnecessary delivery of low-value applications and services.
Waiting	•Slow application response times. •Manual service escalation procedures.
Non-Value Added Processing	•Reporting technology metrics to business managers.
Transportation	•On-site visits to resolve hardware and software issues.
Inventory (excess)	•Underutilized hardware. •Multiple repositories to handle risks and control.
Motion (excess)	•Fire-fighting repeat problems within the IT infrastructure and applications.
Employee knowledge (unused)	•Failing to capture ideas/innovation. •Knowledge and experience retention issues.

Agile

The agile software development emphasizes on four core values.

1. Individual and team interactions over processes and tools
2. Working software over comprehensive documentation
3. Customer collaboration over contract negotiation
4. Responding to change over following a plan

Agile

Agile Model	Waterfall Model
•Agile method proposes incremental and iterative approach to software design	•Development of the software flows sequentially from start point to end point.
•The **agile process** is broken into individual models that designers work on	•The design process is not broken into an individual models
•The customer has early and frequent opportunities to look at the product and make decision and changes to the project	•The customer can only see the product at the end of the project
•Agile model is considered unstructured compared to the waterfall model	•Waterfall model are more secure because they are so plan oriented
•Small projects can be implemented very quickly. For large projects, it is difficult to estimate the development time.	•All sorts of project can be estimated and completed.
•Error can be fixed in the middle of the project.	•Only at the end, the whole product is tested. If the requirement error is found or any changes have to be made, the project has to start from the beginning
•Development process is iterative, and the project is executed in short (2-4) weeks iterations. Planning is very less.	•The development process is phased, and the phase is much bigger than iteration. Every phase ends with the detailed description of the next phase.

Agile

Agile Model	Waterfall Model
•Documentation attends less priority than software development	•Documentation is a top priority and can even be used for training staff and upgrade the software with another team
•Every iteration has its own testing phase. It allows implementing regression testing every time new functions or logic are released.	•Only after the development phase, the testing phase is executed because separate parts are not fully functional.
•In agile testing when an iteration end, shippable features of the product is delivered to the customer. New features are usable right after shipment. It is useful when you have good contact with customers.	•All features developed are delivered at once after the long implementation phase.
•Testers and developers work together	•Testers work separately from developers
•At the end of every sprint, user acceptance is performed	•User acceptance is performed at the end of the project.
•It requires close communication with developers and together analyze requirements and planning	•Developer does not involve in requirement and planning process. Usually, time delays between tests and coding

KANBAN

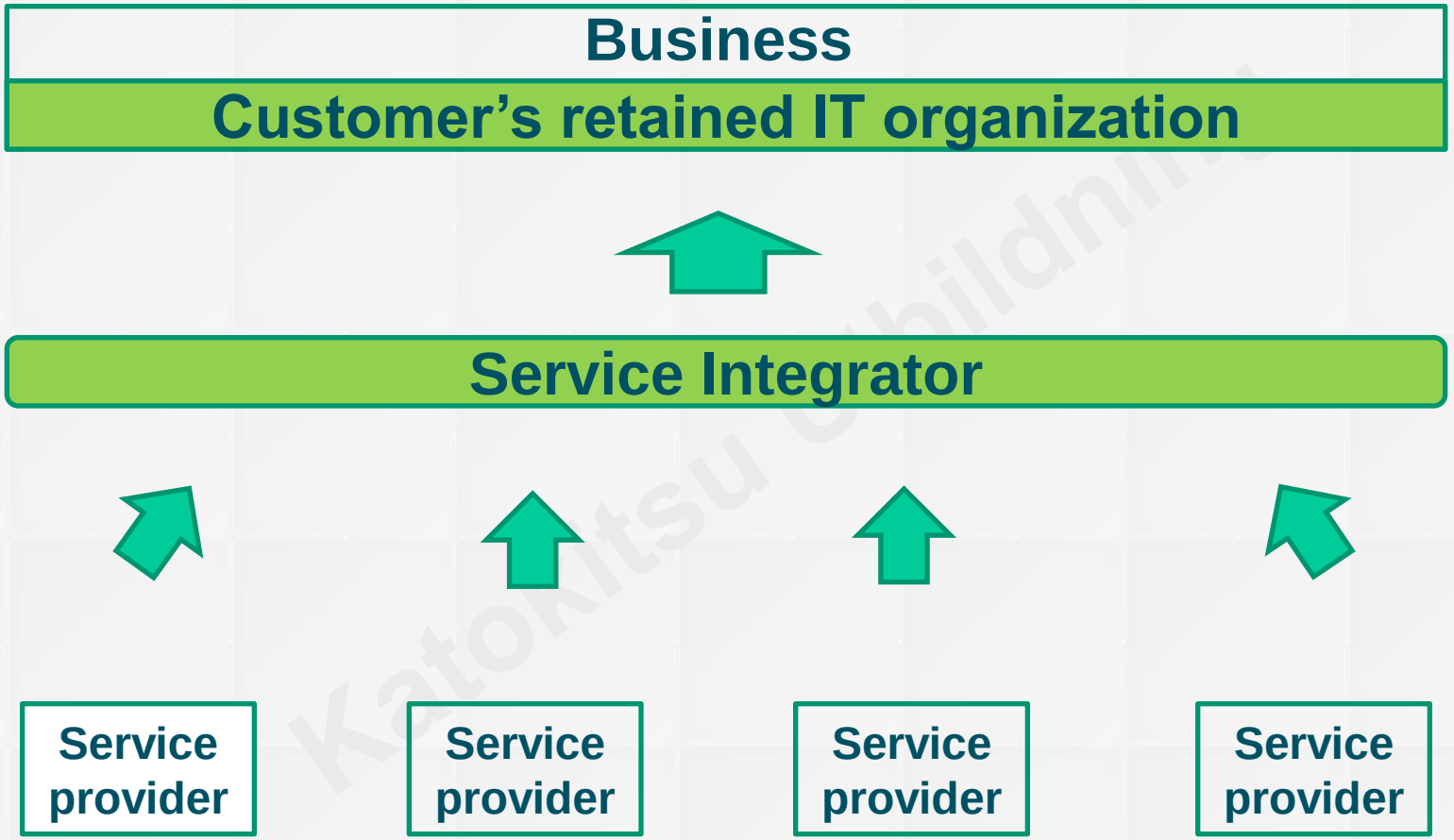
Devops

Wiki – “a set of practices intended to reduce the time between committing a change to a system and the change being placed into normal production, while ensuring high quality”

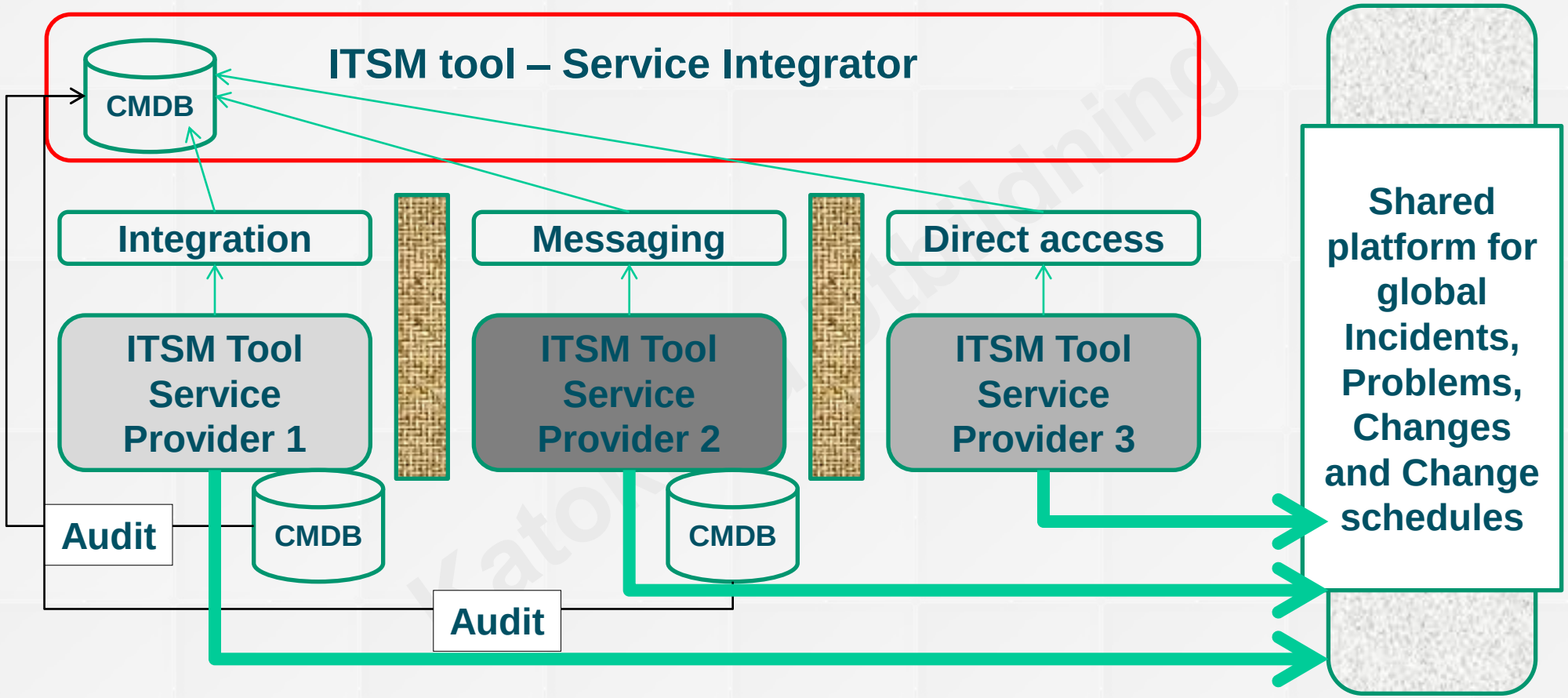
How:

-Automation
-Continuous integration
-Continuous testing
-Release automation
-Continuous delivery, including organizational changes, small and frequent changes, every deliverable is working on its own

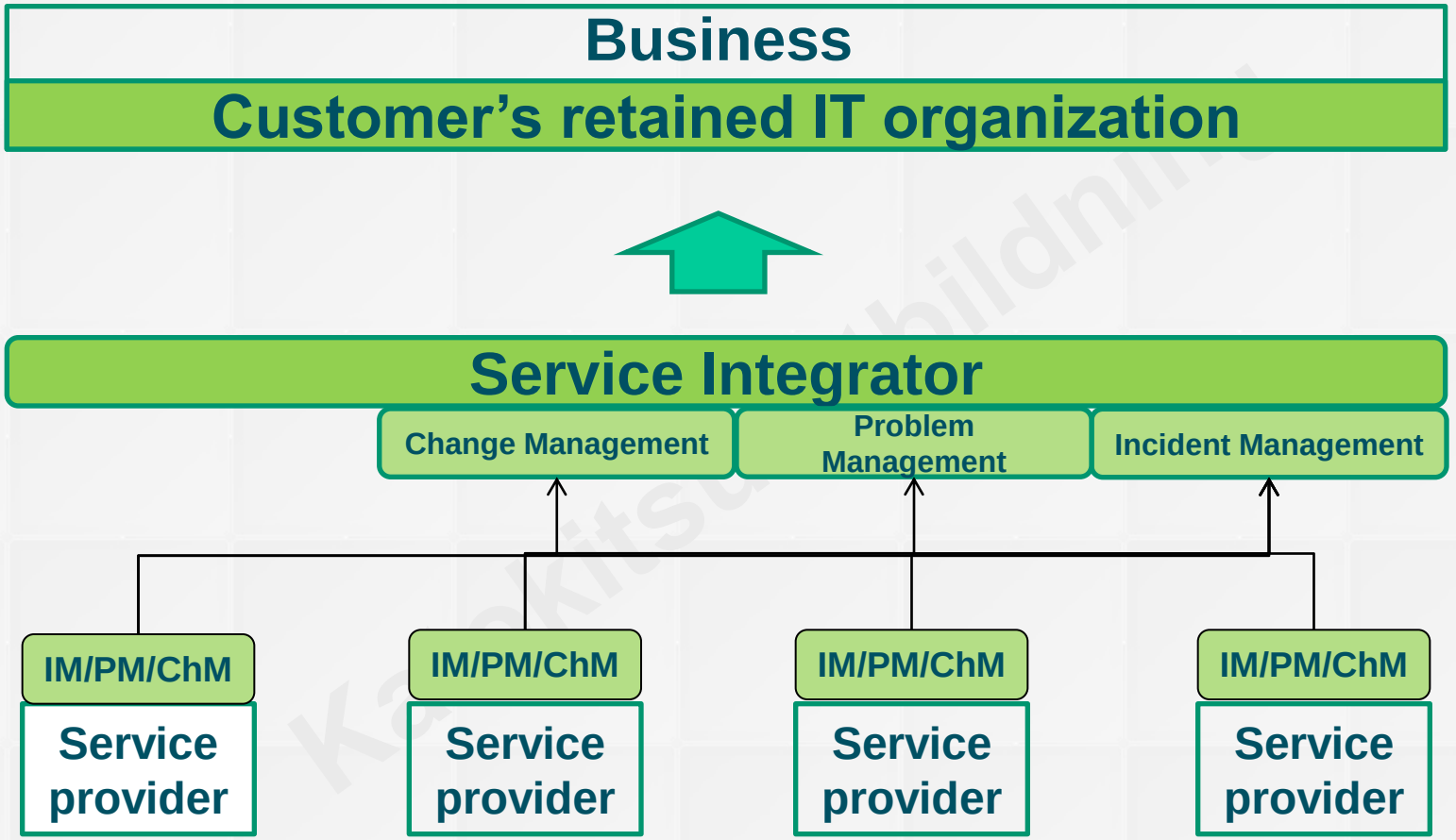
SIAM model



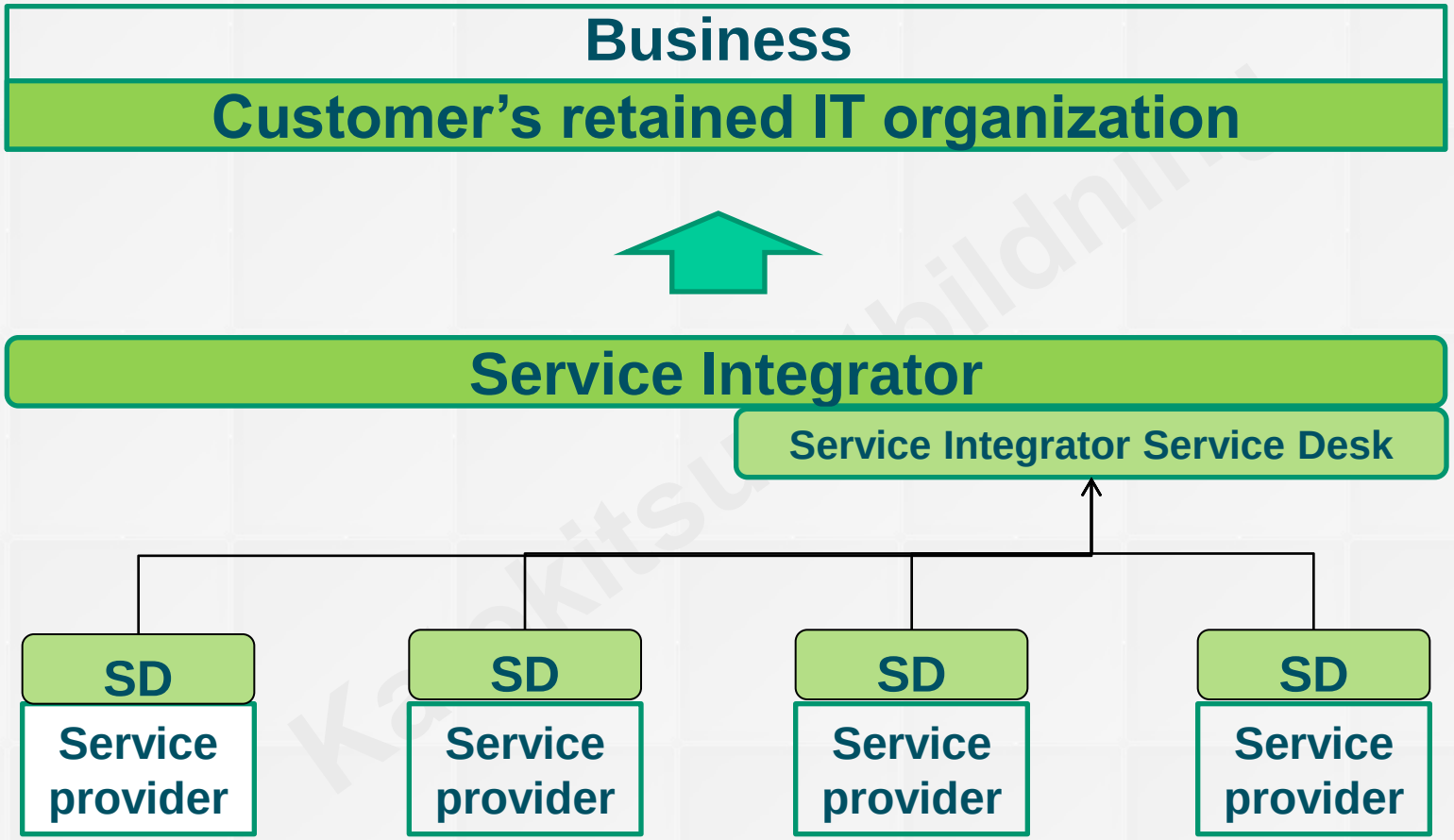
Multiple service providers - CMDB



Global SIAM functions



SIAM Global Service Desk



Release Management - SIAM

Release management

- Release planning and implementation needs to consider all the affected service providers, and the customer organization. This includes coordinating and scheduling releases to avoid negative impact
- **Responsibilities for testing integration between services from different service providers should be defined**
- There should be a consistent format and method for communicating information about releases

Knowledge Management – SIAM

Customer, Service Integrator and Service Provider roles

- The customer organization provides access to information to build a knowledge repository
  e.g. Business processes, stakeholders, business timetable
- **The service integrator documents the Knowledge management strategy and creates the repository. Creates guidelines and procedures on what, when and who can add information to it. Also, measures its use.**
- The service providers contributes, together with the service integrator / process forums.

Service providers might be reluctant to share information, specially with competitors

Security risk - SIAM

Commercially sensitive data might be shared inappropriately between service providers, and security tasks might be duplicated or not carried out at all

Tool support – challenges in SIAM model

The Customer owns the tool
The Customer funds any modifications and development of the tool. The Customer can place specific requirement on the tool's function.
Operations and maintenance of the tool may be outsourced to Service Integrator or to any other party.

The Service Integrator owns the tool
Funding of any modifications need to be negotiated between Service Integrator and Customer.
Changes in functionality may be limited, as the Service Integrator might use the same tool for several Customers.
May require Customer specific installation and operation.

One of the Service Providers owns the tool
Not recommended. The Service Provider may have visibility into other Service Providers' data.
Funding and modification requirements might meet unsolvable disputes.
Service Providers processes might not meet the process requirements from the Customer, thus the tool might not support the Customer's service management process

Agile, devops - SIAM

Agile, rapid, continuous changes might cause challenges on the service providers on several aspects:

- Costs
- Resource coordination
- Technical coordination
- ....

A SIAM model that includes segregation of duties and service elements split between multiple service providers can be in conflict with DevOps thinking

Course objectives

Have you…

- Learned about the IT Service Delivery and Support processes and activities and process management roles?
- Learned most everyday IT Service Management terminology?
- Learned about the relations to LEAN, Agile and Devops?
- Insight in the Service Integration and Management model challenges?

Reflect

Imagine a world in which the vast majority of us wake up inspired, feel safe at work and return home fulfilled at the end of the day.

Simon Sinek

Thank you!
This concludes the Everyday IT Service Management training course.

Contact: Josef Katkits, info@katokitsu.se
http://itilkonsulten.se