What is ITIL?

ITIL stands for

- Information Technology Infrastructure Library

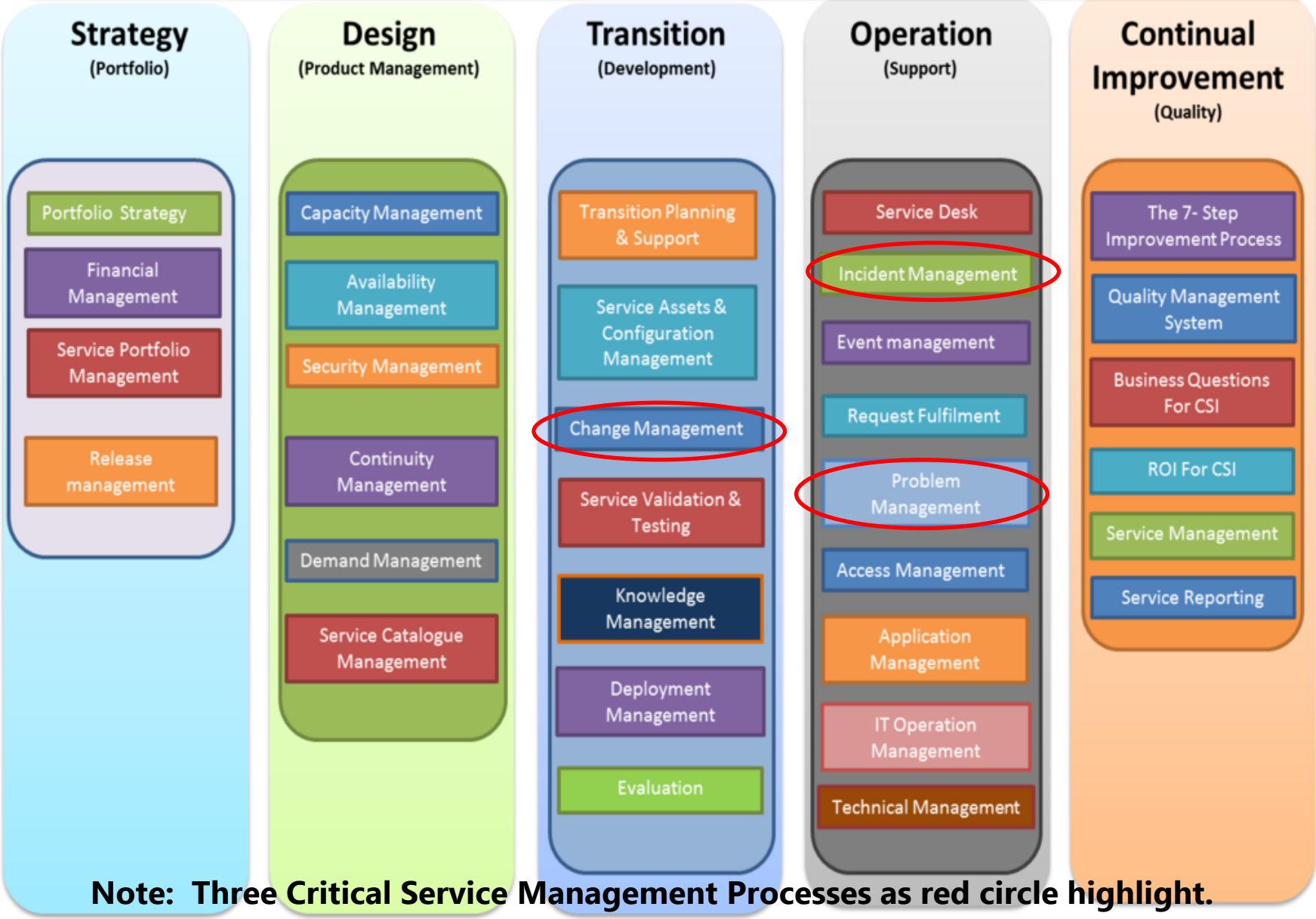
Scope

- A set of industry practices for IT service management (ITSM), including five domains :
  - Service Strategy
  - Service Design
  - Service Transition
  - Service Operation
  - Continual Service Improvement

Purpose

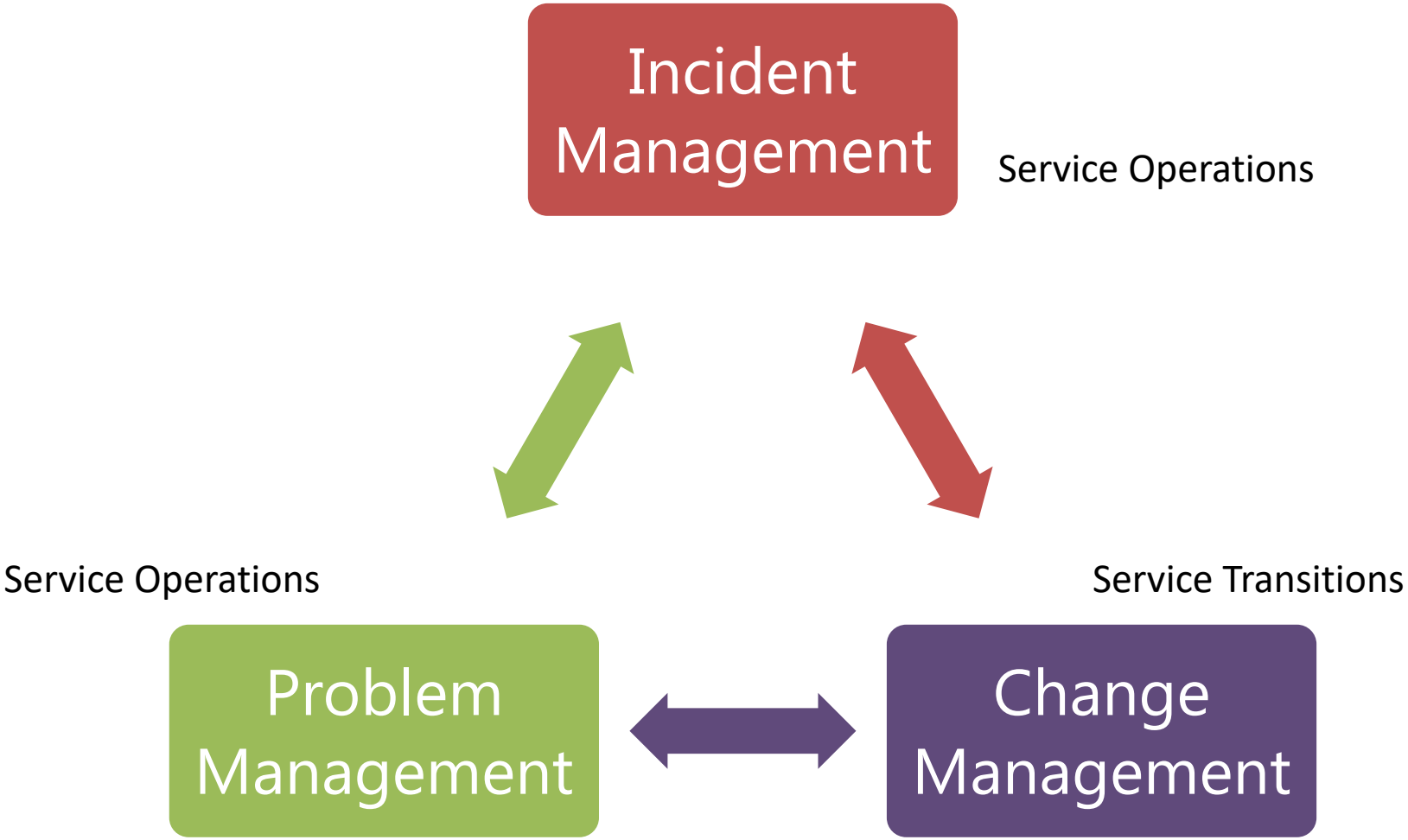
- Aligning IT services with the needs of business.

Processes of ITIL 5 Domains



Note: Three Critical Service Management Processes as red circle highlight.

Three Critical Service Management Processes



Incident Management

What is "Incident Management" ?

Incident

- An unplanned interruption to an IT service or reduction in the quality of an IT Service.
- Example: Printer failure

Purpose of Incident Management

- To restore normal service **as quickly as possible** and minimise the adverse effect on business operations
- Example: In the event of printer failure, IT provide another print queue or carry out immediate printer replacement

Where do Incidents come from?

1. **End users**

   Phone or email a service desk to report an issue that they are experiencing. **IT Service Desk operator** will:

   - gather information about the issue
   - prioritize the issue according to a predefined matrix
   - attempt to resolve it
   - assign it to a support (**Possibly you**) if IT Service Desk cannot resolve it

2. **Monitoring systems**

   Events or alerts that are used to warn us something might break and affect user service. A **monitoring agent** will create an alert when:

   - there is error detected about a service or activity.
   - there is alert threshold being reached.

Process of Incident Management

Incident is created.

- **IT Service Desk**

- Captures information.
- Prioritises the incident.
- Assign to Support team.

Validate and Respond to the Incident

- **Support Team**

- If this is not for me to fix, I will re-assign it and contact the Service Desk.
- Do I have what is needed?
- Assign to a team member.
- Acknowledge case.

Investigate Incident

- **Support Team**
- **User**

- Capture further information.
- Is there a workaround that can be used?
- Develop and execute action plan.
- Management Escalation as required.

Incident Restoration

- **Support Team**
- **User**

- Confirm the success of actions taken.
- Update case with actions taken to resume services.
- Update status of case to "Completed".

Incident closure

- **Service Desk**

- Closure activity is completed by the IT Service Desk.

What next

- **Support Team**

- Incident Reporting.
- Possible Problem management activity.

Key roles in Incident Management

Incident Manager

- Single point of accountability – Drives for timely incident resolution
- Management reporting during incident
- Authority to determine incident declaration and priority

Support teams

- Owner of incident
- Incident Investigation and diagnosis
- Service Recovery

Business Analyst

- Visibility and communication of major incidents to business

2.1 Clarified Incident Priority Definition

New	Definition	Example
S1	Financial, Reputation, Performance, Safety and Regulatory	• Outage of a system Performance during service period • All Operation not working during ticket sales Reputation • Incorrect $ in Public Financial report
S2	System Down	• Outage of a system during service period • Delay in transaction Reports
S3	System function failure with Noticeable Business Impact	• Outage of a system during non-service period • Operation Reporting function outage
S4	System function failure with Minor Business Impact	Individual user failed to print to printer ***"S" stands for Severity***

Notes on escalation

1. Outstanding S2 > 4 hours without resolution will be escalated to S1 (the actual effect is to escalate the reporting time from 60 min to 30 min for more attention)
2. S3 escalation is being handled by existing process of system notification to support manager. Outstanding S3 for overdue resolution time will be reviewed in weekly Incident / Problem review meeting

2.2 Standardized Escalation Procedures

No.	Step	Time		Action
1	Response to suspected S1/S2 incident	start		Operator
2	Determine S1/S2 incident and conduct initial impact assessment (note 1)	within **30** mins after step 1		Operator / Support Teams
		S1	**S2**	
3	If S1/S2 Incident, escalate to Incident Manager	within **15** mins after step 2	within **30** mins after step 2	Operator
4	Determine and escalate to Management Team and BPM (note 2)	within **15** mins after step 3		Incident Manager
5a	Update Management Team	at every **30** mins after step 4	at every **60** mins after step 4	Incident Manager
5b	Notify Business Users (note 3 & 4)	within **15** mins after step 4	within **30** mins after step 4	Business Analyst

Notes:

1. Operator will call 1st/2nd line support, and also call incident managers. Operator should have the mobile contact of ALL IT support members , and also got the vendor contact of ALL vendors with maintenance contract (including hardware, software, DB, middleware, SAN, VM, etc)
2. Incident Manager will instruct Operator to contact Business Analyst for notifying business users.
3. For Services incident, Incident Manager instruct Helpdesk to notify IT users.
4. Business Analyst should have the system owner/key user contact just in case they need to communicate with them.

Example of Service Level Target

Incident Response Target Example

Severity	Expected Response Time
1	15 mins
2	15 mins
3	30 mins
4	1 hour

Service Resume Target Example

Severity	Expected Service Resume Time
1	4 hours
2	4 hours
3	5 days
4	10 days

Update required on IM tool:

- Change the status of the incident from “Open” to “Work In Progress” within the relevant Service Level Target

Aim to resume as soon as possible
Update IM ticket status when done.

- Change the status of the incident from “Work In Progress” to “Completed” within the relevant Service Level Target

Key Points

1. RESUME service as soon as possible

2. Check recent CHANGES

3. COMMUNICATE Outage, Business Impact, and Estimated Time to resume service

Tips

1. All Incidents must be logged.
2. All Incidents will be classified with a priority based on the business impact and urgency.
3. All Incidents will be managed to minimise the impact of the service interruption.
4. Support Teams maintain ownership of the Incident until the end user agrees that the Incident has been resolved.
5. All Incident recovery actions and resolution detail must be documented in the toolset.
6. Communication on Incident and service interruptions must be made available to the appropriate audience including Post Incident analysis. (eg., Incident Reports)
7. Continually monitor and measure the quality of incidents; and distribution of detailed and accurate Incident reports.
8. Incident management process document has to be reviewed yearly to ensure its relevancy to the current situation.

Problem Management

What is “Problem Management” ?

Problem

- A cause of one or more incidents. The cause is not usually known at the time a problem record is created that needs further investigation
- Example: Printer failure caused by driver software bug

Purpose of Problem Management

- To resolve the **root causes** of incidents and thus to minimise the adverse impact of incidents and problems on business
- To **prevent recurrence** of incidents related to these errors.
- Take actions (changes) to implement resolution.

Difference between Incident and Problem

	Incident	Problem
Purpose	Analogy: "fire fighting" **Resolving** service outages or other Incidents as quickly as possible to ensure restoration of the service.	Analogy: " fire prevention" Implementing corrective actions that **eliminate the root cause** of the identified Problem and prevents Incidents from recurring.
Benefits	Getting users working again as quickly as possible.	• Reduce Incidents • Increase customer satisfaction • Decrease costs
Example	Pipe bursts & water is leaking **Workaround** • Putting tape across leak and the leaks stops.	What caused the leak? How to stop it from happening again? **Root Cause** • Poor pipe quality **Corrective Action** • Engage plumber to replace pipes with a higher quality pipe.

Problem Management Process

Identify Problem

- **Incident owner**
- **Incident Manager**
- **Problem Manager**

- Incident Owner creates problem ticket
- Problem Manager requests Incident owner to create Problem ticket
- Incident Manager requests Incident owner to create Problem ticket

Root Cause Analysis

- **Problem owner**
- **Problem Analyst**

- Work out why something isn't working (Root Cause)
- Document findings (with Known Error information)

Known Error

- **Problem Analyst**

- Document what is broken in the environment
- Document any quick fixes (work around)
- Document actions to fix the issue (Corrective Actions)

Corrective Action

- **Problem Analyst**
- **Support teams**

- Raise and relate Change requests
- Implement steps (Corrective Action) to address the issue (Root Cause)
- Update Corrective Actions in toolset

Review & Close Problem

- **Problem Owner**
- **Problem Manager**

- Confirm goal has been achieved with user
- Informs stakeholders work around is no longer required.
- Update/ Close Problem

Know Error

What is Known Error?

- Documented root cause and a workaround. It may be identified by developers or suppliers.

1. **Known Error Statement**
   Documents a fault that has been identified in the customers environment. This statement is typically written once root cause investigations have been completed.

2. **Workaround**
   Is a set of instructions that can be followed in the Incident process to quickly restore services for end users so they can get back to

3. **Corrective Actions**
   Are the steps we take to address the root cause of a Incident.

Example

A faulty RAM module has been identified in Email Server. This caused the Exchange server to halt intermittently and prevented email users from sending or receiving emails

Perform power cycle the Exchange server to restore services as quickly as possible. It has been raised to complete these power cycles while the Known Error is open.

Replace RAM module in Exchange Server.

Tips

1. For S1/S2 incident
   - Create problem ticket to investigate root cause according to KPI
   - Identify Root Cause for within 5 working days for S1 incident and 10 working days for S2 incidents.
2. Implement all the Corrective Actions by the agreed due date.
3. Document workaround for unknown Root Cause.
4. Provide your feedback of Problem management process to Problem manager for process improvement.

KPI and Trend

Incident / Problem Management KPI

Root Cause and Action Identified			
Type of Problem	**Service Target**	**KPI**	**Incident Report Required (Y/N)**
S1	Within 5 working days	100%	Y*
S2	Within 10 working days	>=90%	Y*
Proactive **	Within 30 working days	>=80%	N

Problem Closure		
Type of Problem	**Service Target**	**KPI**
S1	Within 30 working days	100%
S2	Within 60 working days	>=90%
Proactive **	Within 90 working days	>=80%

Incident Volume	
Type of Incident	**KPI**
S1	<= 4
	<= 20 hours of service outage
S2, S3 and S4	Year on year Incident volume reduction by 10%

* Incident Report with suspected/final root cause identified with corrective/preventive action(s)

** Proactive problem can be derived from repetitive S3 / S4 incidents, lesson learnt from project, alerts, etc.

Problem Management – Root Cause Analysis S1/S2

Unavoidable (HW/SW issue)

- ❑ Incident due to software bug or hardware issue.

3rd Party

- ❑ 3rd party vendor or department performed change without notifying IT.

Change

- ❑ Performed change in business hours.
- ❑ Batch job was not tested thoroughly.
- ❑ Business impact of the change was not considered in detail.

Monitoring

- ❑ Unable to monitor some of the transaction when it was halted or abnormal.

DO and DON'T

#	DOs	DON'Ts
1	Restore service is the top priority and try to preserve evidence for RCA if possible.	Keep investigating the root cause while there is service outage.
2	Escalate to Incident Manager immediately if business impact is high or unknown.	Troubleshoot issue without escalating to Incident Manager.
3	Perform change in non-office hour or systems' maintenance window to minimise business impact.	Perform change in office hour which may cause business impact.
4	Provide concise and accurate incident information such as business impact and the resolution progress to Incident Manager who will then provide regular update to management team.	Focus only on troubleshooting and no communication on incident information.
5	Start with the following 3 actions when incident happens: 1. Any standard recovery procedure for the issue? 2. Any Change implemented? Fallback? 3. Restart the service if there is no clear evidence on what component is wrong	Keep troubleshooting without reviewing the recent change list at the first place.

DO and DON'T

#	DOs	DON'Ts
6	Follow proper process to request for : • Password of privilege account • Emergency change for incident resolution	Perform unauthorised change and improper use of privilege account during incident resolution.
7	Detail verification is required before acceptance of all sorts of resilience including power sources for hardware and equipment.	Accept hardware and equipment without detail verification.
8	Contingency site still needs to be considered even pending for project to revamp the system.	Wait until the revamp project complete on the system and do not have contingency plan on how to recover the system in case any issue.
9	DR should be considered as a service restoration option. Team should prepare to trigger DR in parallel if the production service cannot be resumed in a foreseeable period of time.	Wait until all service recovery methods failed to start the DR preparation

Change Management

What is “Change Management” ?

Change

- The addition, modification or removal of anything that could have an effect on IT services..
- Example: System upgrade, server retirement

Purpose of Change Management

- To **control** all changes, enabling beneficial changes to be made within **minimum disruption** to IT services
- To **protect** from the effects of unintended impacts as a result of our actions

Change Lifecycle

Create Change → **Change Assessed** → **Build / Test Change** → **Authorize Change** → **Coordinate Change Implementation** → **Review & Close Change**

- **Change Owner**

- Complete required fields and templates in the toolset.
- Provide both technical information and business areas affected.

- **Change Owner**

- Internal, Peer review
- Ensure Accuracy in the Change record

- **Change Owner**

- All Changes need a Test / Verification Plan
- Does the plan accurately represent what is required?

- **Change Manager**
- **CAB**

- Review the Change plan and relevant supporting materials including UAT sign off
- Approve or Reject Change

- **Change Implementer**

- Ensure CHG is fully approved
- Stick to change window
- Stick to the documented plan

- **Change Owner**
- **Change Manager**

- Complete Post Verification
- Invoke back out plan if required
- Initial PIR for fail change
- Update / Close record

Phase of Change Implementation

Phase	Requirements
Before implementation	Verify the Change record is fully approved
During implementation	Confirm that the expected outcomes have occurred (e.g. health-check running after server reboot).
After implementation	Review 1. verify the change as having met objectives 2. verify the change did not cause any adverse impact 3. record results in the Change record

Types of Change

Type of Change	Comment
Standard	Standard Changes must go through the Minor Change Process at least once and registered (approved) in the standard change library. Standard Change must meet the following criteria: • Low Risk • Repeatable • With procedure in place for the change execution Standard Changes are pre-approved and not discussed in the CAB meeting.
Minor	No business impact, Low priority changes typically repeated and well known implementation procedures (pre-defined standard changes in Change Models)
Major	For project initiation. Change that has high risk and impact and can potentially cause Incident on IT services / applications
Emergency (Urgent)	Emergency change for urgent incident fix. This change requires ECAB approval. Although the change record is allowed to be created retrospectively, the change steps and test still need to be done where applicable.

Change Reviews

Change Advisory Board

- A group of people that support the assessment, prioritization, authorization and scheduling of changes.

KPI Target

KPI	KPI Target
# of unauthorized change detected	**0**
% of Change Success Rate	**>=99%**
# of change causing incident	**0**
% of change request closed on-time	**>=90%**

KEY

Never commence implementing a Change until the Change record is **fully approved**

Change Management

- Must Have Information:
  - Change Title
  - Change Reason
  - Change Description
  - Change Start and End Date
  - Change Implementation Plan with Health check and failback Plan
  - Maintenance Message where there is a downtime

Failed Change

A Failed Change is :

1. A Change induces incident during change implementation, verification or when the change take effects (e.g. night batch)
2. A **fallback procedure** is executed to restore the original system state

Post Implementation Review (PIR)

- Change Manager calls for a PIR when there is a failed change
- Change Owner needs to submit the PIR report
- PIR focuses on reviewing the reason and root cause of the failed changes
- PIR is a must before change owner resubmits the same change request

Unauthorized Change

An Unauthorized Change is any change made to production IT environment without a fully compliant Change record

How are Unauthorized Changes identified?

The most obvious way of detecting an unauthorized change is when there has been an impact to a customers environment resulting in a high severity incident.

Unauthorized changes are also being detected (even where no impact is experienced) by regular review and auditing of change activity by the Change Management team.

Unauthorized Changes may lead to disciplinary actions.

Tips

1. Never implement a change without proper approval or it will become an unauthorized change.
2. Follow change management process and change record needs to be created and updated in toolset
3. Classify the change according to the risk assessment and change categorization decision tree and follow the appropriate process flow and lead time to raise your change request.
4. Ensure emergency changes only applies to urgent incident fix or urgent business critical requirement and have to go through proper approval
5. Document the failed change and go through post implementation review meeting
6. Change Management team needs to ensure change management process and relevant materials are stored and communicated the changes to all stakeholders
7. Change Management team needs to ensure change management process have a regular review to ensure its relevancy to the current situation (at least once a year)