IT INFRASTRUCTURE MANAGEMENT

UNIT-2

Availability/ ITSCM/ Security Testing Schedule

- A schedule for the regular testing of all availability, continuity and security mechanisms, jointly maintained by Availability, **IT Service Continuity** and Information Security Management.

Business Continuity Strategy

- An outline of the approach to ensure the continuity of Vital Business Functions in the case of disaster events. The Business Continuity Strategy is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy.

Disaster Recovery Invocation Guideline

- A document produced by IT Service Continuity Management with detailed instructions on when and how to invoke the procedure for fighting a disaster. Most importantly, the guideline defines the first steps to be taken by 1st Level Support after learning that a (suspected) disaster has occurred.

Index of Disaster-Relevant Information

- A catalogue of all information that is relevant in the event of disasters. This document is maintained and circulated by IT Service Continuity Management to all members of IT staff with responsibilities for fighting disasters.

IT Service Continuity Report

- The IT Service Continuity Report is created at regular intervals and provides other Service Management processes and IT Management with information related to disaster prevention.

IT Service Continuity Plan

- IT Service Continuity Plans underpin the ITSCM Strategy, describing how continuity is ensured for specific disaster events and services. It specifies the measures to enhance the resilience of services and describes how to effectively respond to a disaster event. ITSCM Plans usually include references to more detailed Recovery Plans with specific instructions for returning systems to a working state.

IT Service Continuity Strategy

- The IT Service Continuity Strategy contains an outline of the approach to ensure the continuity of vital services in the case of disaster events. It includes a list of Vital Business Functions and applied risk reduction or recovery options. The IT Service Continuity Strategy should be based on a Business Continuity Strategy. The ITSCM Strategy is underpinned by more detailed ITSCM Plans, describing how continuity is ensured for specific disaster events and services.

Recovery Plan

- Recovery Plans are created mainly by Availability and IT Service Continuity Management. The plans contain detailed instructions for returning specific services and/or systems to a working state, which often includes recovering data to a known consistent state.

Test Report

- A Test Report provides a summary of testing and assessment activities. A Test Report is created for example during Release tests in the Service Transition stage or during tests carried out by Availability, **IT Service Continuity** or Information Security Management.

2. Capacity management

Business Capacity Management

- Process Objective: To translate business needs and plans into capacity and performance requirements for services and IT infrastructure, and to ensure that future capacity and performance needs can be fulfilled.

Service Capacity Management

- Process Objective: To manage, control and predict the performance and capacity of operational services. This includes initiating proactive and reactive action to ensure that the performances and capacities of services meet their agreed targets.

Component Capacity Management

- Process Objective: To manage, control and predict the performance, utilization and capacity of IT resources and individual IT components.

Capacity Management Reporting

- Process Objective: To provide other Service Management processes and IT Management with information related to service and resource capacity, utilization and performance (see "Capacity Report").

Capacity Management Information System

- A virtual repository of all Capacity Management data, usually stored in multiple physical locations.

Capacity Plan

- A Capacity Plan is used to manage the resources required to deliver IT services. The plan contains scenarios for different predictions of business demand, and costed options to deliver the agreed service level targets. *(see: ITIL Checklist Capacity Plan)*

Capacity Report

- The Capacity Report provides other Service Management processes and IT Management with information related to service and resource utilization and performance.

3. Availability management

Availability Design Guidelines

- The Availability Design Guidelines define from a technical point of view how the required availability levels can be achieved, including specific instructions for application development and for externally sourced infrastructure components.

Availability Guidelines for the Service Desk

- Rules produced by Availability Management on how to manage Incidents causing unavailability, to prevent minor Incidents from becoming major Incidents.

Availability Management Information System

- A virtual repository of all Availability Management data, usually stored in multiple physical locations.

Availability Plan

- The Availability Plan contains detailed information about initiatives aimed at improving service and/ or component availability.

Availability/ ITSCM/ Security Testing Schedule

- A schedule for the regular testing of all availability, continuity and security mechanisms, jointly maintained by **Availability**, IT Service Continuity and Information Security Management.

Availability Report

- The Availability Report provides other Service Management processes and IT Management with information related to service and infrastructure component availability.

4. Configuration management

1. CM Planning and Management: a formal document and plan to guide the CM program that includes items such as:
   - Personnel
   - Responsibilities and resources
   - Training requirements
   - Administrative meeting guidelines, including a definition of procedures and tools
   - Baselining processes
   - Configuration control and configuration-status accounting
   - Naming conventions
   - Audits and reviews
   - Subcontractor/vendor CM requirements
2. Configuration Identification (CI): consists of setting and maintaining baselines, which define the system or subsystem architecture, components, and any developments at any point in time. It is the basis by which changes to any part of a system are identified, documented, and later tracked through design, development, testing, and final delivery. CI incrementally establishes and maintains the definitive current basis for Configuration Status Accounting (CSA) of a system and its configuration items (CIs) throughout their lifecycle (development, production, deployment, and operational support) until disposal.
3. Configuration Control: includes the evaluation of all change-requests and change-proposals, and their subsequent approval or disapproval. It covers the process of controlling modifications to the system's design, hardware, firmware, software, and documentation.

4. Configuration Status Accounting: includes the process of recording and reporting configuration item descriptions (e.g., hardware, software, firmware, etc.) and all departures from the baseline during design and production. In the event of suspected problems, the verification of baseline configuration and approved modifications can be quickly determined.
5. Configuration Verification and Audit: an independent review of hardware and software for the purpose of assessing compliance with established performance requirements, commercial and appropriate military standards, and functional, allocated, and product baselines. Configuration audits verify that the system and subsystem configuration documentation complies with the functional and physical performance characteristics before acceptance into an architectural baseline.

5. Incident management

Incidents within a structured organization are normally dealt with by either an incident response team (IRT), or an incident management team (IMT). These are often designated beforehand or during the event, and are placed in control of the organization whilst the incident is dealt with, to restore normal functions.

Usually as part of the wider management process in private organizations, incident management is followed by post-incident analysis where it is determined why the incident happened despite precautions and controls. This analysis is normally overseen by the leaders of the organization, with the view of preventing repetition of the incident through precautionary measures and often changes in policy. This information is then used as feedback to further develop the security policy and/or its practical implementation. In the United States, the National Incident Management System, developed by the Department of Homeland Security, integrates effective practices in emergency management into a comprehensive national framework. This often results in a higher level of contingency planning, exercise and training, as well as an evaluation of the management of the incident.[9]

Computer security incident management

Main article: Computer security incident management

Today, an important role is played by a Computer Security Incident Response Team (CSIRT), due to the rise of internet crime, and is a common example of incident faced by companies in developed nations all across the world. For example, if an organization discovers that an intruder has gained unauthorized access to a computer system, the CSIRT would analyze the situation, determine the breadth of the compromise, and take corrective action. Computer forensics is one task included in this process. Currently, over half of the world's hacking attempts on Trans National Corporations (TNCs) take place in North America (57%). 23% of attempts take place in Europe.[8] Having a well-rounded Computer Security Incident Response team is integral to providing a secure environment for any organization, and is becoming a critical part of the overall design of many modern networking teams.

6. Problem Management

Objective: *Problem Management* aims to manage the lifecycle of all Problems. The primary objectives of this ITIL process are to prevent Incidents from happening, and to minimize the impact of incidents that cannot be prevented. 'Proactive Problem Management' analyzes Incident Records, and uses data collected by other IT Service Management processes to identify trends or significant Problems.

Proactive Problem Identification

- Process Objective: To improve overall availability of services by proactively identifying Problems. Proactive Problem Management aims to identify and solve Problems and/or provide suitable Workarounds before (further) Incidents recur.

Problem Categorization and Prioritization

- Process Objective: To record and prioritize the Problem with appropriate diligence, in order to facilitate a swift and effective resolution.

Problem Diagnosis and Resolution

- Process Objective: To identify the underlying root cause of a Problem and initiate the most appropriate and economical Problem solution. If possible, a temporary Workaround is supplied.

Problem and Error Control

- Process Objective: To constantly monitor outstanding Problems with regards to their processing status, so that where necessary corrective measures may be introduced.

Problem Closure and Evaluation

- Process Objective: To ensure that - after a successful Problem solution - the Problem Record contains a full historical description, and that related Known Error Records are updated.

Major Problem Review

- Process Objective: To review the resolution of a Problem in order to prevent recurrence and learn any lessons for the future. Furthermore it is to be verified whether the Problems marked as closed have actually been eliminated.

Problem Management Reporting

- Process Objective: ITIL Problem Management Reporting aims to ensure that the other Service Management processes as well as IT Management are informed of outstanding Problems, their processing-status and existing Workarounds (see "Problem Management Report").

7. Change Management

Change management for project management

Change management plays an important role in project management because each change request must be evaluated for its impact on the project. Project managers, or the senior executives in charge of change control, must examine how a change in one area of the project could affect other areas and what impact that change could have on the project as a whole. Project areas that change control experts should pay particular attention to include the following:

- **Scope.** Change requests must be evaluated to determine how they will affect the project scope.
- **Schedule.** Change requests must be assessed to determine how they will alter the project schedule.
- **Costs.** Change requests must be evaluated to determine how they will affect project costs. Labor is typically the largest expense on a project, so overages on completing project tasks can quickly drive changes to the project costs.
- **Quality.** Change requests must be evaluated to determine how they will affect the quality of the completed project. An acceleration of the project schedule, in particular, can affect quality as defects can occur if work is rushed.
- **Human resources.** Change requests must be evaluated to determine if additional or specialized labor is required. When the project schedule changes, the project manager may lose key resources to other assignments.

- **Communications.** Approved change requests must be communicated to the appropriate stakeholders at the appropriate time.
- **Risk.** Change requests must be evaluated to determine what risks they pose. Even minor changes can have a domino effect on the project and introduce logistical, financial or security risks.
- **Procurement.** Changes to the project may affect procurement of materials and contract labor.