DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
2300/12
CP

From: Commandant of the Marine Corps

Subj: ENTERPRISE INFORMATION TECHNOLOGY SERVICE MANAGEMENT AVAILABILITY MANAGEMENT PROCESS GUIDE

Ref: (a) MCO 5271.1B

Encl: (1) IRM-2300-12 Enterprise Information Technology Service Management Availability Management Process Guide

1. PURPOSE. The purpose of the Enterprise Information Technology Service Management (ITSM) Availability Management Process Guide is to establish a documented and clear foundation for process implementation and execution across the Marine Corps Enterprise Network (MCEN). Process implementation and execution at lower levels (e.g., Regional, Local and Programs of Record) must align and adhere to directives and schema documented within this guide. The use of this guide enables USMC Information Technology (IT) activities through promoting standardization of work instructions and operating procedures across a continuum of document specificity.

2. CANCELLATION. N/A.

3. AUTHORITY. The information promulgated in this publication is based upon policy and guidance contained in reference (a).

4. APPLICABILITY. This publication is applicable to the Marine Corps Total Force.

5. SCOPE.

a. Compliance. Compliance with the provisions of this publication is required unless a specific waiver is authorized.

b. Waivers. Waivers to the provisions of this publication will be authorized by the Director, Command, Control, Communications and Computers.

6. SPONSOR. The sponsor of this technical publication is HQMC C4 CP.

K. J. NALLY
Brigadier General
U.S. Marine Corps
Director, Command, Control,
Communications and Computers (C4)

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

DISTRIBUTION: PCN 18623001200

Enterprise IT Service Management
Availability Management
Process Guide

Release Date:
06 August 2014

Document Approval / Major Revision Change History Record

This table is used for initial release and subsequent revisions. Major revisions are indicated by the number to the left of the decimal point while minor revisions are indicated by the number to the right. Major revisions are required when the intent or process is changed rendering the prior version obsolete or when the number of minor releases total twenty (20). Changes to this document shall be recorded, described and approved using the table below:

Release Date (MM/DD/YY)	Release No.	Approvals		Change Description
		Author	Process Owner/Approver	
06/05/2014	0.1		Robert Argodale	Initial Draft
		Printed Name	Printed Name	
08/06/2014	1.0		Robert Argodale	Initial Release
		Printed Name	Printed Name	
	1.1			
		Printed Name	Printed Name	
	2.0			
		Printed Name	Printed Name	
	3.0			
		Printed Name	Printed Name	
	4.0			
		Printed Name	Printed Name	
	5.0			
		Printed Name	Printed Name	
	6.0			
		Printed Name	Printed Name	
	7.0			
		Printed Name	Printed Name	

Table of Contents

Section Title Page

List of Tables

List of Figures

1.0 INTRODUCTION

1.1 Purpose

The purpose of this process guide is to establish a documented and clear foundation for process implementation and execution across the Marine Corps Enterprise Network (MCEN). Process implementation and execution at lower levels (e.g., Regional, Local, and Programs of Record) must align and adhere to directives and schema documented within this guide. The use of this guide enables USMC IT activities through promoting standardization of work instructions and operating procedures across a continuum of document specificity as represented in Figure 1-1.

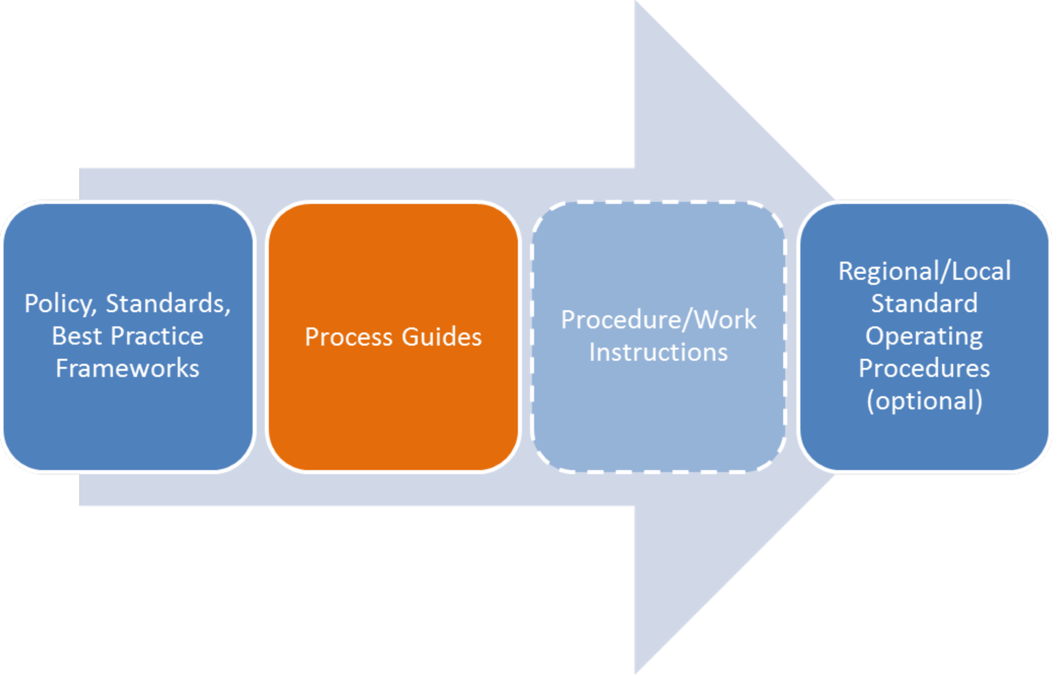
Policy, Standards, Best Practice Frameworks
Process Guides
Procedure/Work Instructions
Regional/Local Standard Operating Procedures (optional)

Figure 1-1. Process Document Continuum

1.2 Scope

The scope of this document covers all services provided in support of the MCEN for both the Secret Internet Protocol Router Network (SIPRNET), and the Non-Secure Internet Protocol Router Network (NIPRNET). Information remains relevant for the global operations and defense of the Marine Corps Enterprise Network (MCEN) as managed by Marine Corps Network Operations and Security Center (MCNOSC) including all Regional Network Operations and Security Centers (RNOSC) and Marine Air Ground Task Force Information Technology Support Center (MITSC) assets and supported Marine Expeditionary Forces (MEF), Supporting Establishments (SE) organizations, and Marine Corps Installation (MCI) commands.

Table 1-1 depicts the various layers of document design. Each layer has discrete entities, each with their own specific authority when it comes to promulgating documentation. This enterprise process operates at Level B, sub processes such as procedures and work instructions are not included within the scope of this document.

Table 1-1. Document Design Layers

	ENTITIES	DOCUMENTS GENERATED
LEVEL A	Federal Govt DoD DoN CMC/HQMC	Statutes/Laws DoD Issuances DoN Policies Marine Corps Orders/IRMS
LEVEL B	HQMC C4 MCNOSC MCSC	MCOs IRMs (Process Guides) Directives MARADMINS
LEVEL C	RNOSC MITSC	Regional Procedures Work Instructions
LEVEL D	MCBs POSTS STATIONS	Locally Generated SOP’s

1.3 Process and Document Control

This document will be reviewed semi-annually for accuracy by the Process Owner with designated team members. Questions pertaining to the conduct of the process should be directed to the Process Owner. Suggested Changes to the process should be directed to USMC C4 CP in accordance with MCO 5271.1 Information Resource Management (IRM) Standards and Guidelines Program.

2.0 PROCESS OVERVIEW

2.1 Purpose, Goals, and Objectives

The purpose of the Availability Management (AvM) process is to ensure that the level of availability delivered in all IT services meets the agreed availability needs and/or service level targets in a cost effective and timely manner. Availability Management is concerned with meeting both the current and future availability needs of the USMC.

The scope of the AvM process covers the design, implementation, measurements, management and improvement of IT service and component availability.

The objectives of AvM include:

- Ensuring that service availability meets agreed targets by managing services and resource-related availability performance.
- Providing advice and guidance to other process areas on availability issues.
- Assisting with the diagnosis and resolution of availability related incidents and problems.
- Ensuring proactive measures are implemented to improve the availability of cost justified services improve the availability of services.
- Producing, maintaining, and publishing an Availability Plan that addresses current and future availability needs.
- Assessing the impact of changes on the Availability Plan and the performance and capacity of services and resources.

2.2 Relationships with other Processes

Many of the E-ITSM processes are interrelated. AvM ensures the confidentiality, integrity, availability, authenticity, and non-repudiation of information is managed effectively across the enterprise and supports and interfaces with other processes. While any one of the E-ITSM processes can operate in the presence of an immature process, the efficiency and effectiveness of each is greatly enhanced by the maturity and integration of all E-ITSM processes.

Figure 2-1 depicts key relationships and dependencies that exist between the AvM process and current E-ITSM processes. These processes underpin the USMC near-term objectives. Note, Figure 2-1 is not all-encompassing and the relationships shown can de direct or indirect.

2.2.1 Relationships with other Processes

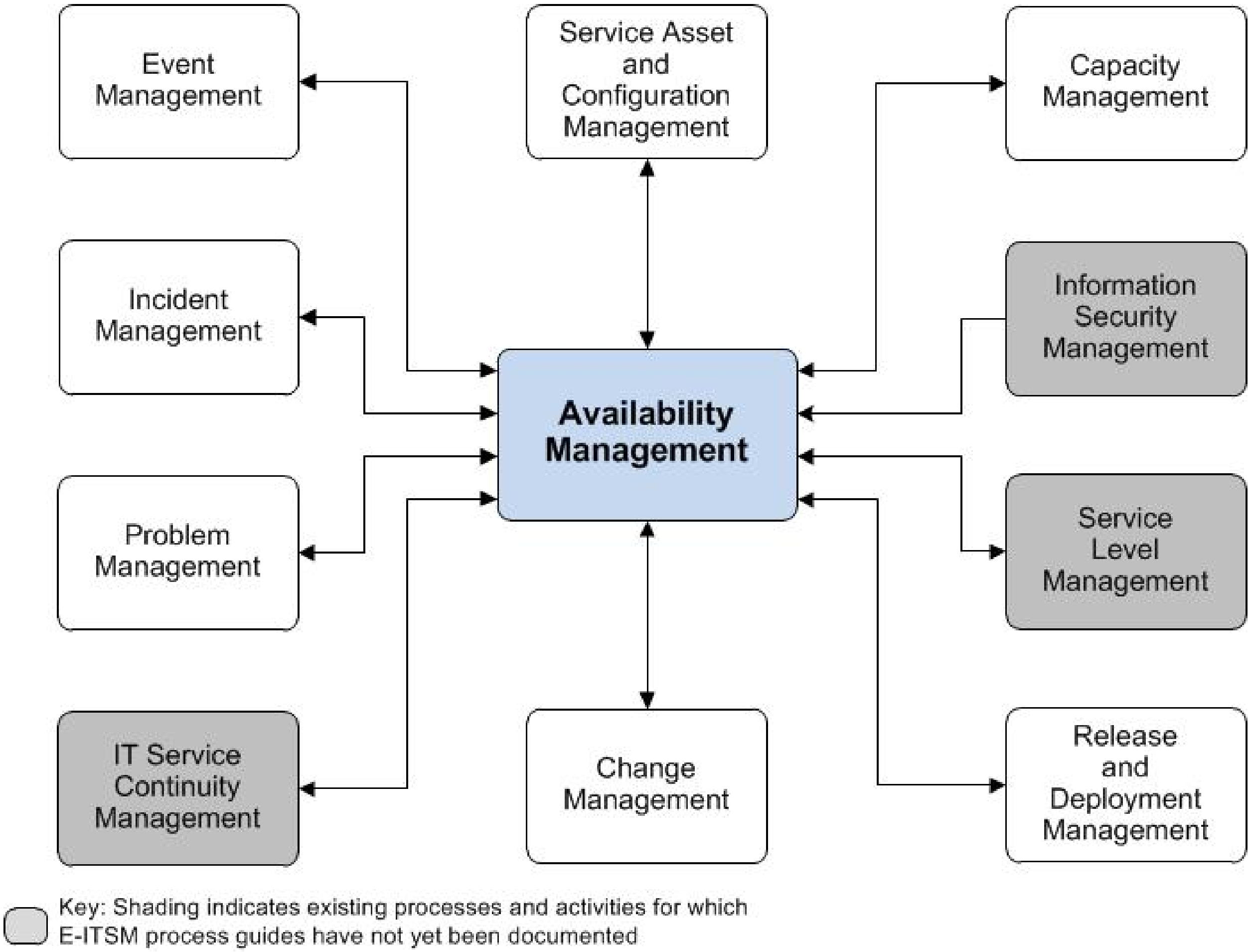
Event Management
Service Asset and Configuration Management
Capacity Management
Incident Management
Information Security Management
Availability Management
Problem Management
Service Level Management
IT Service Continuity Management
Change Management
Release and Deployment Management
Key: Shading indicates existing processes and activities for which E-ITSM process guides have not yet been documented

Figure 2-1. AvM Relationships with E-ITSM Processes

The following highlights the inputs and outputs regarding the relationship between the AvM process and other E-ITSM processes as shown in Figure 2-1.

Capacity Management

Provides to Availability Management

- Capacity Plan: Capacity Management provides Availability Management the Capacity Plan, showing how capacity plans support availability requirements.
- Performance data: Capacity Management provides Availability Management with performance data, including information on performance degradation.

Receives from Availability Management

- Service Availability Plan: Availability Management provides Capacity Management availability, maintainability, and serviceability guidance, including availability techniques deployed to meet documented Service Level Agreements for IT infrastructure components.

- Incident Trend Analysis: Availability Management provides Capacity Management data on availability incident trends.

Service Level Management

Provides to Availability Management

- Service level Requirements (SLRs): Service Level Management provides SLRs to Availability Management for use in baseline reports and assessing compliance.
- Service level Agreements (SLAs), Operational Level Agreements (OLAs) and Underpinning Contracts (UCs): Service Level Management provides SLAs, OLAs and UCs to Availability Management for use in baseline reports and assessing compliance.

Receives from Availability Management

- Service level Agreement (SLA) Development Support: Availability Management provides information to Service Level Management in support of the development of SLAs, including, but not limited to service design recommendations and cost/value data
- Availability Plan: Availability Management provides a plan for proactive improvement to Service Level Management
- Availability Reports: Availability Management provides service availability, reliability and maintainability reports of achievements against targets to Service Level Management

Change Management

Provides to Availability Management

- Proposed Request for Change (RFC): Change Management provides proposed RFCs to Availability Management for assessment
- Updated Request for Change (RFC): Change Management provides RFC updates to Availability Management. This would include status changes such as RFC implementation or backout, and updates to anticipated impacts.
- Change Schedule: Change Management provides the change schedule to Availability Management. This schedule provides anticipated RFC implementation dates.

Receives from Availability Management

- RFC Assessments: Availability Management provides Change Management assessments of impacts that might affect capacity or the ability to achieve expected service levels.
- RFCs: Availability Management provides Capacity RFCs to Change Management.

IT Service Continuity Management

Provides to Availability Management

- Service Continuity Strategy: IT Service Continuity Management provides the continuity strategy to Availability Management to support development of the Availability Plan.

- Service Continuity Design: IT Service Continuity Management provides the continuity design to Availability Management

Receives from Availability Management

- RFC Availability Evaluations: Availability Management provides IT Service Continuity Management with anticipated availability impacts of RFCs to allow the impact on IT Service Continuity Management plans to be assessed
- Availability plan: Availability Management provides the Availability plan to IT Service Continuity Management to reduce risk and to provide minimum agreed service levels.

Problem Management

Provides to Availability Management

- Problem: Problem Management provides problem information to Availability Management for analysis. This may include Known Error information.

Receives from Availability Management

- Availability Reports: Availability Management provides availability data to Problem Management to support investigation of problems
- Availability status and recommendations: Availability management analyses problems, and returns capacity status and recommendations for resolving the problem.

Incident Management

Provides to Availability Management

- Incident: Incident Management provides incident information to Availability Management for analysis.

Receives from Availability Management

- Incident Diagnosis and Recovery Options: Availability Management diagnosis assistance and recovery options to assist in the Incident investigation.
- Availability Reports: Availability Management provides availability data to Incident Management to support investigation of incidents.

Event Management

Provides to Availability Management

- Availability Event: Event Management provides Availability Management with information regarding events that indicate availability alerts or threshold breaches. (The events reported will be dependent upon the ability of the tools to identify the conditions that we would want to observe.)

Receives from Availability Management

- Availability Alert Thresholds: Availability Management provides Event Management with recommendations and guidance related to availability thresholds, based upon the Availability Management understanding of trends and service levels. This guidance includes alert and alarm levels, and recommended response actions.

Configuration Management Database

Provides to Availability Management

- Configuration Data: The CMDB provides Configuration Data (including capacity data) for Configuration Items to Availability Management. This data may be used to support growth estimates based on the CMDB.

Release and Deployment Management

Provides to Availability Management

- Release Plan: Release and Deployment Management provides to Availability Management, prior to rollout, for analysis of availability needs and capabilities.
- Testing Performance Metrics: Release and Deployment Management provides to Availability Management performance metrics recorded during testing.

Receives from Availability Management

- Release Availability Assessment: Availability Management provides Release and Deployment Management an assessment of the availability requirements of a planned release.
- Systems Engineering Technical Review (SETR) participation: Availability Management provides representation on SETR review boards

Information Security Management

Provides to Availability Management

- Security Measures and Policy: Information Security Management provides Availability Management security measures and policies that need to be included in the service design for availability and recovery.

2.3 High-Level Process Model

The Availability Management process ensures that the availability of systems and services matches the evolving agreed needs of the United States Marine Corps. The availability and reliability of IT services can directly influence successful completion of the Marine Corps mission as well as support of the warfighter. Availability management is essential in ensuring that IT delivers the levels of service availability required by the Marine Corps to satisfy its mission objectives and to deliver the quality of service demanded.

The Availability Management process, as with Capacity Management, must be involved in all stages of the Service Lifecycle, from Strategy and Design, through Transition and Operation to Improvement. The appropriate availability and resilience should be identified and documented in Service Strategy, and designed into services and components from the initial design stages. This will ensure not only that the availability of any new or changed service meets its expected targets, but also that existing services and components continue to meet their targets. This is the basis of stable service provisioning.

The following diagram, Figure 2-2, illustrates the Design and Operations activities of AvM, and their interaction with the Availability Management Information System (AMIS).

See Section 2.5 for complete descriptions of the activities.

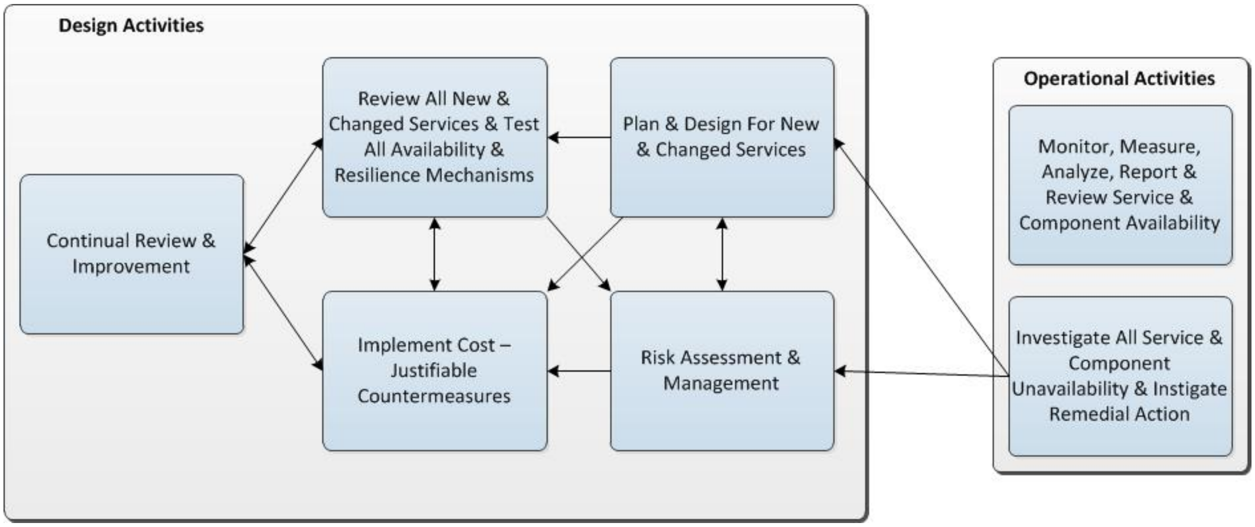
Design Activities
Review All New & Changed Services & Test All Availability & Resilience Mechanisms
Plan & Design For New & Changed Services
Continual Review & Improvement
Implement Cost – Justifiable Countermeasures
Risk Assessment & Management
Operational Activities
Monitor, Measure, Analyze, Report & Review Service & Component Availability
Investigate All Service & Component Unavailability & Instigate Remedial Action

Figure 2-2. High-Level AvM Workflow

2.3.1 Availability Management Process Description

The Availability Management (AvM) process aims to ensure that all operational services meet their agreed availability targets, and that new or changed services are designed appropriately to meet their intended targets, without compromising the performance of existing services. In order to achieve this, AvM performs the Design and Operational activities illustrated in Figure 2-2.

The proactive activities consist of producing recommendations, plans and documents on design guidelines and criteria for new and changed services, and the continual improvement of service and reduction of risk in existing services wherever it can be cost-justified. These are key aspects to be considered within Service Design activities.

The reactive activities of AvM consist of monitoring, measuring, analyzing, reporting and reviewing all aspects of component and service availability. This is to ensure that all agreed service targets are measured and achieved. Wherever deviations or breaches are detected, these are investigated and remedial action instigated. Most of these activities are conducted within the Operations stage of the lifecycle and are linked into the monitoring and control activities, Event and Incident Management processes.

Table 2-1 below contains descriptions of each activity.

Table 2-1. Availability Management Activity Descriptions

Type	Activity	Description
Design	Plan and Design for New and Changed Services	New or changes to existing services are designed appropriately to meet the customer's availability-related requirements, defined in service level targets.
Design	Risk Analysis and Measurement	Determining the impact arising from IT service and component failure in conjunction with ITSCM and, where appropriate, reviewing the availability design criteria to provide additional resilience to prevent or minimize impact to the business.
Design	Implement Cost-Justifiable Countermeasures	Appropriate risk reduction and recovery mechanisms are developed to address the risks identified to service and component availability.
Design	Review all New and Changed Services and Test All Availability and Resilience Mechanisms	During the Service Transition stage, all the elements designed to contribute to service and component availability are regularly reviewed and tested are to ensure that promised levels of availability will be delivered.
Design	Continual Review and Improvement	Regular review of design and supporting technology to enhance availability levels as criticality of service changes. This allow for producing and maintaining an availability plan that prioritizes and plans IT availability improvements.
Operational	Monitor, measure, analyze, report and review service and component availability	Once deployed and operational, probes, tools, and techniques are employed to monitor and measure component and service availability for the business and to the user. Data collected is analyzed to ensure requirements and targets are achieved and reported to the appropriate management.
Operational	Investigate service and component unavailability and instigate remedial action	If an outage or unavailability occurs, it is investigated usually with assistance from incident management and problem management and remedial action taken to restore component and service availability.

2.4 Key Concepts

The following key concepts are utilized extensively in the AvM Process.

2.4.1 Commander's Critical Information Requirements

Commander's Critical Information Requirements (CCIR) is the commander's "need to know immediately" information and response requirements. From MCWP 3-40.2 Information Management, "CCIR are tools for the commander to reduce information gaps generated by uncertainties that he may have concerning his own force, the threat, and/or the environment. They define the information required by the commander to better understand the battle-space, identify risks, and to make sound, timely decisions in order to retain the initiative. CCIR focus the staff on the type and form of quality information required by the commander, thereby reducing information needs to manageable amounts." In the context of Capacity Management, CCIRs would include, but not be limited to, capacity failures, which are a basis for hierarchical escalations.

All commands are required to produce command specific CCIR guidance with detailed ITSM requirements and are required to adhere to the current CCIR guidance of their superior commands. Common CCIR categories are Enterprise Service Management, Network Defense, Content Management, and MCEN, but others may be applicable based upon the commander's requirements.

2.4.2 Configuration Item

A Configuration Item (CI) is a component or service asset that needs to be managed in order to deliver an IT service. Information about each CI is recorded in a configuration record within the Configuration Management System and is maintained throughout its lifecycle by SACM. CIs are under the control of Change Management. CIs may vary widely in complexity, size, and type, ranging from an entire service or system including all hardware, software, documentation, and support staff to a single software module or a minor hardware component. CIs may be grouped and managed together.

2.4.3 Component

Component is a general term for one part of something more complex. Components that need to be managed are Configuration Items.

2.4.4 Configuration Management Database

The Configuration Management Database (CMDB) is a database used to manage configuration records throughout their lifecycle. The Configuration Management Database records the attributes of each Configuration Item, and its relationships with other Configuration Items. A Configuration Management Database may also contain other information linked to Configuration Items, for example Incident, Problem or Change Records.

2.4.5 Incident

An Incident is an unplanned interruption to an IT Service or reduction in the Quality of an IT Service. Any event which could affect an IT Service in the future is also an Incident.

2.4.6 Problem

A Problem is the unknown cause (undiagnosed root cause) of one or more incidents. Each Problem Record documents the lifecycle of a single problem.

2.4.7 Service Level Agreement

A Service-Level Agreement (SLA) is an agreement between an IT service provider and a customer. The SLA describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single SLA may cover multiple IT services or multiple customers.

2.4.8 Availability

Availability is the measurement of the ability of a Configuration Item or IT service to perform its agreed upon function during its agreed upon service time. Availability is determined by reliability, maintainability, serviceability, performance, and security. Availability is usually calculated as a percentage, usually based on Agreed Service Time (AST) and downtime. Availability is generally defined, monitored, measured and reported as service availability or component availability.

Service availability is often more difficult to measure than component availability. Service Availability is frequently calculated based on the availability of the components that support the service. The desired or required service availability is defined in the Service Level Requirements and in Service Level Agreements.

Component availability is the availability of a configuration item. When component availability can be monitored by a tool, availability can be well monitored and measured. Component availability must support the service availability targets.

Availability must be designed into a service solution, providing that solution with agreed upon availability characteristics; fault tolerance, high availability, continuous operation and continuous availability.

2.4.8.1 Reliability

Reliability is a measure of how long a service, component or Configuration Item (CI) can perform its agreed function without interruption. The reliability of a service can be improved by increasing the reliability of individual component or by increasing the resilience of the service to component failure (i.e., increasing the component redundancy by using load-balancing techniques).

2.4.8.2 Maintainability

Maintainability is a measure of how quickly and effectively a Configuration Item or IT service can be restored to normal working after a failure. Maintainability is often measured as Mean Time to Restore Service (MTRS).

2.4.8.3 Serviceability

Serviceability is the ability of a third-party supplier to meet the terms of its contract. The contract includes agreed levels of reliability, maintainability or availability for a Configuration Item.

2.4.8.4 Resilience

Resilience is the ability of a Configuration Item or IT service to resist failure or to recover quickly following a failure.

2.4.8.5 High availability

High availability is an approach or design that minimizes or hides the effects of Configuration Item failure on the users of an IT service. High availability solutions are designed to achieve an agreed level of availability and make use of techniques such as fault tolerance, resilience and fast recovery to reduce the number of incidents and the impact of incidents.

2.4.8.6 Fault tolerance

Fault tolerance is the ability of an IT service, component, or Configuration Item (CI) to continue to operate correctly after failure of one or more component parts. Generally any performance decrease is proportional to the severity of the failure. Fault tolerance allows a system or service to continue to perform its function, possibly with reduced performance, rather than failing completely, when a component fails. The reduced performance may be exhibited in an increase in response time, or a reduction in throughput, or some other performance degradation.

2.4.8.7 Continuous operation

Continuous operation is an approach or design to avoid planned downtime. This requires a means to perform necessary maintenance while services remain available. Continuous operation does not necessarily provide high or continuous availability because there may be unplanned outages.

2.4.8.8 Continuous availability

Continuous availability is an approach to design to eliminate any downtime from any cause, with the goal of achieving 100% availability. It combines the characteristics of high availability and continuous operation to keep services available with no noticeable downtime.

2.4.9 Availability Management Information System

The Availability Management Information System (AMIS) is a set of tools, data and information used to support Availability Management. It is the repository of all Availability Management data. An AMIS may exist within each managed data center.

2.5 Availability Management Activities

The Availability Management process includes the design, implementation, measurement, management and improvement of IT service and component availability. Availability Management needs to understand the service and component availability requirements from the mission or business perspective in terms of the:

- Current mission and business processes, their operation and requirements
- Future mission and business plans and requirements
- Service targets and the current IT service operation and delivery
- IT infrastructure, data, applications and environment and their performance
- Mission and business impacts and priorities in relation to the services and their usage.

Understanding all of this will enable Availability Management to ensure that all the services and components are designed and delivered to meet their targets in terms of agreed business needs.

The Availability Management process is continually working to ensure that all operational services meet their agreed availability targets, and that new or changed services are designed appropriately to meet their intended targets, without compromising the performance of existing services. In order to achieve this, Availability Management should perform the proactive and reactive activities illustrated in Figure 2-3.

The proactive activities of Availability Management address proactive planning, design and improvement of availability. These activities produce recommendations, plans and design guidelines and criteria for new and changed services. They result in the continual improvement of service and reduction of risk in existing services wherever it can be cost-justified. These activities are principally conducted within the Service Design stage of the lifecycle and are linked into Engineering during solution design to ensure availability and continuity requirements are both documented and tested prior to deployment. AvM Design activities also develop, document and publish the Availability Plan, which describes how to achieve the desired availability levels.)

The reactive activities of Availability Management consist of monitoring, measuring, analyzing, reporting and reviewing all aspects of component and service availability. This includes assessing all events, incidents and problems involving unavailability. When deviations or breaches are detected, these are investigated and remedial action instigated. Most of these activities are conducted within the Service Operations stage of the lifecycle and are linked into the monitoring and control activities, Event and Incident Management processes. The objective of these activities is to ensure that all agreed service targets are measured and achieved.

Availability Management continually looks for opportunities to optimize the availability of the IT infrastructure in conjunction with Continual Service Improvement activities. The benefit of this regular review approach is that enhanced levels of availability may be achievable, but with much lower costs. The optimization approach is a logical first step to delivering better value for money. A number of Availability Management techniques can be applied to identify optimization opportunities.

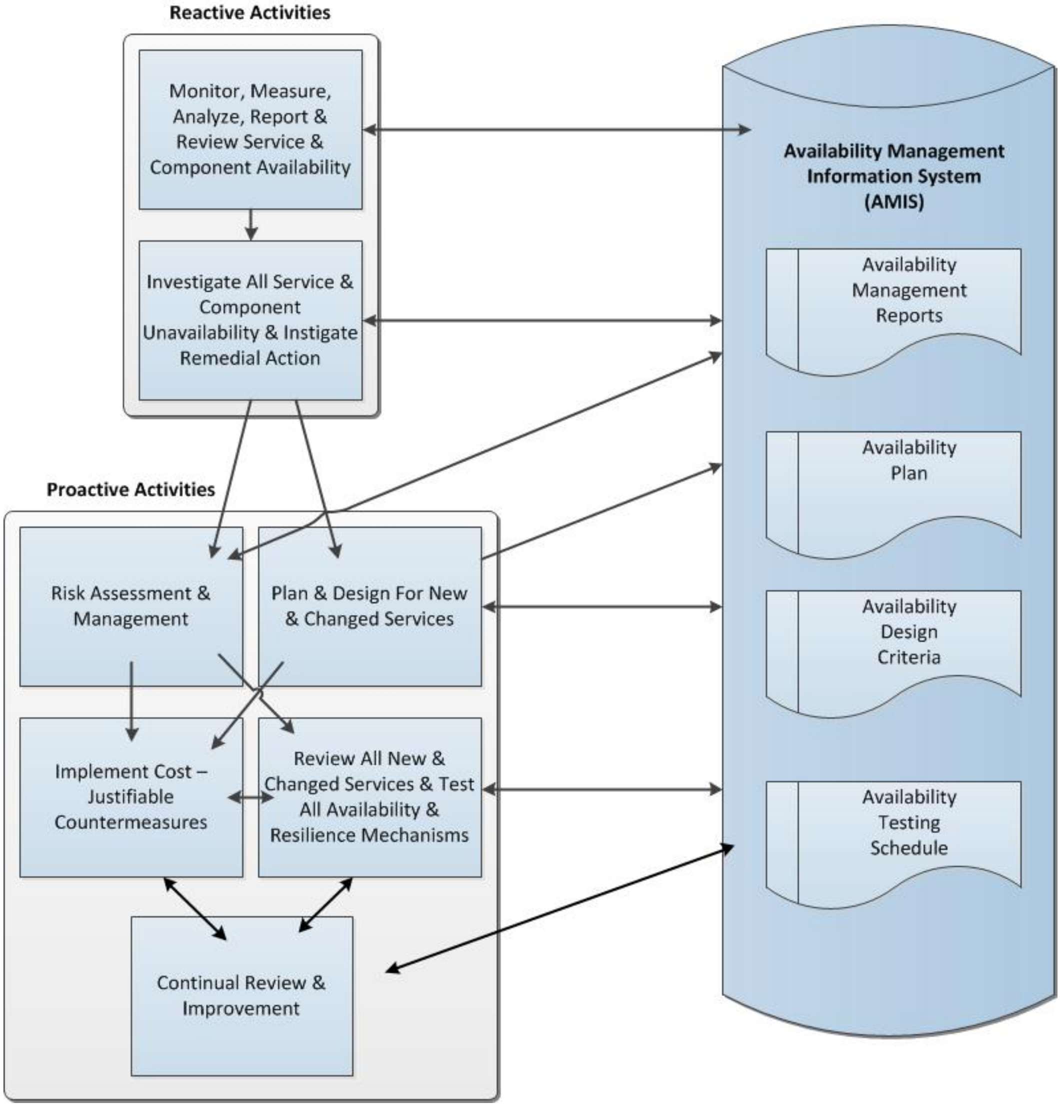
Reactive Activities
Monitor, Measure, Analyze, Report & Review Service & Component Availability
Investigate All Service & Component Unavailability & Instigate Remedial Action
Proactive Activities
Risk Assessment & Management
Plan & Design For New & Changed Services
Implement Cost – Justifiable Countermeasures
Review All New & Changed Services & Test All Availability & Resilience Mechanisms
Continual Review & Improvement
Availability Management Information System (AMIS)
Availability Management Reports
Availability Plan
Availability Design Criteria
Availability Testing Schedule

Figure 2-3. Availability Management Activities and Outputs

2.5.1 Design Activities

Where new and changed IT services are being developed, it is essential that Availability Management takes an early and participating design role in determining the availability requirements. This enables Availability Management to influence positively the IT infrastructure design to ensure that it can deliver the level of availability required. The importance of this participation early in the design of the IT infrastructure cannot be underestimated. There needs to be a dialogue between IT and the business to determine the balance between the business perception of the cost of unavailability and the exponential cost of delivering higher levels of availability.

2.5.1.1 Plan and Design for New and Changed Services

Availability Management translates the mission's need for IT availability into quantifiable availability targets and conditions. This is an important input into the IT Service Design and provides the basis for assessing the capability of the IT design and IT support organization to meet the availability requirements of the mission. The greatest level of availability should be included in the design of those services supporting the most critical of the Vital Business Functions (VBF). A Vital Business Function is used to reflect the business critical elements of the business process supported by an IT service. The service may also support less critical business functions and processes, and it is important that the VBFs are recognized and documented to provide the appropriate business alignment and focus.

Ideally, the mission requirements for IT availability should contain at least:

- Vital Business Functions supported by the IT service
- Definition of Service Downtime (the conditions under which the USMC considers the IT service to be unavailable)
- The mission impact caused by loss of service, together with the associated risk
- Quantitative availability requirements (the extent to which the mission tolerates IT service downtime or degraded service)
- The required service hours (when the service is to be provided)
- An assessment of the relative importance of different working periods
- Specific security requirements
- The service backup and recovery capability.

At the present time, a limited selection of the availability requirements defined for a service may be measureable. Initial metrics will be focused on component availability requirements and their associated metrics. As the AvM process matures, additional metrics will be developed and added to the availability reports.

Determining the availability requirements is an iterative process, especially balancing the mission and business availability requirements against the associated costs. The necessary steps are:

- Determine the mission impact caused by loss of service
- From the mission requirements, specify the availability, reliability and maintainability requirements for the IT service and components supported by the IT support organization

- For IT services and components provided externally, identify the serviceability requirements
- Estimate the costs involved in meeting the availability, reliability, maintainability and serviceability requirements
- Determine, with the mission, if the costs identified in meeting the availability requirements are justified
- Determine, from the mission, the costs likely to be incurred from loss or degradation of service
- Where these are seen as cost-justified, define the availability, reliability, maintainability and serviceability requirements in agreements and negotiate into contracts.

If costs are seen as prohibitive, either:

- Reassess the IT infrastructure design and provide options for reducing costs and assess the consequences on availability; or
- Reassess the business use and reliance on the IT service and renegotiate the availability targets within the SLA.

Availability Management needs to ensure that the design activity for availability looks at the task from two related, but distinct, perspectives:

- **Designing for availability:** The technical design of the IT service covering all aspects of technology, including infrastructure, environment, data and applications to meet the availability requirements of the business.
- **Designing for recovery:** Ensures that in the event of an IT service failure, the service and its supporting components can be reinstated to enable normal business operations to resume as quickly as is possible.

The ability to recover quickly may be crucial. It may not be possible or cost justified to build a design that is highly resilient to failure(s). The ability to meet the availability requirements within the cost parameters may rely on the ability to recover in a timely and effective manner.

The contribution of Availability Management within the design activities is to provide:

- The specification of the availability requirements for all components of the service
- The requirements for availability measurement points (instrumentation)
- The requirements for new/enhanced systems and Service Management
- Assistance with the IT infrastructure design
- The specification of the reliability, maintainability and serviceability requirements for components supplied by internal and external suppliers
- Validation of the final design to meet the minimum levels of availability required by the business for the IT service.

If the availability requirements cannot be met, the next task is to re-evaluate the Service Design and identify cost justified design changes. Improvements in design to meet the availability requirements can be achieved by reviewing the capability of the technology to be deployed in the proposed IT design. For example:

- The exploitation of fault-tolerant technology to mask the impact of planned or unplanned component downtime
- Duplexing, or the provision of alternative IT infrastructure components to allow one component to take over the work of another component
- Improving component reliability by enhancing testing regimes
- Improved software design and development
- Improved processes and procedures
- Systems management enhancements/exploitation
- Improved externally supplied services, contracts or agreements
- Developing the capability of the people with more training.

Component Failure Impact Analysis (CFIA) can be used to predict and evaluate the impact on IT service arising from component failures within the technology. The output from a CFIA can be used to identify where additional resilience should be considered to prevent or minimize the impact of component failure to the mission operation and users.

This is particularly important during the Service Design stage, where it is necessary to predict and evaluate the impact on IT service availability arising from component failures within the proposed IT Service Design. This technique can also be applied to existing services and infrastructure. It is recommended that CFIA be used to reflect the full scope of the IT infrastructure, i.e. hardware, network, software, applications, data centers and support staff. Additionally the technique can also be applied to identify impact and dependencies on IT support organization skills and competencies amongst staff supporting the new IT service. This activity is often completed in conjunction with ITSCM and possibly Capacity Management.

The output from a CFIA provides vital information to ensure that the availability and recovery design criteria for the new IT service is influenced to prevent or minimize the impact of failure to the mission operation and users. CFIA achieves this by providing and indicating:

- Single Points of Failure that can impact availability
- The impact of component failure on the mission operation and users
- Component and people dependencies
- Component recovery timings
- The need to identify and document recovery options
- The need to identify and implement risk reduction measures.

A Single Point of Failure (SPoF) is any component within the IT infrastructure that has no backup or fail-over capability, and has the potential to cause disruption to the mission, customers or users when it fails. It is important that no unrecognized SPoFs exist within the IT infrastructure design or the actual technology, and that they are avoided wherever possible.

The use of SPoF analysis or CFIA as techniques to identify SPoFs is recommended. SPoF and CFIA analysis exercises should be conducted on a regular basis, and wherever SPoFs are identified, CFIA can be used to identify the potential mission, customer or user impact and help determine what alternatives can or should be considered to cater for this weakness in the design or the actual infrastructure. Countermeasures should then be implemented wherever they are cost-justifiable. The impact and disruption caused by the potential failure of the SPoF should be used to cost-justify its implementation.

Fault Tree Analysis (FTA) is a technique that can be used to determine the chain of events that causes a disruption to IT services. FTA, in conjunction with calculation methods, can offer detailed models of availability. This can be used to assess the availability improvement that can be achieved by individual technology component design options. Using FTA:

- Information can be provided that can be used for availability calculations
- Operations can be performed on the resulting fault tree; these operations correspond with design options
- The desired level of detail in the analysis can be chosen.

FTA distinguishes the following events:

- **Basic events** – terminal points for the fault tree, e.g. power failure, operator error. Basic events are not investigated in great depth. If basic events are investigated in further depth, they automatically become resulting events.
- **Resulting events** – intermediate nodes in the fault tree, resulting from a combination of events. The highest point in the fault tree is usually a failure of the IT service.
- **Conditional events** – events that only occur under certain conditions, e.g. failure of the air-conditioning equipment only affects the IT service if equipment temperature exceeds the serviceable values.
- **Trigger events** – events that trigger other events, e.g. power failure detection equipment can trigger automatic shutdown of IT services. These events can be combined using logic operators, i.e.:
- **AND-gate** – the resulting event only occurs when all input events occur simultaneously
- **OR-gate** – the resulting event occurs when one or more of the input events occurs
- **Exclusive OR-gate** – the resulting event occurs when one and only one of the input events occurs
- **Inhibit gate** – the resulting event only occurs when the input condition is not met

Modeling will allow you to assess if new components within a design can match the stated requirements, it is important that the testing regime instigated ensures that the availability expected can be delivered. Inputs to the modeling process include descriptive data of the component reliability, maintainability and serviceability. This information can then be used to forecast user demand for the new IT system to ensure components continue to operate under anticipated volume and stress conditions.

2.5.1.2 Risk Analysis and Measurement

Risk Analysis and Management is used to identify and quantify risks and justifiable countermeasures that can be implemented to protect the availability of IT systems. The identification of risks and the provision of justified countermeasures to reduce or eliminate the threats posed by such risks can play an important role in achieving the required levels of availability for a new or enhanced IT service. Risk Analysis is done during the design phase for the IT technology and service to identify:

- Risks that may incur unavailability for IT components within the technology and Service Design
- Risks that may incur confidentiality and/or integrity exposures within the IT technology and Service Design.

Risk Analysis involves the identification and assessment of the level (measure) of the risks calculated from the assessed values of assets and the assessed levels of threats to, and vulnerabilities of, those assets. Risk is also determined to a certain extent by its acceptance.

Risk management involves the identification, selection and adoption of countermeasures justified by the identified risks to assets in terms of their potential impact on services if failure occurs, and the reduction of those risks to an acceptable level. Risk management provides sufficient confidence that:

- All possible risks and countermeasures have been identified
- All vulnerabilities have been identified and their levels accurately assessed
- All threats have been identified and their levels accurately assessed
- All results are consistent across the broad spectrum of the technology reviewed
- All expenditure on selected countermeasures can be justified.

2.5.1.3 Implement Cost-Justifiable Countermeasures

The risks identified to service and component availability should be addressed through appropriate risk reduction measures and the development of effective recovery mechanisms. These countermeasures may be implemented as part of the overall design of the new or changed service, maintenance activities and continual review and improvements. Counter-measures to reduce the impact of an event, or the probability of an event occurring, or both, are implemented wherever they are cost-justifiable.

One of these countermeasures is Planned and Preventive Maintenance. During this countermeasure all IT components should be subject to a planned maintenance strategy. The frequency and levels of maintenance required varies from component to component, taking into account the technologies involved, criticality and the potential mission benefits that may be introduced. Planned maintenance activities enable the IT support organization to provide:

- Preventative maintenance to avoid failures
- Planned software or hardware upgrades to provide new functionality or additional capacity
- Mission requested changes to the business applications
- Implementation of new technology and functionality for exploitation by the mission.

Planned downtime influences the level of availability that can be delivered for an IT service. In determining the availability requirements, the amount of downtime and the resultant loss of service required for planned maintenance may not be acceptable to the mission. For those services that have a high availability requirement, it is essential that continuous operation is a core design feature to enable maintenance activity to be performed without impacting the availability of IT services. Availability Management needs to determine the most effective approach to balance the requirements for planned maintenance against the loss of service to the mission. Unless mechanisms exist to allow continuous operation, scheduled downtime for planned maintenance is essential if high levels of availability are to be achieved and sustained.

Where the required service hours for IT services are less than 24 hours per day and/or seven days per week, it is likely that the majority of planned maintenance can be accommodated without impacting IT service availability. For all IT services, there should logically be a ‘low-impact’ period which should be provided initially when determining the availability requirements. This ‘low-impact’ period may be the best time for the implementation of maintenance. Once the requirements for managing scheduled maintenance have been defined and agreed, these should be documented as a minimum in:

- SLAs
- OLAs
- Underpinning contracts (Supplier Management)
- Change Management schedules
- Release and Deployment Management schedules.

2.5.1.4 Review all New and Changed Services and Test All Availability and Resilience Mechanisms

During Service Transition all elements contributing to the service need to be reviewed and tested to ensure that availability requirements can be met. These testing procedures should be included in the overall transition process to ensure required availability levels will be delivered.

During Service Operation, regularly scheduled availability reviews and tests provide the most reliable method to ensure the ongoing effectiveness of the service design. The Availability Management process develops the availability testing schedule. This is a schedule for the regular testing of all availability mechanisms. Some availability mechanisms, such as load balancing, are used in the provision of normal service on a day-by-day basis; others are used on a fail-over or manual reconfiguration basis. It is essential that all availability mechanisms are tested in a regular and scheduled manner to ensure that they work when needed. This schedule needs to be maintained and widely circulated so that all areas are aware of its content and so that all other proposed activities can be synchronized with its content, such as:

- The change schedule
- Release plans and the release schedule
- All transition plans, projects and programs
- Planned and preventative maintenance schedules
- The schedule for testing IT service continuity and recovery plans
- Business plans and schedules.

2.5.1.5 Continual Review and Improvement

Changing mission needs and customer demand may require the levels of availability provided for an IT service to be reviewed. The criticality of services may change and it is important that the design and the technology supporting such services is regularly reviewed and improved by Availability Management to ensure that the change of importance in the service is reflected within a revised design and supporting technology.

Availability Management will continually to look at opportunities to optimize the availability of the IT infrastructure in conjunction with Continual Service Improvement activities. The benefit of these regular reviews is that enhanced levels of availability may be achievable with much lower costs. This optimization is a sensible first step to delivering better value for money.

Mission-driven metrics demonstrate the impact of deficiencies in the technology and underpinning processes and procedures on mission operation, and also help quantify the benefits of improvement opportunities. Availability Management can play an important role in helping the IT service provider organization recognize opportunities to add value by exploiting its technical skills and competencies in an availability context. The continual improvement technique can be used by Availability Management to harness this technical capability.

Availability Management should take a proactive role in identifying and progressing cost-justified availability improvement opportunities within the Availability Plan. The ability to do this places reliance on having appropriate and meaningful availability measurement and reporting. To ensure availability improvements deliver benefits to the mission and users, it is important that measurement and reporting reflects not just IT component availability but also availability from a mission operation and user perspective.

Production of the Projected Service Outage (PSO) document

Availability Management supports the production and maintenance of the PSO document. This Change Management document contains details of all scheduled and planned service downtime within the agreed service hours for all services. This document is based on input from:

- The change schedule
- The release schedules
- Planned and preventative maintenance schedules
- Availability testing schedules
- ITSCM and Business Continuity Management testing schedules.

Once the PSO has been agreed, the Service Desk should ensure that it is communicated to all relevant parties so that everyone is made aware of any additional, planned service downtime.

2.5.2 Operational Activities

With Availability Management (AvM) having conducted design activities, AvM has agreed component and IT service requirements; targets for availability, reliability, and maintainability from technical specifications, infrastructure risks and resilience, recovery criteria, and an availability plan, AvM performs operational activities. A proactive result of performing operational activities is input to the Service Improvement Plan (SIP).

2.5.2.1 Monitor

Monitoring is repeated observation of a component or IT service to detect events and to ensure that the current status is known. Monitoring needs to be specific to the components and services, so that the monitors collect all the data needed by AvM to conduct analysis on the data and report any findings. The monitors need to collect data for availability as well as performance. The thresholds and baselines are determined by SLA targets. Events and alarms are employed to notify when targets are about to be breached or are breached.

2.5.2.2 Measure

If it is not measured it cannot be managed and if it is not measured it cannot be improved so it is essential that availability and performance of components and service be measured. The user views service availability from the frequency, duration, and scope, as well as response time. The user can view poor response times as an outage. The IT service provider views component availability and service availability as availability, reliability, and maintainability. Differences in the user and IT service provider viewpoints means AvM needs to consider the spectrum of measures needed to report the same level of availability in different ways.

Component availability measurements can include:

- Percent available
- Percent unavailable
- Duration
- Frequency of failure
- Impact of failure

It is also important to measure availability from the business / IT service and user perspective, such measures are:

- Frequency of downtime
- Duration of downtime
- Scope of impact
- Percent available
- Percent unavailable

Measurements are analyzed and included in reports along with recommendations for change to improve component or service availability.

2.5.2.3 Service Failure Analysis

Service Failure Analysis (SFA) provides a structured approach to identifying and diagnosing the underlying causes of component and service interruptions as reported by monitoring the components and service. An SFA strives to identify improvements in technology and in the IT support organization, process, procedures, and tools by conducting trend analysis to identify common failures or fragile components or IT services. SFA is similar to Problem Management and the activities can be performed jointly. The objectives of SFA are:

- Improve overall IT service availability through recommended improvements
- Identify underlying causes of service interruption
- Assess effectiveness of IT support and processes
- Generate a report with findings and recommendations
- Availability improvements resulting from SFA are measured.

2.5.2.4 Tuning

The analysis of the monitoring data is employed to identify components or services that could be tuned to improve utilization or performance of components or services. Tuning is part of performance management and is employed to plan changes in component or IT services to obtain the efficient use of resources. Prior to implementing any recommendations that result from tuning, it may be necessary to test the recommendations.

2.5.2.5 Report

The result of operational activities are component and IT service availability, maintainability, reliability reports that targets have been achieved and the detected and recorded deviations from targets. Any report has to clearly show where the loss of availability occurred and provide recommendations. Recommendations can be categorized as:

- Detection
- Reduction
- Avoidance

Also, as necessary update the risk register, the Availability Plan, test schedules, maintenance schedules, and Service Improvement Plan (SIP).

Typical reports can be:

- Monthly availability reports
- Service Failure Analysis status reports

2.6 Quality Control

2.6.1 Metrics, Measurements and Continual Process Improvement

Continual Process Improvement depends on accurate and timely process measurements and relies upon obtaining, analyzing, and using information that is practical and meaningful to the process. Measurements of process efficiency and effectiveness enable the USMC to track performance and improve overall end user satisfaction. Process metrics are used as measures of how well the process is working, whether or not the process is continuing to improve, or where improvements should be made.

Effective operation and management of the process requires the use of metrics and measurements. Reports need to be defined, executed, and distributed to enable the managing of process-related issues and initiatives. Daily management occurs in Service Operations, at the process manager level. Long-term trending analysis and management of significant process activities occurs in Service Design, under the responsibilities of the process owner.

The essential components of any measurement system are Critical Success Factors (CSFs) and Key Performance Indicators (KPIs).

2.6.2 Critical Success Factors with Key Performance Indicators

CSFs and KPIs establish the baseline and mechanism for tracking performance. CSFs are those factors that must be done well within the process; KPIs ensure each CSF is met.

- **Critical Success Factor (CSF) –** A Critical Success Factor is a metric that represents key operational performance requirements and indicates whether a process or operation is performing successfully from a customer or business perspective.

- **Key Performance Indicator (KPI)** – A KPI is used to measure the achievement of each Critical Success Factor. Many metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the process, IT service, or activity. A KPI should lead to action and be a driver for improvement.
- **Metric** – A metric is a measure for quantitatively or qualitatively assessing, controlling or selecting a person, process, event, or institution along with the procedures to carry out measurements for interpretation. Metrics may be used to help manage an IT process, service, or activity.

Table 2-2 describes CSFs and KPIs that can be used to judge the efficiency and effectiveness of the Availability Management process. Results of the analysis provide input to improvement programs (i.e., continual service improvement). At the current level of process development and maturity, the critical objectives of AvM are to publish the Availability Plan when needed for the budget cycle, and avoidance of failures due to availability issues.

Table 2-2. AvM Critical Success Factors and Key Performance Indicators

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
1	Manage availability and reliability of IT service	1	Percentage reduction in the unavailability of services and components	Enterprise components and services maintain a high level of stability and reliability. High percentage of reductions in the number of service breaks and the mean time to restore the service. There is also a reduction in the number of incidents.
		2	Percentage increase in the reliability of services and components	
		3	Effective review and follow-up of all SLA, OLA and underpinning contract breaches	
		4	Percentage improvement in overall end-to-end availability of service	
		5	Percentage reduction in the number and impact of service breaks	
		6	Improvement in the MTBF (Mean Time Between Failures)	
		7	Improvement in the MTBSI (Mean Time Between Systems Incidents)	
		8	Reduction in the MTRS (Mean Time to Restore Service).	
2	Satisfy business needs for access to IT services	9	Percentage reduction in the unavailability of services	With a fulfillment of agreed service levels and an incremental increase of availability levels, the customer perceives a better quality of service.
		10	Percentage reduction of the cost of business overtime due to unavailable IT	
		11	Percentage reduction in critical time failures, e.g. specific business peak and priority availability needs are planned for	
		12	Percentage improvement in business and users satisfied with service (by CSS results).	
3	Availability of IT infrastructure achieved at optimum costs	13	Percentage reduction in the cost of unavailability	Reduction in the costs associated with a given level of availability. Controls costs related to maintaining SLAs
		14	Percentage improvement in the Service Delivery costs	

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
		15	Timely completion of regular Risk Analysis and system review	and reduces the amount of time needed to review and report on service availability. Availability Management personnel can focus on IT infrastructure rather than locating infrastructure failures or incidents that reduce performance. Reduction in budget overruns due to additional time needed for system availability analysis, review and reporting.
		16	Timely completion of regular cost-benefit analysis established for infrastructure Component Failure Impact Analysis (CFIA)	
		17	Percentage reduction in failures of third-party performance on MTRS/MTBF against contract targets	
		18	Reduced time taken to complete (or update) a Risk Analysis	
		19	Reduced time taken to review system resilience	
		20	Reduced time taken to complete an Availability Plan	
		21	Timely production of management reports	
		22	Percentage reduction in the incidence of operational reviews uncovering security and reliability exposures in application designs	

3.0 ROLES AND RESPONSIBILITIES

Each process has roles and responsibilities associated with design, development, execution and management of the process. A role within a process is defined as a set of responsibilities. There will be instances where roles are combined and a person will be responsible for multiple roles. This is based on factors such as the area or responsibility, size of user base, and/or size of the process support team which will dictate exactly which roles require a dedicated person(s) and the total number of persons performing each role.

While the goal is to have a single Availability Management Process Owner at the enterprise level, the USMC will initially use a shared process ownership framework. There will be a Process Owner for Marine Corps System Command (MCSC), as well as a Process Owner for the operational sector inclusive of all other USMC organization at the enterprise, regional, and local levels. The AvM process owners will serve as the authoritative process point of contact for any higher headquarters (DoN or DoD) or adjacent organization engagement or coordination.

The Process Manager provides direct support to the process owner by daily operational management of the AvM process. The Process Manager reports deviations in the processes and recommend corrective action to the respective process owner.

3.1 Roles

The following abstract drawing (Figure 3-1) depicts Availability Management process roles for the USMC, followed by a description of these roles. Table 3-1 describes the roles and responsibilities in more detail.

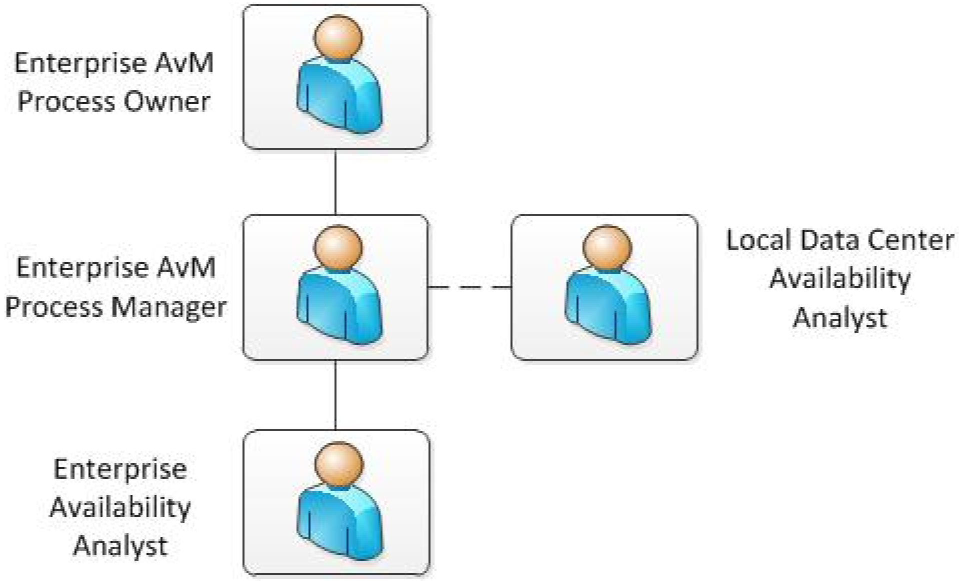
Enterprise AvM Process Owner
Enterprise AvM Process Manager
Local Data Center Availability Analyst
Enterprise Availability Analyst

Figure 3-1. Availability Management Roles

Table 3-1 describes roles and responsibilities of Availability Management roles:

Table 3-1. AvM Roles and Responsibilities

Description	Overall Responsibility
Enterprise Availability Management Process Owner	
The Enterprise Process Owner owns the process and the supporting documentation for the process. At this time, the USMC Enterprise Availability Management process owner role is shared by MCSC and MCNOSC.	The Process Owner shall act on behalf of the Commanding Officer to establish and ensure adherence to and enterprise AvM process. Duties include[1]: • Review and understand all references pertaining to the appointment • In coordination with the Marine Corps System Command (MCSC) AvM Process Owner, document and publicize the AvM process • Ensure updates to the AvM Process Guide, once established and approved, are performed according to the Change Management Process • Define the Key Performance Indicators (KPIs) to evaluate the effectiveness and efficiency of the AvM Process • Review KPIs and take action required following the analysis • Assist with and be ultimately responsible for the AvM Process design • Ensure the effectiveness and efficiency of the AvM Process and working practices through continuous improvement • Review any proposed enhancements to the AvM Process • Develop and provide input to the AvM Process Improvement Plan • Address any issues with the execution of the process • Ensure all relevant staff have the required training and are aware of their role in the AvM Process • Ensure that the AvM Process, roles, responsibilities and documentation are regularly reviewed and audited • Interface with the appropriate organizations to ensure the process receives the necessary staff resources • Ensure all stakeholders are sufficiently involved in the AvM Process • Ensure tight linkage between AvM Processes and other related Marine Corps Information Technology Service Management Processes • Ensure organizational adherence to the AvM Process Additional **Design** responsibilities include: • Ensure that acquisitions support the reliability, maintainability, resilience and serviceability requirements • Provide input to the AvM tool/system selection • Ensures AvM processes and tools integrate with other ITSM processes and that requirements for the tools are defined • Provide input for the requirement and guidelines of the AvM tool usage • Benchmark the process performance • Participate in other ITSM process initiatives and process reviews
Enterprise Availability Management Process Manager	
The AvM Process Manager ensures effective coordination of the activities necessary to execute the Availability Management process.	**Design:** • Awareness of USMC and DoD directives • Support Change Review processes and review boards • Manage interfaces with external processes • Maintain availability baselines • Develop and manage availability plans

[1] The Process Owner responsibilities shown are from the MCNOSC letter "Appointment as Process Owner for the Enterprise Information Technology Service Management Availability Management Process", 27 February 2013.

Description	Overall Responsibility
	• Identify opportunities to improve the process • Work with CSI ad AvM process owner to review and prioritize improvement opportunities • Conduct Systems Engineering Technical Review (SETR) reviews for AvM development this pertains to when Availability Management initiates changes, particularly to the process. These changes will go thru a series of reviews as development of the change progresses - the SETR process. The Process Manager is responsible for conducting these reviews. • Support SETR reviews instigated by other processes • Provide Availability support to Programs and Projects to make sure business and service requirements are met • Support incorporation of Availability Management into development and testing • Identify areas for availability-related improvement during development • Update Availability baselines • Ensure availability levels requested are cost-justified • Develop and maintain an availability testing schedule for all availability mechanisms • Assist IT Security Management and IT Service Continuity Management in the identification, assessment and management of risks • Develop availability and recovery design criteria to guide infrastructure design • Support development and maintenance of AvM process guide **Operational:** • Monitor and report on AvM process performance • Publish availability related reports • Interface with system engineering and system architecture to ensure services can meet the required availability levels • Ensure service levels specified in agreed upon SLAs are met
Enterprise Availability Analyst	
The Enterprise Availability Analyst is a senior technical expert with experience in Availability Management, responsible for the day to day operational responsibilities of AvM.	**Design:** • Contribute to the development of Availability Plans • Support development and maintenance an availability testing schedule for all availability mechanisms • Support development of availability and recovery design criteria to guide infrastructure design • Evaluate RFC's **Operational:** • Adhere to standards • React to Events, Incidents and Problems • Issue resolution • Support root cause analysis • If the cause of availability issues cannot be determined, work with Problem Management to engage a wider team • Support development and implementation of metrics • Produce statistics and reports from the AvM tools • Design, develop and produce new reports as well as modify existing reports • Establish and maintain automatic reporting capabilities

Description	Overall Responsibility
	• Establish and maintain the AvM reporting architecture and user reporting portal • Produce standard reports for Service Level Management and service analysis • Participate in data gathering and trend analysis • Support update of Availability baselines • Support threshold development • Perform availability testing for all availability mechanisms
Local Data Center Availability Analyst	
The Local Availability Analyst is a technical expert that supports the Enterprise Availability Management process, supporting the day to day operational responsibilities of AvM.	**Design:** • Contribute to the development of Availability Plans **Operational:** • Adhere to standards • React to Events, Incidents and Problems • Issue resolution • Support root cause analysis • If the cause of availability issues cannot be determined, work with Problem Management to engage a wider team • Support development and implementation of metrics • Produce statistics and reports from the AvM tools • Participate in data gathering and trend analysis • Support update of Availability baselines • Support threshold development

3.2 Responsibilities

The processes span organizational boundaries; therefore, procedures and work instructions within the process need to be mapped to roles within the process. These roles are then mapped to job functions, IT staff and departments. The process owner is accountable for ensuring process interaction by implementing systems that allow smooth process flow.

The Responsible, Accountable, Support, Consulted, and Informed, (RASCI) model is a method for assigning the type or degree of responsibility that roles (or individuals) have for specific tasks.

Responsible — Completes the process or activity; responsible for action/implementation. The degree of responsibility is determined by the individual with the "A."

Accountable — Approves or disapproves the process or activity. Individual who is ultimately answerable for the task or a decision regarding the task. Typically, the Process Owner is Accountable for a process, and there must be only one Accountable specified for each task or deliverable.

Support **—** Resources allocated to Responsible, and will assist in completing the task.

Consulted — Gives needed input about the process or activity. Prior to final decision or action, these subject matter experts or stakeholders are consulted.

Informed — Needs to be informed after a decision or action is taken. May be required to take action as a result of the outcome. This is a one-way communication.

Both proactive and reactive activities are necessary to manage IT availability successfully. Proactive activities are those necessary to ensure that new or changed services will meet the agreed upon availability requirements, and that appropriate availability measurements are in place:

- Planning and designing services (new or changed). This includes
  - Identifying Vital Business Functions (VBFs)
  - Determining service availability requirements and formulating the availability and recovery design criteria
  - Defining availability and reliability targets for infrastructure components
  - Ensuring prevention of and recovery from service or component unavailability thru risk assessment and management activities
  - Designing services to meet the design criteria and agreed service levels
  - Establishing metrics and reports identifying availability, reliability, and maintainability
- Risk Assessment and Management, which includes determining the impact from service or component failure
- Implementing cost-justified counter measures including risk reduction and recovery
- Reviewing new and changed services
- Testing availability and resilience
- Participating in Continual Service Improvement efforts for both services and the Availability Management process

Reactive Availability Management activities support delivery of agreed up on levels of availability, and appropriate responses to service level breeches. These activities include:

- Monitoring, measuring, analyzing, reporting and reviewing service and resource availability
- Investigating service and resource unavailability and initiating remedial action

Table 3-2 establishes responsibilities for high-level process activities by role.

Table 3-2. Responsibilities for Availability Management

AvM Process Activities	Enterprise AvM Process Owner	Enterprise AvM Process Manager	Enterprise Availability Analyst	Local Data Center Availability Analyst
Maintain Availability Management Process Guide	AR	S		
Producing and maintaining an Availability Plan	I	AR	S	S
Ensuring upgrades and improvements meet requirements	I	AR		
Estimating future requirements	I	AR	S	S
Modeling predicted changes in services	I	AR	S	S
Monitoring, measuring, reporting and reviewing availability	I	AR	S	S
Tuning the performance of services and components	I	AR	S	
Responding to all availability related events	I	AR	S	
Addressing availability issues	I	AR	S	
Participating in Continual Service Improvement	I	AR	S	

4.0 AVAILABILITY METRICS

4.1 Availability

Availability Management is completed at two interconnected levels:

- **Service availability:** involves all aspects of service availability and unavailability and the impact of component availability, or the potential impact of component unavailability on service availability
- **Component availability:** involves all aspects of component availability and unavailability.

Availability Management relies on the monitoring, measurement, analysis and reporting of the following aspects:

Availability: the ability of a service, component or CI to perform its agreed function when required. It is often measured and reported as a percentage:

$$\textbf{Availability}\ (\%) = \frac{\textbf{Agreed Service Time}\ (\textbf{AST}) - \textbf{downtime}}{\textbf{Agreed Service Time}\ (\textbf{AST})}\ \textbf{X 100}\%$$

Note: Downtime should only be included in the above calculation when it occurs within the Agreed Service Time (AST). However, total downtime should also be recorded and reported.

4.2 Reliability

Reliability: a measure of how long a service, component or CI can perform its agreed function without interruption. The reliability of the service can be improved by increasing the reliability of individual components or by increasing the resilience of the service to individual component failure (i.e. increasing the component redundancy, e.g. by using load-balancing techniques). It is often measured and reported as Mean Time Between Service Incidents (MTBSI) or Mean Time Between Failures (MTBF):

$$\textbf{Reliability}\ (\textbf{MTBSI in hours}) = \frac{\textbf{Available Time in Hours}}{\textbf{Number of Breaks}}$$

$$\textbf{Reliability}\ (\textbf{MTBF in hours}) = \frac{\textbf{Available Time in Hours} - \textbf{Total Downtime in Hours}}{\textbf{Number of Breaks}}$$

4.3 Maintainability

Maintainability: a measure of how quickly and effectively a service, component or CI can be restored to normal working after a failure. It is measured and reported as Mean Time to Restore Service (MTRS) and should be calculated using the following formula:

$$\textbf{Maintainability (MTRS in Hours)} = \frac{\textbf{Total Downtime in Hours}}{\textbf{Number of Service Breaks}}$$

MTRS should be used to avoid the ambiguity of the more common industry term Mean Time To Repair (MTTR), which in some definitions includes only repair time, but in others includes recovery time. The downtime in MTRS covers all the contributory factors that make the service, component or CI unavailable:

- Time to record
- Time to respond
- Time to resolve
- Time to physically repair or replace
- Time to recover.

Example: A situation where a 24 x 7 service has been running for a period of 5,020 hours with only two breaks, one of six hours and one of 14 hours, would give the following figures:

Availability = (5,020-(6+14)) / 5,020 x 100 = 99.60%

Reliability (MTBSI) = 5,020 / 2 = 2,510 hours

Reliability (MTBF) = 5,020-(6+14) / 2 = 2,500 hours

Maintainability (MTRS) = (6+14) / 2 = 10 hours

4.4 Serviceability

Serviceability is the ability of a third-party supplier to meet the terms of their contract. Often this contract will include agreed levels of availability, reliability and/or maintainability for a supporting service or component.

Appendix A – ACRONYMS

The official list of E-ITSM acronyms can be found on the Enterprise Information Technology Service Management site (https://eis.usmc.mil/sites/irm/ITSM/default.aspx). The link to the document is referenced below:

https://eis.usmc.mil/sites/irm/ITSM/Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Firm%2FITSM%2FDocuments%2FE%2DITSM%20Acronym%20List&FolderCTID=0x0120001918760B7D35A5478C0474985E3ACBCD&View={9CD820B3-EF85-4D2C-BD0C-A255AEE9E40D}

Appendix B – GLOSSARY

Term	Definition
Change Schedule	A Change Schedule is a document that lists all approved changes and their planned implementation dates.
Configuration Item	A Configuration Item (CI) is any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System (CMS) and is maintained throughout its life cycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT services, hardware, software, buildings, people and formal documentation such as process documentation and SLAs.
CI Type	CI Type is a category used to Classify CIs. The CI Type identifies the required attributes and relationships for a configuration record. Common CI Types include: server, document, user, etc.
Component Availability	Involves all aspects of component availability and unavailability.
Configuration Management Database	A Configuration Management Database (CMDB) is a database used to store configuration records throughout their life cycle. The Configuration Management System (CMS) maintains one or more CMDBs and each CMDB stores attributes of CIs and relationships with other CIs.
Configuration Management System	A Configuration Management System (CMS) is a set of tools and databases used to manage an IT service provider's configuration data. The CMS also includes information about incidents, problems, known errors, changes, and releases and may contain data about employees, suppliers, locations, units, customers and users. The CMS includes tools for collecting, storing, managing, updating and presenting data about all CIs and their relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management processes.
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted.
DoD IT Based Resource	DoD-provided IT devices, systems, applications, and services, and the information and data contained within them.
DoD Resource	A DoD IT-based resource or electronically-protected DoD physical resource such as physical locations, facilities, or other physical objects.
Environment	Environment is a subset of the IT infrastructure used for a particular purpose (e.g., live environment, test environment or build environment). It is possible for multiple environments to share a CI (e.g., test and live environments may use different partitions on a single mainframe computer). In the term physical environment, environment can be defined as the accommodation, air conditioning, power system, etc. Environment can be used as a generic term defined as the external conditions that influence or affect something.
Environmental Attributes	Attributes, not specifically about the subject or the resource, but about the current environment at the time of the transaction itself. Environment attributes are critical for fine-grained access control because many of the policies that are enforced on information are conditional on some outside environmental factor rather than just the attributes of the subject requesting access (FICAM).
Escalation	Escalation is an activity that obtains additional resources when needed to meet service-level targets or customer expectations.
Event	An Event is a piece of data that provides information about one or more system resources. Most events are benign. Some events show a change of state which has significance for the management of a CI or IT service. The term 'event' is also used to define an alert or notification created by any IT service, CI, or monitoring tool. Events typically require IT operations personnel to take actions and often lead to incidents being logged.
Exit and Entry Criteria (Pass/Fail)	These are criteria (defined well in advance and accepted by the stakeholders) defined at authorized points in the Release and Deployment Process to set expectations of acceptable/unacceptable results.
Governance	Governance is the process of ensuring policies and strategy are actually implemented and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring, and reporting and taking actions to resolve any issues identified.
Incident	An Incident is an unplanned interruption, degradation or reduction in IT Service quality.
Key Performance Indicator	A Key Performance Indicator (KPI) is a metric used to help manage a process, IT service, or activity. Many metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the process, IT service, or activity. KPIs are selected to ensure that efficiency, effectiveness, and cost-effectiveness are all managed.

Term	Definition
Known Error	A Known Error is a problem that has a documented root cause and a work-around. Known errors are created and managed throughout their life cycle by Problem Management. Known errors may also be identified by SIE or suppliers.
Known Error Database (KEDB)	A database containing all Known Error Records. This database is created by Problem Management and used by Incident and Problem Management.
Mean Time Between failures (MTBF)	Metric for measuring and reporting reliability. MTBF is the average time that a Configuration Item or IT service can perform its agreed function without interruption. This is measured from when the CI or IT service starts working until it next fails.
Mean Time Between Service Incidents (MTBSI)	Metric used for measuring and reporting reliability. MTBSI is the mean time from when a system or IT service fails, until it next fails. MTBSI is equal to MTBF + MTRS.
Mean Time to Restore Service (MTRS)	Average time taken to restore a Configuration Item or IR to service after a failure. MTRS is measured from when the Configuration Item or IT service fails until it is fully restored and delivering its normal functionality.
Monitoring	Monitoring is the process of repeated observation of a CI, IT service, or process to detect events and to ensure that the current status is known.
Proactive Activity	Involves proactive planning, design and improvement of Availability Management.
Problem	A cause of one or more incidents. The cause is not usually known at the time a problem record is created and the problem management process is responsible for further investigation.
Process	A Process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process may include any of the roles, responsibilities, tools, and management controls required to reliably deliver the outputs. A process may define policies, standards, guidelines, activities, and work instructions, if needed.
Quality Assurance	Quality Assurance (QA) is the process responsible for ensuring the quality of a product and also ensuring it will provide its intended value.
Reactive Activity	Involve the monitoring, measuring, analysis, and management of all events, incidents, and problems involving unavailability.
Risk	A possible event that could cause harm or loss, or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred.
Reliability	A Measure of how long a service, component, or Configuration Item can perform its agreed function without interruption.
Role	A Role refers to a set of connected behaviors or actions that are performed by a person, team, or group in a specific context.
Service Availability	Involves all aspects of service availability and unavailability and the impact of component availability, or the potential impact of component unavailability on service availability.
Service Improvement Plan	A Service Improvement Plan (SIP) is a formal plan to implement improvements to a process or IT service.
Service Level Agreement	A Service-Level Agreement (SLA) is an agreement between an IT service provider and a customer. The SLA describes the IT service; documents service-level targets; and specifies the responsibilities of the IT service provider and the customer. A single SLA may cover multiple IT services or multiple customers.
Single Point of Contact	A Single Point of Contact (SPOC) is an agreement used to assign a single, consistent way to communicate within an organization or unit. For example, the Service Desk will be the SPOC for a service provider.
Systems Engineering Technical Review	Systems Engineering Technical Review (SETR) process provides a framework for structured systems engineering management, including assessment of predicted system performance. SETRs also provide independent subject matter assessments of program technical health and maturity at key points in the development life cycle.