Information Technology
Service Management Program
Volume 1

Incident Management Process

Version 1.2

Table of Contents

Table of Figures

Document Revision History

Version	Date	Resource	Revision Description
1.0	2008.01.25	Julie Villarreal	Content written
1.1	2008.02 – 2008.09	Julie Villarreal	Content creation/ compilation, revision, formatting, and review
1.2	2008.09.22	Julie Villarreal	Final version generated

Wyndham Hotel Group's Service Management Program Overview

Wyndham Hotel Group (WHG) Information Technology (IT) has defined its vision to be an agile and efficient IT services organization that improves the business value of the group through innovative people and technology and streamlined processes. The Service Management Program implementation is part of the drive to streamline processes within the organization based on ITIL best practices. ITIL - Information Technology Infrastructure Library - defines the organizational structure and skill requirements of an IT organization and a set of standard operational management procedures and practices to allow the organization to manage an IT operation and the associated infrastructure. ITIL has become the de-facto industry approach to IT service management.

ITIL (v2) defines eleven processes within the library: Incident Management

- Problem Management
- Change Management
- Release Management
- Configuration Management
- Service Level Management
- Financial Management
- IT Continuity Management
- Availability Management
- Capacity Management
- Security Management

The WHG IT Service Management team assessed IT process maturity and organizational culture based on the best-practice framework. From an analysis of the results, each of the process areas adopted a phased approach/ strategy for implementation.

The **goal of Phase One** is to implement Incident Management, Change Management, and Service Level Management. These processes have been identified as those for which WHG will realize immediate short-term business value if implemented immediately. Other process implementations will follow in other phases after the completion of Phase One.

- **Incident Management (IM)** has a primary objective to restore normal service operation as quickly as possible and minimize the adverse impact on business operations. Advantages of managing incidents include a reduced business impact of incidents, the ability to identify issues proactively, improved monitoring, and elimination of lost incidents.

- **Change Management**, in contrast, is focused on the identification, recording, and reporting of all IT components under the control and scope of Configuration Management. Change Management is a process in which lack of maturity can have the most dramatic impact on the business. Un-approved, unplanned, and uncoordinated changes can negatively impact the business customer.

  Additionally, without the ability to control when, how, and by whom items are changed in the Production environment, other processes such as Release Management and Configuration Management cannot be effectively implemented. A controlled Change Management process is a dependency for several other IT business practices. Other benefits include more accurate information of Configuration Items (CIs), better adherence to legal obligations, and support for service continuity and IT financial planning.

- **Service Level Management** has a primary objective to maintain and improve IT service quality through a constant cycle of agreeing, monitoring, and reporting to meet the customers' business objectives. The benefits include services that are designed to meet service level requirements, monitoring for specific targets with more focus on business needs, and service improvements.

This document focuses on IM processes. Other related documents have been published for the other processes in scope for Phase One.

.

Incident Management

1. Process Overview

The purpose of this document is to provide a general overview of Wyndham Hotel Group's Incident Management Process in terms of its goals and objectives, scope, benefits, key terms, and roles and responsibilities.

The content within this general overview is based on the best practices of the Information Technology Infrastructure Library (ITIL®).

1.1 Business Objectives

Process goals and objectives define why Incident Management is important to Wyndham Hotel Group's overall vision for delivering and supporting effective and efficient IT services. This section establishes the fundamental goals and objectives that underpin Incident Management. The agreed and documented goals and objectives provide a point of reference to check implementation and operational decisions and activities.

The process goals are broad statements that define what the organization wants to achieve by successfully implementing Incident Management. The process objectives are more specific statements than the goal and are characterized by a set of tasks in pursuit of reaching the goal.

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

To achieve this goal Wyndham Hotel Group aims to pursue the following objectives:

- Forge a close link with the Service Level Management process to obtain necessary Incident response targets. Review Incident resolution times so that they are meeting the goals set forth in Service Level Agreements (SLAs). Timely incident resolution will satisfy customers and end users
- Review, audit, and analyze the process constantly to ensure proper adherence by all the different and diverse Information Technology (IT) groups using the process
- Monitor the effectiveness of Incident Management and make recommendations for continual improvement of the process

1.2 Key Terms Defined

The following key terms and definitions for the Incident Management process have been agreed by the Incident Management Project Team on behalf of the Wyndham Hotel Group. These terms and definitions will be used throughout the process documentation, communications, training materials, tools, and reports.

Escalation: An activity that obtains additional resources when these are needed to meet Service Level Targets or customer expectations. Escalation may be needed within any IT Service Management Process but is most commonly associated with Incident Management, Problem Management and the management of customer complaints.

Event: An alert or notification created by any IT service, Configuration Item, or a monitoring tool. Events typically require IT Operations personnel to take actions and often lead to incidents being logged.

Failure: Loss of ability to operate to specification or to deliver the required output. The term ‘failure’ may be used when referring to IT services, processes, activities, and configuration Items. A failure often causes an incident.

Function: A team or group of people and the tools they use to carry out one of more processes or activities, for example, the Service Desk.

Group: A number of people who are similar in some way. People who perform similar activities, even though they may work on different technology or report into different organizational structures or even in different companies.

Impact: A measure of the effect of an incident, problem, or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.

Incident: An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a Configuration Item that has not yet impacted service is also an incident, for example, failure of one disk from a mirror set.

Incident Management: The process responsible for managing the lifecycle of all incidents. The primary objective of Incident Management is to return the IT service to customers as quickly as possible.

Incident Model: A way of predefining the steps that should be taken to handle a process for dealing with a particular type of incident in an agreed way.

Incident Record: A record containing the details of an incident. Each Incident Record documents the life cycle of a single incident.

Major Incident: The highest category of impact for an incident. A major incident results in significant disruption to the business.

Normal Service Operation: The service operation defined within the Service Level Agreement (SLA) limits.

Priority: A category used to identify the relative importance of an incident, problem, or change. Priority is based on impact and urgency and is used to identify required times for actions to be taken. For example, the Service Level Agreement (SLA) may state that Priority 2 incidents must be resolved within 12 hours.

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.

Role: A set of responsibilities, activities and authorities granted to a person or team. A role is defined in a process. One person or team may have multiple roles, for example, the roles of Configuration Manager and Change Manager may be carried out by a single person.

Service Desk: The Single point of contact between the service provider and the users. A typical Service Desk manages Incidents and Service Requests and also handles communication with the users.

Service Request (as opposed to the definition of an Incident): A request from a user for information, advice, a standard change or access to an IT service, for example, to reset a password or to provide standard IT services for a new user. Service Requests are usually handled by the Service Desk and do not require a Request for Change (RFC) to be submitted.

Urgency: A measure of how long it will be until an incident, problem, or change has a significant impact on the business. For example, a high impact incident may have low urgency, if the impact will not affect the business until the end of the financial year. Impact and urgency are used to assign priority.

User: A person who uses the IT service on a day-to-day basis. Users are distinct from customers, as some customers do not use the IT service directly.

1.3 Scope

Scope refers to the boundaries or extent of influence to which Incident Management applies at Wyndham Hotel Group. This section provides a general best practice statement of scope for Incident Management.

Incident Management includes any event that disrupts or that could disrupt an agreed IT service. This includes Events that are communicated directly by users, either through the Service Desk or through a Web interface, events that are detected by event management tools, and events that are discovered by technical staff.

Incident Management encompasses all IT service providers, internal and third parties, reporting, recording, or working on an Incident.

1.4 Benefits

There are several qualitative and quantitative benefits that can be achieved, for both the Information Technology (IT) service providers and the customers, by implementing an effective and efficient Incident Management process. The Incident Management Project Team has agreed that the following benefits are important to Wyndham Hotel Group and will be assessed for input to continuous process improvement throughout the Incident Management process life cycle.

1.4.1 To Information Technology (IT) Service Providers

Incident Management is highly visible to the business, and it is easier to demonstrate its value than most areas in Service Operation. A successful Incident Management process can be used to highlight other areas that need attention:

- Improved ability to identify potential improvements to IT services
- Better prioritization of efforts
- Better use of resources
- More control over IT services
- Better alignment between departments
- More empowered IT staff
- Better control over vendors through Incident Management metrics

1.4.2 To the Customers

- Reduced business impact of incidents by timely detection and resolution, thereby increasing availability
- IT is better aligned to real-time business priorities and can allocate resources as necessary
- Improved user and customer satisfaction
- Improved quality of service
- Clarity for incident resolution times
- More professional and accurate communication between the Service Desk and users on behalf of the IT organization

1.5 Process Interfaces

Incident Management (IM) has key integration points to other Service Management processes. The short-term goal is to reach integration with the processes included in Phase One of the Wyndham Hotel Group Service Management Program (SMP): Service Level Management and Change Management. As process designs for the other process areas are completed, a certain level of integration (inputs becoming outputs) should be attained naturally or by design.

In the description of the interfaces in this section, the output lists what is typically exchanged between the process areas.

1.5.1 To Change Management

- Communicate on any incidents that are created due to changes, allowing the Change Manager to assess the quality of the change
- Communicate upcoming changes to the Service Desk to allow staffing levels to be adjusted accordingly
- Create an awareness of permanent solutions to chronic incidents
- Communicate change status information to the Service Desk for the benefit of the customer

1.5.2 From Change Management

- Details of change
- Post Implementation Review (PIR) feedback
- Provide Forward Schedule of Changes
- Review and approval of Request for Change (RFC) to resolve incidents
- Provide details of changes that were implemented, rejected, delayed, not approved
- Projected service availability
- Procedure to accept Request for Change (RFC)
- Change Advisory Board (CAB) meeting minutes

1.5.3 To Service Level Management

- Agreement/conference to incident priorities and escalation procedures as part of the Service Level Management process and documenting them within the Service Level Agreements
- Ensure that some of the most important targets set in the Service Level Agreements relate to service availability and thus require incident resolution within agreed periods
- Communicate change status information to the Service Desk for the benefit of the customer

1.5.4 From Service Level Management

- Establish priorities for work
- Provide escalation and support criteria
- Provide criteria for classifying incidents (impact and priority)
- Service Level Agreement ownership
- Service catalogue
- Service levels

1.6 Key Roles and Responsibilities

A role refers to a set of connected behaviors or actions that are performed by a person, team or group in a specific context. Process roles are defined by the set of responsibilities, activities, and authorities granted to the designated person, team, or group.

Some process roles may be full-time jobs while others are a portion of a job. One person or team may have multiple roles across multiple processes. Caution is given to combining roles for a person, team, or group where separation of duties is required. For example, there is a conflict of interest when a software developer is also the independent tester for his or her own work.

Regardless of the scope, role responsibilities should be agreed by line management and incorporated into existing job descriptions and/ or included in yearly objectives. Once roles are assigned, the assignees must be empowered to execute the role activities and given the appropriate authority for holding other people accountable.

All roles and designated person(s), team(s), or group(s) should be clearly communicated across the organization. This should encourage or improve collaboration and cooperation for cross-functional process activities.

Appendix E – Incident Management Key Roles and Responsibilities lists role attributes in detail.

1.6.1 Incident Manager

- Ensures that the Key Performance Indicators (KPIs) are met
- Establishes the Service Desk as the single point of contact within the end-user community
- Ensures that the Incident Management process operates effectively and efficiently through first-, second-, and third-line support, as well as with third-party vendors, using qualitative and quantitative KPIs to make recommendations for improvement
- Identifies training requirements and ensures that all staff is properly trained
- Drives the efficiency of the Incident Management process
- Ensures that incidents are resolved correctly and timely and that the resolutions comply with Service Level Agreements (SLAs) and Operational Level Agreements (OLAs)

1.6.2 Process Owner

- Owns the design of the process, periodically auditing the process to ensure compliance
- Defines Key Performance Indicators (KPIs) to evaluate the effectiveness and efficiency of the process
- Defines reporting specifications and requirements
- Take necessary action following KPI analysis
- Ensures staff is trained appropriately and that all resources understand and are able to fulfill their roles within the Incident Management process
- Reviews integration issues between other processes
- Owns the design of the process, periodically auditing the process to ensure compliance

1.6.3 N-level support

Incidents are escalated to N-level functional support resources, who provide more technical expertise for incident resolution.

1.6.4 Service Desk

The Service Desk resource provides initial handling of user contacts with the Service Desk, communicates incident updates to affected customers, and validates the resolution of incidents prior to incident closure.

1.6.5 Major Incident Team

A group of resources gathered to quickly diagnose and resolve an incident or provide work-arounds for major incidents to minimize negative impact to users.

2. Process Policies

Incident Management global process policies represent decisions made by the Incident Management Process Owner and the Incident Management team for end-to-end management and execution of the Incident Management process. All technologies, organizations, and staff defined in Wyndham Hotel Group (WHG) Incident Management scope are expected to adhere to these global policies.

2.1 Escalation (Functional and Hierarchical)

- **Policy Statement**

  High-priority incidents are escalated by passing information to and/ or requesting action from more senior staff in order to efficiently resolve high-priority tickets. Both functional and hierarchical escalation may occur within the Incident Management process; these escalation types are not mutually exclusive, as both functional and hierarchical escalation may be required simultaneously.

- **Purpose**

  To ensure incidents are resolved expeditiously within the terms of the Service Level Agreement (SLA)

- **Scope**

  All internal and external business entities involved in the life cycle of an incident

- **Benefits**

  Senior-level management supports and facilitates the efficient resolution of high-priority incidents.

- **Related Policies and Procedures**
  - Appendix B – Functional Escalation Flow Diagram
  - Appendix C – Hierarchical Escalation Flow Diagram
  - Appendix D – Functional and Hierarchical Escalation Flow Diagram

- **Policy Owner**

  Incident Management Process Manager

2.2 First Point of Contact

- **Policy Statement**

  The Service Desk is the first point of contact relating to incidents and service requests.

- **Purpose**

  To ensure that all incidents are consistently managed and assigned correctly

- **Scope**

  All internal and external business entities that are involved in the life cycle of an incident

- **Benefits**
  - Provides a single point of contact for the end user/ customer
  - Centralizes a data repository for incidents and provides a consistent entry point for the initiation of process activities

- **Related Policies and Procedures**
  - Incident Management processes
  - Incident Management procedures

- **Policy Owner**
  Incident Management Process Manager

2.3 Incident Assignment

- **Policy Statement**
  Incidents that are not classified as high-priority are assigned to the appropriate individual/ group or ‘n’ level of functional support.

- **Purpose**
  To ensure that incidents are handled in a consistent manner and effectively directed to the correct individual or group

- **Scope**
  All internal and external parties reporting, recording, or working on an incident

- **Benefits**
  Ensures all incidents are handled in a consistent, efficient, and predictable manner with the goal of minimizing impact to business operations

- **Related Policies and Procedures**
  - Escalation policy
  - Incident Management processes

- **Policy Owner**
  Incident Management Process Manager

2.4 Incident Classification and Prioritization

- **Policy Statement**
  All incidents must be assessed for impact, urgency, and expected effort.

- **Purpose**
  To manage effectively the priority in which an incident is addressed

- **Scope**
  All internal and external business entities that are involved in the life cycle of an incident

- **Benefits**
  Prioritizing by Tier 1 through Tier 4 ensures that systems-related incidents are addressed in the most beneficial sequence to enhance revenue and customer service

3. High-Level Process and Procedures

3.1 Incident Management Process

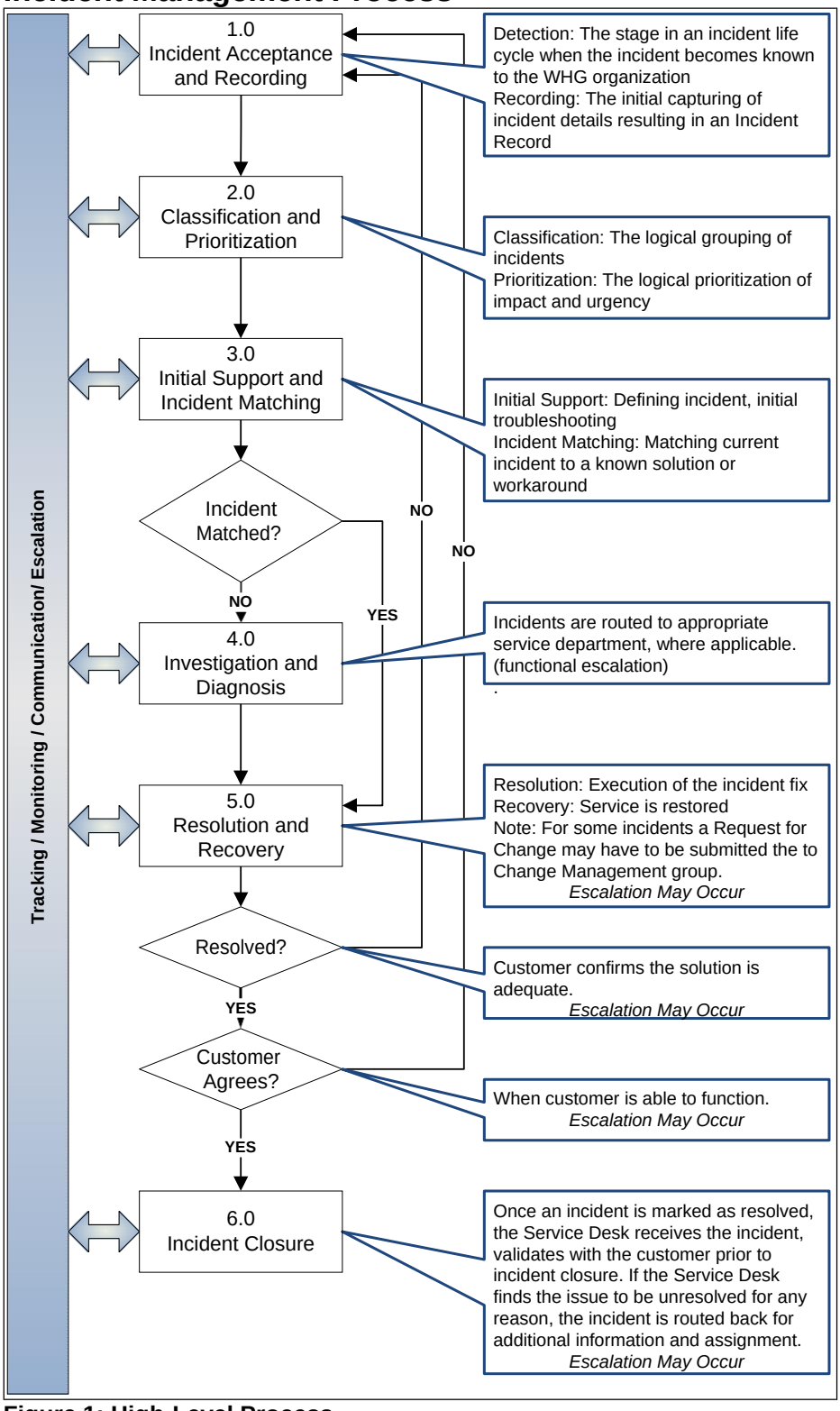


Figure 1: High-Level Process

4. Detailed Processes and Procedures

4.1 1.0 Incident Detection and Recording

4.1.1 Flow Diagram

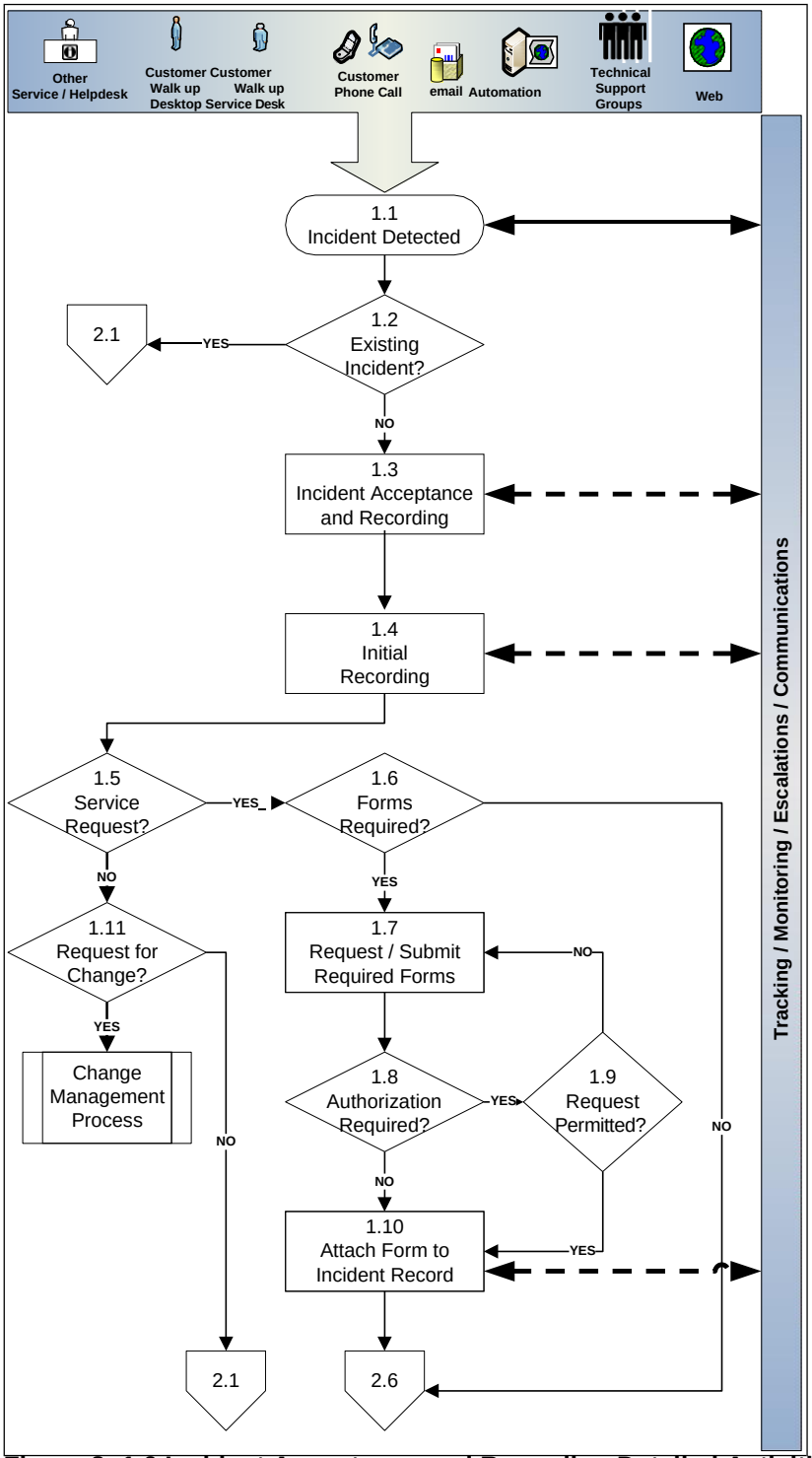


Figure 2: 1.0 Incident Acceptance and Recording Detailed Activities

4.1.2 Description

Once an incident is detected and reported to the Service Desk, the agent accepts the incident, records details in the Incident Record, and classifies the incident according to Configuration Item (CI), severity (impact), and urgency. Next, the Service Desk resource determines if the incident constitutes a service request and if so, invokes the Service Request process.

4.1.3 Input(s)

- Reported incident to the Service Desk
- System reports incident and automatically generates an alert

4.1.4 Detailed Activities

1.1 Incident Detected

- **Description:** Either a user or the Information Technology (IT) organization recognizes an incident.
- **Responsible Resources:**
  - Customer or technical-support groups
  - Proactive monitoring
  - automated alerts

1.2 Existing Incident?

- **Description:** An incident is classified as ‘existing’ if it has been previously recorded and the status is not set to ‘closed.’
- **Responsible Resource:** Service Desk agent

1.3 Incident Acceptance and Recording

- **Description:** The Service Desk resource accepts and records the incident as defined by Incident Management process.
- **Responsible Resource:** Service Desk agent

1.4 Initial Recording

- **Description:** The Service Desk resource classifies the incident by Configuration Item (CI), severity (impact), and urgency.
- **Responsible Resource:** Service Desk agent

1.5 Service Request?

- **Description:** The Service Desk resource determines if the reported incident qualifies as a Service Request. Service Requests are simple tasks or requests for information that are not caused by the service itself, but rather by a (unique) facet of an existing, functioning system (for example, a user can not log into Outlook.)
- **Responsible Resource:** Service Desk agent

1.6 Forms Required?

- **Description:** All security-related incidents require completed forms
- **Responsible Resource:** Service Desk agent

1.7 Request/ Submit Required Forms

- **Description:** For some Service Requests, the appropriate level of authorization is required to meet compliancy standards.
- **Responsible Resources:**
  - Service Desk agent
  - Requestor

1.8 Authorization Required?

- **Description:** Authorization is necessary if the incident has been categorized as requiring management-level approval.
- **Responsible Resources:**
  - Service Desk agent
  - Requestor

1.9 Request Permitted?

- **Description:** The request is permitted if the forms received contain the appropriate signature confirmation.
- **Responsible Resources:**
  - Service Desk agent
  - Requestor

1.10 Attach Form to Incident Record

- **Description:** The Service Desk agent receives the required form from the customer or department head.
- **Responsible Resource:** Service Desk agent

1.11 Request for Change?

- **Description:** If a Request for Change is required, the Change Management process is invoked.
- **Responsible Resources:**
  - Service Desk agent
  - Data Operations
  - N-level support

4.1.5 Outputs

- Standard Incident Record with correct incident and customer details
- Verification of Configuration Management Database (CMDB) customer details
- Potential major incident notification
- Regular communication with all parties involved
- Status update in the CMDB

4.1.6 Related Processes and Procedures

- **Change Management**
  - Request for Change (RFC) submitted for any changes to Configuration Management Database (CMDB)
  - Use of Forward Schedule of Changes (FSC)
- **Configuration Management**
  - Captures Configuration Management Database (CMDB) information
  - Verifies customer information against CMDB
  - Exceptions in CMDB
  - Assessments for impact of incidents
- **Problem Management**
  - Potential reporting of major incidents becoming problems
- **Release Management**
  - Use of Forward Schedule of Changes (FSC)
- **Service Level Management**
  - Informed of potential breaches

4.2 2.0 Classification and Prioritization

4.2.1 Flow Diagram

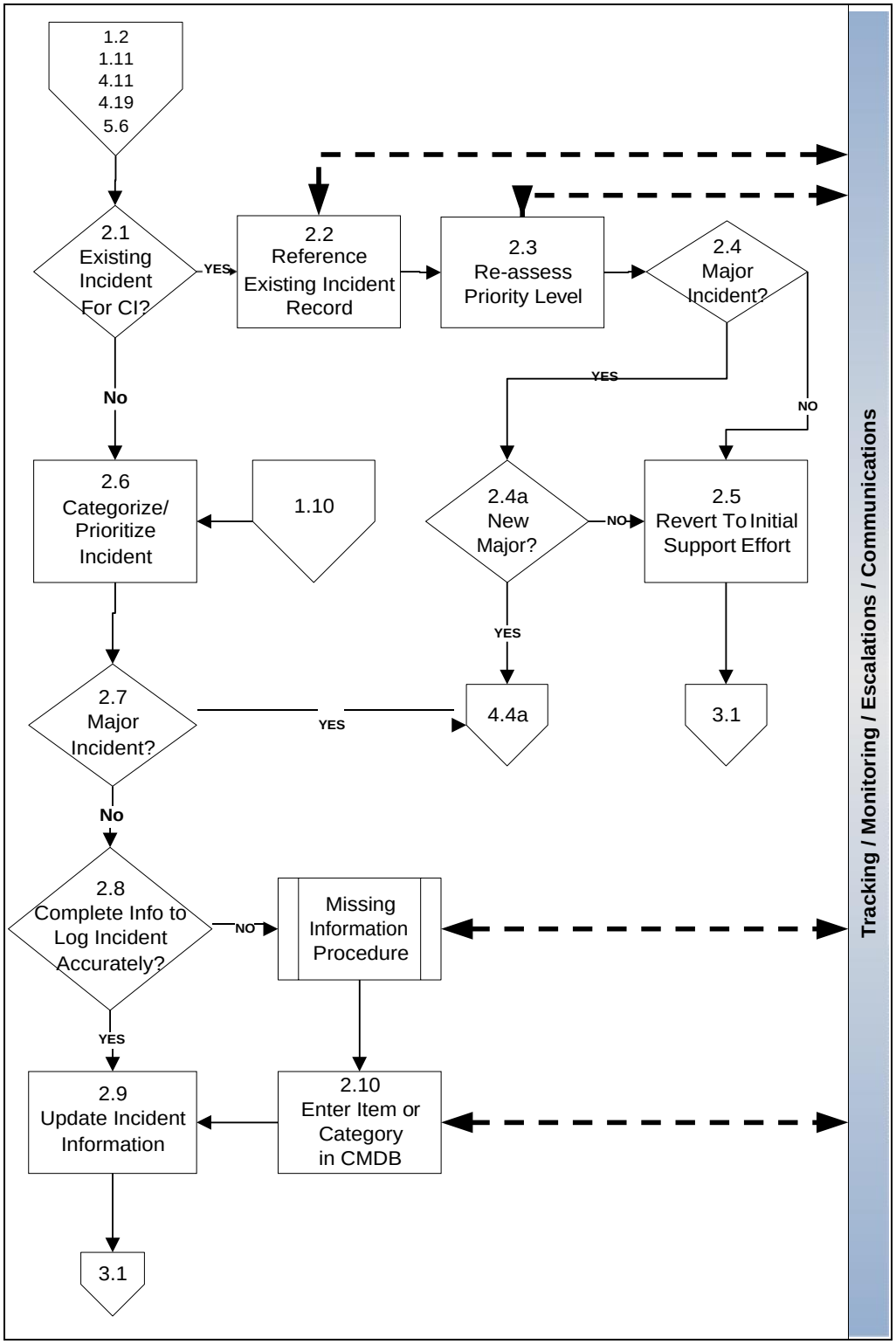


Figure 3: 2.0 Classification and Prioritization Detailed Activities

4.2.2 Description

The Service Desk agent determines if an incoming Incident is new or existing. The agent links incoming incidents to existing tickets in the Knowledge Base in order to re-assess the priority level with all available information. The Service Desk resource also categorizes the incident and ensures all information in the Incident Record is accurate and up to date.

4.2.3 Input(s)

- Open incident
- Verification of customer details in Configuration Management Database (CMDB)

4.2.4 Detailed Activities

2.1 Existing Incident for Configuration Item (CI)?

- **Description:** Service Desk resource checks the incoming incident against the Configuration Management Database (CMDB) to assess if the incident is new or existing.
- **Responsible Resource:** Service Desk agent

2.2 Reference Existing Incident Record

- **Description:** If the incident exists, the Service Desk resource links the incoming incident to the existing incident in the Configuration Management Database (CMDB).
- **Responsible Resource:** Service Desk agent

2.3 Re-assess Priority Level

- **Description:** The Service Desk resource adds any supplemental information to the Incident Record and re-evaluates the impact and priority of the incident, which may change depending on the severity and number of associated incidents.
- **Responsible Resource:** Service Desk agent

2.4 Major Incident?

- **Description:** An Incident is considered major if it has a high impact, or potentially high impact, which requires a more urgent response than that given to normal incidents.
- **Responsible Resource:** Service Desk agent

2.4 a New Major Incident?

- **Description:** The Service Desk agent determines if the major incident already exists in the database.
- **Responsible Resource:** Service Desk agent

2.5 Revert to Initial Support Effort

- **Description:** To resolve the Incident effectively, all resolution efforts should focus on the initial, or first-recorded, Incident.
- **Responsible Resource:** Service Desk agent

2.6 Categorize/ Prioritize Incident

- **Description:** The Service Desk agent codes the incident to ensure that the incident is assigned to the appropriate group in a timely manner. *Appendix A – Incident Prioritization Model* provides more information about assigning a priority value to incidents.
- **Responsible Resource:** Service Desk agent

2.7 Major Incident?

- **Description:** If the reported incident is causing, or potentially could cause, a high impact to the business, requiring a more urgent response than normal incidents.
- **Responsible Resource:** Service Desk agent

2.8 Enough Information for the Service Desk to Log Incident Information Accurately?

- **Description:** The Service Desk agent determines if the Configuration Management Database (CMDB) contains appropriate classification options and if the Configuration Item (CI) is missing from the CMDB.
- **Responsible Resource:** Service Desk agent

2.9 Update Incident Information

- **Description:** The Service Desk agent updates the Incident Record with all relevant information.
- **Responsible Resource:** Service Desk agent

2.10 Enter Item or Category in the CMDB

- **Description:** The Service Desk agent enters the missing item or category if appropriate classification options do not exist in the Change Management Database (CMDB) or if the Configuration Item (CI) does not exist in the CMDB.
- **Responsible Resource:** Service Desk agent

4.2.5 Outputs

- Standard Incident Record with required information
- Possible link to problem or known error
- Possible workaround
- Notification to management for high-impact incidents
- Regular communication with all parties involved
- Status update in the Configuration Management Database (CMDB)

4.2.6 Related Processes and Procedures

- **Configuration Management**
  - Provides Configuration Item (CI) details from Configuration Management Database (CMDB)
  - Receives any changes/ discrepancies related to Configuration Item (CI) data

- **Problem Management**
  - Provides service problem, known error, and work-around information
  - Receives potential problems based on multiple and/ or high impact incidents
  - Links problems and known errors to Incident Records

- **Service Level Management**
  - Provides Service Level Agreement (SLA) information for priority and escalation

4.3 3.0 Initial Support and Incident Matching

4.3.1 Flow Diagram

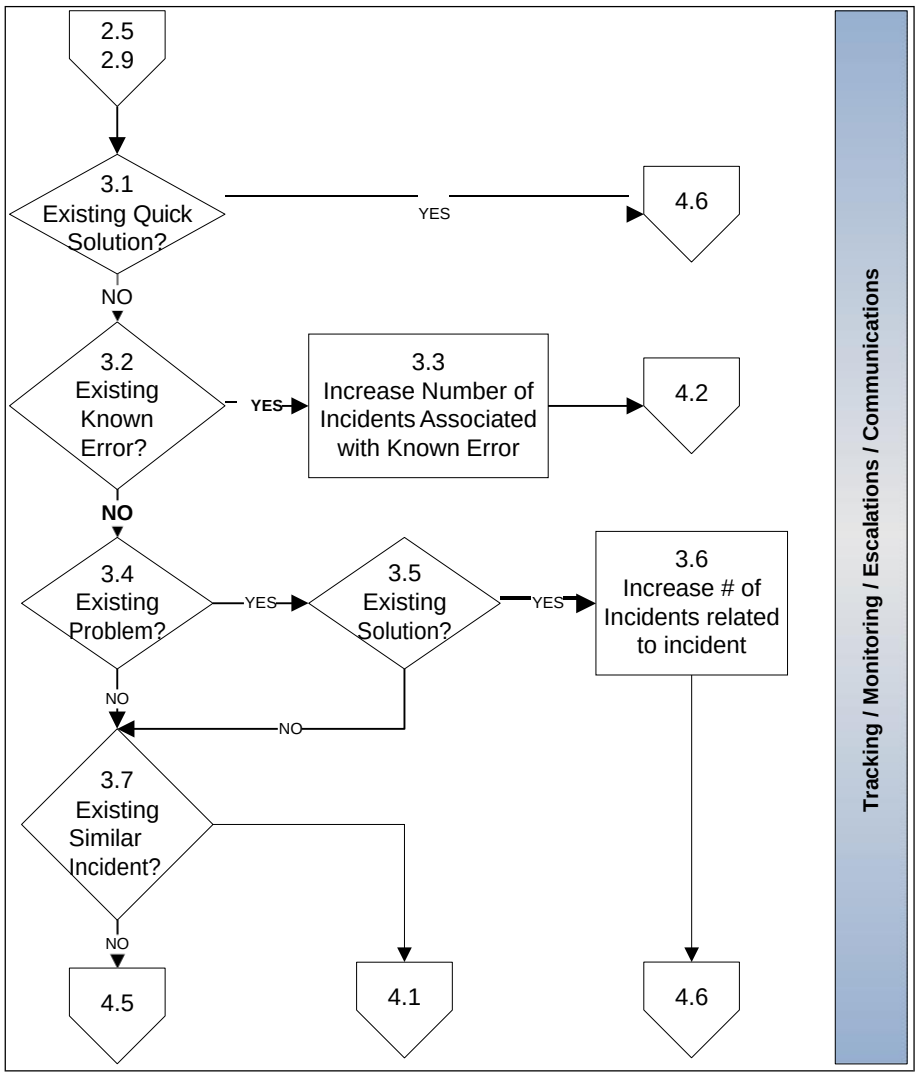


Figure 4: 3.0 Initial Support and Incident Matching Detailed Activities

4.3.2 Description

The Service Desk agent analyzes all the information entered into the Incident Record about the incident. Next, the agent determines if the incident is a known error or a known problem. Matching current incidents to previous errors and problems brings together all available information regarding symptoms, effects, and resolution.

4.3.3 Input(s)

- Updated incident details
- Configuration Item (CI) details from Configuration Management Database (CMDB)

4.3.4 Detailed Activities

3.1 Existing Quick Solution?

- **Description:** The Service Desk agent analyzes all information available about the incident. After review, the agent verifies and modifies, if necessary, incident classification information. The agent also decides if there is an easy resolution to the incident.
- **Responsible Resource:** Service Desk agent

3.2 Existing/ Known Error?

- **Description:** Service Desk resource checks the incoming incident against the database of existing errors to assess if the incident is new or existing. If existing, the Service Desk agent links the incident to the error.
- **Responsible Resource:** Service Desk agent

3.3 Increase Number of Incidents Associated with Known Error

- **Description:** Increasing the number of incidents associated with a known error allows the known error to be prioritized according to the level of attention required.
- **Responsible Resource:** Service Desk agent

3.4 Existing Problem?

- **Description:** The Service Desk resource checks the incoming incident against the database of existing problems to assess if the incident is new or existing. If existing, the Service Desk agent links the incident to the problem.
- **Responsible Resource:** Service Desk agent

3.5 Existing Solution?

- **Description:** The Service Desk agent looks for a known solution that is readily available.
- **Responsible Resource:** Service Desk agent

3.6 Increase Number of Incidents Associated with Problem

- **Description:** If an incident already exists, the Service Desk agent increases the number of incidents linked to this problem so that more information may be available for resolution.
- **Responsible Resource:** Service Desk agent

3.7 Existing Similar Incident?

- **Description:** The Service Desk agent tries to match the incident to similar incidents in the database to assist in resolving the incident.
- **Responsible Resource:** Service Desk agent

4.3.5 Outputs

- Updated Incident Record details
- Possible work-arounds or resolutions
- Regular communication with all parties involved
- Status update in the Configuration Management Database (CMDB)

4.3.6 Related Processes and Procedures

- **Configuration Management**
  - Provides Configuration Item (CI) details from Configuration Management Database (CMDB)
- **Problem Management**
  - Reviews work-arounds and problem/ known error records

4.4 4.0 Investigation and Diagnosis

4.4.1 Flow Diagram

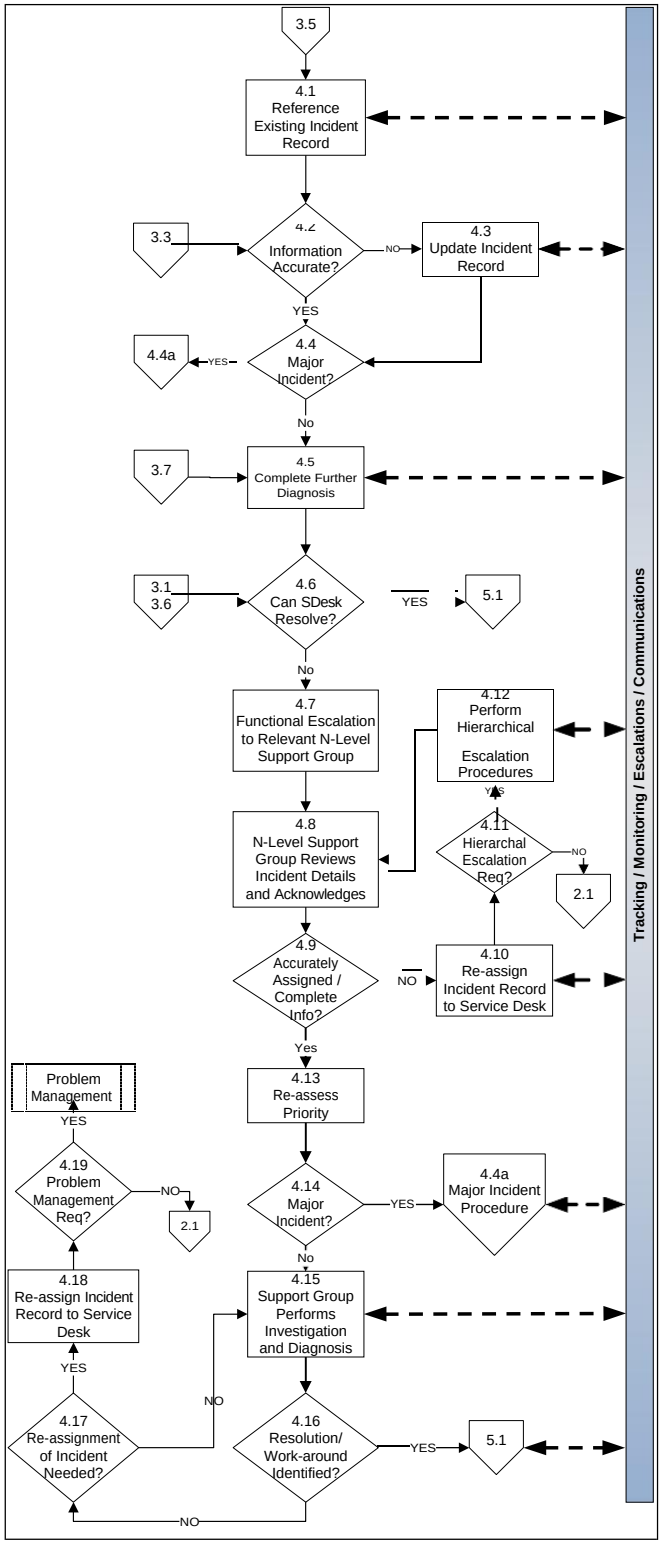


Figure 5: 4.0 Investigation and Diagnosis Detailed Activities

4.4.2 Flow Diagram for Major Incidents

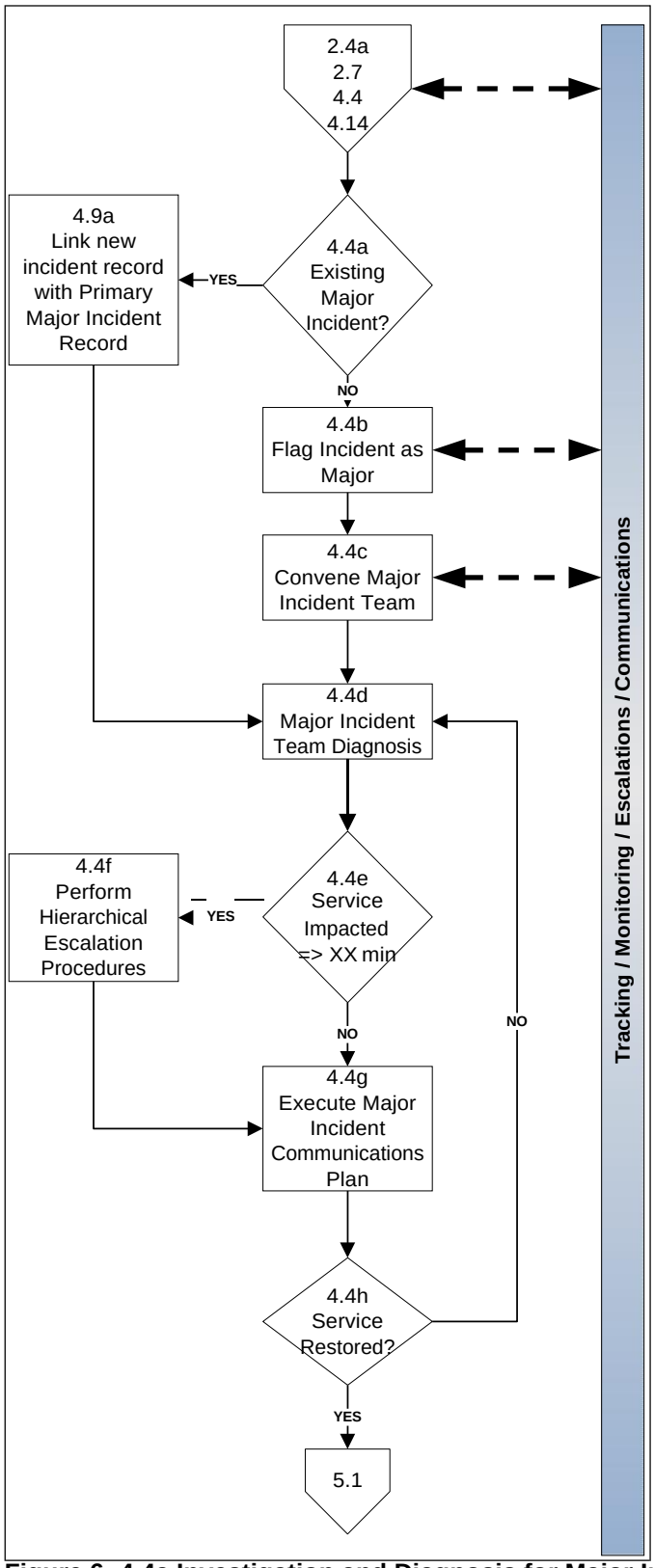


Figure 6: 4.4a Investigation and Diagnosis for Major Incidents

4.4.3 Description

The Service Desk resource reviews the Incident Record to ensure that all information is correct. When all incident information has been accurately captured, the agent determines if the Service Desk can resolve or if the incident must be escalated and assigned to an appropriate service department.

4.4.4 Input

Updated Incident Record details

4.4.5 Detailed Activities

4.1 Reference Existing Incident Record

- **Description:** Service Desk resource looks up incident information contained in the Incident Record
- **Responsible Resource:** Service Desk agent

4.2 Information Accurate?

- **Description:** The Service Desk agent reviews Incident Record information to ensure that all information is recorded accurately.
- **Responsible Resource:** Service Desk agent

4.3 Update Incident Record

- **Description:** If any information is not recorded accurately, the Service Desk resource updates the Incident Record with appropriate data.
- **Responsible Resource:** Service Desk agent

4.4 Major Incident?

- **Description:** An incident is considered major if it is causing or potentially could cause, a high impact to the business and requires a response that is above and beyond that given to normal incidents.
- **Responsible Resource:** Service Desk agent

4.5 Complete Further Diagnosis

- **Description:** The Service Desk resource re-assesses all the details contained in the Incident Record to collect and analyze all related information, including checking error logs.
- **Responsible Resource:** Service Desk agent

4.6 Can Service Desk Resolve?

- **Description:** After investigating all incident information, the Service Desk agent determines if the Service Desk can resolve the Incident. If the Service Department can fix the incident, then the *5.0 Resolution and Recovery* process begins. If not, the Service Desk resource escalates the incident to the next level of support.
- **Responsible Resource:** Service Desk agent

4.5 5.0 Resolution and Recovery

4.5.1 Flow Diagram

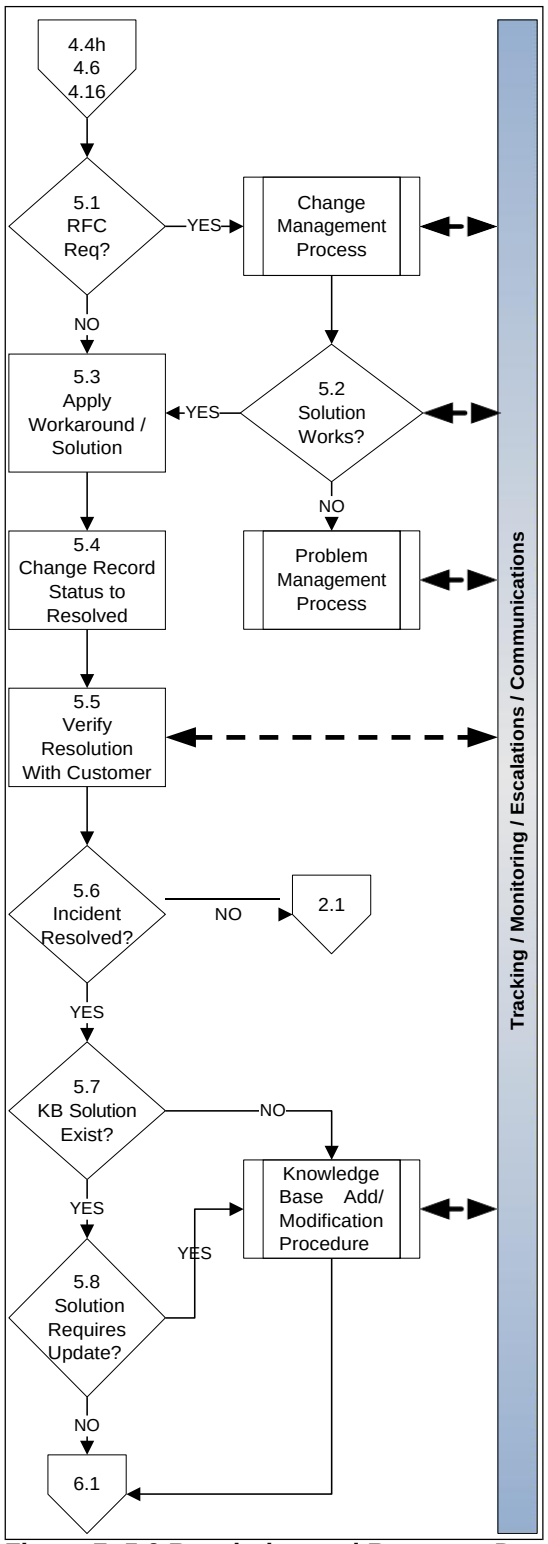


Figure 7: 5.0 Resolution and Recovery Detailed Activities

4.5.2 Description

Either the Service Desk agent or the assigned service department fixes the incident, the resolution of which the agent confirms with the customer. The agent updates the existing Incident Record with applicable solution information or creates a new Knowledge Base solution record, as appropriate.

4.5.3 Input(s)

Updated Incident Record details

4.5.4 Detailed Activities

5.1 Request for Change (RFC) Required?

- **Description:** The Service Desk agent determines if the solution requires submission of an RFC? If so, the Change Management process is invoked.
- **Responsible Resource:** Service Desk agent

5.2 Solution Works?

- **Description:** The solution works if it adequately resolves the reported incident when applied. The customer should be able to perform work duties after the solution has been applied.
- **Responsible Resource:** Customer

5.3 Apply Work-around/ Solution

- **Description:** Either a known work-around or non-documented work-around solution is applied to keep service to the customer functional.
- **Responsible Resource:** Service support group

5.4 Change Incident Record Status to 'Resolved'

- **Description:** The Service Desk agent marks the status of the ticket as 'resolved'.
- **Responsible Resource:** Service Desk agent

5.5 Verify Resolution with Customer

- **Description:** Once the resolution has been implemented, the Service Desk agent verifies the solution meets the customer's requirements.
- **Responsible Resource:** Service Desk agent

5.6 Incident Resolved?

- **Description:** If the customer does not approve of the incident's resolution, the Service Desk resource changes the incident's status to 'open' and further investigates and diagnoses the incident.
- **Responsible Resource:** Service Desk agent

5.7 Does a Knowledge Base Solution Exist?

- **Description:** The Service Desk agent searches the Knowledge Base to see if the incident exists.
- **Responsible Resource:** Service Desk agent

5.8 Solution Requires Update?

- **Description:** If the Knowledge Base does not contain all relevant information pertaining to the incident and its resolution, the Service Desk agent invokes the Knowledge Base Add/ Modification process to add all pertinent details.
- **Responsible Resource:** Service Desk agent

4.5.5 Outputs

- Resolution of incident
- Recovery details
- Results of Request for Change (RFC), as required
- Updated incident details in Knowledge Base
- Regular communication with all parties involved
- Status update in the Configuration Management Database (CMDB)

4.5.6 Related Processes and Procedures

- **Availability Management**
  - Receives the required information for service availability reports
- **Change Management**
  - Possible Request for Change (RFC)
- **Problem Management**
  - Receives results of work-around
  - Possible recovery solutions
  - Information regarding trends analysis
- **Service Level Management**
  - Provides information pertaining to Service Level Agreement (SLA) information and Operational Level Agreements (OLAs) with respect to resolution and recovery

4.6 6.0 Incident Closure

4.6.1 Flow Diagram

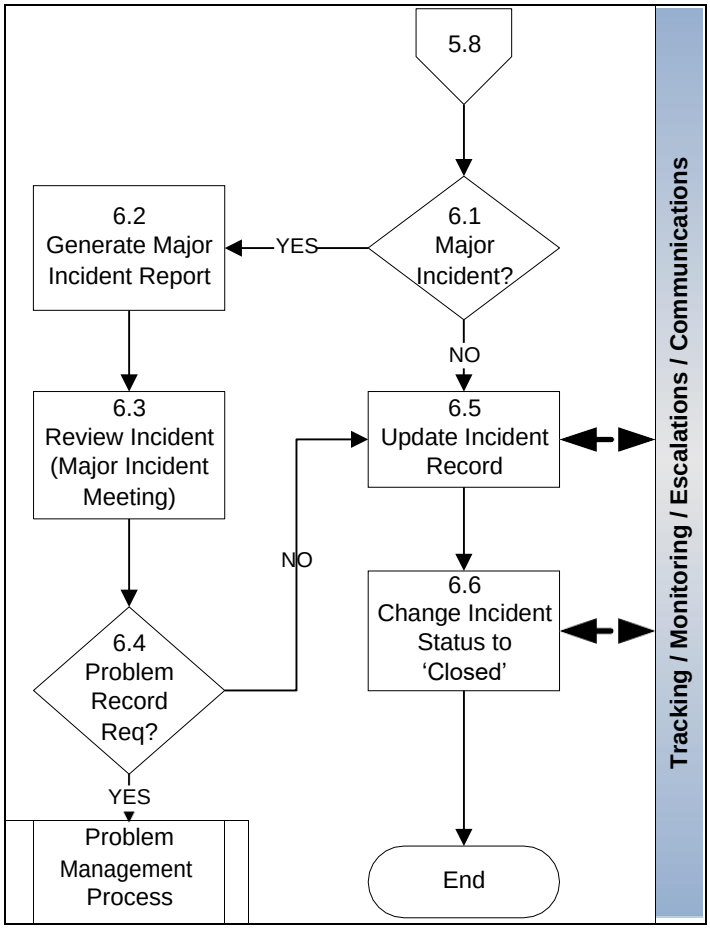


Figure 8: 6.0 Incident Closure Detailed Activities

4.6.2 Description

When the Configuration Item (CI) is returned to a working state or the Service Request is fulfilled, the Service Desk agent updates the Incident Record and marks its status as closed.

4.6.3 Input(s)

Updated Incident Record details

4.6.4 Detailed Activities

6.1 Incident Prioritized as Major?

- **Description:** The Service Desk agent determines if the incident is a major incident. If yes, the agent runs a report and sets up a meeting. If not, the status is changed to 'closed.'

- **Responsible Resources:**
  - Service Desk
  - N-level support

6.2 Generate Major Incident Report

- **Description:** A major incident report is created and generated in PDF format to present during major incident review meeting. The major incident report is on a per-incident basis.
- **Responsible Resource:** Incident Manager

6.3 Review Incident (Major Incident Meeting)

- **Description:** A meeting is set up to include all technical support department personnel who are associated with the major incident, as well as a representative from the Data Operations team and the Wyndham Hotel Group Service Desk.
- **Responsible Resources:**
  - Service Desk agent
  - Incident Manager
  - Operations resource
  - major incident support staff

6.4 Problem Record Required?

- **Description:** A decision is made during the major incident review meeting if a problem record will be created.
- **Responsible Resource:** Service Desk agent

6.5 Update Incident Record

- **Description:** The Service Desk agent updates the information on the Incident Record in the Knowledge Base.
- **Responsible Resource:** Service Desk agent

6.6 Change Incident Status to ‘Closed’

- **Description:** The Service Desk resource updates the status of the incident to ‘closed’.
- **Responsible Resource:** Service Desk agent

4.6.5 Outputs

- Closed incident
- Updated incident details in Knowledge Base
- Regular communication with all parties involved
- Status update in the Configuration Management Database (CMDB)

4.6.6 Related Processes and Procedures

- **Change Management**
  - Possible Request for Change (RFC)
- **Service Level Management**
  - Provides information pertaining to Service Level Agreement (SLA) information and Operational Level Agreements (OLAs) with respect to resolution and recovery

4.7 Roles and Responsibilities Matrix (ARCI Matrix)

The following table lists Detailed Activities and the role each key resource plays in carrying out the task, using the letters A, R, C, and I to denote the extent of resource involvement.

A – Accountable: The resource is accountable for the final result.
R – Responsible: The individual executes the task.
C – Consulted: The resource is consulted for additional information
I – Informed: The resource is kept up to date on activity progress

Step	Activity/ Task	Incident Process Owner	Incident Manager	Service Desk	Data Operations Center	N-Level Support	Customer
1.0 Incident Acceptance and Recording							
1.1	Incident Detected	A	I	R/C/I	R/C/I	R/C/I	C/I
1.2	Existing Incident?	A	I	R/C/I	C/I	C/I	C/I
1.3	Incident Acceptance and Recording	A	I	R	C/I	C/I	C/I
1.4	Initial Recording	A	I	R	C/I	C/I	C/I
1.5	Service Request?	A/I	A/I	R	C/I	C/I	C/I
1.6	Forms Required?	A/I	A/I	R	C/I	C/I	C/I
1.7	Request/ Submit Required Forms	A/I	A/I	R	C/I	C/I	R/C/I
1.8	Authorization Required?	A/I	A/I	R	R/C/I	R/C/I	C/I
1.9	Request Permitted?	A/I	A/I	R	R/C/I	R/C/I	C/I
1.10	Attach Form to Incident Record	A/I	A/I	R	C/I	C/I	C/I
1.11	Request for Change?	A/I	A/I	R	C/I	C/I	C/I
2.0 Classification and Prioritization							
2.1	Existing Incident for CI?	A	I	R/C/I	R/C/I	C/I	C/I
2.2	Reference Existing Incident Record	A	I	R/C/I	R/C/I	R/C/I	I
2.3	Re-assess Priority Level	A	I	R/C/I	R/C/I	R/C/I	C/I
2.4	Major Incident?	A	I	R/C/I	C/I	C/I	I
2.4a	New Major Incident?	A	I	R/C/I	C/I	C/I	I
2.5	Revert to Initial Support Effort	A	I	R/C/I	C/I	C/I	I
2.6	Categorize/ Prioritize Incident	A	I	R/C/I	C/I	C/I	I
2.7	Major Incident?	A	I	R/C/I	C/I	C/I	I
2.8	Enough Information for Service Desk to Log Incident Info Accurately?	A	I	R/C/I	C/I	C/I	I

Step	Activity/ Task	Incident Process Owner	Incident Manager	Service Desk	Data Operations Center	N-Level Support	Customer
2.9	Update Incident Information	A	I	R/C/I	R/C/I	R/C/I	I
2.10	Enter Item or Category in the CMDB	TBD	TBD	TBD	TBD	TBD	TBD
3.0 Initial Support and Incident Matching							
3.1	Existing Quick Solution?	A	C/I	R/C/I	R/C/I	R/C/I	
3.2	Existing/ Known Error?	A	C/I	R/C/I	R/C/I	R/C/I	
3.3	Increase Number of Incidents Associated with Known Error	A	C/I	R/C/I	R/C/I	C/I	
3.4	Existing Problem?	A	I	R/C/I	R/C/I	C/I	
3.5	Existing Solution?	A	I	R/C/I	R/C/I	C/I	
3.6	Increase Number of Incidents Associated with Problem	A	I	R/C/I	R/C/I	C/I	
3.7	Existing Similar Incident?	A	I	R/C/I	R/C/I	C/I	
4.0 Investigation and Diagnosis							
4.1	Reference Existing Incident Record	A	I	R/C/I	R/C/I	R/C/I	C/I
4.2	Information Accurate?	A	R/C/I	R/C/I	R/C/I	R/C/I	C/I
4.3	Update Incident Record	A	C/I	R/C/I	R/C/I	R/C/I	C/I
4.4	Major Incident?	A	C/I	R/C/I	R/C/I	R/C/I	I
4.5	Complete Further Diagnosis	A	C/I	R/C/I	C/I	C/I	I
4.6	Can Service Desk Resolve?	A	I	R/C/I	C/I	C/I	I
4.7	Functional Escalation to Relevant N-level Support Group	A	I	R/C/I	R/C/I	R/C/I	
4.8	N-level Support Group Reviews Incident Details and Acknowledges.	A	I	R/C/I	R/C/I	R/C/I	
4.9	Accurately Assigned / Complete Information?	A	I	R/C/I	R/C/I	R/C/I	
4.10	Re-assign Incident Record to Service Desk	A	I	C/I	R/C/I	R/C/I	
4.11	Hierarchal Escalation Required?	A	I	R/C/I	R/C/I	R/C/I	I
4.12	Perform Hierarchical Escalation Procedures	A	I	R/C/I	R/C/I	R/C/I	
4.13	Re-assess Priority	A	I	R/C/I	R/C/I	R/C/I	I
4.14	Major Incident?	A	I	R/C/I	R/C/I	R/C/I	

Step	Activity/ Task	Incident Process Owner	Incident Manager	Service Desk	Data Operations Center	N-Level Support	Customer
4.15	Support Group Performs Investigation and Diagnosis	A	I	R/C/I	R/C/I	R/C/I	
4.16	Resolution or Work-around Identified?	A	I	R/C/I	R/C/I	R/C/I	
4.17	Re-assignment of Incident Needed?	A	I	R/C/I	R/C/I	R/C/I	
4.18	Re-assign Incident Record to Service Desk	A	I	R/C/I	R/C/I	R/C/I	
4.19	Problem Management Required?	A/I	A/I	R/C/I	R/C/I	R/C/I	
4.4a	Existing Major Incident?	A	I	R/C/I	R/C/I	R/C/I	
4.4b	Flag Incident as Major	A	I	R/C/I	C/I	C/I	
4.4c	Convene Major Incident Team	A	I	R/C/I	R/C/I	I	
4.4d	Major Incident Team Diagnosis	A	I	R/C/I	R/C/I	R/C/I	
4.4e	Service Impacted > XX Minutes?	A	I	R/C/I	R/C/I	R/C/I	
4.4f	Perform Hierarchical Escalation Procedures	A	I	R/C/I	R/C/I	R/C/I	I
4.4g	Execute Major Incident Communications Plan	A	I	R/C/I	R/C/I	I	I
4.4h	Service Restored?	A	I	R/C/I	R/C/I	R/C/I	C/I
5.0 Resolution and Recovery							
5.1	RFC Required?	A	I	C/I	C/I	R/C/I	I
5.2	Solution Works?	A	R/C/I	R/C/I	R/C/I	R/C/I	C/I
5.3	Apply Work-around/ Solution	A	C/I	R/C/I	R/C/I	R/C/I	C/I
5.4	Change Record Status to Resolved	A	C/I	R/C/I	R/C/I	R/C/I	I
5.5	Verify Resolution with Customer	A	C/I	R/C/I	C/I	C/I	I
5.6	Incident Resolved?	A	I	R/C/I	C/I	C/I	I
5.7	Knowledge Base Solution Exist?	A	I	R/C/I	R/C/I	R/C/I	
5.8	Solution Requires Update?	A	I	R/C/I	R/C/I	R/C/I	
6.0 Incident Closure							
6.1	Incident Prioritized as Major?	A	I	R/C/I	R/C/I	R/C/I	

Step	Activity/ Task	Incident Process Owner	Incident Manager	Service Desk	Data Operations Center	N-Level Support	Customer
6.2	Generate Major Incident Report	A	R	I	I	I	
6.3	Review Incident (Major Incident Meeting)	A	R	C/I	C/I	C/I	
6.4	Problem Record Required?	TBD	TBD	TBD	TBD	TBD	TBD
6.5	Update Incident Record	A	I	R/C/I	R/C/I	R/C/I	C/I
6.6	Change Incident Status to ‘Closed’	A	I	R/C/I	C/I	C/I	I

5. Management and Reporting Information

Best practices in Service Management identify the following four quadrants as a representation of a dashboard by which the Process Owners can determine the health of a process. A minimum of one or two measurements is recommended to be used for each quadrant to ensure a balanced perspective on the use and effectiveness of the process. The categories/quadrants are:

- **Value:** Reports or surveys to measure the effectiveness and perceived value of the process to the stakeholders and users.
- **Quality**: Process quality indicators are typically activity based and are established to measure the quality of individual or key activities as they relate to the objective of the end-to-end process.
- **Performance**: Metrics established under this quadrant measure the average process throughput or cycle time. (E.g. Metrics to capture the speed and performance of the stated process objective and output)
- **Compliance**: Process compliance seeks to measure the percentage of process deployment across the IT organization. A process may have a good perceived value, good quality and speedy throughput but only be adhered to by a fraction of the IT organization

Value represents the extent to which what we are doing is making a difference. Quality represents how well we are doing it, performance is how quickly we are able to do it, and compliance represent to what extent we are actually doing what we set out to do.

5.1 Critical Success Factors (CSFs) and Related Key Performance Indicators (KPIs)

5.1.1 CSF: Quickly Resolve Incidents

Key Performance Indicator (KPI)	Standard		Target	Report Name
Total volume of non-closed/ non-resolved incidents (standard = resolved before breaching SLA; target would be based on tier : SLA – "x" hrs	**SD**	TBD	TBD	TBD
	TSS	5 open tickets per tech at any one time. This includes those open for monitoring, health checks.	3 open tickets per tech	Daily Dashboard
Mean Time to Repair based on reported time and MTTR based on time the incident occurred	**SD**	Priority 1 = 938 min Priority 2= 130 min Priority 3= 878 min Priority 4= 1156 min Priority 5= 5882 min	Priority 1 = 80 min Priority 2= 130 min Priority 3= 170 min Priority 4= 340 min Priority 5= 340 min	Priority MTTR
	TSS	Priority 1 = TBD Priority 2= TBD Priority 3= TBD Priority 4= TBD Priority 5= TBD	TBD	Priority MTTR
Total Incident Volume	**SD**	TBD	TBD	Priority MTTR
	TSS	TBD	TBD	TSS Daily Dashboard

5.1.2 CSF: Maintain IT Service Quality

Key Performance Indicator (KPI)	Standard		Target	Report Name
Total number of incidents opened	SD	TBD	TBD	SD Reopened
	TSS	TBD	TBD	TBD
Total Number of reassignments	SD	TBD	TBD	TBD
	TSS	TBD	TBD	TBD

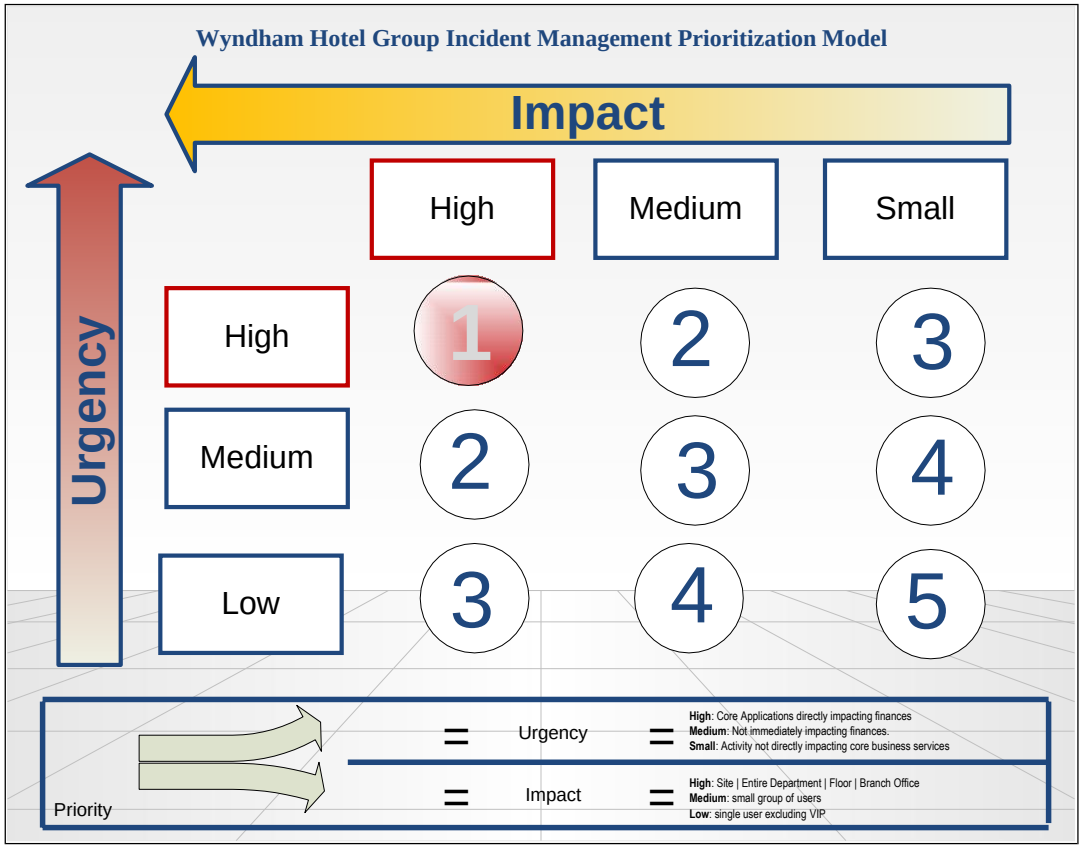
5.1.3 CSF: Improve IT and Business Productivity

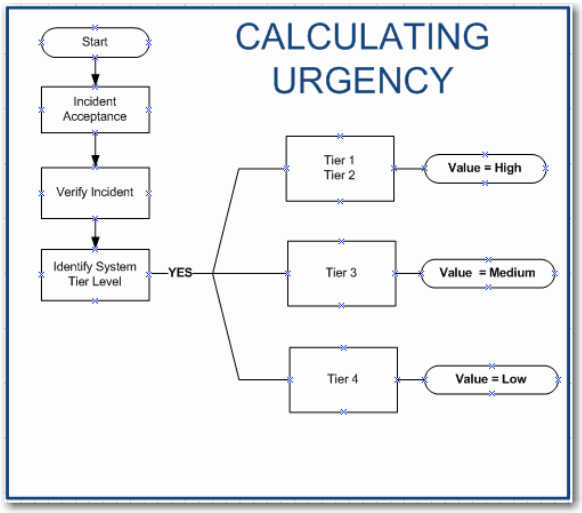
Key Performance Indicator (KPI)	Standard		Target	Report Name
Abandon Rate	SD	<10%	<8%	SD Telecom
	TSS	<15%	<8%	TSS Daily Dashboard
Average Speed of Answer	SD	<25 seconds	<20 seconds	SD Telecom
	TSS	<45 minutes	<35 minutes	TSS Daily Dashboard
Total number of reassignments	SD	<3	<2	SD Priority MTTR
	TSS	TBD	TBD	TBD
Percentage reduction in average cost of handling incidents	SD	5%	3%	SD Cost Per Contact
	TSS	2.6	3%	SD Cost Per Contact

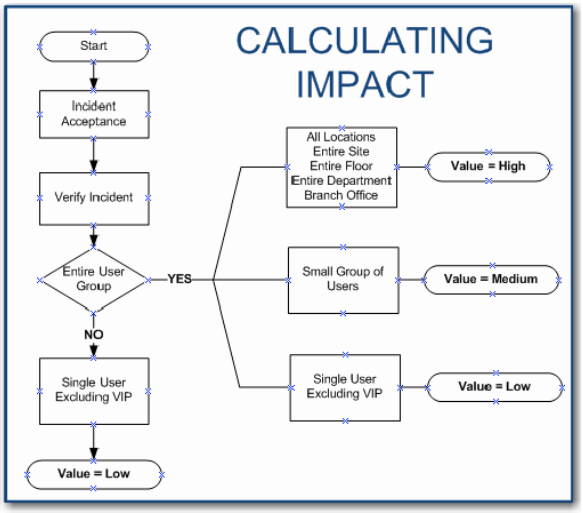
5.1.4 CSF: Maintain User Satisfaction

Key Performance Indicator (KPI)	Standard		Target	Report Name
Breach SLA Detail by Tier	**SD**	TBD	TBD	SD Tier MTTR
	TSS	TBD	TBD	TSS Daily Dashboard
Volume of non-closed/non-resolved incidents by priority level and support group	**SD**	TBD	TBD	SD Unresolved
	TSS	TBD	TBD	TSS Daily Dashboard

Appendix A – Incident Prioritization Model







Sample Urgency Calculation

- CRS – All Brands (HIGH)
- Opera ORS (HIGH)
- CMOR (HIGH)
- CTI (MEDIUM)
- Shared Drive (LOW)

Sample Impact Calculation

- Single User Finance Department (LOW)
- Single User Finance Department VIP (MEDUIUM)
- All General Reservations Agents Saint John (HIGH)

!

Figure 9: Incident Prioritization Model

Appendix B – Functional Escalation Flow Diagram

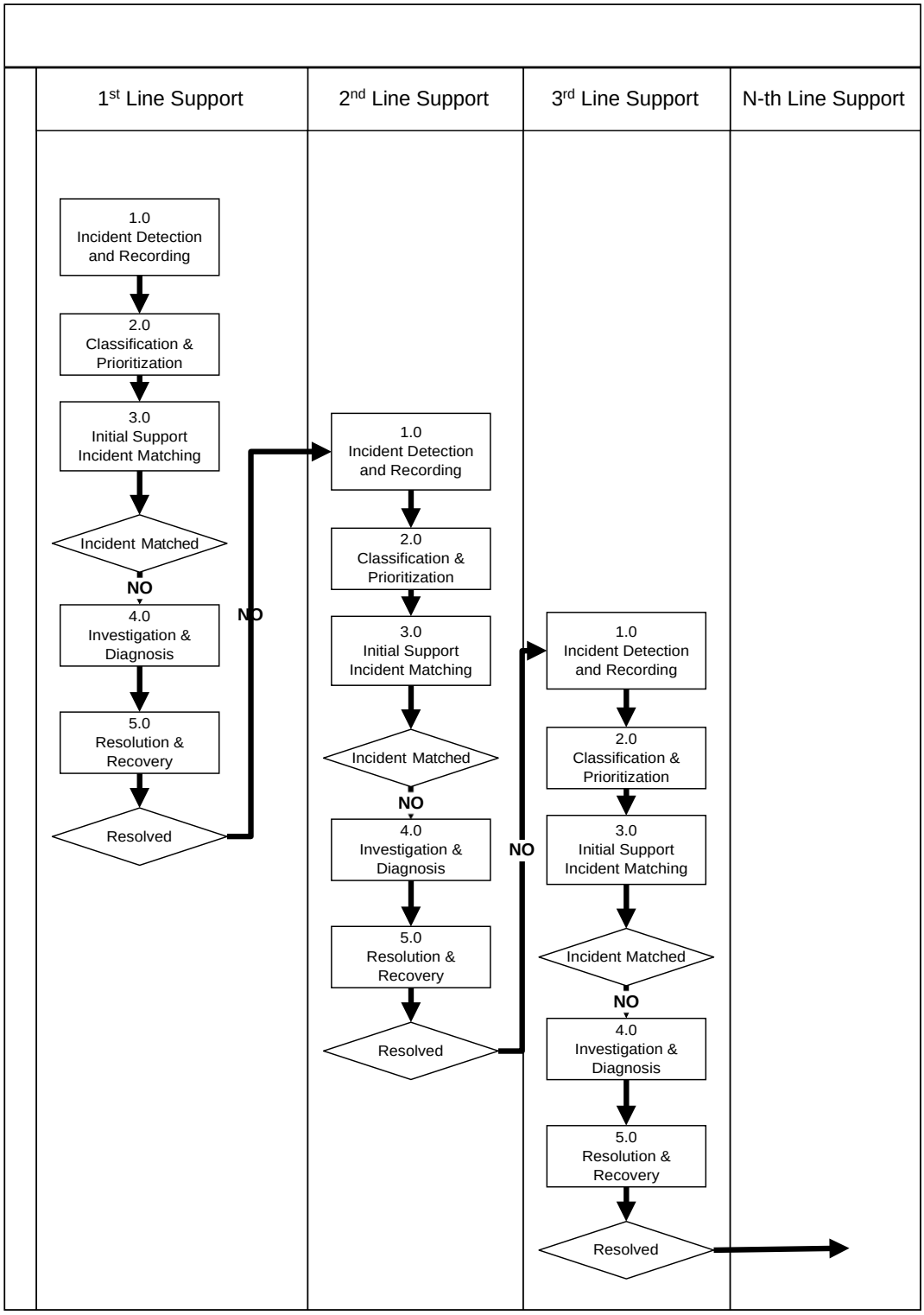


Figure 10: Functional Escalation Flow Diagram

Appendix C – Hierarchical Escalation Flow Diagram

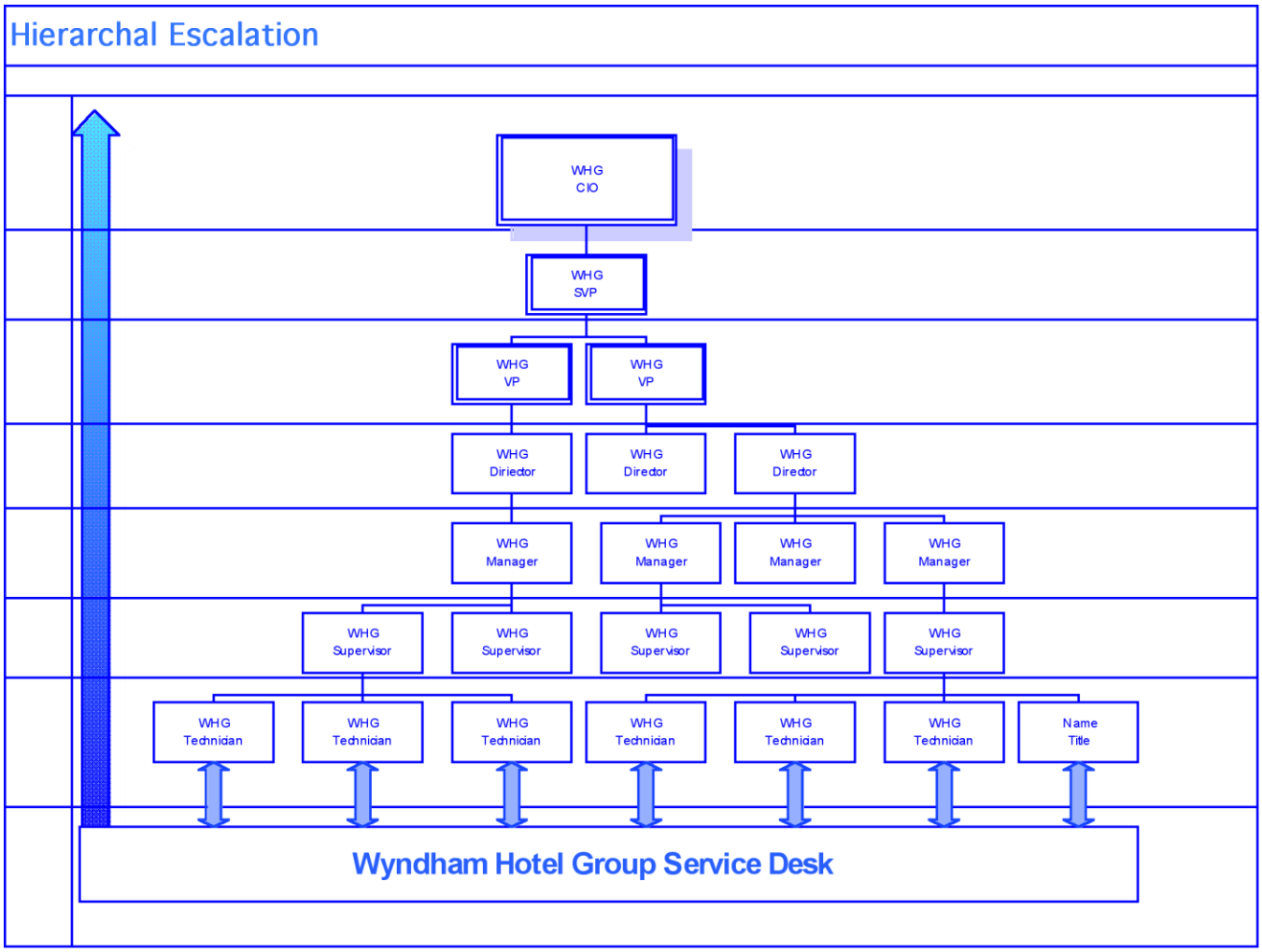


Figure 11: Hierarchical Escalation Flow Diagram

Appendix D – Functional and Hierarchical Escalation Flow Diagram

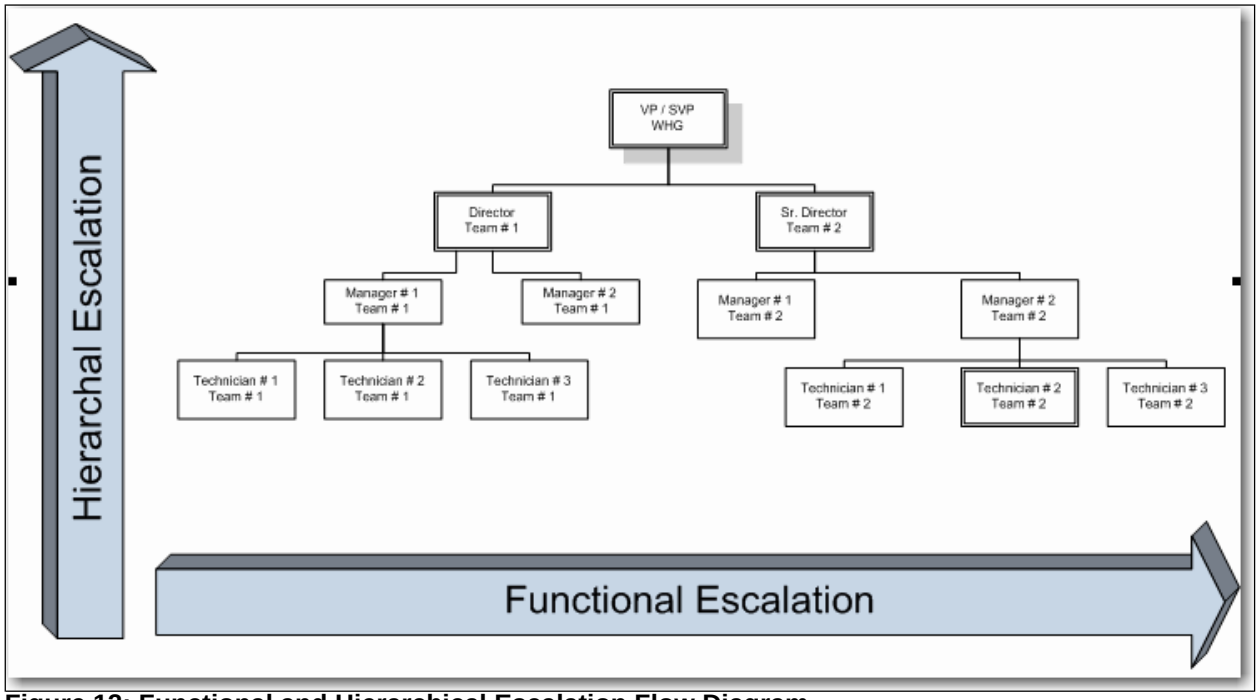


Figure 12: Functional and Hierarchical Escalation Flow Diagram

Appendix E – Incident Management Key Roles and Responsibilities

The following is a summary of roles and responsibilities defined by the IM process team in support of process execution and management.

6. Process Owner

6.1 Role

The person fulfilling this role is responsible for ensuring that the process is being performed according to the agreed and documented process and is meeting the aims of the process definition.

In general the Incident Management Process Owner:

- Has strong process competencies
- Has visibility at an executive management level
- Is respected for his or her process knowledge and ability to hold others accountable for day-to-day process operations
- Is customer focused and has a broad understanding of the customer's business processes enabled by IT services
- Works within the scope of the overall IT Service Management program
- Can coach and mentor the Incident Manager

There will be one, and only one, Incident Management Process Owner.

6.2 Responsibilities

- Assist with and ultimately be responsible for the process design
- Document and publicize the process
- Define appropriate policies and standards to be employed throughout the process
- Define Key Performance Indicators (KPIs) to evaluate the effectiveness and efficiency of the process and design reporting specifications
- Ensure that quality reports are produced, distributed and utilized
- Review KPIs and take action required following the analysis
- Periodically audit the process to ensure compliance to policy and standards
- Address any issues with the running of the process
- Review opportunities for process enhancements and for improving the efficiency and effectiveness of the process
- Ensure that all relevant staff have the required technical and business understanding, knowledge and training in the process and are aware of their role in the process
- Ensure that the process, roles, responsibilities and documentation are regularly reviewed and audited
- Interface with the line management, ensuring that the process receives the needed staff resources
- Provide input to the on-going Service Improvement Program
- Communicate process information or changes, as appropriate, to ensure awareness
- Review integration issues between the various processes
- Integrate the process into the line organization
- Promote the Service Management vision to top-level/senior management
- Function as a point of escalation when required
- Ensure that there is optimal fit between people, process and technology/tool

- Ensure that the Incident Management process is Fit for Purpose
- Attend top-level management meetings to assess and represent the Incident Management Requirements and provide Management Information

6.3 Authority

The Incident Management Process Owner:

- Has authority over the Incident Manager and Incident Management Analysts, where process activities are concerned
- Cannot enforce the use of the Incident Management Process, but can escalate any breaches to top-level management
- Should take remedial action as a result of any process non-compliance
- Has the authority to approve proposed changes to the Incident Management Process
- Can initiate research into changing tooling; however, the tool owner is responsible for the tool and will have the final say
- Can organize training for IT employees and can nominate staff. Cannot compel any staff to follow training, but can escalate to line management should training be required
- Will negotiate with the relevant Process Owner if there is a conflict between processes
- Is ultimately accountable for ensuring that capacity of the infrastructure matches the demand of the business in the most cost effective and timely manner

6.4 Other Information

The Incident Management Process Owner should possess an ITIL Foundation Certificate and be moving forward to achieve the ITIL Service Management Certificate

7. Incident Manager

7.1 Role

The Incident Manager is accountable to the Incident Management Process Owner and performs the day-to-day operational and managerial tasks demanded by the process activities.

In general the Incident Manager has:

- End-to-end responsibility for ensuring effective and efficient resolution of Incidents across the IT organization (1st, 2nd, 3rd levels and third party suppliers)
- Visibility at a senior management level
- Awareness of the customer's business priorities, objectives and business drivers
- Awareness of the role IT plays in enabling the business objectives to be met
- Customer service skills
- Awareness of what IT can deliver to the business, including the latest capabilities
- The ability to use, understand and interpret the Best Practice policies and procedures to ensure adherence
- Good influencing skills and is a good negotiator, as he or she often does not have authority over staff working with his or her processes
- The competence, knowledge and information necessary to perform the role

7.2 Responsibilities

- Promote and ensure that the Incident Management process is used correctly
- Provide management and other processes with strategic decision making information related to Incidents and potential Problems
- Ensure that the Incident Management Key Performance Indicators are met

- Ensure that the Incident Management process operates effectively and efficiently through 1st, 2nd, and 3rd line support and Third Party organizations
- Ensure that Incident Management Staff are empowered in their jobs
- Maximize the fit between people, process and technology
- Establish the Service Desk as a Single Point of Contact within the end-user community Work with the Service Desk Manager to ensure that the Service Desk is established as a Single Point of Contact within the end user community
- Ensure that remedial action takes place if it is discovered that contacts are going directly to second line or third line staff members instead of the Service Desk
- Provide the resolution of Incidents in a proper and timely manner as it is the end-responsibility of Incident Management. Ensure that Incidents are resolved in a proper and timely manner and the resolutions adhere to objectives set forth in Service Level Agreements
- Participate with the Incident Management Process Owner and Project Team in developing and maintaining the Incident Management Process, policies and procedures
- Drive the efficiency and effectiveness of the Incident Management Process
- Manage the work of the cross-functional Incident support staff (1st, 2nd and 3rd line)
- Produce Management Information
- Monitor the Incident Management process, using qualitative and quantitative Key Performance Indicators and make recommendations for improvement
- Play a key role in developing and maintaining the Incident Management systems
- Manage Major Incidents
- Function as a point of escalation for Incident Analysts
- Escalate to Line Management if Service Levels are threatened to be breached
- Coach Incident Management Analysts in the correct use of the process
- Identify training requirements of first line, second line and third line support staff and ensure that proper training is provided to meet the requirements
- Highlight customer and end user training and education needs through trending analysis and ensure that proper training is provided where necessary
- Contribute to the identification of recurring outages through trending analysis so that Problem Management is notified for assistance in eliminating recurring incidents that the business wants to eliminate
- Identify opportunities for improving the tools used
- Audit the Incident Management process
- Escalate to Line Management and the Incident Management Process Owner in the event of a conflict between process and Line Management
- Promote the Service Desk with the end-user community, through the maintenance of a web-page, info mails, bulletins and training Service Desk staff in communication skills, where needed
- Provide Service Desk staff with appropriate information to enable them to perform their function effectively. This includes process information, technical knowledge, record allocation information, and access to Known Error information

7.3 Authority

The Incident Manager:

- Has the accountability and authority to plan and manage end-to-end Incident Management requirements across all the IT services
- Functions as a point of escalation for Incident Management Analysts
- Escalates Service Level Agreement breaches to line management (directly to section managers, where applicable) and Process Management

- Escalates to Line Management and the Incident Management Process Owner in case of a conflict between process and Line Management. Escalation reports are sent to the Process Owners and Line Management
- Reports on all changes, specified per service, process, department and any other Key Performance Indicator that will be established
- Recommends service improvements
- Manages Incidents effectively through 1st, 2nd, and 3rd line support groups
- Monitors the Incident Management Activities and compliance for all departments and report results to Line Management or above
- Reports on all Incidents, specified per service, process, department, and any other Key Performance Indicator that will be established
- Escalates Service Level Agreement breaches to Line Management (where applicable directly to section managers) and Process Management
- Recommends improvements to people, process, and technology (tools)

7.4 Other Information

The Incident Manager should possess an ITIL Foundation Certificate and be moving forward to achieve the Practitioners Certificate for his or her specific process

8. Incident Management Analyst

8.1 Role

Incident Management Analysts are the line staff who are the subject matter experts for assessing, planning and monitoring Incident Management for their functional organization and specific technology platform. They function as contact people between the different departments for a specific process and may be responsible for the design of processes within their own departments.

In general the Incident Management Analyst:

- May be internal or external (vendor)
- Is a Subject Matter Expert in a specific technology platform
- Understands how the specific technology fits in with the overall IT service and Service life cycle
- Must be an effective communicator
- Is a respected member of a department who is able to combine daily departmental activities with the coordination role
- Knows how to ‘get things done’
- Has knowledge of specific IT Infrastructure to understand and analyze the data produced by the different monitors

8.2 Responsibilities

- Understand the process, procedures, work instructions, policies, required documentation and tools
- Use the process, procedures, work instructions, policies, required documentation and tools as designed
- Analyze usage and performance data for his or her specific technology platform and report on Performance against targets contained in Service Level Agreements (SLAs) and Operational Level Agreements (OLAs)
- Escalate to the Incident Manager, if required

8.3 Authority

The Incident Management Analyst:

- Signals and escalates (horizontally or vertically) Service Level Agreement breaches for Incident Management related issues
- Resists any pressure to bypass the Incident Management process.
- Escalates and/or indicates a need for more training and/or technical and organizational information

8.4 Other Information

The Incident Management Analyst should possess an ITIL Foundation Certificate

Appendix F – Glossary of Acronyms

Acronym	Definition
AIS	Application Integration Services
ARCI	Accountable/ Responsible/ Consulted/ Informed (responsibility matrix)
CAB	Change Advisory Board
CapEx	Capital Expenditure
CI	Configuration Item
CMDB	Configuration Management Database
CMS	Configuration Management System (CMDB)
CR	Change Record
DCR	Data Change Record
EC	Emergency Committee
EPIP	Enhancement Project Implementation Process
ET	Eastern Time
FIFO	First In First Out
FSC	Forward Schedule of Changes
HIT	Hotel Information Technology
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSC	Information Technology Service Continuity
KPI	Key Performance Indicators
LOS	Loss of Service
OLA	Operational-Level Agreement
PCB	Project Control Board
PIR	Post-Implementation Review
PM(S)	Property Management (System)
PMO	Project Management Office
PRF	Project Request Form
PSA	Projected Service Availability
QA	Quality Assurance
QCC	Quality Control Center (also QMO)
QMO	Quality Management Organization
RFC	Request For Change
SACM	Service Asset and Continuity Management
SCD	Supplier and Contract Database
SCM	Service Catalog Manager
SD	Service Desk
SDLC	Service Delivery Life Cycle
SIP	Service Improvement Plan/ Program
SLA	Service Level Agreement
SLR	Service Level Requirements
SMP	Service Management Program
SOC	Senior Operating Committee
TSS	Technical Support Services
UC	Underpinning Contract
VSAT	Video Satellite
WHG	Wyndham Hotel Group

Appendix G – Glossary of Terms, Roles, & Artifacts

Term	Definition
Availability	Ability of a component or service to perform its required function at a stated instant or over a stated period of time. It is usually expressed as the availability ratio, i.e. the proportion of time that the service is actually available for use by the customers within the agreed service hours.
Assyst	A commercial off-the-shelf Service Desk application tool from Axios installed and used by WHG
Axios	Axios provides WHG with Assyst, a Service Desk tool
Backout	Reverting to previous, trusted version or state
Baseline	A 'snapshot', or position, which is recorded. Although this position may be updated later, the baseline remains unchanged and available as a reference of the original state and as a comparison against the current position. An example of a baseline is an MTTR of 3 hours.
Build	The final stage in producing a usable configuration. The process involves taking one of more input Configuration Items and processing them (building them) to create one or more output Configuration Items e.g. software compile and load.
Business Unit	A segment of the business that has its own plans, metrics, income, and cost. Each business unit owns assets, which it uses to create value for customers in the form of goods or services.
Category	Classification of a group of Configuration Items, change documents, or problems
Change	The addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build, or associated documentation
Change Advisory Board (CAB)	A group of people who can give expert advice to the Change Management team on the implementation of changes. This Board is likely to be comprised of representatives from all areas within IT and representatives from business units.
Change Category	A group that is given the authority to approve change (for example. by a project board). Sometimes referred to as the Configuration Board.
Change Control	The procedure to ensure that all changes are controlled, including the submission, analysis, decision making, approval, implementation, and post-implementation of the change.
Change History	Auditable information that records, for example, what was done, when it was done, by whom, and why.
Change Implementer	The resource who is responsible for putting changes into the Production environment
Change Management	Process of controlling changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved changes with minimum disruption.
Change Record	A record containing details of which Configuration Items are affected by an authorized change (planned or implemented), and how. Each Change Record documents the life cycle of a single change. A Change Record is created for every Request for Change (RFC) that is received, even those that are subsequently rejected. Change Records reference the

	Configuration Items that are affected by the Change.
Change Requestor	The person or entity who asks for a change, which instigates the Change Management process
Classification (of Change)	Process of formally grouping Configuration Items by type (for example, software, hardware, documentation, environment, application.)
Configuration Item (CI)	Component of an infrastructure or an item, such as a Request for Change, associated with an infrastructure – that is (or is to be) under the control of Configuration Management. Configuration Items (CIs) may vary widely in complexity, size and type from an entire system (including all hardware, software and documentation) to a single module or a minor hardware components.
Configuration Management	The process of identifying and defining Configuration Items in a system, recording, and reporting the status of Configuration Items and Requests for Change, and verifying the completeness and correctness of Configuration Items
Configuration Management Database (CMDB)	A database that contains all relevant details of each Configuration Item (CI) and details of the important relationships between CIs
Critical Success Factor (CSF)	A factor that is vital to the success of the organization such that if the objectives associated with these factors are not achieved, the organization will fail, perhaps catastrophically so. CSFs are repeatable processes for making changes.
Customer	A person who buys goods or services. The customer of an IT service provider is the person or group that defines and agrees to the service level targets.
Downtime	The total period that a service or component is not operational, within agreed-upon service times
Emergency Change	A change that must be introduced as soon as possible; for example, to resolve a major incident or implement a security patch. The Change Management process will normally have a specific procedure for handling emergency changes.
Environment	A collection of hardware, software, network communications, and procedures that work together to provide a discrete type of computer service. There may be one or more environments on a physical platform (e.g. test, Production). An environment has unique features and characteristics that dictate how they are administered in similar, yet diverse, manners.
Escalation	If an incident can not be resolved by the first-line support team within the agreed-upon time, then the Service Desk consults resources with more expertise or authority.
Event	An alert or notification created by any IT service, CI, or monitoring tool. Events often require IT Operations personnel to take action and may lead to a logged incident.
(IT) Executive Sponsor	The executive-level sponsor for the business unit
Expedited Change	A change that needs to be implemented as soon as possible, but there is usually time for testing.
Failure	Loss of ability to operate to specification or to deliver the required output. IT services, processes, activities, and CIs may warrant the term ‘failure’; failures often lead to a logged incident.
First-Line Support	Member(s) of the Service Desk team who log and resolve all calls for the agreed-upon areas of support
Forward Schedule of	A schedule that contains details of all the changes approved for

Changes (FSC)	implementation and their proposed implementation dates. It should be agreed with the customers and the business, Service Level Management, the Service Desk and Availability Management. Once agreed, the Service Desk should communicate to the user community at large any planned additional downtime arising from implementing the changes, using the most effective methods available.
Group	A number of people who are similar in some way. People who perform similar activities, even though they may work on different technology or report into different organizational structures or even in different companies.
Hospitality Information Technology (HIT)	Wyndham Hotel Group's Information Technology group
Impact	Measure of the business criticality of an incident. Often equal to the extent to which an Incident leads to distortion of agreed or expected service levels
Incident	Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service
Incident Management	The process responsible for managing the lifecycle of all incidents. The primary objective of Incident Management is to return the IT service to customers as quickly as possible. The Incident Management process strives to resolve all incidents and to resolve services quickly.
Incident Record	A record of all Incident details that documents the life cycle of an incident
(IT) Infrastructure	The components of Wyndham Hotel Group's Information Technology hardware, software, data, telecommunication, facilities, procedures, and documentation
Key Performance Indicator (KPI)	A parameter for measuring progress relative to key objectives or Critical Success Factors in Wyndham Hotel Group; used to judge process performance with clearly defined objectives with measurable targets. An example of a KPI is a certain percentage of a reduction in the average time it takes to make changes.
Known Error	A problem becomes a known error when the team has identified the root cause and a temporary workaround or permanent alternative
Lead Time	The duration of time between the Request for Change and change implementation
Major Incident	The highest category of impact for an incident. A major incident results in significant disruption to the business.
Metrics	A measurable element of a specific process activity (for example, the number of RFCs received)
Mean Time Between Failures (MTBF)	The mean time between the recovery from one incident to the occurrence of the next incident. Also known as 'uptime', this metric relates to the reliability of the service.
Mean Time to Repair (MTTR)	The average time between the occurrence of a known fault and the recovery of service. Also known as 'downtime', MTTR is the sum of the detection time and the resolution time and relates to the recoverability and serviceability of the service
Operational Level Agreement	An internal arrangement detailing the delivery of services supporting Wyndham Hotel Group's Information Technology service delivery. An agreement between an IT service provider and another part of the same organization. An OLA supports

	the IT service provider's delivery of IT services to customers and defines the goods or services to be provided, as well as the responsibilities of both parties.
Post-Implementation Review (PIR)	A meeting held to discuss the lessons learned after a change has been implemented
Prioritization	The logical precedence of impact and urgency
Priority	A category used to classify the relative importance of an incident or change. Priority determines the sequence in which action must be taken is based on impact and urgency.
Problem	Unknown underlying cause of one or more incidents. Problems become known errors when the root cause is known and a temporary workaround or permanent alternative has been identified.
Procedure	A description of logically related activities and the resources that perform these tasks
Process	A logically related series of activities performed to achieve a defined objective
Process Owner	The Process Owner designs, coaches, and advocates for the process. This role remains after the process has been implemented and continues as an ongoing resource.
Recovery	Service has been restored to users.
Release	A collection of new and/ or changed CIs which are tested and introduced into the live environment together.
Request for Change (RFC)	Form, or screen, used to record details of a request for a Change to any CI within an infrastructure or to procedures and items associated with the infrastructure. It includes details of the proposed change.
Release	A collection of new and/ or changed CIs that are tested and introduced into the live environment together.
Risk	A measure of the vulnerability to which Wyndham Hotel Group may be subjected; risk is the combination of the probability of a business disruption and any associated losses.
Role	A set of responsibilities, activities and authorities granted to a person or team. A role is defined in a process. One person or team may have multiple roles, for example, the roles of Configuration Manager and Change Manager may be carried out by a single person.
Second-Line Support	Support once an incident has been referred to a technical support department for further diagnosis and action
(IT) Service	A set of related functions that Information Technology (IT) provides that act as a self-contained entity; a business-enabling function that one or more IT systems provide (for example, email); a service is a means of delivering value to the customer by facilitating the outcome the customer wants to achieve without the ownership of specific costs and risks. An IT service uses IT to support the customer's business processes.
Service Catalog	A database or structured document with information about all live IT services, including those available for deployment. The Service Catalog is the only part of the service portfolio published to customers and is used to support the sale and delivery of IT services. The Service Catalog includes information about deliverables, prices, contact points, ordering, and request processes.
Service Catalog Manger (SCM)	The resource responsible for managing the IT Service Catalog

Service Desk	The central point of contact between users and the Information Technology service management. The Service Desk processes incidents and requests, as well as provides an interface for the activities of other process areas
Service Improvement Plan/ Program (SIP)	An initiative to improve service quality and performance to meet customer needs
Service Level	A service level is a measured and reported achievement against one or more service level targets. The term is sometimes used informally to mean service level target.
Service Level Agreement (SLA)	A written agreement between a service provider and customer(s) that documents agreed-upon service levels for a service. The SLA describes the IT service, documents service level targets, and specifies the responsibilities of both the IT service provider and the customer. A single SLA may cover multiple IT services or multiple customers.
Service Level Management	The process of defining, agreeing upon, documenting, and managing the degree of service that is required and cost-justified. SLM is the process responsible for negotiating Service Level Agreements and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management processes, Operational Level Agreements, and Underpinning Contracts are appropriate for the agreed-upon service level targets. The SLM process monitors and reports on service levels and holds regular customer reviews.
Service Level Requirements	The blueprint for designing a service and its associated Service Level Agreements (SLAs); SLAs contain detailed customer needs and are used to develop, modify, and initiate services. An SLR is a customer requirement for an aspect of an IT service. SLRs are based on business objectives and are used to negotiate agreed service level targets.
Service Level Requirement	A commitment that is documented in a Service Level Agreement. Service level targets are based on Service Level Requirements and are needed to ensure that the IT service design is fit for purpose. Service level targets should be measurable and are usually based on Key Performance Indicators (KPIs).
Service Portfolio	The complete set of services that are managed by a Service Provider. The Service Portfolio is used to manage the entire life cycle of all services and includes three categories: Service pipeline (proposed or in development); Service Catalog (live or available for deployment); and retired services.
Service Portfolio Management	The process responsible for managing the Service Portfolio. Service Portfolio Management considers services in terms of the business value that they provide.
Service Provider	An organization supplying services to one or more internal or external customers. Service Provider is often used as an abbreviation for IT Service Provider.
Service Request	A request from a user for support, delivery, information, advice, or documentation that is not related to a failure in the Information Technology infrastructure. Service Requests are usually handled by the Service Desk and do not require an RFC.
System	An integrated composite that consists of one or more of the processes, hardware, software, facilities, and people, that provides a capability to satisfy a stated need or objective.

Third party	A person, group or business who is not part of the Service Level Agreement for an IT service, but is required to ensure successful delivery of that IT service. Requirements for third parties are typically specified in Underpinning Contracts or Operational Level Agreements.
Underpinning Contract	An agreement with an external supplier covering the delivery of services that support Wyndham Hotel Group's Information Technology' delivery of services. The third party provides goods or services that support delivery of an IT service to a customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed service level targets in an SLA.
Urgency	A measure of the business criticality of an Incident or Change based on the business needs of the customer
User	An individual who uses Information Technology services to perform routine activities
Work-around	Method of avoiding an incident or problem, either from a temporary fix or from a technique that means the customer is not reliant on a particular aspect of a service that is known to have a problem.

Notes