CWDS
Incident Management ITIL High Level Design

Created by:

Project Name: CWDS Service Desk Support Services Document
Document ID: Incident Management High Level Design
Version: 1.0
Issue Date: 2/23/2018

Revision History

Date	Version	Description	Author
12-Dec-17	1.0	Incident Management ITIL High Level Design	Jim McKennan

Approvals

Approver Name	Department/Role	Signature	Date

Table of Contents

1. Introduction

The purpose of this document is to provide a High Level or Management view of CWDS Incident Management (IM) process. The IM High Level Process Flow is the focal point for this document, with a corresponding section that defines each of the IM High Level Process Activities.

Global Process Policies spanning the entire IM Process, decided and agreed by CWDS IM Process Team, define the expected behavior for each Service Provider (internal and external) with responsibilities for the day-to-day process operations.

Touch points with other Service Management Processes are listed in the final section. These touch points identify process inputs and outputs that are necessary for successful IM operations. The IM Process Team should consider these inputs and outputs, regardless of organizational plans to fully implement additional processes.

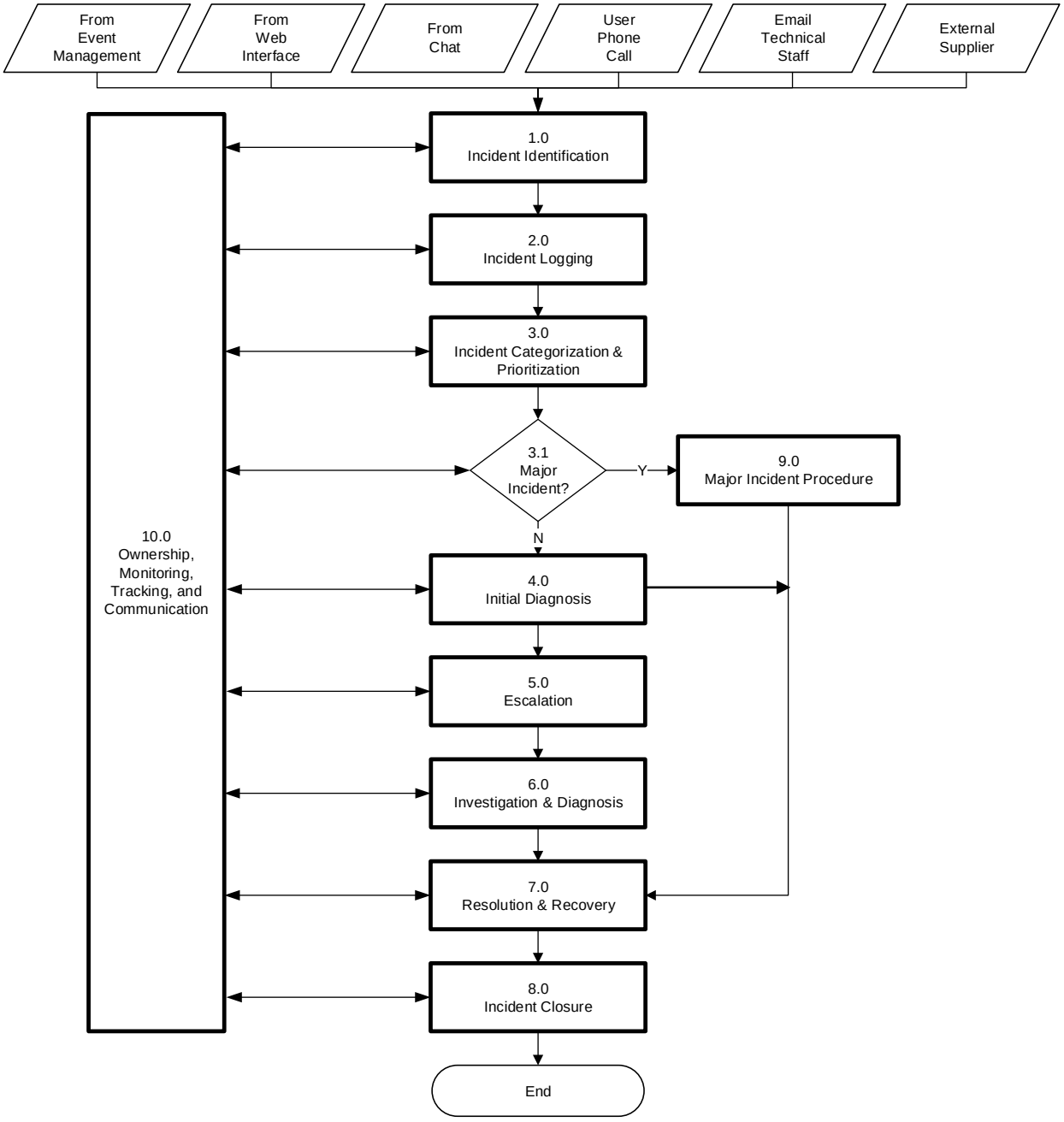
The content within this document is based on the ITIL® framework[1].

2. High Level Incident Management Process Flow

At a very high level, there are ten (10) activities for the IM process. These ten process activities are illustrated in the IM High Level Process Flow diagram on the following page.

[1] ITIL® is a Registered Trade Mark of the Cabinet Office.

Incident Management High Level Process Flow



3. Incident Management High Level Process Activity Descriptions

The following table provides a description of each activity[2] in the IM high level process flow diagram:

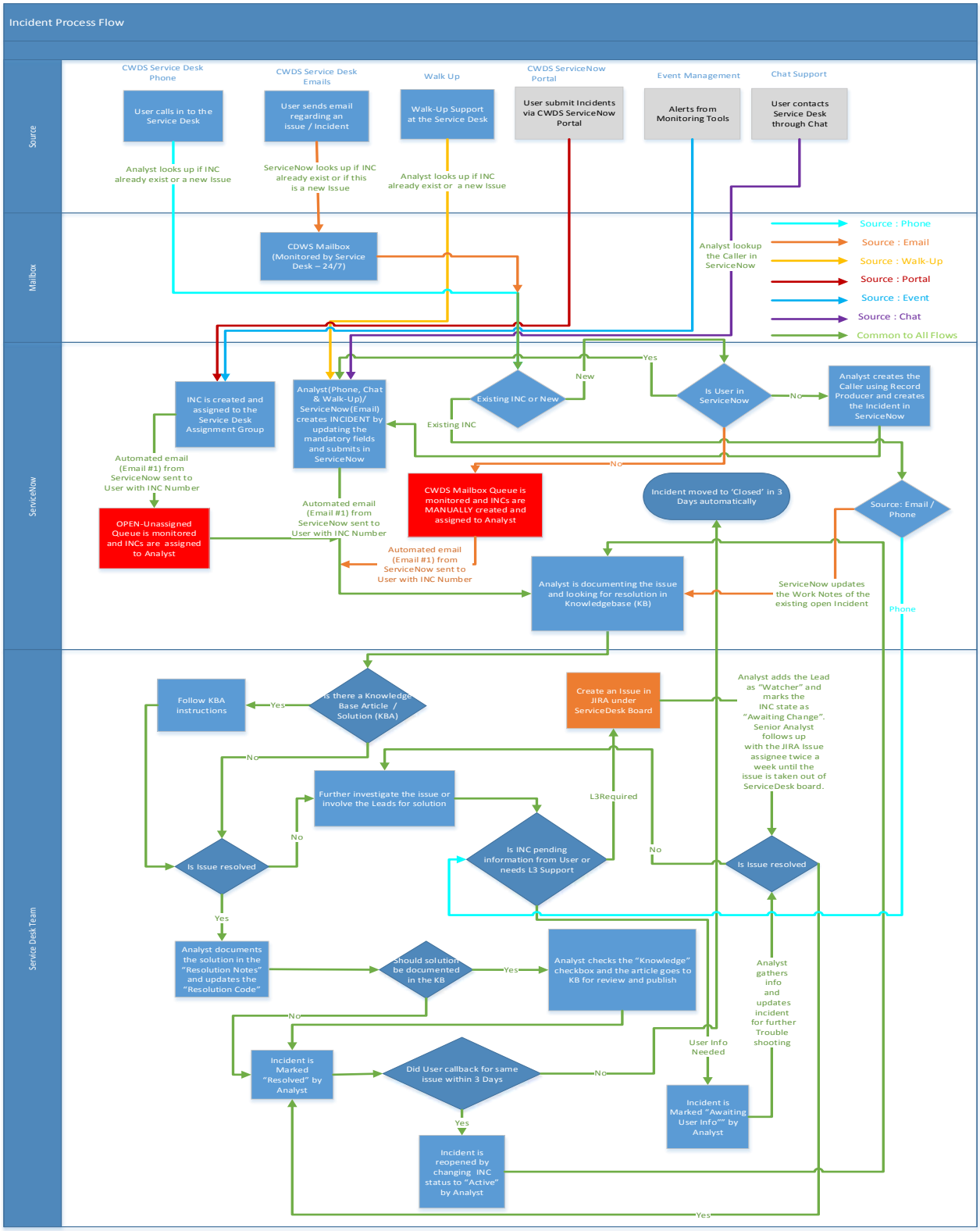
Activity	Description
1.0 Incident Identification	Incidents may be identified by many sources: Users, Service Providers, monitoring of key IT services and Service components. Ideally, Incidents should be identified and resolved before they have an impact on users.
2.0 Incident Logging	All relevant information relating to the nature of the Incident must be logged so that a full historical record is maintained. At a minimum, the following Incident details are input during initial Incident Recording: • Unique reference number (ServiceNow Incident record #) • Date/time recorded • Name and/or group recording the Incident • Name/department/phone/location of user • Description of symptoms • Activities undertaken to resolve the Incident
3.0 Incident Categorization & Prioritization	Incidents are categorized so the exact type of call is recorded. This helps later with reporting, trend analysis and matching Incidents to Problems, Known Errors and validated workarounds. Incidents are prioritized by assessing impact and urgency. Priority is used to determine how the Incident is used by staff and support tools.
4.0 Initial Diagnosis	The Service Desk performs initial diagnosis for any Incidents for which the users have contacted them. This is typically done while the user is still on the phone, and, ideally, the Incident can be successfully resolved and closed.
5.0 Escalation	As soon as it becomes clear that the Service Desk is unable to resolve the Incident, it must be escalated to the appropriate second/third-level support team. High impact and/or urgent Incidents may need to be escalated to management, even if just for notification purposes. Incidents may also be escalated to management if they are taking too long to resolve or if management authorization is needed to resolve the Incident.

[2] Adapted from ITIL Service Operation 4.2.5

Activity	Description
6.0 Investigation & Diagnosis	Investigation and diagnosis is first done at the Service Desk where Analysts delve into the Incident to determine solutions and next steps. Investigation and diagnosis may become an iterative process, starting with a different specialist support group and following elimination of a previous possible cause. It may involve multi-site support groups. It may continue overnight with a new shift of support staff taking over the next day. This requires a rigorous, disciplined approach and a comprehensive record of actions taken, with corresponding results.
7.0 Resolution & Recovery	After successful execution of the resolution or some circumvention activity, service recovery actions can be carried out, often by specialist staff (second- or third-level support). All events and actions during the resolution and recovery activity should be documented in the Incident record so that a full history is maintained. The person or group who resolves the Incident should pass it back to the Service Desk for Incident closure.
8.0 Incident Closure	The Service Desk should ensure that: • Details of the actions taken to resolve the Incident are concise and readable • Classification is complete and accurate according to the determined cause • Resolution/action is agreed with the customer – verbally or, preferably, by email. • All details applicable to this phase of the Incident control are recorded, such that: o The customer is satisfied o The time spent on the Incident is recorded o The person, date and time of closure are recorded
9.0 Major Incident Procedure	Major Incidents are referred to a separate procedure with shorter timelines and greater urgency. The decision criteria and policy for Major Incidents is defined, agreed upon and documented within OSI's ITIL IM Detailed Design plan.

Activity	Description
10.0 Ownership, Monitoring, Tracking, and Communication	The Service Desk is responsible for owning and overseeing the resolution of all outstanding Incidents, whatever the initial source, whatever the ultimate escalation destination by: • Regularly monitoring all open Incidents for status, progress towards resolution and service level commitments • Noting Incidents that move between different specialist support groups, as this may be indicative of uncertainty and, possibly, a dispute between support staff. In excessive cases, Incidents may be referred to Problem Management • Giving priority to monitoring high-impact Incidents • Keeping affected users informed of progress • Checking for similar Incidents

4. Incident Management High Level Process Flow (CWDS)



5. Incident Management High Level Authority Matrix

An authority matrix (RACI) is a tool used to help understand which parties are involved in activities and their level of involvement. Because this is a high level view, there are several levels of involvement shown. More detailed RACIs are provided in the detailed design.

Process Roles **Process Activities**	**Incident Management Process Owner**	**Incident Manager**	**Sr. Service Desk Analyst Service Desk Analyst (Service Desk Staff)**	**Incident Management Process Analyst**	**N-Level Support Group**	**User**
1.0 Incident Identification	A	C	R/I	R/C	R/C	R/C/I
2.0 Incident Logging	A	C/I	R/I	R	R	I
3.0 Incident Categorization & Prioritization	A	C/I	R	R/I	R/I	I
4.0 Initial Diagnosis	A	C	R	C	R/C	I
5.0 Escalation	A	C/I	R/I	C/I	R/C/I	R/C/I
6.0 Investigation & Diagnosis	A	C	R	C	R/C	I
7.0 Resolution & Recovery	A	C	I	C	R	I
8.0 Incident Closure	A	C	R	C	C	C/I
9.0 Major Incident Procedure	A	R/C/I	R/I	R/C/I	R/C/I	R/C/I
10.0 Ownership, Monitoring, Tracking and, Communication	A	C/I	R/I	C/I	C/I	I

Legend:

R = Responsible: Executes the task
A = Accountable: Accountable for final result
C = Consulted: Consulted about the task to provide additional information
I = Informed: Needs to be kept up-to-date on activities/tasks

6. Distinguishing between an Incident and a Service Request

Incident: An unplanned interruption to an IT service or a reduction in the quality of an IT service. Failure of a Configuration Item (CI) that has not yet affected service is also an incident. For example, failure of one disk from a mirrored set. An incident is often related to a technical fault. Another way of describing an incident is to say when "something is broken or not working properly" it is an incident. The Incident Management process will be used to resolve incidents.

Service Request: A formal request from a user for something to be provided. For example, a request for information or advice; to reset a password; or to install a workstation for a new user, a request to install additional software application onto a particular workstation, a request to relocate some items of desktop equipment. Many of these are typically requests for small changes that are low risk, frequently performed, low cost, etc. (ITIL standard changes). Service Requests are managed by the ITIL Request Fulfillment process, usually in conjunction with the Service Desk. Service requests may be linked to a request for change as part of fulfilling the request.

Service requests are the mechanism by which users formally request something from the Service Desk. Service requests are transactional and associated with the standard services that the Service Desk is delivering. Here are some other examples of service requests:

As part of desktop support:

- Install a desktop/laptop
- Move a desktop
- Upgrade a desktop
- Remove a desktop
- Replace a desktop
- Add a keyboard

As part of email support:

- Add a user
- Delete a user
- Change a password
- Increase a mailbox size
- Add a group of users

As part of development support:

- Install a developer workstation
- Restore a development environment
- Migrate code from development to test environment
- Install a development server

7. Global Process Policies For Incident Management

Incident Management Global Process Policies represent decisions made by the Incident Management Process Owner and Incident Management team for end-to-end management and execution of the Incident Management Process. All technologies, organizations and staff defined in CWDS Incident Management Scope are expected to adhere to these Global Policies.

The Incident Management Global Process Policies are designed to ensure that all Service Provider organizations (internal and external) work together to successfully meet CWDS Incident Management Goals. Policies required supporting external regulations (i.e.: Legislation) and/or business customer requirements are also included.

The Incident Management Global Process Policies are owned and monitored by the Incident Management Process Owner. They will provide Management Information to senior- and middle-managers to demonstrate overall process effectiveness and efficiency, compliance at an organizational level and compliance at a department and individual level. The Incident Management Process Owner is also accountable for ensuring that Global Policies add value to the organization and are reviewed and updated on a regular basis.

The following table provides a list of Global Process Policies for Incident Management. These should be discussed, modified (if necessary) and agreed among the Service Management Program Team (all of OSI), Incident Management Process Owner, and Incident Management Process Implementation Team. The Incident Management Process Owner is accountable to ensure end-to-end compliance to these policies. In this position the Incident Management Process Owner must have the authority to make sure middle-management holds its teams accountable for effective and efficient execution of Incident Management Activities.

Policy Statement	Reason For Policy	Benefits
One Incident Management process based on ITIL will be utilized throughout OSI.	To ensure consistent and quality management of Incidents from detection through resolution and closure.	• Consistency in managing Incidents for all users • Consistency in policies and procedures when Incidents are escalated • Faster restoration of services • Faster resolution of incidents • Improved customer communication and satisfaction • Improved management information

Policy Statement	Reason For Policy	Benefits
The Incident Management Process Owner is accountable for the entire Incident Management process and has the authority to develop policies and procedures pertaining to the process.	Provides a single point of accountability for the Incident Management process across OSI.	Ensures consistency in the execution of Incident Management across entire OSI.
Incident Management will provide a single definition of an Incident that will be common and utilized throughout IT and other processes.	To ensure consistency in the management of Incidents.	Provides a clear understanding of an Incident.
Incident Management has the responsibility for supporting only the software and hardware that have been deemed required and approved by both IT and OSI through Service Level Management and the Service Lifecycle.	To ensure that any changes or modifications (by Service Providers or users) to the production environment follow the change control process.	• The customer computing environment becomes more stable • Reduces support costs • Reduces customer calls related to unsupported technologies
All Incidents, regardless of where they are detected, will be logged and updated in ServiceNow.	To ensure that all Incidents and Service Requests are logged, updated and closed in ServiceNow.	• Consistent logging and tracking for all Incidents • The performance of the IT environment can be measured more accurately • Facilitates Incident matching and Problem identification • Eliminates cost of redundant tools
The Service Desk will be the first point of contact for users.	To ensure that all Incidents are consistently dealt with centrally and are assigned correctly.	Enables the application of a centralized data repository for Incidents and a consistent entry point for the initiation of process activities.

Policy Statement	Reason For Policy	Benefits
Service Requests identified through the Incident Management process will be referred to the Request Fulfillment process.	To ensure Incidents are handled using Incident policies, models, and service levels which are separate and different from Service Request.	• Reduces confusion regarding using the appropriate policies and procedures for resolving Incidents • Appropriate reporting against Service Level Agreements (SLA) for Incident resolution separate from Service Requests
All Incidents will be prioritized based upon impact and urgency defined in the Prioritization Model that has been created for Incident, Problem and Change Management.	To effectively manage Incidents.	• Business critical Incidents are more quickly identified • The speed and resources needed to solve an Incident are assessed
In the event the Incident resolution exceeds the ability of the Service Desk or any other support level, the Incident will be escalated to the appropriate individual/group or 'n' level of functional support.	To ensure that all Incidents are effectively dealt with and handled by the correct individuals/groups.	Incidents are resolved as quickly as possible.
All work and progress toward Incident resolution, regardless of the support level or staff member, will be clearly documented in ServiceNow in a timely basis.	To ensure timely and accurate updates to Incident records and maintain a lifecycle or history of all Incidents.	• Accurate and up-to-date information to provide to users • Incidents can be assessed for potential service breaches and need for hierarchical escalation • Accurate data to support Problem detection and Root Cause Analysis
Status of Incidents will be provided or made available to customers/users throughout the lifecycle of the Incident through resolution and recovery.	To notify customers of Incident resolution progress.	• Increases customer satisfaction • Reduces the volume of incoming follow-up calls to the Service Desk

Policy Statement	Reason For Policy	Benefits
The Service Desk will own the lifecycle of all Incidents. All activities associated with the Incident are the responsibility of the individuals and groups involved in the resolution of the Incident.	To effectively manage Incidents.	• Ensures all Incidents receive the appropriate and timely support regardless of which functional group is working on it; as defined in appropriate operational levels • Improves ability to resolve all Incidents within SLA
Communication will be provided to OSI and its customers/users concerning any known or expected degradation of service and impact to OSI and/or their customers.	To ensure organization wide awareness surrounding any Incidents and Problems that impact IT services.	• Customer expectations will be set accurately • Reduces calls for updates, since customers know what is happening • Increases customer satisfaction and perception of OSI's image • Easier for support personnel to associate calls with Known Errors and Problems
Incident Management will provide an escalation policy in accordance with business needs to ensure Incidents are dealt with in a timely manner.	To ensure that Incidents are resolved in accordance with the requirements of OSI and to ensure that service levels are maintained.	• Timely closure of Incidents • Increases customer satisfaction • Increases IT staff understanding of roles and responsibilities and, therefore, their effectiveness • Ensures that appropriate levels of management are notified of the Incident and its status

Policy Statement	Reason For Policy	Benefits
Any Incident that meets the criteria for a Major Incident (see Major Incident Criteria in section 9.0 of the IM Detailed Design Plan) will be resolved by using the Major Incident Procedure (see Major Incident Procedure in section 9.0 of the IM Detailed Design Plan)	To ensure that all Incidents with the highest impact and highest urgency (Major Incidents) are resolved with greater urgency and shorter resolution timescales	• Reduces downtime experienced by Customers • Improves productivity when disruptions occur due to major outages
Incident closure is the result of the customer validating that the resolution to the Incident has been met and the service has been restored to the customer's satisfaction.	To ensure that all Incident solutions or workarounds are agreed upon with business needs and satisfy SLA.	• Improves the recording of pertinent management information • Increases customer satisfaction and feeling of empowerment • Reduces volume of incoming follow-up calls
Incident Management metrics and management reports will be provided to Management, staff and customers in accordance with outlined procedures and agreements.	To assess performance measures (e.g., efficiency and effectiveness) of the Incident Management process.	• Identifies CWDS's performance for end-to-end Incident resolution • Identifies any issues with Operational Level Agreements (OLAs) or Underpinning Contracts (UCs) for rapid restoration of services • Provides trend analysis for the Incident Management process and Incident handling • Identifies opportunities for improvement
Reviews are conducted by the IM Process Owner on a regular basis, at the IM Process Owner's discretion. Reviews will focus on the process consistency and repeatability and Key Performance Indicators (KPI).	To maximize process benefits and reduce costs.	• Identifies opportunities for process, tool and staff improvements • Identifies opportunities for staff training on process and tools

8. Applicable COBIT® Controls[3] (Control OBjectives for Information and related Technologies)

The COBIT 4.1 controls that correspond most closely[4] to the Incident Management process are the following[5]:

DS Deliver and Support

DS8 Manage Service Desk and Incidents

DS8.1 Service Desk

Establish a service desk function, which is the user interface with IT, to register, communicate, dispatch and analyze all calls, reported incidents, service requests and information demands. There should be monitoring and escalation procedures based on agreed-upon service levels relative to the appropriate SLA that allow classification and prioritization of any reported issue as an incident, service request or information request. Measure end users' satisfaction with the quality of the service desk and IT services.

DS8.2 Registration of Customer Queries

Establish a function and system to allow logging and tracking of calls, incidents, service requests and information needs. It should work closely with such processes as incident management, problem management, change management, capacity management and availability management. Incidents should be classified according to a business and service priority and routed to the appropriate problem management team, where necessary. Customers should be kept informed of the status of their queries.

DS8.3 Incident Escalation

Establish service desk procedures, so incidents that cannot be resolved immediately are appropriately escalated according to limits defined in the SLA and, if appropriate, workarounds are provided. Ensure that incident ownership and life cycle monitoring remain with the service desk for user-based incidents, regardless which IT group is working on resolution activities.

DS8.4 Incident Closure

Establish procedures for the timely monitoring of clearance of customer queries. When the incident has been resolved, ensure that the service desk records the resolution steps, and confirm that the action taken has been agreed to by the customer. Also record and report unresolved incidents (known errors and workarounds) to provide information for proper problem management.

See the official COBIT 4.1 documentation at www.isaca.org for more details.

[3] COBIT® is a registered trademark of ISACA®.

[4] COBIT® Control mapping from *COBIT® Mapping: Mapping of ITIL v3 With COBIT® 4.1*, 2008, IT Governance Institute

[5] COBIT® Control language is from *COBIT® 4.1*, 2007, IT Governance Institute

9. Integration With Other Processes & Functions

As each process is designed, it is important to recognize that there are key integrations between processes and functions. Even if the goal is not to reach integration, there is a certain level of integration (inputs become outputs) that naturally takes place.

The following tables describe key areas where Incident Management interacts and integrates with other Processes and Functions. The 'Actions Taken…' column shows activities taken or activity-initiating triggers presented by one process for another. The 'Information Provided…' column describes the data or output that is transferred to another process for information or for reporting purposes.

9.1. From Incident Management to Another Process/Function

Provider: Incident Management		**Recipient: *Process/Function***
Recipient *Process/Function*	**Actions Taken For Recipient By Incident Management**	**Information Provided To Recipient By Incident Management**
Access Management	• Initiate and manage Access-related Incidents to resolution • Provide Access-related Incidents to Access Management	• Incident data • IM policies and procedures, roles and responsibilities
Application Management	• IM Process Data • Coach staff in Compliance to ITIL IM Process • Input into activities of Problem Management performed by Application Management	• IM Policies • IM Process • IM Compliance Data • IM Component Data • IM Service Data • IM policies and procedures, roles and responsibilities
Availability Management	• Incident data is used as an input to Availability Management reporting and planning activities	• Incident data • Instructions to track and recover from service failures • Bypass options and rapid fixes • Historical data • Prioritization/escalation of information • IM policies and procedures, roles and responsibilities

Provider: Incident Management		**Recipient: *Process/Function***
Recipient *Process/Function*	**Actions Taken For Recipient By Incident Management**	**Information Provided To Recipient By Incident Management**
Capacity Management	• IM can provide a trigger for performance monitoring where there appears to be an issue with performance • IM can provide feedback from customers and users regarding service performance • Inform customers of known capacity issues • Execution of pre-authorized capacity adjustments (load balancing and demand mitigation)	• Incident data • User requirements • Impact of Capacity Management. activity • Trends • IM policies and procedures, roles and responsibilities
Change Management	• Associate Incident records with Change records suspected of causing the Incident • Associate Incident records with Requests for Change (RFC's) submitted to investigate and/or resolve the Incident • Reinforce Change Management policy for changes requested to resolve or research incidents • Detect and resolve Incidents that arise from failed Changes • Assist in scheduling Changes • Notify Change Management of unauthorized Changes • Communicate Change information • Provide feedback on changes and 'change success' as input to Post Implementation Review (PIR) meetings • Participation in the Change Advisory Board (CAB)	• Incidents resulting from Changes • Impact of Changes (good or bad) • Peaks in volume or workload from Changes or associated failures • User reaction to Changes • RFC's raised during execution of the IM process • IM policies and procedures, roles and responsibilities

Provider: Incident Management		**Recipient: *Process/Function***
Recipient *Process/Function*	**Actions Taken For Recipient By Incident Management**	**Information Provided To Recipient By Incident Management**
Continual Service Improvement	Provide Incident data and IM Process measures for the Continual Service Improvement (CSI) 7 Step Improvement Process.	• Incident data • IM Process measures and targets • IM policies and procedures, roles and responsibilities
Demand Management	Refer demand-related Incidents to Demand Management after resolution for analysis.	• References and access to Demand-related Incidents • IM policies and procedures, roles and responsibilities
Event Management	• Manage Event related Incidents to resolution • Provide ServiceNow Incident record # to the Event Management system for Incidents opened automatically by the Event Management system • Provide global IM requirements • Request Event Management process, and technology improvements • Accept Automatic Incident creation and update requests from the Event Management system	• Event-Initiated ServiceNow Incident record # • IM monitoring, Event Management and logging requirements • Event log access requests • IM policies and procedures, roles and responsibilities
Financial Management	• Collect and verify incident business cost • Collect and verify IM operating cost parameters (headcount, suppliers, etc.)	• Incident duration and impact data • IM Operations data • IM policies and procedures, roles and responsibilities
Information Security Management	• Report all security related incidents to Information Security Management • Maintain restricted access to security Incidents • Comply with Information Security Policies • Maintain Information Security Incident access controls	• Incidents related to Information Security Management • Incident data related to Information Security • Priority matrix • IM policies and procedures, roles and responsibilities

Provider: Incident Management		**Recipient: *Process/Function***
Recipient *Process/Function*	**Actions Taken For Recipient By Incident Management**	**Information Provided To Recipient By Incident Management**
IT Operations Management	• IM Process Data • Coach staff in Compliance to ITIL IM Process • Input IM record details for activities of Problem Management performed by Operations Management	• IM Policies • IM Process • IM Compliance Data • IM Component Data • IM Service Data • IM policies and procedures, roles and responsibilities
IT Service Continuity Management	• Major Incidents need to be assessed for potential invocation of business and/or IT Continuity Plans • IM should provide Management Information regarding Major Incidents, minor emergencies and disasters	• Major Incidents • IM information • IM policies and procedures, roles and responsibilities
Knowledge Management	Provide Knowledge Management data utilization and feedback data	• Knowledge Management entry and access feedback • IM policies and procedures, roles and responsibilities
Problem Management	• Warning of potential Problems • IM may provide resolution steps or workarounds to Problem Management for validation and acceptance into the Problem database • Provide Incident records for Problem Management processing	• Current Incidents • Resolution steps • Potential impact • Identification of Change impact • Priorities and required time scales • Incidents to be matched to existing Problems or to spawn new Problems • IM policies and procedures, roles and responsibilities
Release & Deployment Management	• Identifies release-related Incidents • Impact of releases causing Incidents	• Incidents related to releases • IM policies and procedures, roles and responsibilities

Provider: Incident Management		**Recipient: *Process/Function***
Recipient *Process/Function*	**Actions Taken For Recipient By Incident Management**	**Information Provided To Recipient By Incident Management**
Request Fulfillment	• IM is able to detect and resolve Incidents that arise from failed Service Requests • Assistance in evaluating the guidelines for Service Request List • Communication channel • Provide input for the procedures in transferring a Service Request to the IM process and vice versa	• Incidents resulting from Service Requests • Impact of Service Requests (good or bad) • User reaction and feedback to Request Fulfillment • IM policies and procedures, roles and responsibilities
Service Asset & Configuration Management	• Associate Incident records with symptom, cause, workaround, and a fixed CI and affected service CI's • Impact assessment of failed CI's • Notification of data issues in the Configuration Management Database (CMDB) and/or Configuration Management System (CMS) • Incident data can be used to update and maintain the status information of faulty CI • Provide Incidents related to a specific CI's	• Verification of CI information • Data discrepancies • Update of CI capability (current status) • Notice of changes • Incidents linked to CI's • IM policies and procedures, roles and responsibilities

Provider: Incident Management		**Recipient: *Process/Function***
Recipient *Process/Function*	**Actions Taken For Recipient By Incident Management**	**Information Provided To Recipient By Incident Management**
Service Catalog Management	• Provide access to information requested • Manage Service Catalog information errors through creation of Incidents	• Number of Incidents by priority (logged against the Service and related underlying infrastructure) over a rolling meaningful recent interval • Long term trends • Present the Incident resolution compliance rate over the same rolling meaningful recent interval • Link to the prioritization (impact and urgency), categorization, and escalation rule sets for the Service • Link to the support chain contact list for the Service • Incident status and outcome • IM policies and procedures, roles and responsibilities
Service Desk	Provides IM expectations, policies, etc.	• Policies and procedures • Roles and responsibilities • Training • IM policies and procedures, roles and responsibilities
Service Level Management	• Warning of potential SLA breaches • Provide Customer satisfaction with IM specific to Service • Provide Incident data specific to Service • Set Priority Matrix to fit Service Level	• Statistical Information • Historical data and trends • IM policies and procedures, roles and responsibilities
Service Portfolio Management	• Provide defect feedback on implemented services • Provide access to information requested	• Number of Incidents and impact of the Incidents by implemented service • IM policies and procedures, roles and responsibilities
Service Validation & Testing	Provide Incident summary data for future testing criteria and Service Validation analysis	• Incident data following new deployments • IM policies and procedures, roles and responsibilities

Provider: Incident Management		**Recipient: *Process/Function***
Recipient *Process/Function*	**Actions Taken For Recipient By Incident Management**	**Information Provided To Recipient By Incident Management**
Supplier Management	• Provide training for and integration of supplier support teams • Provide interfaces and integrations between supplier and OSI's IM processes and tools	• Incident information and triggers to supplier support teams • IM policies and procedures, roles and responsibilities
Technical Management	• IM Process Data • Coach staff in Compliance to ITIL IM Process • Input into activities of Problem Management performed by Technical Management	• Policies • Procedures • IM Compliance Data • IM Component Data • IM Service Data • IM policies and procedures, roles and responsibilities

9.2.From Another Process/Function To Incident Management

Provider: *Process/Function*		**Recipient: Incident Management**
Provider *Process/Function*	**Actions Taken By Provider For Incident Management**	**Information Provided By Provider To Incident Management**
Access Management	• Respond with expert advice and action for incidents involving Access rights, features, etc. • Respond to requests for Access Management information regarding available rights, groups and governing policies along with the current status of rights for users and groups	• Individual user access rights, groups membership, status • Group access rights and status • Access Management policies and procedures, roles and responsibilities
Application Management	• Perform IM tasks and activities as requested and in conformance with respective policies and procedures • Execute Incident assignment acknowledgement, triage, responses, log/status updates, resolution, restoration and closure activities	• Incident Status communication • Incident symptom and resolution with CI information • Application Support Plan • Answers to requests for information • Acknowledgement of requests • Request completion notice • Application Management policies and procedures, roles and responsibilities
Availability Management	• Availability Management can be used to assess and improve the Incident lifecycle • Availability Monitoring • Availability Management Policies integrate with and support IM Policies	• Availability Requirements • Availability Management policies and procedures, roles and responsibilities
Capacity Management	• Capacity Management may develop workarounds for IM • Capacity Monitoring • With Demand – demand/capacity conflict forecasts	• Performance criteria • Known Capacity issues • Capacity workarounds and load balancing rules • Capacity Management policies and procedures, roles and responsibilities

Provider: *Process/Function*		**Recipient: Incident Management**
Provider *Process/Function*	**Actions Taken By Provider For Incident Management**	**Information Provided By Provider To Incident Management**
Change Management	• Review and approval of RFC's required to resolve Incidents • Information about Changes that were implemented, rejected or delayed • Procedure to accept RFC's when they are identified or entered through the IM process • CAB meeting minutes • Provide schedule of planned changes to Service Desk and Support Teams	• Change Schedule • Projected Service Outage (PSO) • Change details • Post Implementation Review feedback • Change Management policies and procedures, roles and responsibilities
Continual Service Improvement	• Provide IM related Vision and Targets • Solicit IM improvement input • Support IM improvement initiatives	• Vision • As-Is assessment • To-Be targets • As-Is reassessments • CSI policies and procedures, roles and responsibilities
Demand Management	• Provide service utilization drivers and driver patterns • Demand monitoring • With Capacity – demand / capacity conflict forecasts	• Service demand drivers and patterns • Demand event rules • Demand Management policies and procedures, roles and responsibilities
Event Management	• Automated Creation of Incident Records • Consistent Prioritization of Incident Record fields • Pre-defined and often automated response actions	• Event detail posted in Incident Log • Mandatory and some optional Incident Record fields loaded using Event rules • Event notifications that may relate to an Open Incident
Financial Management	• Collection and calculation of Service outage financial impact • Collection and calculation of IM Operations costs • Collaboration on IM benefit calculations	• Business/Service outage costs for priority matrix • IM Process Operations Financials • Financial Management policies and procedures, roles and responsibilities

Provider: *Process/Function*		**Recipient: Incident Management**
Provider *Process/Function*	**Actions Taken By Provider For Incident Management**	**Information Provided By Provider To Incident Management**
Information Security Management	• Provides Information Security Incident processing policies, standards, and guidelines to IM and Service Desk • Participates in Incident resolution whenever Information Security is affected or at risk	• Information Security Incident processing policies, standards, and guidelines • Information Security Classifications with required responses • Training • Information Security Management policies and procedures, roles and responsibilities
IT Operations Management	• Assists in implementing IM Process • Identifies and resolves Incidents as well collaborating on Major Incidents • Collaborates on continual improvement opportunities	• Policies • Process Metrics • Incident Data related to IT Operations • Tracking against Service Improvement Plans (SIP) • Monitoring • Operations Logs • Operations Reports • Facility access reports • IT Operations Management policies and procedures, roles and responsibilities
IT Service Continuity Management (ITSCM)	Business Continuity Management (BCM) and ITSCM provide clear criteria to IM to assess whether a Major Incident should be assessed as a disaster.	• Business and ITSCM plans and criteria • Assessment of Business Impact Analysis (BIA) for Priority calculations • ITSCM policies and procedures, roles and responsibilities
Knowledge Management	• Audit IM knowledge entries • Accept IM Knowledge Artifact (KA) • Provide access paths to knowledge management items for Service Desk and IM Analysts and customers/users	• Knowledge Management entries for use in Incident resolution activities • Knowledge Management policies and procedures, roles and responsibilities

Provider: *Process/Function*		**Recipient: Incident Management**
Provider *Process/Function*	**Actions Taken By Provider For Incident Management**	**Information Provided By Provider To Incident Management**
Problem Management	• Problems raised because of multiple Incidents can be solved to prevent further Incidents from occurring • Problem Management staff may provide education and training to IM staff (e.g., the Service Desk) on investigation and diagnosis	• Information on Problems and Known Errors • Workarounds and temporary solutions • Reports on Major Problem reviews • Incident associations with Problems and Known Errors • Problem Management policies and procedures, roles and responsibilities
Release & Deployment Management	• Knowledge about environment • Training of IM staff (e.g. Service Desk) • Documentation about Releases	• Release policy • Known Errors associated with Release development • Deployment schedules • Release & Deployment policies and procedures, roles and responsibilities
Request Fulfillment	• Review and approval of Service Requests required to resolve Incidents that are routine in nature i.e. Password reset • Information about Service Requests that were implemented, rejected, delayed or failed • Procedure to accept Service Requests when they are identified or entered through the IM process	• Daily, weekly and monthly reports of Service Requests volume and nature • Notification of Incidents coming to Service Request process and having to be submitted to IM • Information on Incidents discovered during Service Request activities • Request Fulfillment policies and procedures, roles and responsibilities

Provider: *Process/Function*		**Recipient: Incident Management**
Provider *Process/Function*	**Actions Taken By Provider For Incident Management**	**Information Provided By Provider To Incident Management**
Service Asset & Configuration Management	• CMS data can be used to assess the impact of an Incident • CMS data can be used to identify which Incident categories should be assigned to which support group • CMS data can be used to identify users affected by Incidents and potential Problems • Accept CMS data quality Incidents from IM	• CI relationships and dependencies • CI owners • Number of users affected • Information on Service Providers and Vendors • Service Asset & Configuration Management policies and procedures, roles and responsibilities
Service Catalog Management	• Present the number of Incidents by Urgency and Impact, logged against the Service and related underlying infrastructure over a rolling meaningful recent interval • Present the long term trend • Present Statistical Process Control variability vector • Present the Incident resolution compliance rate over the same rolling meaningful recent interval • Present a link to the prioritization (impact and urgency), categorization, and escalation rule sets for the Service • Present a link to the support chain contact list for the Service • Raise Incident records for Service Catalog information errors	• Service Catalog information accuracy incident information • Service Catalog Management policies and procedures, roles and responsibilities
Service Desk	• Registration of incidents • Monitoring of incident • Communication of incidents • Escalation of incidents	• Incident data • Audit information • Service Desk policies and procedures, roles and responsibilities

Provider: *Process/Function*		**Recipient: Incident Management**
Provider *Process/Function*	**Actions Taken By Provider For Incident Management**	**Information Provided By Provider To Incident Management**
Service Level Management	• Service Level Requirements specify the level of support and Incident resolution times requested by the customer • Service Level Agreements provide information to IM relating to the agreed and acceptable levels of service	• Service Catalog • Service Level Requirements • Service Level Agreements • Operational Level Agreements • Service Level Management policies and procedures, roles and responsibilities
Service Portfolio Management	Provide notice of Change to service which may impact Incident resolution and escalation activities	• Advance notice of Portfolio changes affecting production • Service Portfolio Management policies and procedures, roles and responsibilities
Service Validation & Testing	• Collaborate on IM test requirements for Services being Changed or Evaluated • Provide known issues to IM for newly tested CI's • Perform emergency tests for Changes made to resolve Incidents	• Known errors in new CI's • Emergency test results • Service Validation & Testing policies and procedures, roles and responsibilities
Supplier Management	• Collaborate on defining and fulfilling IM goals and requirements for supplier services • Facilitate conflict resolution • Coordinate establishment of IM training and how to execute coordination activities for supplier and IM • Conduct Supplier Satisfaction Survey • Participate in Incident Resolution escalation	• Supplier contracts & contacts • Requirements from users, suppliers and organization • Supplier Incident and escalation contact information • Supplier satisfaction surveys • Supplier survey reports • Supplier Management policies and procedures, roles and responsibilities
Technical Management	• Perform IM tasks and activities as requested and in conformance with respective policies and procedures • Execute Incident assignment acknowledgement, triage, responses, log/status updates, resolution, restoration and closure activities	• Answers to requests for information • Acknowledgement of requests • Request completion notice • Technical Management policies and procedures, roles and responsibilities