

NASA

**IT Incident Management Process Document
Version 1.0**

April 16, 2009

Table of Contents:

Document Abstract	3
Document Owner	3
Revision History.....	3
IT Incident Management Purpose	4
IT Incident Management Scope.....	4
IT Incident Management Description	4
IT Incident Management Process Flow	7
IT Incident Management Roles and Responsibilities	18
Identification of Incidents and Logging of Incident Tickets	19
Sample Incident Ticket (captured through the NASA incident management system managed by the NASA Enterprise Service Desk).....	19
Sample Known Error Ticket.....	19
IT Incident Support Timing.....	20
IT Incident Management Performance Measures.....	20
IT Incident Management - Key Integration Points.....	20
Document Maintenance	21

Document Abstract

This document provides all involved parties (including staff, management, partners, providers, and contractors), regardless of physical location with a guide and reference to **NASA's** IT incident management processes, procedures, and standards.

Document Owner

The IT incident management process document is owned by the Architecture and Infrastructure Division within the NASA Office of the Chief Information Officer.

Revision History

Version	1.0
Revision Date	4/16/2009
Authors	
Incidents	
Approval:	
Next Revision:	

IT Incident Management Purpose

NASA recognizes the need to establish reasonable guidelines for the effective use, management, and maintenance of underlying IT incident management. In doing so, **NASA** seeks to protect the integrity of its production environment and ensure adherence to **NASA** standard IT service management practices.

The purpose of this document is to provide all involved parties (including staff, management, partners, providers, and contractors), regardless of physical location with a guide and reference to **NASA's** IT incident management processes, procedures, and standards.

This document also serves to ensure that all parties involved in **NASA's** IT incident management processes, procedures, and standards, understand the requirements associated with **NASA's** IT incident management processes, procedures, and standards.

IT Incident Management Scope

This document is intended to cover all IT incidents associated with **NASA's** IT environment including, but not limited to,:

- Internal customers
- External customers
- Technology partners
- HW
- SW
- Operating Systems
- Applications
- Telecommunications
- Networks
- Systems
- Patches, Upgrades, Modifications
- People/Organizational Structure
- Process
- Service Levels

IT Incident Management Description

The IT incident management process at **NASA** is a complex set of tasks, activities, and functions that seek to restore normal service operations to customers as quickly as possible: to minimize any negative impacts to business operations; to ensure that expected service levels are appropriately maintained; and that any additions to service requirements are addressed. The IT incident management process is responsible for the identification and management of all

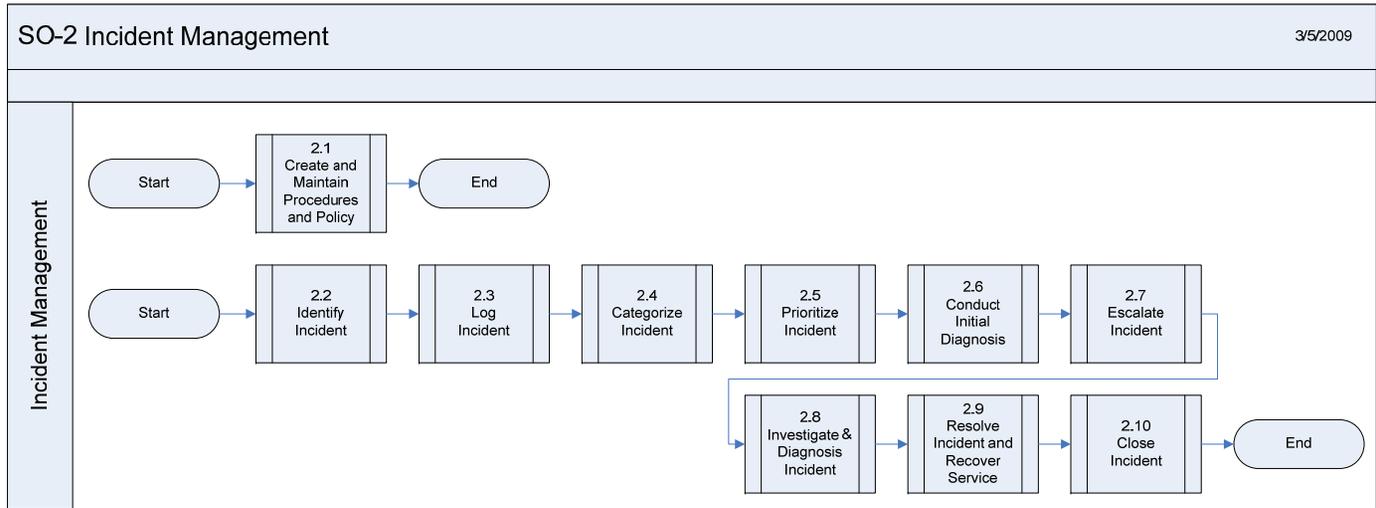
IT incidents (both internally and externally generated) relating to **NASA's** IT environment.

The IT incident management process at **NASA** is comprised of the following tasks:

- Incident Detection
 - Incident detection is the point at which the service provider becomes aware that there has been a negative impact to expected service levels, or if there has been a request for additional service.
- Recording of The Incident
 - Documentation of the incident is critical to ensure proper tracking and information management of the incident. Recording of incidents often occurs through the use of a ticketing/workflow engine (e.g., Remedy/BMC, Peregrine/HP).
- Incident Classification
 - Incident classification is the activity that seeks to ensure that incidents are attended to with the appropriate urgency and by the appropriate parties. Incident classification often utilizes the change management categorization schedule to facilitate classification, and may be performed in concert with both the change management and problem management processes.
- Initial Support
 - Initial support for incidents may be performed by any number of individuals within the service provider's organization. Initial support is the first look into the incident and does not guarantee that the issue will be resolved without additional support. Well-known and easily resolved incidents, however, may be resolved at this point.
- Matching Incidents Against Known Errors
 - There is often information available regarding incidents that have occurred in the past (e.g., those impacted, the types of impact, effected systems, possible resolutions) which may be useful to the resolution of the incident in question. This task seeks identify and utilize that information.
- Incident Investigation/Diagnosis
 - Incident investigation/diagnosis is the task during which the incidents that cannot be resolved during the "initial support" task are analyzed and for which an appropriate fix may be identified.
- Incident Resolution/Recovery
 - Incident resolution/recovery is the task for which well-known and easily resolved incidents may also be undertaken to simply restore service (e.g., a reboot). It should be noted that true fixes (i.e., alterations to the configuration of the system) are not applied at this part of the process. Fixes for incidents are applied in the change management process.
- Confirmation With Customers

- Following the resolution/recovery task, the service provider should check with service customers to ensure that services have been restored to expected service levels.
- Incident Closure
 - Incident closure is the final completion of the incident and may include closing out the incident ticket, documentation of any information relevant to the “known-error” database, etc.

IT Incident Management Process Flow



Purpose, Goals and Objectives:

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. "Normal service operation" is defined here as service operation within SLA limits.

Triggers:

Incidents can be triggered in many ways. The most common route is when a user calls the Service Desk or completes a web-based incident-logging screen, but increasingly incidents are raised automatically via Event Management tools.

Primary Interfaces:

The interfaces with Incident Management include:

- Problem Management – Incidents are often caused by underlying problems, which must be solved to prevent the incident from recurring.
- Configuration Management – provides data used to identify and progress incidents.
- Change Management – where a change is required to implement a workaround or resolution, this will need to be logged as an Request for Change (RFC) and progressed through Change Management.
- Capacity Management – may develop workarounds for incidents.
- Availability Management – uses incident management data to determine the availability of IT services and looks at where the incident lifecycle can be improved.
- Service Level Management – Incident management enables SLM to define measurable responses to service disruptions. It also provides reports that enable SLM to review SLAs objectively and regularly. SLM defines the acceptable levels of service within which Incident Management works, including: incident response time, impact definitions, target fix times, service definitions mapped to users, and rules for requesting service.

Information Management:

Most information used in Incident Management comes from the following sources:

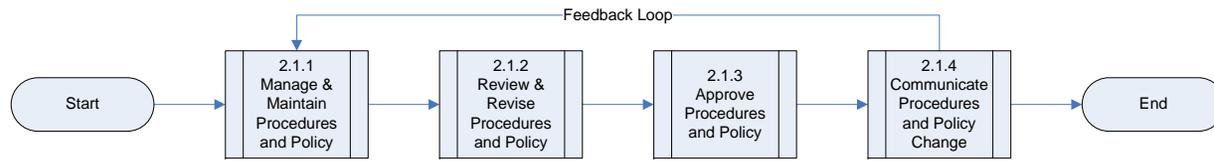
- Incident Management tools contain information about: incident and problem history, categories, action taken to resolve incidents, and diagnostic scripts.
- Incident Records containing: unique reference number, incident classification, date and time of recording, name and identify of the recorder, name/organization/contact details of the affected user(s), description of the incident symptoms, details of any actions taken, incident category, impact, urgency and priority, relationship with other incidents, problems, changes, or Known Errors, and closure details.
- Incident Management also requires access to the Change Management System (CMS), this helps identify the Configuration Items (CIs) affected.
- The Known Errors Database provides valuable information and possible resolutions and workarounds.

SO-2.1 Create and Maintain Incident Management Procedures and Policies

3/5/2009

NASA Business
User
Community

(SIM) Incident
Management



Other NASA
Retained Authority

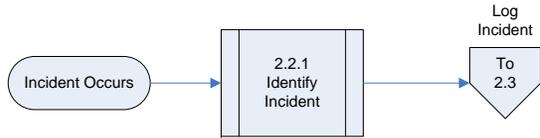
Provider – Primary
Services

Provider – Support
Services

SO-2.2 Identify Incident

3/5/2009

NASA Business User Community



(2.2) Identify Incident:

Work cannot begin on dealing with an incident until it is known that an incident has occurred. It is usually unacceptable, from a business perspective, to wait until a user is impacted and contacts the Service Desk.

As far as possible, all key components should be monitored so that failures or potential failures are detected early so that the incident management process can be started quickly. Ideally, incidents should be resolved before they have an impact on users.

Service Desk (3rd Party)

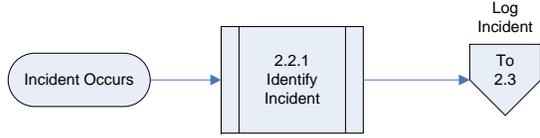
Other NASA Retained Authority

In ITIL terminology, an "Incident" is defined as:

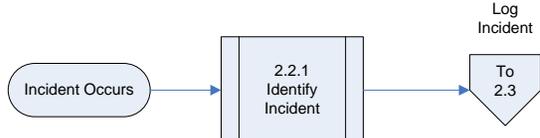
An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service is also an incident, for example failure of one disk from a mirror set.

Incident Management is the process for dealing with all incidents; this can include failures, failures, questions or queries reported by users (usually via a telephone call to the Service Desk), by technical staff, or automatically detected and reported by event monitoring tools.

Provider – Primary Services

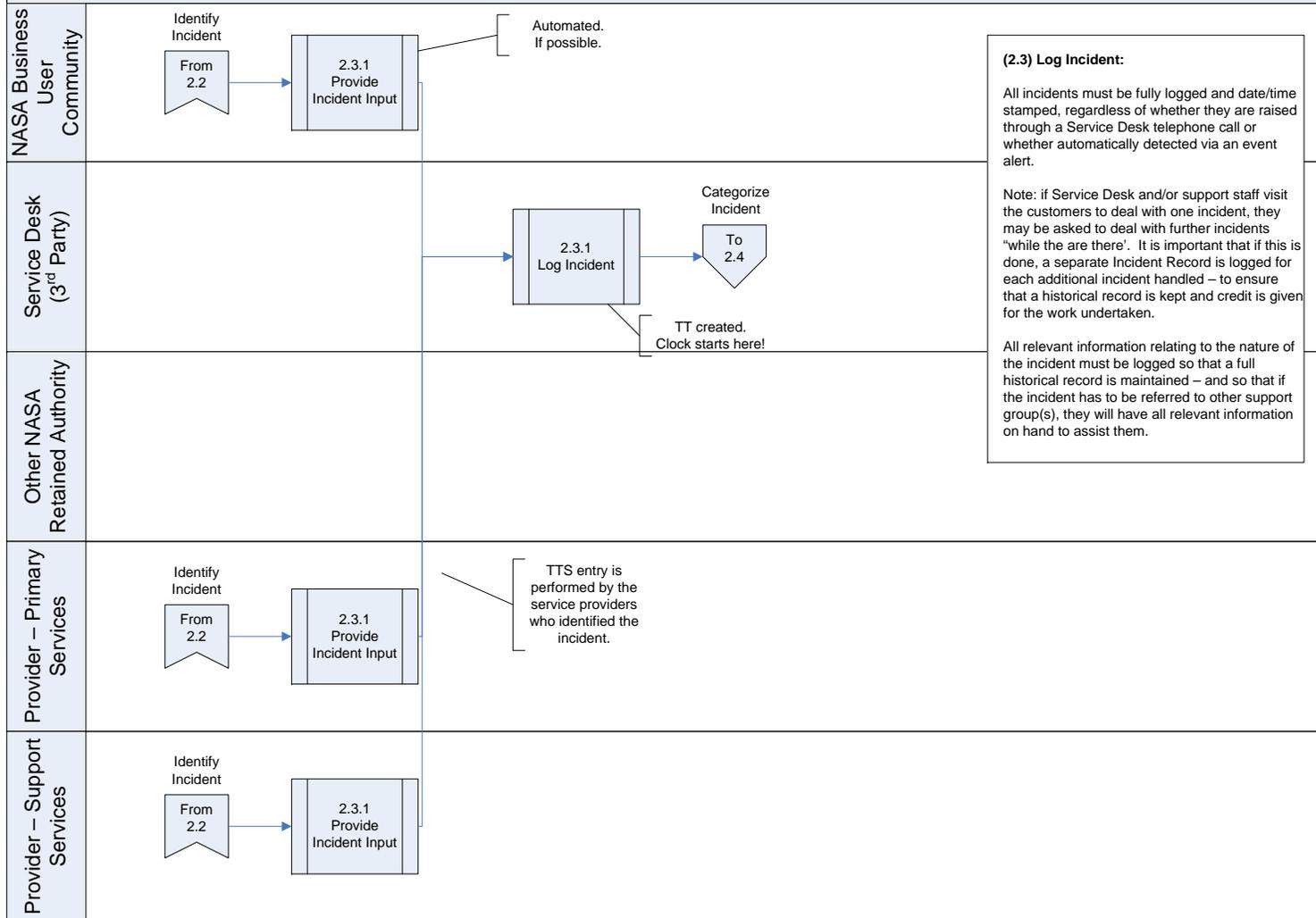


Provider – Support Services



SO-2.3 Log Incident

3/5/2009



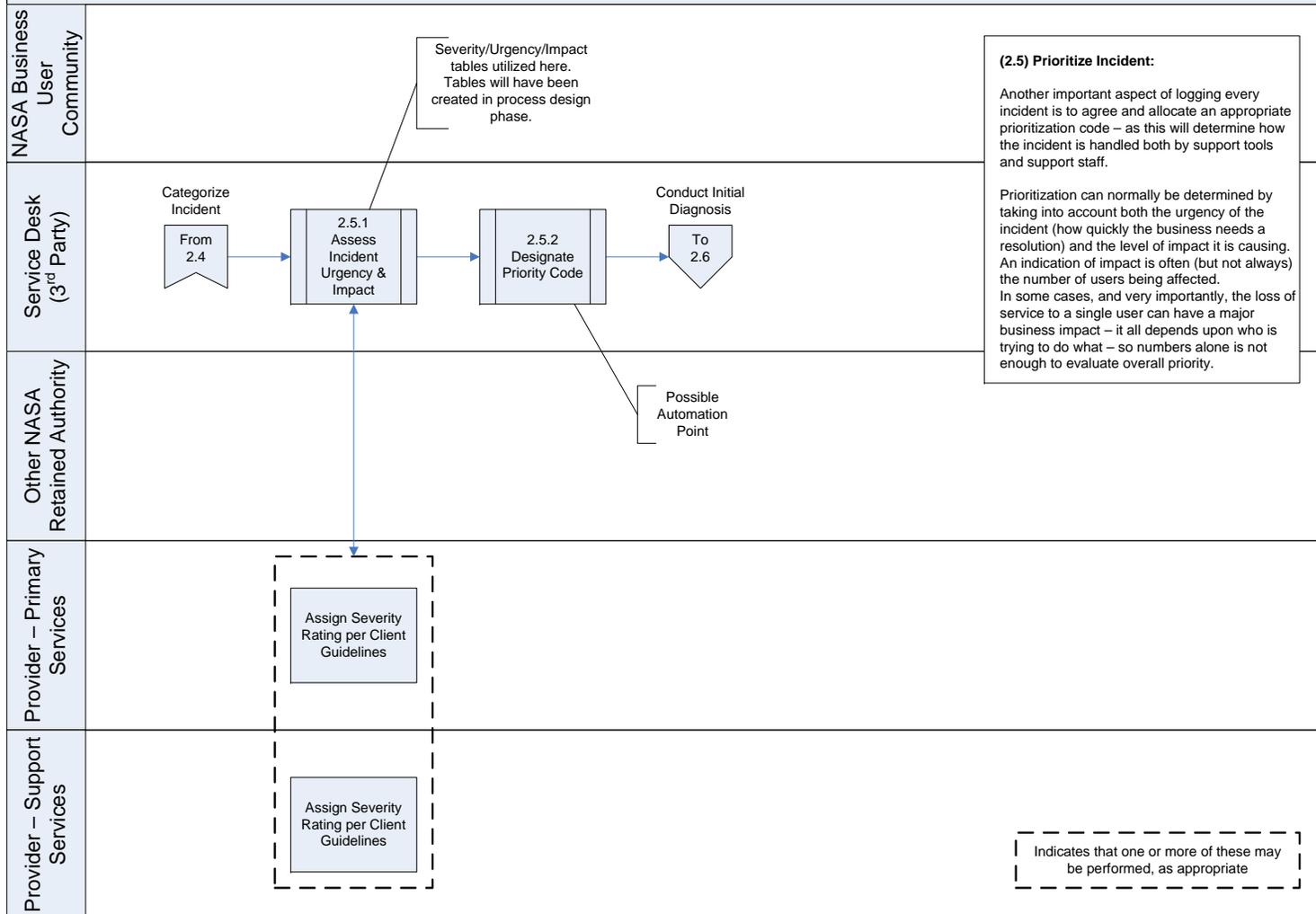
SO-2.4 Categorize Incident

3/5/2009

NASA Business User Community	<div data-bbox="1283 383 1633 927" style="border: 1px solid black; padding: 5px;"> <p>(2.4) Categorize Incident:</p> <p>Part of the initial logging must be to allocate suitable incident categorization coding so that the exact type of the call is recorded. This will be important later when looking at incident types/frequencies to establish trends for use in Problem Management, Supplier Management and other ITSM activities.</p> <p>Note that the check for Service Requests in this process does not imply that Service Requests are incidents. This is simply recognition of the fact that Service Request are sometimes incorrectly logged as incidents.</p> <p>Multi-level categorization is available in most tools- usually three or four levels of granularity.</p> <p>Note: Sometimes the details available at the time an incident is logged may be incomplete, misleading or incorrect. It is therefore important that the categorization of the incident is verified/ validated and updated if necessary, at call closure time (in a separate closure categorization field, so as not to corrupt the original categorization).</p> </div>
Service Desk (3 rd Party)	<div data-bbox="365 548 793 667"> <pre> graph LR A[Log Incident From 2.3] --> B[2.4.1 Categorize Incident] B --> C[Prioritize Incident To 2.5] </pre> </div>
Other NASA Retained Authority	
Provider – Primary Services	<div data-bbox="491 959 669 1105" style="border: 1px dashed black; padding: 5px; width: fit-content;"> <p>Perform initial event profiling in concert with the Service Desk</p> </div>
Provider – Support Services	<div data-bbox="491 1157 669 1304" style="border: 1px dashed black; padding: 5px; width: fit-content;"> <p>Perform initial event profiling in concert with the Service Desk</p> </div> <div data-bbox="1318 1271 1640 1336" style="border: 1px dashed black; padding: 5px; width: fit-content; margin-top: 20px;"> <p>Indicates that one or more of these may be performed, as appropriate</p> </div>

SO-2.5 Prioritize Incident

3/5/2009



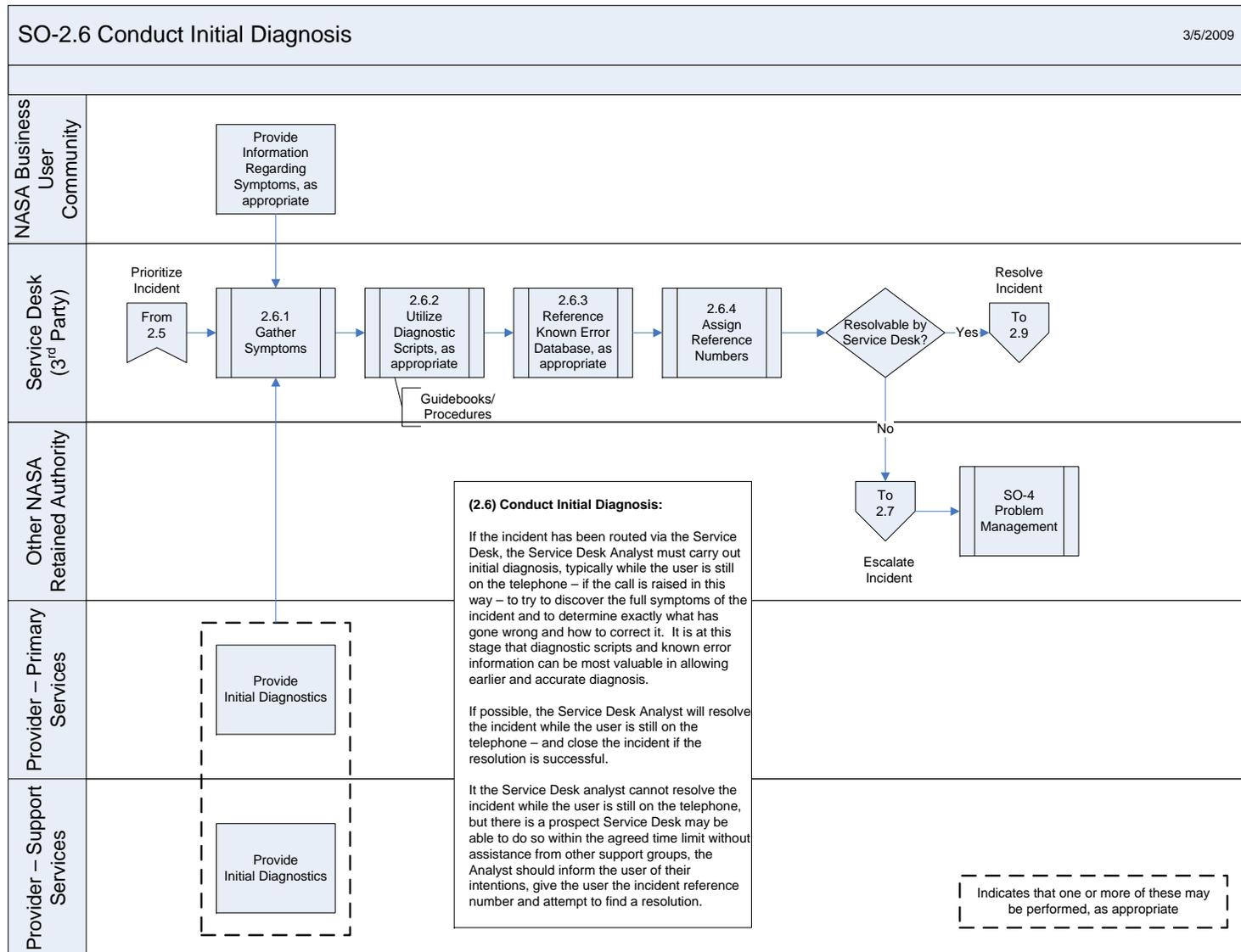
(2.5) Prioritize Incident:

Another important aspect of logging every incident is to agree and allocate an appropriate prioritization code – as this will determine how the incident is handled both by support tools and support staff.

Prioritization can normally be determined by taking into account both the urgency of the incident (how quickly the business needs a resolution) and the level of impact it is causing. An indication of impact is often (but not always) the number of users being affected. In some cases, and very importantly, the loss of service to a single user can have a major business impact – it all depends upon who is trying to do what – so numbers alone is not enough to evaluate overall priority.

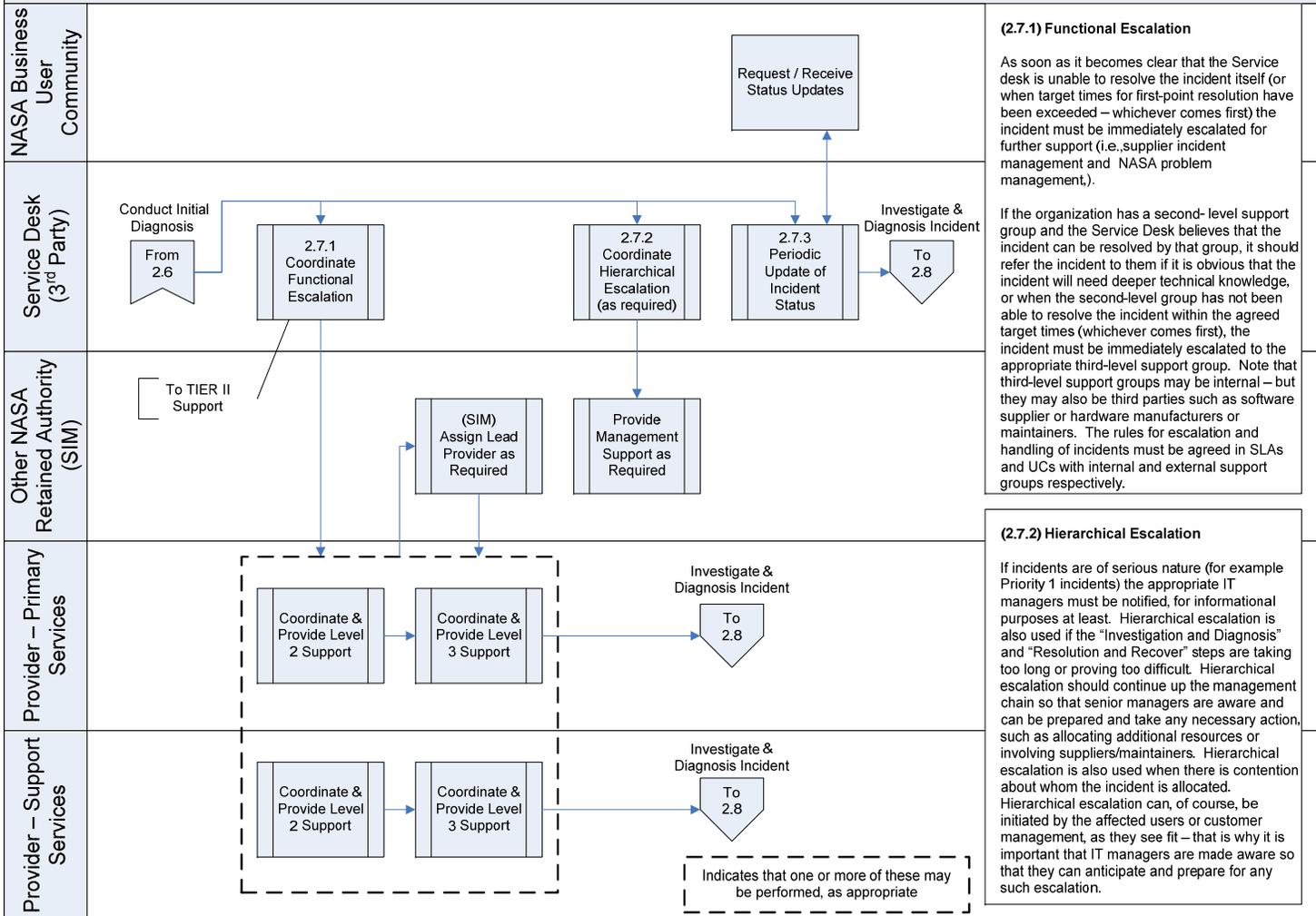
SO-2.6 Conduct Initial Diagnosis

3/5/2009



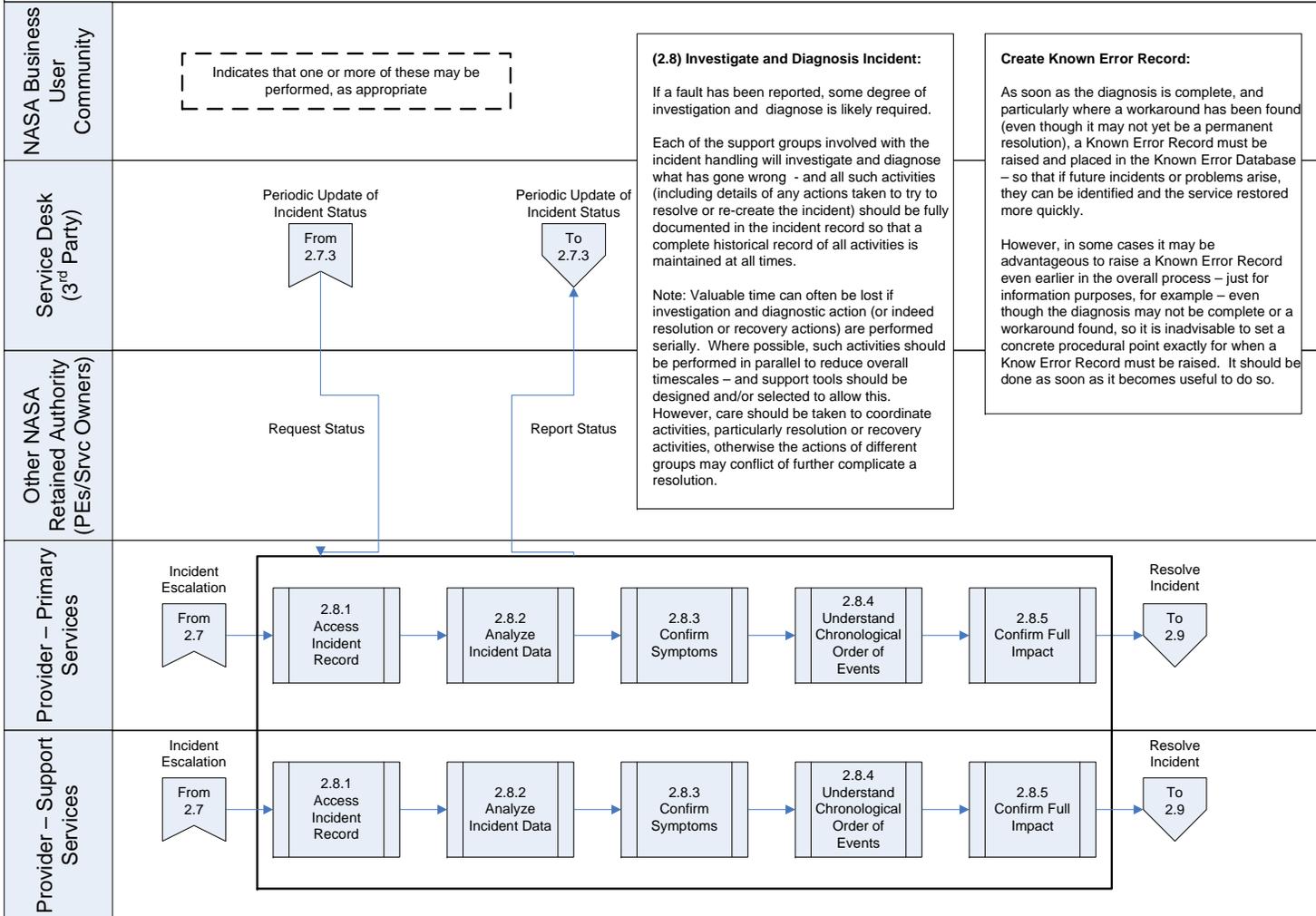
SO-2.7 Escalate Incident

3/5/2009



SO-2.8 Investigate & Diagnosis Incident

3/5/2009



SO-2.9 Resolve Incident

3/5/2009

NASA Business User Community

Service Desk (3rd Party)

Other NASA Retained Authority

Provider – Primary Services

Provider – Support Services

(2.9) Resolve Incident:

When a potential resolution has been identified, this should be applied and tested. The specific actions to be undertaken and the people who will be involved in taking the recovery actions may vary depending upon the nature of the fault – but could involve:

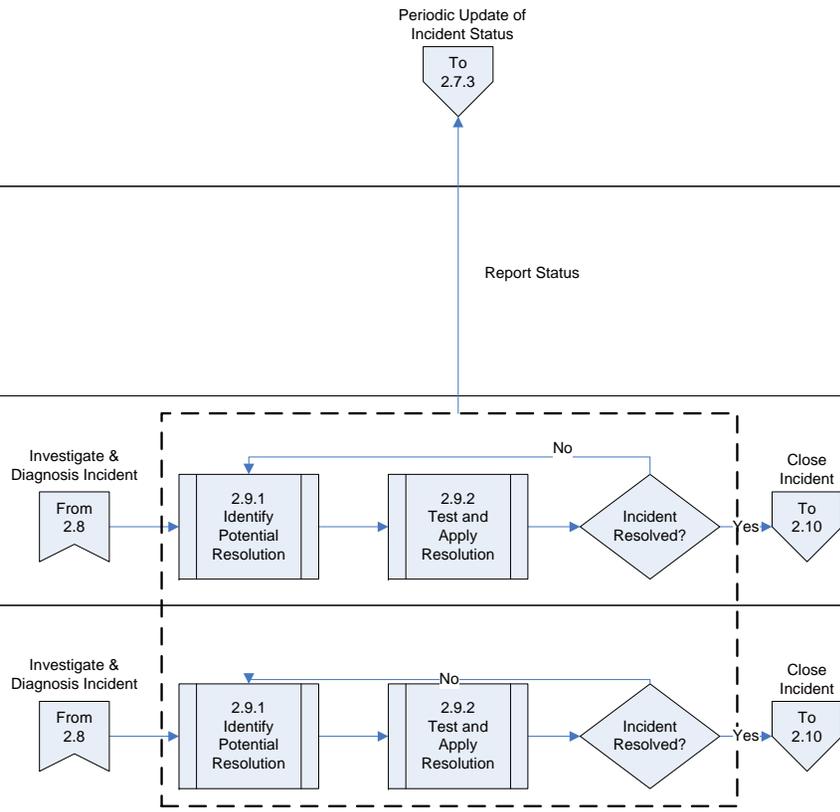
- Asking the user to undertake directed activities on their own desk top or remote equipment.
- The Service Desk implementing the resolution either centrally (say, rebooting a server) or remotely using software to take control of the user's desktop to diagnose and implement a resolution
- Specialist support groups being asked to implement specific recovery actions (e.g. Network Support reconfiguring a router)
- A third-party supplier or maintainer being asked to resolve the fault

Even when a resolution has been found, sufficient testing must be performed to ensure that recovery action is complete and that the service has been fully restored to the user(s).

In some cases it may be necessary for two or more groups to take separate, though perhaps coordinated, recovery actions for an overall resolution to be implemented. In such cases Incident Management must coordinate the activities and liaise with all parties involved.

Regardless of the actions taken, or who does them, the Incident Record must be updated accordingly with all relevant information and details so that a full history is maintained.

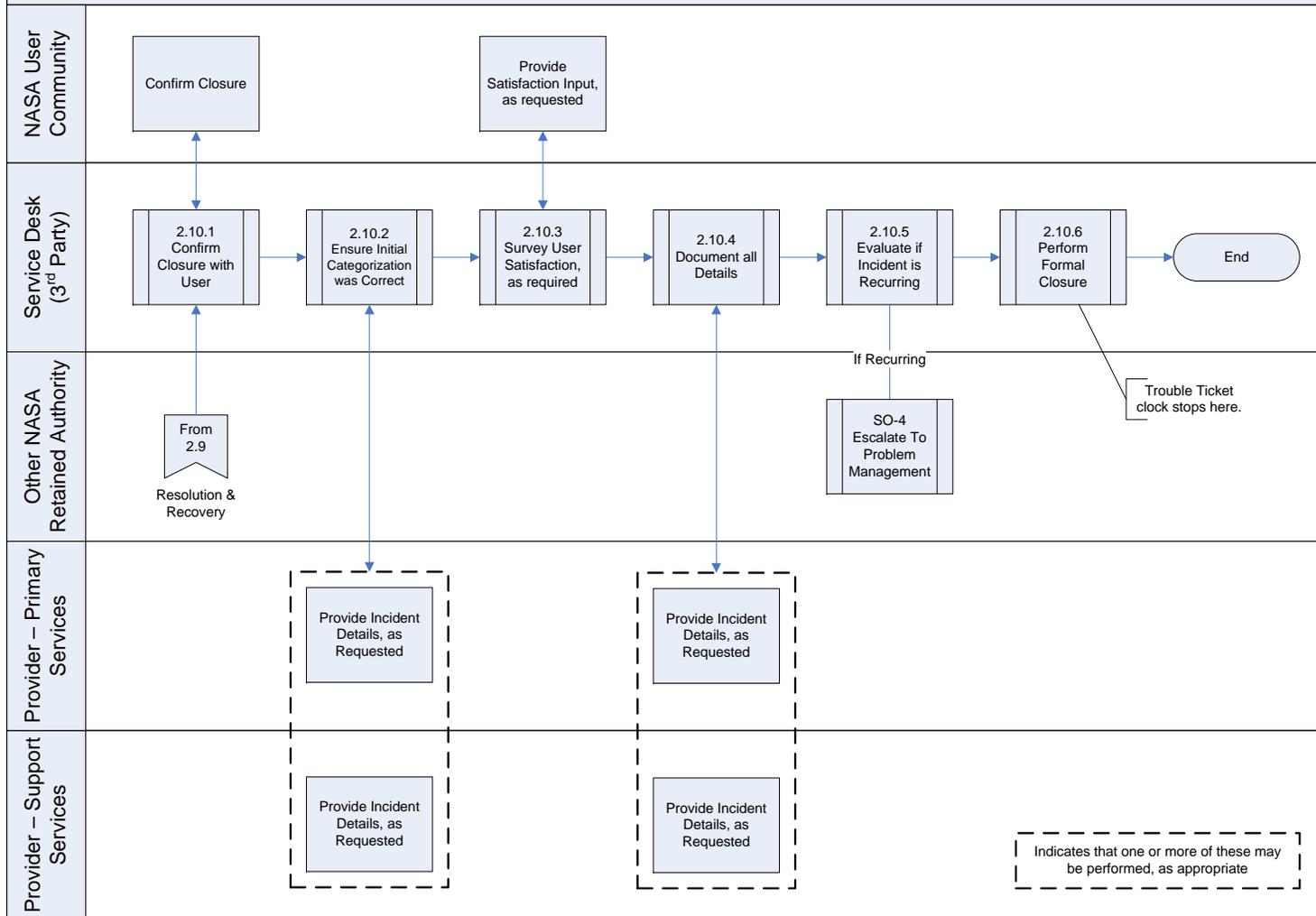
The resolving group should pass the incident back to the Service Desk for closure action.



Indicates that one or more of these may be performed, as appropriate

SO-2.10 Close Incident

3/5/2009



IT Incident Management Roles and Responsibilities

A number of roles and responsibilities have been identified as essential to the IT incident management process. The purpose of this section is to define those functional roles and responsibilities necessary for effective IT incident management, including but not limited to, **NASA's** staff, management, partners, providers, and contractors, regardless of physical location, involved in identifying and supporting IT incidents relating to **NASA's** IT environment.

Roles	Responsibilities
(SIM) Incident Management Process Owner	<ul style="list-style-type: none"> • Responsible for the documentation, modification, and update of all IT incident management process documentation • Responsible for assuring that the incident process meets organizational performance expectations • Ensures that individuals/groups adhere to the incident process • Accountable for the efficiency, effectiveness, and accountability of the process • Responsible for incident management performance reporting
Incident Coordinator	<ul style="list-style-type: none"> • Participates in weekly Change Advisory Board (CAB) meetings • Accountable for management of incident ticket completeness, timeliness of responses and follow-up, and integration with other processes (e.g., change management) • Monitors the effectiveness of incident management and makes recommendations for improving it • Manages incident support staff • Allocates resources for incident support effort • Assists with incident management reporting and documentation • Assists with incident ticket completeness, timeliness of responses and follow-up, and integration with other processes (e.g., change management)
Incident Support	<ul style="list-style-type: none"> • May help with entry of incident ticket • May participate in 1st, 2nd, and/or 3rd level incident support • May participate in 1st, 2nd, and/or 3rd level problem support • Identifies incidents (e.g., customer calls, via monitoring, by analyzing incident data, etc.) • Investigates incidents, according to impact, through to restore, handoff to problem management, or error identification • Matches incidents to known errors • Advises incident management staff, and/or acts, on the best available work-arounds for incidents related to known errors • May enter/update known error information

Identification of Incidents and Logging of Incident Tickets

An incident will be recognized when a variation from standard IT operating performance has been identified or is likely to occur, as well as when IT customers require assistance. Incidents include, but are not limited to:

- Degradations in expected IT performance
- Requests from customers
- Impacts to IT service levels

Incidents may be identified by: any person (including staff, management, partners, providers, and contractors, regardless of physical location) responsible for supporting, or receiving support from, NASA's IT environment.

IT incident management tickets are to be filled out for any/all incidents reported, concerning **NASA's** IT environment.

Known incident information is to be filled submitted to the NASA Enterprise Service Desk incident management system for any/all current or previously encountered but unreported incidents.

Sample Incident Ticket (captured through the NASA incident management system managed by the NASA Enterprise Service Desk)

Submission date/time	
Submission #	
Incident information	
Incident classification	
Priority	
Effected parties/locations	
Possible causes of incident	
Hand-offs to other processes (e.g., change request form)	
Responsible support personnel	
Estimated resolution time	
Incident status – logged, assessed, rejected, accepted, on hold	

Sample Known Error Ticket

Submission date/time	
Submission #	
Known error information	
Known error classification	
Criticality	
Effected parties/locations/platforms	

Relevant support personnel	
Possible causes of known error	
Workaround information	
Estimated resolution time	
Estimated cost to repair	

IT Incident Support Timing

IT incident management is ongoing. When incidents are discovered, support will be provided according to pre-defined incident management support and service levels defined within each supporting contract.

IT Incident Management Performance Measures

NASA will measure and maintain the performance of its IT incident management process through the NASA Enterprise Service Desk with the following performance measures:

- # of incidents during the period (week)
- % of incidents initiated by customers
- Mean time to incident resolution
- % of incidents handled within agreed response time
- Avg. cost per incident
- % first call resolution
- # of incidents processed per service desk employee
- % of incidents resolved via self service
- % of incidents resulting from changes% Incidents resulting from change
- Customer satisfaction rating (1=low, 5=high)
- # of repeat inquiries
- Average cost per call
- # of escalations

IT Incident Management - Key Integration Points

Effective IT incident management requires significant integration between those technology and business communities that support, or request support of, **NASA's** IT environment. As such, the IT incident management process should include, but not be limited to, the following process integration points:

- Inputs
 - Monitoring
 - Systems/network management event generation
 - Security threat/weakness/vulnerability
 - Request/Demand Management
 - Customers
 - Project Management
 - Applications Development

- Architecture
- Operations
- Business Relationship Management
- Configuration Management (known errors)
- Outputs
 - Problem Management
 - Configuration Management (known errors)

Document Maintenance

NASA's Service Integration Management office will review the IT incident management process document annually for detail and periodic refinement.

Additional reviews may be conducted as needed to amend policies to reflect changes in **NASA's** IT and business strategies, service offerings, and changing conditions in legal, regulatory, and market conditions. Suggestions or feedback regarding the IT incident management process document may be submitted to the document owner, who will formalize and submit draft document revisions for review and approval by the document review board. Once approved, the document owner will update and distribute the document.