

BMC Software Consulting Services

Fermilab Computing Division

Incident Management Business Process and Procedure

| | |
|-----------|----------|
| Client: | Fermilab |
| Date : | 01/30/09 |
| Version : | 1.0 |



| GENERAL | | | |
|------------------------|--|----------------------|-------------------------|
| Description | This document establishes an Incident Management (IM) process and procedures for the Fermilab Computing Division. Adoption and implementation of this process and supporting procedures ensures the timely recovery of services provided by the Computing Division for Fermilab. | | |
| Purpose | This document supports the Incident Management Process | | |
| Applicable to | All Fermilab Computing Division Employees | | |
| Supersedes | None. | | |
| Document Owner | Computing Division Incident Manager | Owner Org | Computing Division Head |
| Effective Dates | 02-01-2009 – 01-31-2010 | Revision Date | 01-30-09 |

| VERSION HISTORY | | | |
|------------------------|-----------|-----------------------------|---------------------------|
| Version | Date | Author(s) | Change Summary |
| 1.0 | 1-30-2009 | David Whitten – Plexent LLP | Initial Document Creation |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

TABLE OF CONTENTS

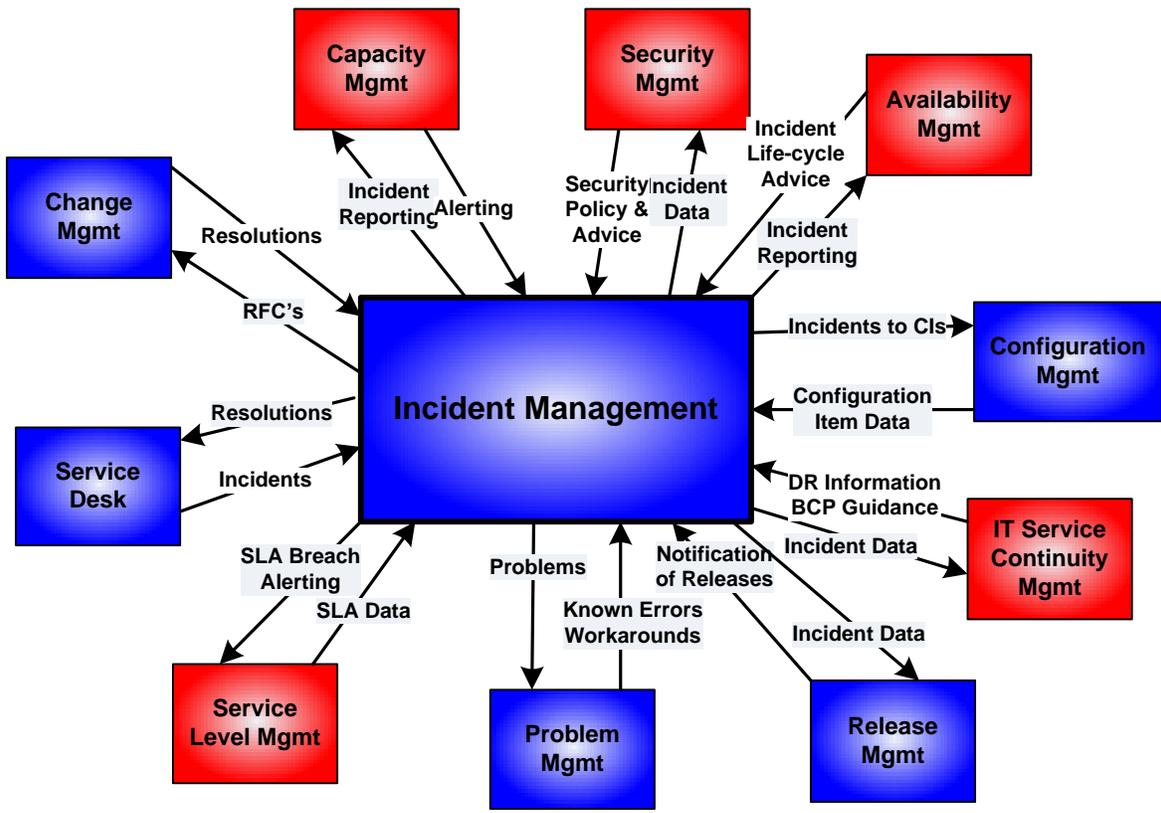
| | |
|--|-----------|
| Incident Management..... | 5 |
| Process Context Diagram Interfacing Process Flow | 5 |
| Incident Management Process Flow..... | 6 |
| Incident Management Process Roles and Responsibilities | 7 |
| Recommended Incident Management Process Measurements | 8 |
| Recommended Incident Management SLA Metrics | 9 |
| Process Integration Points | 11 |
| 1.1 Incident Detection & Recording Procedure Flow | 13 |
| 1.1 Incident Detection & Recording Procedure Rules | 14 |
| 1.1 Incident Detection & Recording Procedure Narrative | 14 |
| 1.2 Incident Classification Procedure Flow | 15 |
| 1.2 Incident Classification Procedure Business Rules..... | 17 |
| 1.2 Incident Classification Procedure Narrative | 17 |
| 1.3 Incident Initial Support Procedure Flow..... | 19 |
| 1.3 Incident Initial Support Procedure Business Rules..... | 20 |
| 1.3 Incident Initial Support Procedure Narrative..... | 20 |
| 1.4 Incident Investigation & Diagnosis Procedure Flow..... | 21 |
| 1.4 Incident Investigation & Diagnosis Procedure Business Rules | 23 |
| 1.4 Incident Investigation & Diagnosis Procedure Narrative..... | 23 |
| 1.5 Incident Resolution Procedure Flow | 25 |
| 1.5 Incident Resolution Procedure Business Rules..... | 27 |
| 1.5 Incident Resolution Procedure Narrative | 27 |
| 1.6 Incident Restoration Procedure Flow | 29 |
| 1.6 Incident Restoration Procedure Business Rules | 30 |
| 1.6 Incident Restoration Procedure Narrative | 30 |
| 1.7 Incident Closure Procedure Flow..... | <u>32</u> |
| 1.7 Incident Closure Procedure Business Rules | <u>33</u> |
| 1.7 Incident Closure Procedure Narrative..... | <u>33</u> |
| 1.8 Incident Ownership, Monitoring, Tracking & Communication Procedure Flow..... | <u>35</u> |
| 1.8 Incident Ownership, Monitoring, Tracking & Communication Procedure Business Rules..... | <u>36</u> |
| 1.8 Incident Ownership, Monitoring, Tracking & Communication Procedure Narrative..... | <u>36</u> |
| 1.9 Critical Incident Communication Procedure Flow | <u>38</u> |
| 1.9 Critical Incident Procedure Business Rules | <u>39</u> |
| 1.9 Critical Incident Procedure Narrative | <u>39</u> |
| Appendix 1 – Incident Management Ticket Pending Procedure..... | <u>41</u> |
| Appendix 2 - Related Documents | <u>42</u> |
| Appendix 3 – Tools | <u>43</u> |
| Appendix 4 – RACI Matrix | <u>44</u> |
| Appendix 5 – Tools | <u>49</u> |
| Appendix 6 – Process Specific Techniques | <u>50</u> |
| Appendix 7 - Repositories | <u>51</u> |
| Appendix 8 – Communication Plan..... | <u>52</u> |

TABLE OF CONTENTS

| | |
|---|--------------------|
| Appendix 9 – Forms, Templates | 56 |
| Service Desk Manual Ticket Logging Form | 56 |
| Appendix 10 - Impact Matrix..... | 57 |
| Appendix 11 – Urgency Matrix..... | 58 |
| Incident Management Escalation Table..... | 59 |

INCIDENT MANAGEMENT

PROCESS CONTEXT DIAGRAM INTERFACING PROCESS FLOW

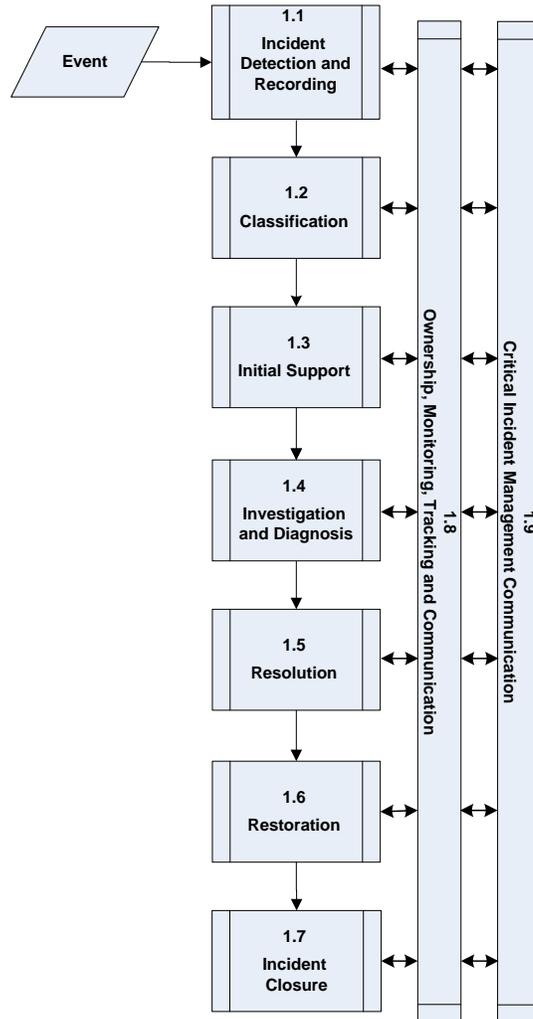


Service Support: Blue
 Service Delivery: Red

© 2009 Plexent

NOTE: This graphic illustrates the basic interactions between Incident Management and the ITIL processes at a high level and does not represent detailed dependencies. This document will describe the direct dependencies as prescribed for the Fermi National Laboratory Computing Division.

INCIDENT MANAGEMENT PROCESS FLOW



© 2009 Plexent

| INCIDENT MANAGEMENT PROCESS ROLES AND RESPONSIBILITIES | |
|---|--|
| Roles | Responsibilities |
| Incident Manager | <ul style="list-style-type: none"> • Drive the efficiency and effectiveness of the IM process. • Produce management information. • Monitor the effectiveness of IM and make recommendations for improvement. • Develop and maintain the IM systems. • Monitor the status and progress towards resolution of all open incidents. • Keep affected users informed about progress. • Escalate the incident if necessary. |
| Critical Incident Manager | <ul style="list-style-type: none"> • Responsible for accepting the critical incident. • Determine and document the impact of the issue to the customer. • Determine, in conjunction with Service Delivery and the customer, the action planned to resolve the critical incident. • Update the Critical Incident portal to provide consistent communication within Computing Division and the Scientific and Research community as well as communicating to the end-user. • After restoration, the critical incident manager is responsible for a post mortem and assembling recommendations to prevent reoccurrence in coordination with Incident and Problem Management. |
| Tier 1 (Service Desk) and Tier 2 (Operations) Support Staff | <ul style="list-style-type: none"> • Record the incident. • Provide initial support and classification. • Determine and provide ownership, monitoring, tracking, and communication. • Resolve and recover incidents not assigned to Tier 2 • Monitor incident details, including the configuration items (CIs) affected. • Investigate and diagnose incidents. Include resolution when possible. • Detect possible problems and assign them to the Problem Management team for them to raise problem records. • Resolve and recover assigned incidents. • Close incidents |
| Configuration Manager | Ensure accuracy, accessibility, and timeliness of decision making information about Configuration Items. |
| Problem Manager | <ul style="list-style-type: none"> • Provide support to the IM process by providing them access to the Known Error database which can assist in supporting the resolution and restoration of the service. • Receive identified problems from Incident Management • Provide assistance identifying Incident trends, indicating a possible Problem. |
| Change Manager | <ul style="list-style-type: none"> • Provide IM with information about scheduled changes and status. • Manage emergency change requests for restoration of services. • Receives change requests from Incident Management |
| Availability | Provide availability requirements and Incident Management Lifecycle Advice to IM. |

| INCIDENT MANAGEMENT PROCESS ROLES AND RESPONSIBILITIES | |
|---|---|
| Roles | Responsibilities |
| Management | |
| Service Level Management | Receive management information such as SLA Breach warnings, SLA targets and data from IM. |
| Tier 3 (R&D/3rd Party) | Support the hardware and software systems. Tier 3 consists of vendors and developers. |
| Stakeholders | Participate in audits, reviewing results of the audit & performing corrective actions. |

| RECOMMENDED INCIDENT MANAGEMENT PROCESS MEASUREMENTS | | | | |
|--|------------------|---|--|--|
| Key Performance Indicators | Frequency | Upper/Lower Control Limits | Objective | Data Capture |
| Average time to resolve Incidents | Monthly | Upper limits will vary slightly based on the SLA. Critical (Priority1) Incidents 4 hours to resolve High (Priority 2) incidents 16 hours to resolve Medium (Priority 3) incidents 5 business days to resolve Low (Priority 4) Incidents 30 business days to resolve | Objective: To identify the average time required to resolve incidents. A decrease in the average time to resolve incidents shows an improvement in the effectiveness of the Incident Management process. Formula: <u>Time to Resolve Incidents</u> # of Incidents Additional Guidance: Since we are looking for a trend in the average time to resolve incidents, the metric becomes valuable only after we have three months of data. Also, to maintain the integrity of the information being trended, only the last thirteen months should be included in the report. | Incident Resolution Procedure, Step 1.5.10 |
| Percentage of Incidents handled within agreed response times | Monthly | Minimum limit is 90% incident within Help Desk response targets | Objective: To track the percentage of incidents handled based on agreed response times. The increased percentage of incidents being handled within agreed response times shows an improvement in the effectiveness of the | SLA reports |

| RECOMMENDED INCIDENT MANAGEMENT PROCESS MEASUREMENTS | | | |
|---|------------------|--|--|
| | | | Incident Management process. Formula: # of incidents meeting SLA targets # of incidents |
| Operational Reports | Frequency | Objective | Data Capture |
| Morning Report | Daily | Measure total number of tickets and number of unresolved incidents and service requests. | Incident Detection and Recording Step 1.1 |
| Open Ticket Aging Report | Daily | Measure open incident tickets by group and time open. | Incident Resolution and Incident Closure Procedure Flows 1.5 and 1.7 |
| Open Ticket Summary & Detail Report | Weekly | Open tickets broken down by priority. | Computing Division Incident Resolution and Incident Closure Procedure flows 1.5 and 1.7 |

| RECOMMENDED INCIDENT MANAGEMENT SLA METRICS | | | | | | |
|--|---|--|-----------------|---------------------|----------------------------|--------------------------|
| SLA | Category | Requirement | Measure | Target | Minimum Performance | Report Repository |
| 1.11 | Critical Data Center (FCC)– Incident Resolution | Priority Critical – Mail server, Enstore system events | Time to Resolve | < 2 hours | 0.9 | SharePoint |
| 1.12 | Critical Data Center (FCC)– Incident Resolution | Priority Critical – Other Events resolution time | Time to Resolve | <8 hours | 0.9 | SharePoint |
| 1.13 | Critical Data Center (FCC)– Incident Resolution | Priority High resolution time | Time to Resolve | < 8 hours | 0.95 | SharePoint |
| 1.14 | Critical Data Center | Priority Medium resolution time | Time to Resolve | < 16 business hours | 0.95 | SharePoint |

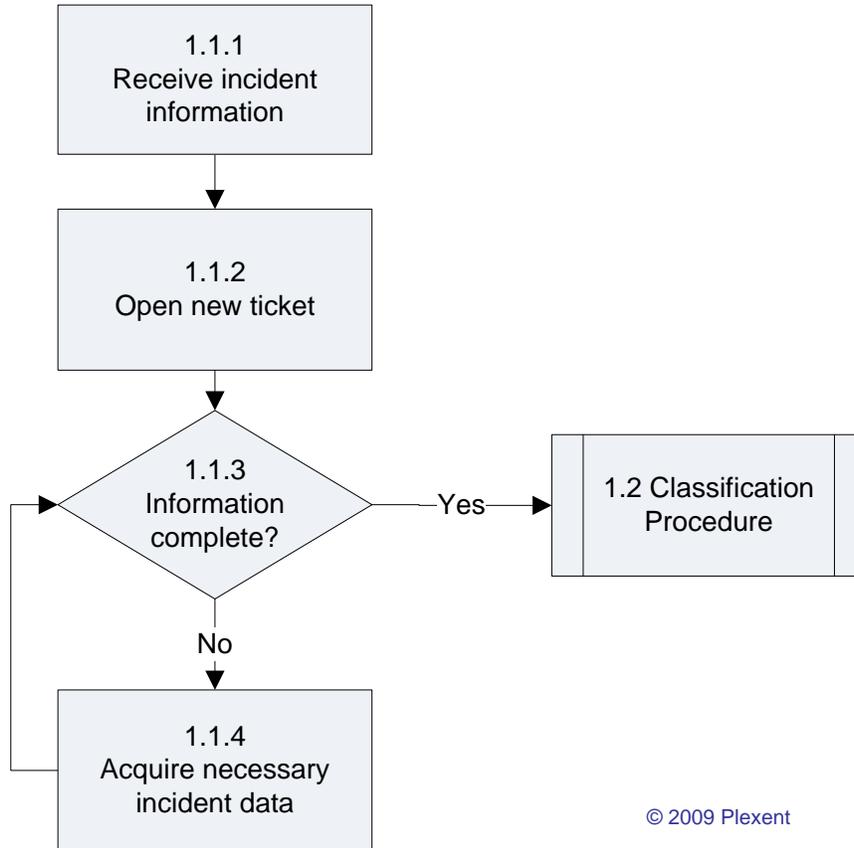
| RECOMMENDED INCIDENT MANAGEMENT SLA METRICS | | | | | | |
|--|---|------------------------------------|--------------------|---|----------------------------|--------------------------|
| SLA | Category | Requirement | Measure | Target | Minimum Performance | Report Repository |
| | (FCC)– Incident Resolution | | | | | |
| 1.15 | Critical Data Center (FCC)– Incident Resolution | Priority Medium resolution time | Time to Resolve | As prioritized by Vendor per schedule | 0.95 | SharePoint |
| 1.16 | Critical Data Center (FCC)– Incident Resolution | Critical Incident reporting | Time to Report | Initial finding within 24 business hours of Incident Resolution | 0.95 | SharePoint |
| 1.21 | Other Locations – Incident Resolution | Critical Resolution time | Time to Resolve | < 8 hours | 0.85 | SharePoint |
| 1.22 | Other Locations – Incident Resolution | High Resolution time | Time to Resolve | < 16 hours | 0.9 | SharePoint |
| 1.23 | Other Locations – Incident Resolution | Medium Resolution time | Time to Resolve | < 18 business hours | 0.9 | SharePoint |
| 1.24 | Other Locations – Incident Resolution | Low Resolution time | Time to Resolve | As prioritized by Vendor per schedule | 0.95 | SharePoint |
| 1.25 | Other Locations – Incident Resolution | Critical Incident reporting | Time to Report | Initial findings within 24 business hours of Incident Resolution | 0.95 | SharePoint |

| PROCESS INTEGRATION POINTS | | | |
|-----------------------------------|----|--------------------------|---|
| Process | | Process | Information |
| Incident Management | to | Problem Management | <ul style="list-style-type: none"> Incident information and records for proper trending and analysis. Problem Management may be consulted regarding Critical Incidents. |
| Problem Management | to | Incident Management | <ul style="list-style-type: none"> Known Error Database containing solutions and workarounds to assist resolve incidents. Problem information and records. |
| Incident Management | to | Change Management | <ul style="list-style-type: none"> Change request to address an identified incident. Change related incidents. |
| Change Management | to | Incident Management | Approved and authorized change request to address identified incident. |
| Incident Management | to | Service Level Management | Incident management reports regarding incident response times and resolution times. |
| Service Level Management | to | Incident Management | <ul style="list-style-type: none"> Service catalog Agreed service level response times and resolution for incidents based on incident priority level. |
| Incident Management | to | Capacity Management | Performance and capacity related incident records |
| Capacity Management | to | Incident Management | Resolution assistance for capacity related incidents |
| Incident Management | to | Financial Management | Incident information and records. |
| Financial Management | to | Incident Management | Cost details of reported incidents. |
| Incident Management | to | Configuration Management | Incident information to assist Configuration Management determines inaccurate configuration items (CIs). |
| Configuration Management | to | Incident Management | CI details from the Configuration Management Database (CMDB) to assist Incident Management effectively diagnose the faulty CI. |
| Incident Management | to | Release Management | Incident information and records on possible failed releases. |
| Release Management | to | Incident Management | Release schedule |
| Incident Management | to | Availability Management | Incident information for Expanded Incident Lifecycle |
| Availability Management | to | Incident Management | <ul style="list-style-type: none"> Recommendations to improve incident resolution times Resolution assistance for capacity related incidents |

PROCESS INTEGRATION POINTS

| Process | | Process | Information |
|---------------------|----|--|---|
| Incident Management | to | IT Service Continuity Management (ITSCM) | Critical incident and outage information. |
| ITSCM | to | Incident Management | Invocation process and procedures to follow in the event of a major disaster. |

1.1 INCIDENT DETECTION & RECORDING PROCEDURE FLOW



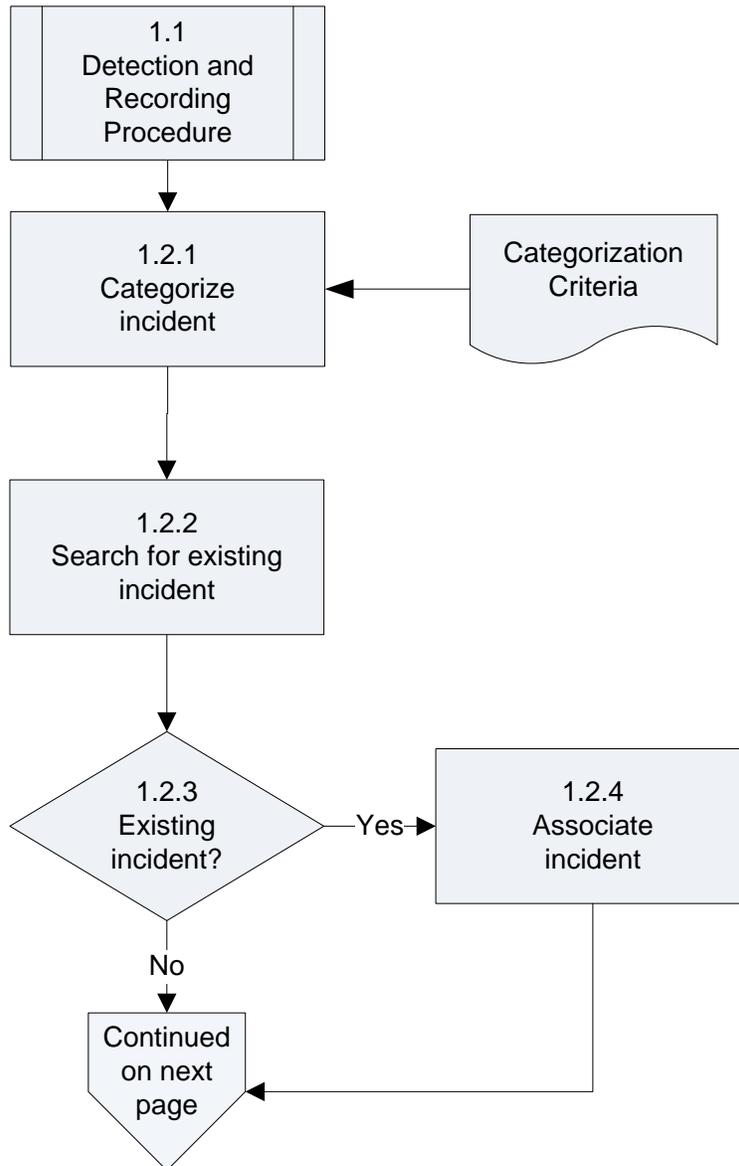
1.1 INCIDENT DETECTION & RECORDING PROCEDURE RULES

| | |
|-------------------------|---|
| Triggers | <ul style="list-style-type: none"> • User Contacts • Monitoring Event (Service Threshold being exceeded) |
| Inputs | <ul style="list-style-type: none"> • Monitoring Events • Incidents • Contact Information • Email • Web intranet • Phone |
| Outputs | <ul style="list-style-type: none"> • New Incident Records • Classification Information • Information to User |
| General Comments | The purpose of this procedure is to ensure adequate information is collected and recorded to enable efficient and effective resolution of the incident. |

1.1 INCIDENT DETECTION & RECORDING PROCEDURE NARRATIVE

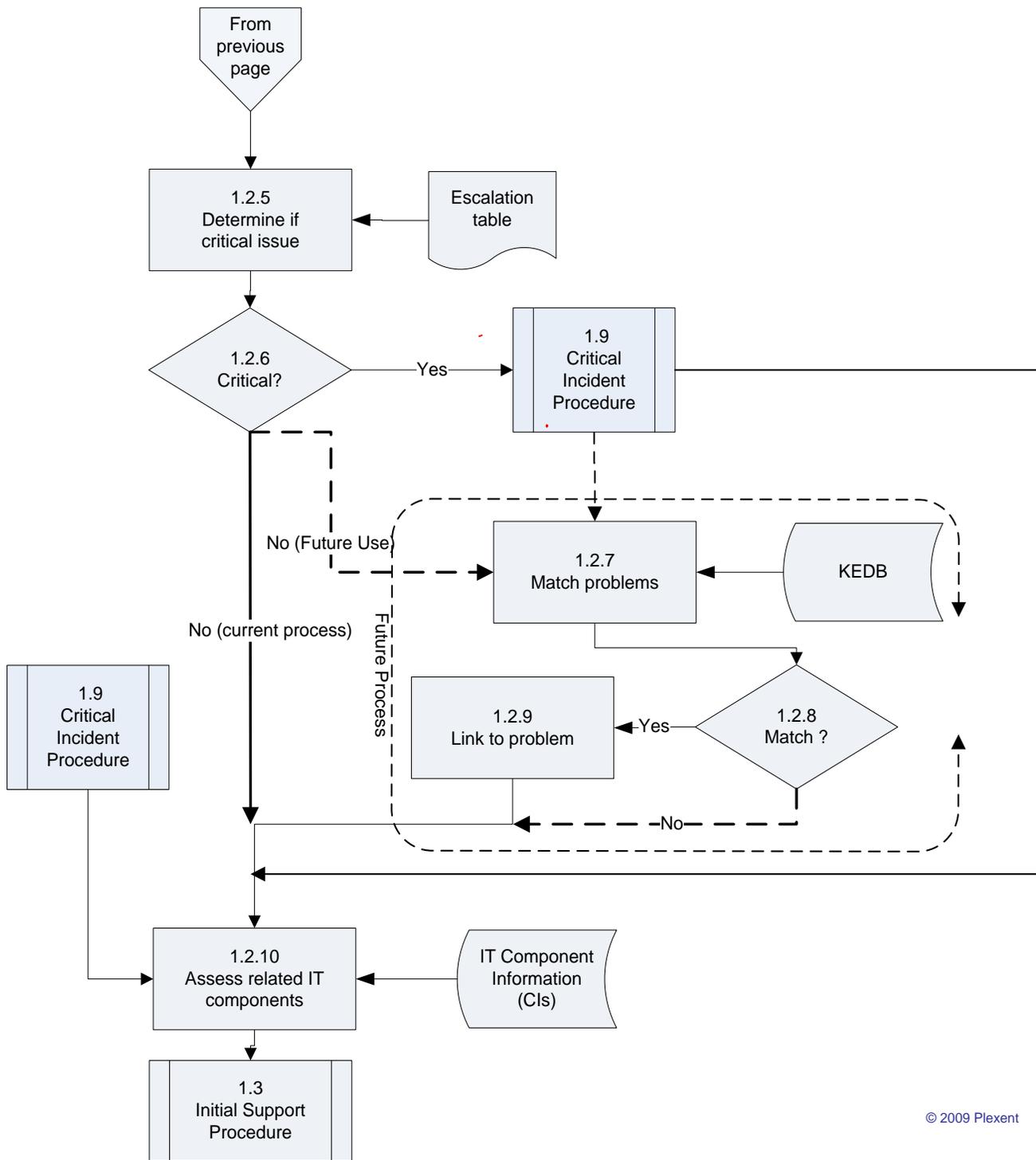
| Step | Responsible Role | Action |
|-------|--|---|
| 1.1.1 | Incident Manager/ Tier 1 Service Desk Analyst | Receive incident information by telephone, email, alert, web ticket, etc. |
| 1.1.2 | Incident Manager/ Tier 1 Service Desk Analyst | Open a new ticket. All incidents are recorded as incident tickets in the Service Desk database system. Initial basic information recorded includes: <ul style="list-style-type: none"> • Requestor information • A description of the incident • Asset/configuration item (CI) affected or impacted. |
| 1.1.3 | Incident Manager/ Tier 1 Service Desk Analyst | Has complete information been captured? <ul style="list-style-type: none"> • If complete execute the Incident Classification Procedure • If the information is incomplete, acquire necessary incident data. |
| 1.1.4 | Incident Manager/ Tier 1 Service Desk Analyst | <ul style="list-style-type: none"> • If the information is incomplete, acquire necessary incident data. • Once the information is complete, execute the Incident Classification Procedure |

1.2 INCIDENT CLASSIFICATION PROCEDURE FLOW



© 2009 Plexent

1.2 INCIDENT CLASSIFICATION NARRATIVE PROCEDURE CONTINUED



© 2009 Plexent

1.2 INCIDENT CLASSIFICATION PROCEDURE BUSINESS RULES

| | |
|-------------------------|---|
| Triggers | <ul style="list-style-type: none"> Any New Incident (Especially Critical Incidents) Follow-up Updates |
| Inputs | <ul style="list-style-type: none"> System Category Information Management (SCIM) Impact/Urgency Table Known Error Database Problem Records CI information from Configuration Management SLAs Existing Incident Records Problem Record from Problem Management |
| Outputs | <ul style="list-style-type: none"> Updated Incident Record Associated Problem or Incident Record Critical Notification Incident Linkage to Configuration Item |
| General Comments | The purpose of this procedure is to ensure timely and accurate initial categorization for efficient and effective resolution of the incident. |

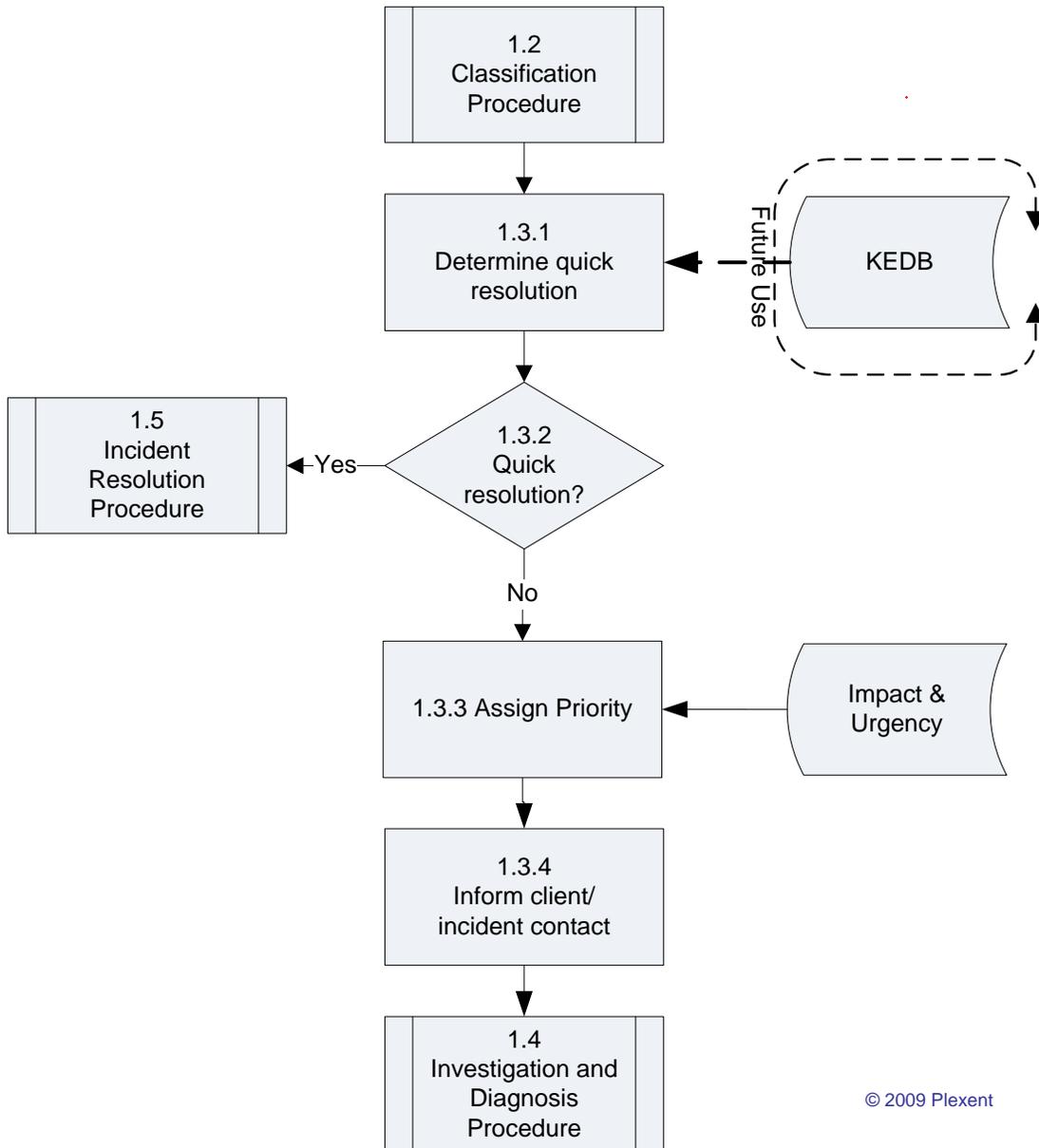
1.2 INCIDENT CLASSIFICATION PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|-------|---|---|
| 1.2.1 | Service Desk Analyst - Tier 1/Tier 2 | Assign a category to the incident. Valid examples of categories include software, hardware, network, etc. These Product and Operational categories are common to Change, Configuration and Problem Management processes. |
| 1.2.2 | Service Desk Analyst - Tier 1/Tier 2 | Search for an existing open incident for this issue. |
| 1.2.3 | Service Desk Analyst - Tier 1/Tier 2 | <ul style="list-style-type: none"> If an existing incident is found, go to step 1.2.4. If there is no existing incident, go to step 1.2.5. |
| 1.2.4 | Incident Manager / Service Desk Analyst - Tier 1/Tier 2 | Associate the two incidents on the related records tab |
| 1.2.5 | Service Desk Analyst - Tier 1/Tier 2 | <ul style="list-style-type: none"> Determine if the incident is a critical issue according to the guidance provided by the Critical Incident Manager, the Service Catalog, and (Future Use: The SLA). |

1.2 INCIDENT CLASSIFICATION PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|--------|--------------------------------------|---|
| 1.2.6 | Service Desk Analyst - Tier 1/Tier 2 | <ul style="list-style-type: none"> • If the incident is critical, go to step procedure 1.9 Critical Incident Procedure • If the incident is not critical go to 1.2.10 • If the incident is not critical, go to step 1.2.7. (Future Use) |
| 1.2.7 | Service Desk Analyst - Tier 1/Tier 2 | Using the Known Error Database (KEDB), search for a matching problem or known error. (Future Use) |
| 1.2.8 | Service Desk Analyst - Tier 1/Tier 2 | <p>(Future Use)</p> <ul style="list-style-type: none"> • If a match is found, go to step 1.2.10. • If no match is found, go to the Problem Management Process, which will determine if a new Problem record should be created. |
| 1.2.9 | Service Desk Analyst - Tier 1/Tier 2 | <p>(Future Use)</p> <p>Link the problem to the incident using the related records tab.</p> |
| 1.2.10 | Service Desk Analyst - Tier 1/Tier 2 | <ul style="list-style-type: none"> • Assess related IT components to ensure scope and impact of the incident is accurately captured. • Go to Incident Initial Support Procedure. |

1.3 INCIDENT INITIAL SUPPORT PROCEDURE FLOW



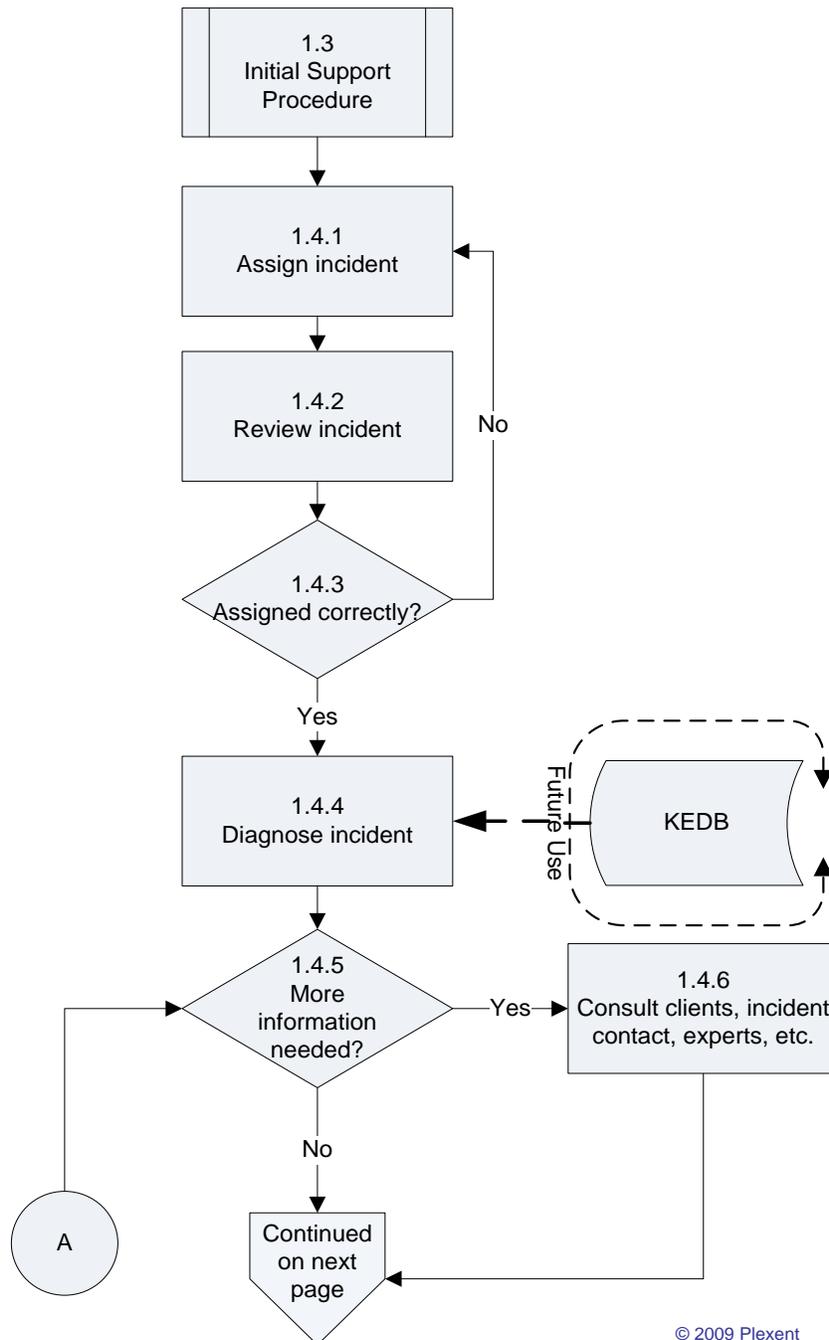
1.3 INCIDENT INITIAL SUPPORT PROCEDURE BUSINESS RULES

| | |
|-------------------------|--|
| Triggers | Exceeding SLA Thresholds requiring Functional and/or Hierarchical Escalation |
| Inputs | <ul style="list-style-type: none"> • SLAs • Updated Incident Records • Handling Procedures • Escalation Procedures • User Contact Information • Escalation Table • Known Errors and Solutions from Problem Management • Known Error Database from Problem Management • FAQs |
| Outputs | <ul style="list-style-type: none"> • Updated Incident Record • User Communication |
| General Comments | <ul style="list-style-type: none"> • The purpose of this procedure is to ensure timely and accurate routing of the incident for effective and efficient resolution. |

1.3 INCIDENT INITIAL SUPPORT PROCEDURE NARRATIVE

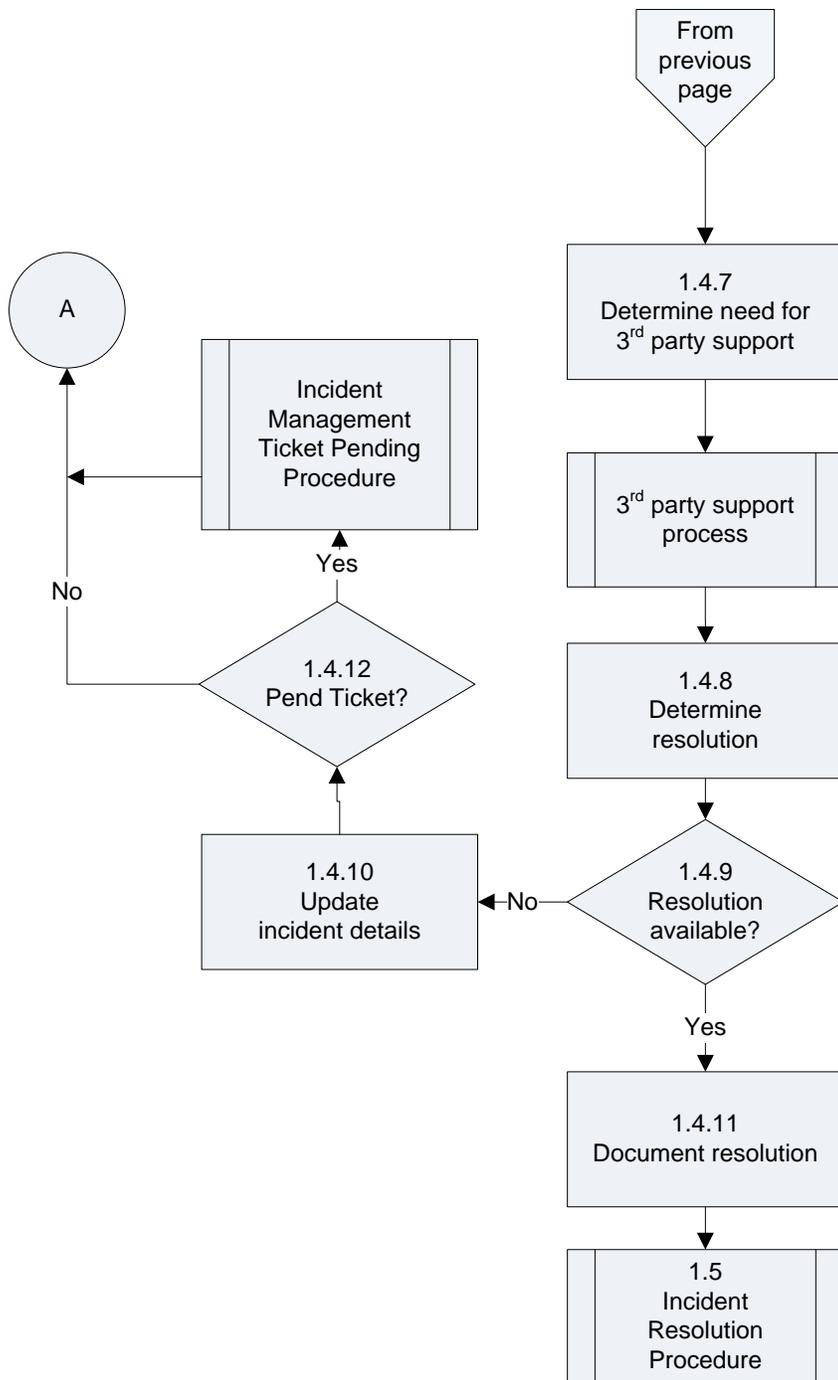
| Step | Responsible Role | Action |
|-------|--------------------------------------|--|
| 1.3.1 | Service Desk Analyst - Tier 1/Tier 2 | Determine if a quick resolution for the incident is available by using the Known Error Database (KEDB). |
| 1.3.2 | Service Desk Analyst - Tier 1/Tier 2 | <ul style="list-style-type: none"> • If a quick resolution is available, go to Incident Resolution Procedure. • If a quick resolution is not available, go to step 1.3.3. |
| 1.3.3 | Service Desk Analyst - Tier 1/Tier 2 | Determine the impact and urgency of the incident based on user urgency as defined by Service Level Management and the system will set the priority. <ul style="list-style-type: none"> - Reference the Impact and Urgency Matrix in Appendix 10 and 11 of this document |
| 1.3.4 | Service Desk Analyst - Tier 1/Tier 2 | <ul style="list-style-type: none"> • Inform the client of the incident priority. • Go to Incident Management Investigation and Diagnosis Procedure. |

1.4 INCIDENT INVESTIGATION & DIAGNOSIS PROCEDURE FLOW



© 2009 Plexent

1.4 INCIDENT INVESTIGATION & DIAGNOSIS PROCEDURE FLOW CONTINUED



© 2009 Plexent

1.4 INCIDENT INVESTIGATION & DIAGNOSIS PROCEDURE BUSINESS RULES

| | |
|-------------------------|---|
| Triggers | Incident Assignment |
| Inputs | <ul style="list-style-type: none"> • Incident Records • Known Error Database from Problem Management Solutions • On-Call List • Escalation Table • Escalation Procedures • Vendor Contact Information • Vendor Technical Publications and Articles • List of In-House Subject Matter Experts • Workarounds |
| Outputs | <ul style="list-style-type: none"> • Documented Resolution or Workaround • Updated Incident Record |
| General Comments | The purpose of this procedure is to ensure timely and accurate diagnosis of incidents for effective and efficient resolution of the incident. |

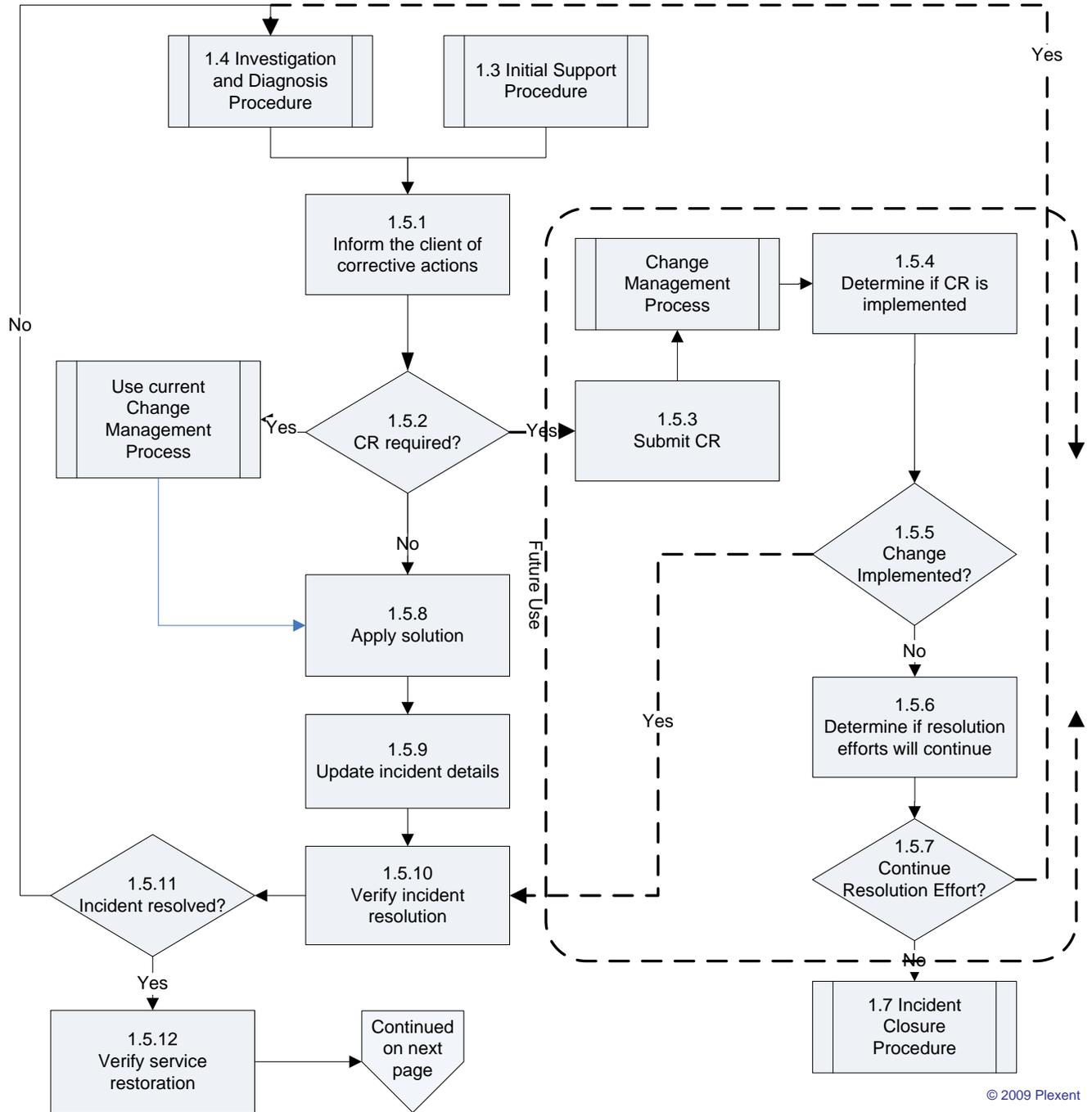
1.4 INCIDENT INVESTIGATION & DIAGNOSIS PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|-------|---|---|
| 1.4.1 | Tier 1 | <ul style="list-style-type: none"> • Assign the incident to the appropriate assignment group. • Assign the appropriate support group depending on which system is affected, the type of incident, and priority. An incident may be assigned to On-Call, Service Desk, or escalated as needed. • Reference the Impact & Urgency Matrix in Appendix 10 & 11 • Record assignments in the incident record. |
| 1.4.2 | Tier 2/Support Teams -Tier 3 | Review the incident to determine if it is assigned correctly. |
| 1.4.3 | Tier 2/Support Teams -Tier 3 | <ul style="list-style-type: none"> • If it is assigned correctly, go to step 1.4.4. • If it is assigned incorrectly, reassign the incident to the Service Desk for proper assignment and go back to step 1.4.1. |
| 1.4.4 | Service Desk Analyst - Tier 2/ Support Teams - Tier 3 | <ul style="list-style-type: none"> • Diagnose the incident using the initial data gathered. • Determine actions needed to recover service quality and to resolve the incident. This includes evaluating available workarounds, actions taken on similar or related incidents (using the known error database (KEDB)), and results of root cause analysis. • Determine if additional information is needed for work-around or resolution. |

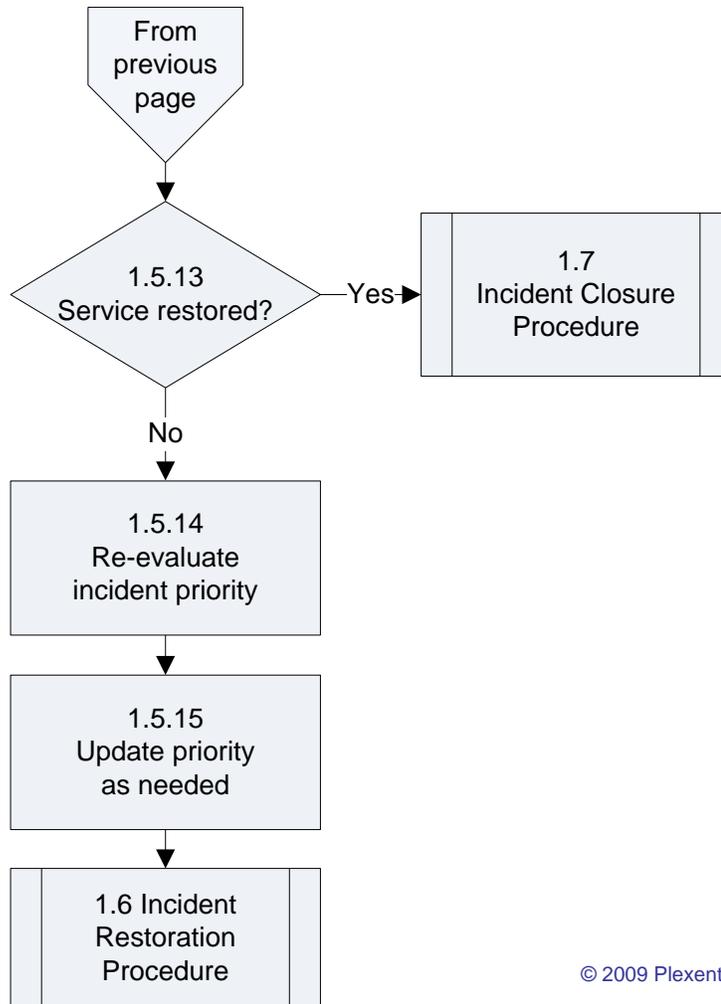
1.4 INCIDENT INVESTIGATION & DIAGNOSIS PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|--------|--|--|
| 1.4.5 | Service Desk Analyst - Tier 2/ Support Teams - Tier 3 | <ul style="list-style-type: none"> If additional information is needed, go to step 1.4.6. If no additional information is needed, go to step 1.4.7. |
| 1.4.6 | Service Desk Analyst - Tier 2/ Support Teams - Tier 3 | Consult clients, incident contact, and other experts to determine incident resolution. |
| 1.4.7 | Service Desk Analyst - Tier 2/ Support Teams - Tier 3 | <ul style="list-style-type: none"> If third party support (e.g., vendor) is needed, contact the appropriate party and negotiate arrangements for support. Contact the vendor using the process as defined in the underpinning contract. Document the information in the ticketing system. |
| 1.4.8 | Service Desk Analyst - Tier 2/ Support Teams - Tier 3 | Determine resolution actions based on the diagnosis. |
| 1.4.9 | Service Desk Analyst - Tier 2/ Support Teams - Tier 3 | <ul style="list-style-type: none"> If a resolution is unable to be determined, go to step 1.4.10. If a resolution is determined, go to step 1.4.11. |
| 1.4.10 | Service Desk Analyst - Tier 2/ Support Teams - Tier 3 | <ul style="list-style-type: none"> Update the incident ticket to reflect no resolution status. Go back to step 1.4.5. |
| 1.4.11 | Service Desk Analyst - Tier 2/ Support Teams - Tier 3 | Document the resolution in the incident ticket and go to Incident Resolution Procedure to implement the resolution. |
| 1.4.12 | Service Desk Analyst - Tier 2/ Support Teams - Tier 3 | <p>Determine if incident meets suspend criteria of Incident Management Suspend Incident Procedure.</p> <ul style="list-style-type: none"> If yes, go to Incident Management Suspend Incident Procedure. If no, go to 1.4.5. |

1.5 INCIDENT RESOLUTION PROCEDURE FLOW



1.5 INCIDENT RESOLUTION PROCEDURE FLOW CONTINUED



© 2009 Plexent

1.5 INCIDENT RESOLUTION PROCEDURE BUSINESS RULES

| | |
|-------------------------|--|
| Triggers | <ul style="list-style-type: none"> Working Solution or Workaround |
| Inputs | <ul style="list-style-type: none"> Solution Updated Incident Record Associated Problem Record |
| Outputs | <ul style="list-style-type: none"> User Communication Updated Incident Record CR Information/ CR to Change Management Applied Solution |
| General Comments | The purpose of this procedure is to ensure timely and verified resolution of incidents. |

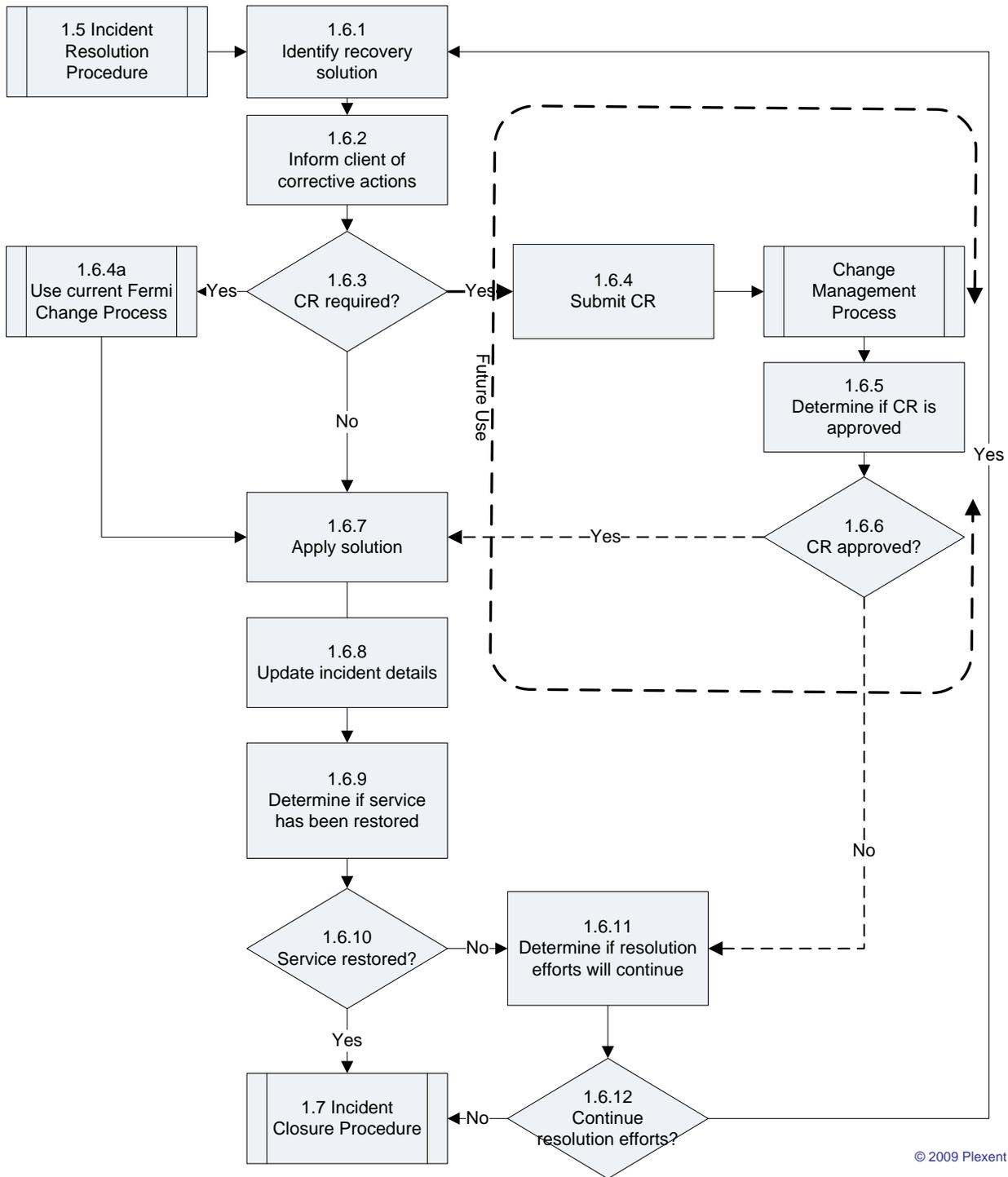
1.5 INCIDENT RESOLUTION PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|-------|--|--|
| 1.5.1 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Inform the client of corrective actions that will be applied to resolve the incident. |
| 1.5.2 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Determine if a change is required and use your current Change Process to perform the change. Determine if a request for Change Request (CR) is required for incident resolution as defined within the Computing Division Change Management process and procedures (future requirement) |
| 1.5.3 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Submit CR to Change Management Process. (future requirement) |
| 1.5.4 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Determine if CR is implemented (future requirement) |
| 1.5.5 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | <ul style="list-style-type: none"> If CR is implemented, go to step 1.5.8 (future requirement) If the CR is not implemented, go to step 1.5.10 (future requirement) |
| 1.5.6 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Determine if resolution efforts will continue. |

1.5 INCIDENT RESOLUTION PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|--------|---|---|
| 1.5.7 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | <ul style="list-style-type: none"> • If resolution efforts will continue, return to the Incident Investigation and Diagnosis Procedure. • If resolution efforts will not continue, go to the Incident Closure Procedure. |
| 1.5.8 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Apply solution to resolve the incident. |
| 1.5.9 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Update all incident details in the ticketing system. |
| 1.5.10 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Verify incident resolution. Use the 3 strikes and you're out methodology. (i.e. contact the user 3 different times to verify incident resolution, if no contact, then close the ticket with an email to the user stating that the ticket is closed and provide instructions on how to reopen the ticket.) |
| 1.5.11 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | <ul style="list-style-type: none"> • If the incident is resolved, go to step 1.5.12. • If the incident is not resolved, got to the Incident Investigation and Diagnosis Procedure. |
| 1.5.12 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Verify service restoration. |
| 1.5.13 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | <ul style="list-style-type: none"> • If service is restored, go to the Incident Closure Procedure. • If service has not been restored, go to step 1.5.14. |
| 1.5.14 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Re-evaluate incident priority. |
| 1.5.15 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | <ul style="list-style-type: none"> • Update priority as needed. • Go to Incident Restoration Procedure. |

1.6 INCIDENT RESTORATION PROCEDURE FLOW



1.6 INCIDENT RESTORATION PROCEDURE BUSINESS RULES

| | |
|-------------------------|---|
| Triggers | Resolved Incident with Applied Solution |
| Inputs | <ul style="list-style-type: none"> • Incident Records • Information about CR • Known Solution or Workaround • User Feedback • |
| Outputs | <ul style="list-style-type: none"> • Updated CR Information/CR to Change Management • User Communication • Applied Solution to Problem Management • Known Error to Problem Management • Updated Incident Record • Confirmation if Service is Restored |
| General Comments | The purpose of this procedure is to ensure timely and accurate restoration of service after incident resolution. |

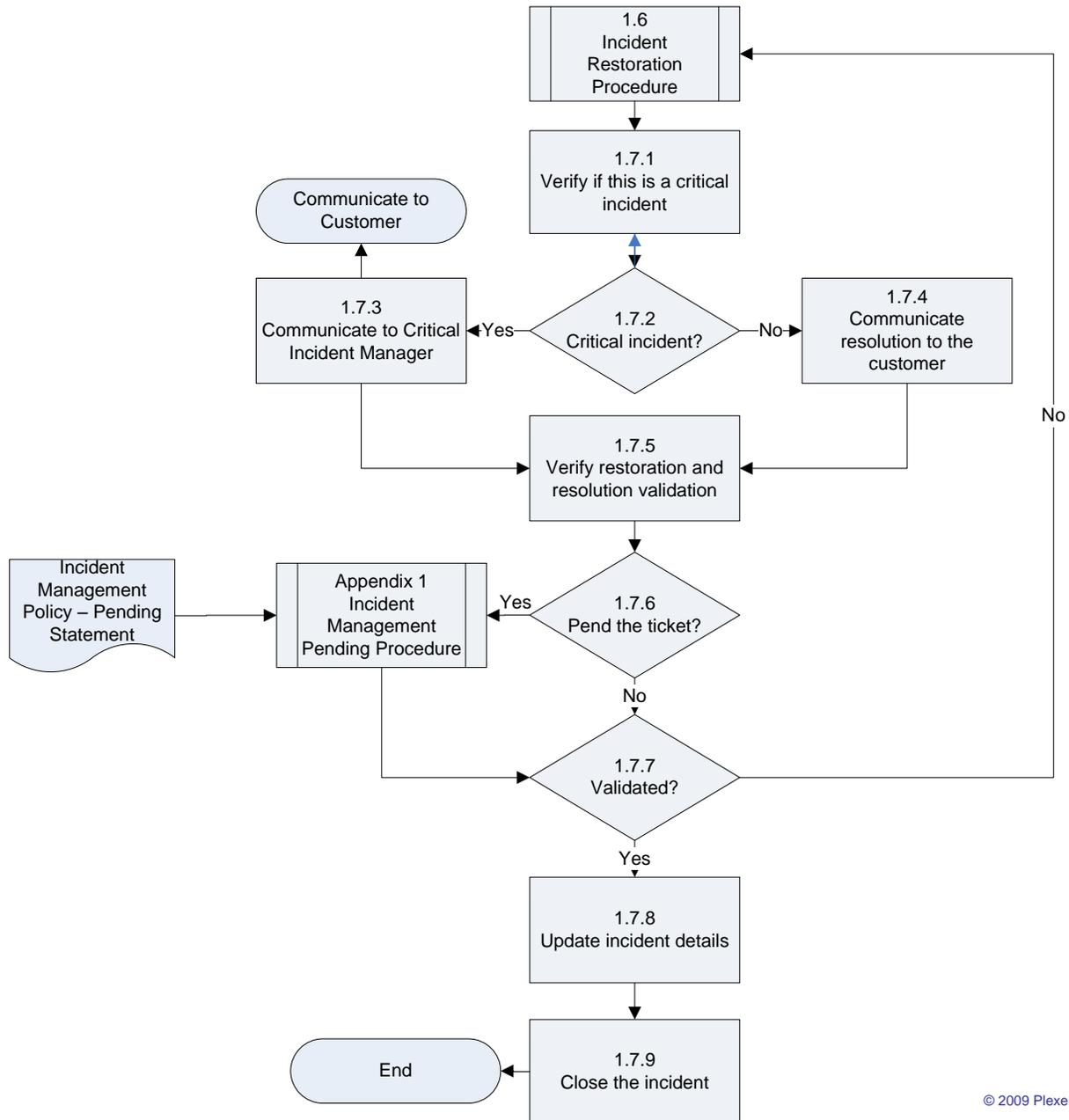
1.6 INCIDENT RESTORATION PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|--------|--|--|
| 1.6.1 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Identify the solution to restore service. |
| 1.6.2 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Inform the client of corrective actions to be taken to restore service. |
| 1.6.3 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Determine if CR is required: <ul style="list-style-type: none"> • If a CR is required, go to step 1.6.4. (1.6.4a) • If a CR is not required, go to step 1.6.7. |
| 1.6.4a | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Perform Change as required by Fermilab current change process |
| 1.6.4 | Service Desk Analyst - Tier 1/ | (Future Use) Submit a CR. Go to the Computing Division Change Management |

1.6 INCIDENT RESTORATION PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|--------|--|--|
| | Support Teams - Tier 2 | Process. |
| 1.6.5 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | (Future Use) Determine if the CR is approved. |
| 1.6.6 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | (Future Use) <ul style="list-style-type: none"> • If CR is approved, go to step 1.6.7. • If the CR is not approved, go to step 1.6.8. |
| 1.6.7 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Apply the solution to restore service. |
| 1.6.8 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Update all incident details in the ticketing system. |
| 1.6.9 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Determine if the service has been restored. |
| 1.6.10 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | <ul style="list-style-type: none"> • If service has been restored, go to the Computing Division Incident Management Incident Closure Procedure. • If service has not been restored, go to step 1.6.11. |
| 1.6.11 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Determine if resolution efforts will continue. |
| 1.6.12 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | <ul style="list-style-type: none"> • If resolution efforts will continue, return to step 1.6.1. • If resolution efforts will not continue, go to the <i>Computing Division Incident Management Incident Closure Procedure</i>. |

1.7 INCIDENT CLOSURE PROCEDURE FLOW



© 2009 Plexent

1.7 INCIDENT CLOSURE PROCEDURE BUSINESS RULES

| | |
|-------------------------|--|
| Triggers | <ul style="list-style-type: none"> • User Acceptance • Service Restored |
| Inputs | <ul style="list-style-type: none"> • Updated Incident Record • User Feedback • Known Error Database from Problem Management |
| Outputs | <ul style="list-style-type: none"> • Updated and Closed Incident Record • Updated Incident based on Known Error information |
| General Comments | The purpose of this procedure is to ensure incidents are closed properly and documentation is complete. |

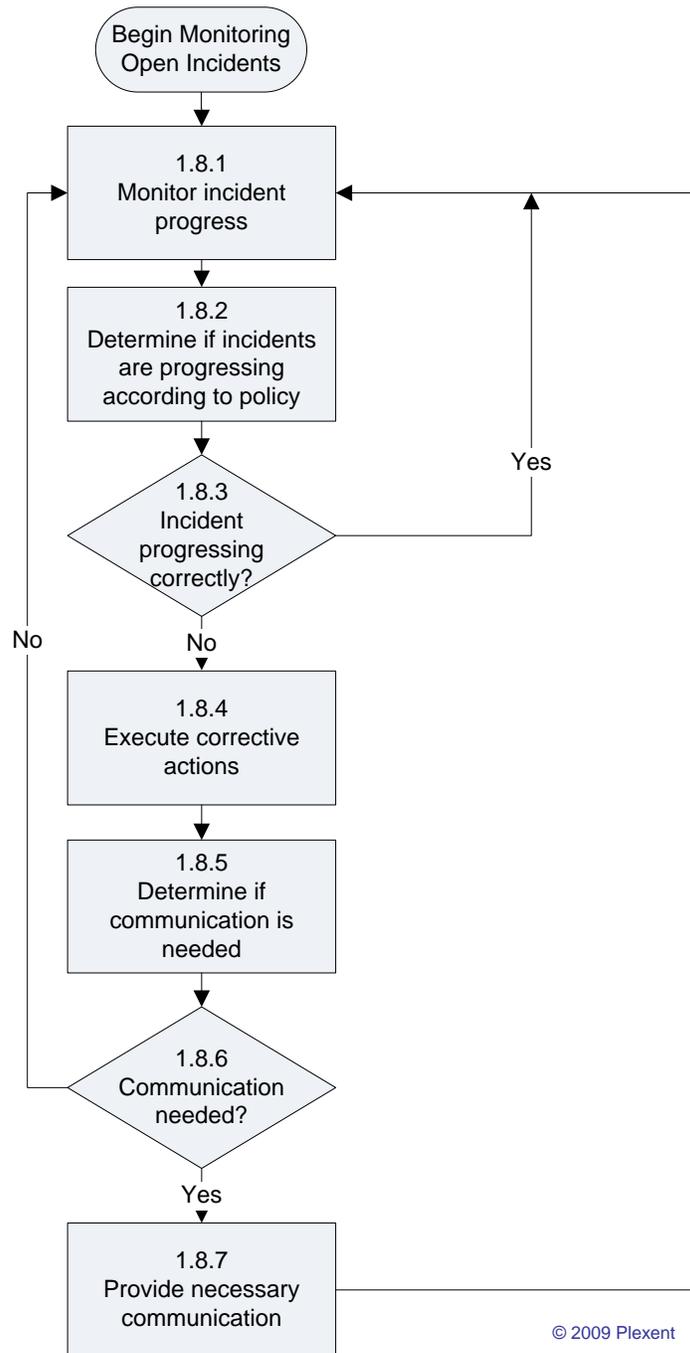
1.7 INCIDENT CLOSURE PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|-------|--|--|
| 1.7.1 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Determine if this is a critical incident. |
| 1.7.2 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | <ul style="list-style-type: none"> • If it is a critical incident, go to step 1.7.3. <p>NOTE: All critical incidents will be handled and managed by the assigned Critical Incident Manager that has the appropriate authority. The Critical Incident will be managed in accordance with the Incident Management Process.</p> <ul style="list-style-type: none"> • If it is not a critical incident, go to step 1.7.4. |
| 1.7.3 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Communicate to Critical Incident Manager, go to step 1.7.5. Critical Incident Manager will then communicate the results to the customer if required |
| 1.7.4 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | <ul style="list-style-type: none"> • Communicate resolution to the customer, go to step 1.7.5. • Communicate to the customer via Fermilab defined customer contact information • Bidirectional communication is not required. |
| 1.7.5 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Validate restoration and resolution of the incident with the customer. |

1.7 INCIDENT CLOSURE PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|-------|--|---|
| 1.7.6 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | If unable to verify a decision a decision to pend will be made based on the pending criteria as stated in the Incident Management policy – Pending Statement <ul style="list-style-type: none"> • If yes proceed to Incident Management Pending Procedure. • If no, procedure to step 1.7.7. |
| 1.7.7 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | <ul style="list-style-type: none"> • If they have been validated, go to step 1.7.8. • If they have not been validated, execute the <i>Computing Division Incident Management Incident Restoration Procedure</i>. |
| 1.7.8 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Update incident details. <ul style="list-style-type: none"> • Review the documented resolution for validity. • Search the incident database for additional incident reports and other pertinent information. • Update categorization and correct as necessary. • Ensure that the correct CI(s) are listed. • Analyze the information using the <i>Computing Division Incident Management Process</i> and <i>Computing Division Problem Management Process</i>. |
| 1.7.9 | Service Desk Analyst - Tier 1/ Support Teams - Tier 2 | Close the incident. |

1.8 INCIDENT OWNERSHIP, MONITORING, TRACKING & COMMUNICATION PROCEDURE FLOW



© 2009 Plexent

1.8 INCIDENT OWNERSHIP, MONITORING, TRACKING & COMMUNICATION PROCEDURE BUSINESS RULES

| | |
|-------------------------|---|
| Triggers | <ul style="list-style-type: none"> • Management Request for Reports • Service Thresholds Exceeded • Exceptions Occurring • Service Evaluation • After Action Reviews • Customer Request |
| Inputs | <ul style="list-style-type: none"> • Incident Record • User Feedback • Incident Management Policy section of the Computing Division ITIL Policy document • SLAs • Management Reports |
| Outputs | <ul style="list-style-type: none"> • User Communication • Management Reports • SLA deadline driven escalations and reassignments • SLA breach communications • Corrective Actions • Employee Communication |
| General Comments | <p>The purpose of this procedure is to ensure oversight of all incidents and comprehensive communication with all stakeholders to ensure control of the incident and satisfaction with its management. This procedure is carried out throughout the life of the incident and will vary based on the priority of the incident.</p> |

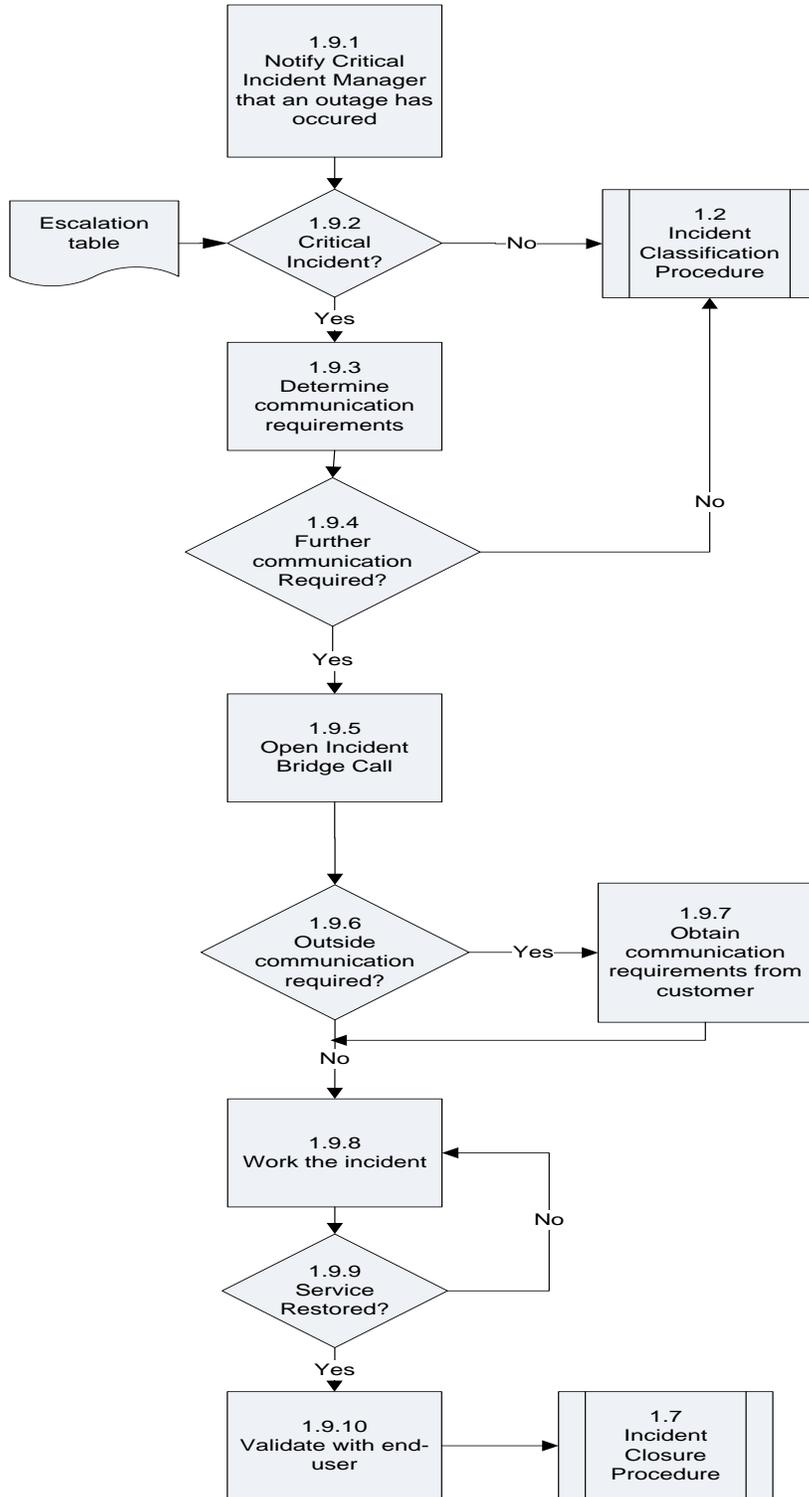
1.8 INCIDENT OWNERSHIP, MONITORING, TRACKING & COMMUNICATION PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|-------|------------------|---|
| 1.8.1 | Incident Manager | <ul style="list-style-type: none"> • Monitor the progress of open incidents. |
| 1.8.2 | Incident Manager | <p>Determine if incidents are progressing according to this document's process flows and are in adherence to the Fermilab Incident Management Policy.</p> <p>(future requirement)</p> <p>Determine if incidents are progressing according to Incident Management policies and procedures as defined in the</p> <ul style="list-style-type: none"> • Service Level Agreements |

1.8 INCIDENT OWNERSHIP, MONITORING, TRACKING & COMMUNICATION PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|-------|------------------|---|
| 1.8.3 | Incident Manager | <ul style="list-style-type: none">• If an incident is progressing per Incident Management criteria, continue monitoring• If not, go to step 1.8.4. |
| 1.8.4 | Incident Manager | Define and execute corrective actions as determined by the Incident Manager during the incident. |
| 1.8.5 | Incident Manager | Determine if communication is needed. |
| 1.8.6 | Incident Manager | <ul style="list-style-type: none">• If communication is needed, go to step 1.8.7.• If not, go to step 1.8.1. |
| 1.8.7 | Incident Manager | Provide necessary communication. Go to step 1.8.1. |

1.9 CRITICAL INCIDENT COMMUNICATION PROCEDURE FLOW



© 2009 Plexent

1.9 CRITICAL INCIDENT PROCEDURE BUSINESS RULES

| | |
|-------------------------|--|
| Triggers | <ul style="list-style-type: none"> • Critical Incident Occurs • Service Thresholds Exceeded |
| Inputs | <ul style="list-style-type: none"> • Incident Record • SLAs |
| Outputs | <ul style="list-style-type: none"> • Customer Communication • Technician Communication |
| General Comments | <p>The purpose of this procedure is to ensure oversight of all Critical Incidents and comprehensive communication with all support teams and customers to ensure control of the incident and satisfaction with its management. This procedure is carried out throughout the life of the Critical Incident and will vary based on the communication requirements of the customer.</p> |

1.9 CRITICAL INCIDENT PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|-------|--|---|
| 1.9.1 | Service Desk/Support Technician | <ul style="list-style-type: none"> • Notifies the Critical Incident Manager that a critical or major incident has occurred |
| 1.9.2 | Critical Incident Manager | <ul style="list-style-type: none"> • Determines the scope and impact of the event, validates that this meets the definition of a critical incident |
| 1.9.3 | Critical Incident Manager | <ul style="list-style-type: none"> • Contacts the respective department head to update on status and determine whether the incident requires further communication |
| 1.9.4 | Critical Incident Manager/Group Leader | <ul style="list-style-type: none"> • If further communication is required, the Critical Incident Manager will open a conference (Bridge) call with the different members of the team participating on the call. The call will stay open as long as required as determined by the Critical Incident Manager • If further communication is not required, then the support team can resume the standard IM process |
| 1.9.5 | Critical Incident Manager | <ul style="list-style-type: none"> • Open a communication bridge with the necessary support teams in order to coordinate the service restoration of the incident |
| 1.9.6 | Critical Incident Manager/Group | <ul style="list-style-type: none"> • Determine if communication is required to the customer of the service, if |

1.9 CRITICAL INCIDENT PROCEDURE NARRATIVE

| Step | Responsible Role | Action |
|--------|---------------------------|--|
| | Leader | so, then coordinate a separate means of communicating to the customer based on the customer requirements (i.e. email updates at regular intervals, a telephone call hourly, or a continuous open conference line for the customer) |
| 1.9.7 | Critical Incident Manager | <ul style="list-style-type: none">• Provide communication to the customer based on their requirements as defined in 1.9.6 |
| 1.9.8 | Support Team | <ul style="list-style-type: none">• Continue to work the incident to resolution |
| 1.9.9 | Critical Incident Manager | <ul style="list-style-type: none">• Determine if service is restored, if not, then continue working the incident |
| 1.9.10 | Service Desk | <ul style="list-style-type: none">• Validate that the user is able to function to an agreeable level of service proceed to the Incident Closure Procedure |

APPENDIX 1 – INCIDENT MANAGEMENT TICKET PENDING PROCEDURE

| Step | Responsible Role | Action |
|------|------------------|--|
| 1 | Support Team | Determine if the incident fits the pending policy statement |
| 2 | Support Team | If the requirements fit the pending policy statement, then place the ticket into "Pend" status |
| 3 | Support Team | Remove the pending status and place into In Progress status based on the Pending policy statement. |

APPENDIX 2 - RELATED DOCUMENTS

| Document Name | Relationship |
|--|------------------------|
| ITIL Glossary (CD DOCDB 3086) | Terms and Definitions |
| Fermilab Incident Management Policy (CD DOCDB 3067) | Policy |
| Fermilab Incident Management Business Process and Procedures (CD DOCDB 3064) | Process and procedures |
| | |
| | |
| | |

APPENDIX 3 – TOOLS

| Tool | Description | Reference |
|------------|---|----------------------------------|
| BMC Remedy | BMC Remedy Incident Management module is utilized to track and catalog all Incident Management activities. Remedy also enables the integration of Incident Management with related process areas. | All procedures utilize this tool |
| | | |

R - Responsible Role responsible for getting the work done
A - Accountable Only one role can be accountable for each activity
C - Consult The role who are consulted and whose opinions are sought
I - Inform The role who are kept up-to-date on progress

| | |
|--|--------------------------|
| | Primary Roles in Process |
| | Primary Interactions |
| | Secondary Roles |

| APPENDIX 4 – RACI MATRIX | | | | | | | | | | |
|--|------------------|-----------------------|-----------------------------------|------------------------|-----------------------|-----------------|----------------|---------------|-----------------------|---------------|
| Incident Management RACI Matrix | | | | | | | | | | |
| Process Activities | Incident Manager | Tier 1 (Service Desk) | Tier 2 (Operations Support Staff) | Tier 3 (Analyst /Tech) | Configuration Manager | Problem Manager | Change Manager | Process Owner | Service Level Manager | Stake holders |
| Incident Detection and Recording | | | | | | | | | | |
| Receive Incident Information | | R | | | | | | A | | |
| Open new Incident | | R | | | | | | A | | |
| Acquire Incident Information/Data | | R | | | | | | A | | |
| Incident Classification | | | | | | | | | | |
| Categorize | | R | | | | | | A | | |
| Search for Existing Incident | | R | | | | | | A | | |
| Associate Incident | | R | | | | | | A | | |
| Determine if Critical Issue | C | R | | | | C | | A | C | C |
| <i>Match Problems</i> | | R | | | | C | | A | | |
| <i>Link to Problem</i> | | R | | | | C | | A | | |
| <i>Assess Related IT Configuration Items</i> | | R | | | C | | | A | | |
| Initial Support | | | | | | | | | | |
| <i>Determine Quick Solution</i> | | R | | | | | | A | | |

R - Responsible Role responsible for getting the work done
A - Accountable Only one role can be accountable for each activity
C - Consult The role who are consulted and whose opinions are sought
I - Inform The role who are kept up-to-date on progress

 Primary Roles in Process
 Primary Interactions
 Secondary Roles

| APPENDIX 4 – RACI MATRIX | | | | | | | | | | |
|--|-------------------------|------------------------------|--|-------------------------------|------------------------------|------------------------|-----------------------|----------------------|------------------------------|----------------------|
| Incident Management RACI Matrix | | | | | | | | | | |
| Process Activities | Incident Manager | Tier 1 (Service Desk) | Tier 2 (Operations Support Staff) | Tier 3 (Analyst /Tech) | Configuration Manager | Problem Manager | Change Manager | Process Owner | Service Level Manager | Stake holders |
| Determine Priority | | R | | | | | | | I | |
| Inform Client / Incident Contact | | R | | | | | | A | | I |
| Investigation & Diagnosis | | | | | | | | | | |
| Assign Incident | | R | | | | | | A | | |
| Review Incident | | | R | R | | | | A | | |
| <i>Diagnose Incident</i> | | | <i>R</i> | <i>R</i> | | | | <i>A</i> | | |
| Consult Subject Matter Experts/Vendors | | | R | R | | | | A | | |
| Determine Need for 3 rd Party Support | | I | R | R | | C | | A | I | I |
| Determine Resolution | | | R | R | C | | | A | | |
| Update Incident Details | | I | R | R | | | | A | | |
| Document Resolution | | I | R | R | | | | A | | |
| Incident Resolution | | | | | | | | | | |
| Inform User | | R | | | | | | A | | |
| <i>Determine RFC</i> | | | <i>R</i> | <i>R</i> | | | | <i>A</i> | | |

R - Responsible Role responsible for getting the work done
A - Accountable Only one role can be accountable for each activity
C - Consult The role who are consulted and whose opinions are sought
I - Inform The role who are kept up-to-date on progress

| | |
|--|--------------------------|
| | Primary Roles in Process |
| | Primary Interactions |
| | Secondary Roles |

| APPENDIX 4 – RACI MATRIX | | | | | | | | | | |
|---|------------------|-----------------------|-----------------------------------|------------------------|-----------------------|-----------------|----------------|---------------|-----------------------|---------------|
| Incident Management RACI Matrix | | | | | | | | | | |
| Process Activities | Incident Manager | Tier 1 (Service Desk) | Tier 2 (Operations Support Staff) | Tier 3 (Analyst /Tech) | Configuration Manager | Problem Manager | Change Manager | Process Owner | Service Level Manager | Stake holders |
| Apply Solution | | R | R | R | I | | | A | I | |
| Update Incident Details | | R | R | R | | | | A | | |
| Verify Incident Resolution | | I | R | R | | | | A | C | C |
| Incident Restoration | | | R | R | | | | A | | |
| Identify Recovery Solution | | R | C | C | C,I | | | A | | |
| Inform Client of Corrective Actions | | R | | | | | | A | I | I |
| <i>Submit RFC</i> | | | R | R | | C | C | A | | |
| <i>Determine If RFC Approved</i> | | | R | R | | C | C | A | | |
| <i>Apply Solution</i> | | | R | R | | | | A | | |
| Update Incident Details | | I | R | R | | | | A | | |
| Determine if Service has been Restored | | | R | R | | | | A | I | |
| Determine if resolution efforts will continue | | | R | R | | | | A | I | |

R - Responsible Role responsible for getting the work done
A - Accountable Only one role can be accountable for each activity
C - Consult The role who are consulted and whose opinions are sought
I - Inform The role who are kept up-to-date on progress

 Primary Roles in Process
 Primary Interactions
 Secondary Roles

| APPENDIX 4 – RACI MATRIX | | | | | | | | | | |
|--|-------------------------|------------------------------|--|-------------------------------|------------------------------|------------------------|-----------------------|----------------------|------------------------------|----------------------|
| Incident Management RACI Matrix | | | | | | | | | | |
| Process Activities | Incident Manager | Tier 1 (Service Desk) | Tier 2 (Operations Support Staff) | Tier 3 (Analyst /Tech) | Configuration Manager | Problem Manager | Change Manager | Process Owner | Service Level Manager | Stake holders |
| Incident Closure | | | | | | | | | | |
| Determine if this is a Critical Incident | | | R | R | | | | A | | |
| Validate Resolution with Senior Management | | | R | R | | | | | C | C |
| Validate Resolution with Customer | | R | C | C | | | | A | C | C |
| Verify Restoration and Resolution Validation | | I | R | R | | | | A | C | C |
| Update Incident Details | | I | R | R | | | | A | | |
| Close Incident | | R | C | C | | | | A | I | |
| Ownership, Monitoring, Tracking & Communication | | | | | | | | | | |
| Monitor Progress | R | C | C | C | | | | A | C | |
| Determine if Incidents are Progressing According to Policy | R | C | C | C | | | | A | C | |

R - Responsible Role responsible for getting the work done
A - Accountable Only one role can be accountable for each activity
C - Consult The role who are consulted and whose opinions are sought
I - Inform The role who are kept up-to-date on progress

 Primary Roles in Process
 Primary Interactions
 Secondary Roles

| APPENDIX 4 – RACI MATRIX | | | | | | | | | | |
|--|-------------------------|------------------------------|--|-------------------------------|------------------------------|------------------------|-----------------------|----------------------|------------------------------|----------------------|
| Incident Management RACI Matrix | | | | | | | | | | |
| Process Activities | Incident Manager | Tier 1 (Service Desk) | Tier 2 (Operations Support Staff) | Tier 3 (Analyst /Tech) | Configuration Manager | Problem Manager | Change Manager | Process Owner | Service Level Manager | Stake holders |
| Execute Corrective Actions | R | C | C | C | | C | C | A | C | |
| Determine Required Communications | R | C | C | C | | | | A | C | I |
| Provide Necessary Communications | | | | | | | | A | I | I |

APPENDIX 5 – TOOLS

| Tool | Description | Reference |
|------------|---|----------------------------------|
| BMC Remedy | BMC Remedy Incident Management module is utilized to track and catalog all Incident Management activities. Remedy also enables the integration of Incident Management with related process areas. | All procedures utilize this tool |
| | | |

APPENDIX 6 – PROCESS SPECIFIC TECHNIQUES

| Technique | Description | Reference |
|-----------------------|--|---------------------------------------|
| Brainstorm sessions | Brainstorming is a group creativity technique designed to generate a large number of ideas for the resolution to an Incident. | Investigation and Diagnosis Procedure |
| Precision questioning | Use scripts, customer centric trainings and precision questioning training to ensure that initial categorization and diagnostics are rapid and accurate. | Investigation and Diagnosis Procedure |

APPENDIX 7 - REPOSITORIES

| Repository | Description | Reference |
|-------------|---|---|
| Remedy v7.0 | Remedy v7.0 is the main support and Incident Management tool used by Fermi National Laboratories in the support of all of the Departments and research projects | Place specific references from the work instructions here |
| DOCDB | DOCDB is the document repository used by the Computing Division | ITIL Processes and Functions |
| Sharepoint | Sharepoint maintains the ISO20000 Project | http://sharepoint/iso20k/default.aspx |
| | | |

APPENDIX 8 – COMMUNICATION PLAN

The ITIL Implementation will bring into alignment all Service Management offerings provided by Computing Division. In order for the process and procedures to be executed effectively and efficiently, the following communication plan will identify all ad-hoc and on-going communication required.

Key messages:

- Through *Incident Management* Incidents are resolved faster and with reduced accelerator operations impact
- By documenting and eliminating Errors, *Problem Management* improves IT service quality and management
- *Problem Management* also enhances everyone's knowledge of the environment with trend analysis reports that help prevent new Incidents
- Through *Availability Management* the customer's IT business requirements are assessed, planned for and met
- *Capacity Management* ensures that upgrades to IT performance and capacity address current and forecast business needs across the enterprise
- Overall, ITIL-based IT Service Management will lead to:
 - Sustained availability of the Computing Division and Scientific and Research services
 - Measurably improved quality of Computing Division services over time

Approach: This plan details tasks that apply generally to all ITIL processes as well as specifically to the Incident Management Process. The plan assumes that there will be a combination of face-to-face training/meeting events and broadcast communications designed to both increase awareness of the processes among stakeholders and to ensure high performance of the new processes among key service delivery staff.

Goals of the Communication Plan:

Encourage participation of the target audiences:

- Service Delivery Staff
- Transformation Teams
- Application Support Staff

Coordinate communication that facilitates:

- Effective use of all related ITIL tools
- Good management decisions, plans & activities

Timely infrastructure changes that minimally impact end-users

| | Activity | Timing | Responsible Party | Target Audience | Purpose |
|---|---|------------------------|---------------------------|--|--|
| 1 | Operations Meeting | Weekly | Incident Manager | Computing Division | Review prior day's incidents; determine accuracy of ticket categorization and priority levels. Discuss resolution for all critical incidents |
| 2 | Critical Incident Bridge Call | Ad Hoc | Critical Incident Manager | Support teams managing the Critical Incident | Keeps the team focused on the critical incident, ensures that everyone on the bridge call is up to date and aware of the situation. Call lasts until the Critical Incident is resolved |
| 3 | Customer Critical Incident Bridge Call | Ad hoc | Service Manager | Department Heads outside of Computing Division directly impacted by a Critical Outage affecting their department | Provide status updates to impacted Departments. |
| 4 | | | | | |
| 5 | | | | | |
| 6 | | | | | |
| 7 | | | | | |
| 8 | | | | | |
| 9 | | | | | |
| | | | | | |

Each type of communication has a specific focus; however, a common approach can be taken to define and formulate the specific communication activities. The steps listed below formulate the approach to be taken to compose those activities:

| Activities |
|---|
| <p>Step 1 – Formulation</p> <ul style="list-style-type: none">• Formulate goals and objectives of communication• Formulate core message• Identify all parties involved• Integrate with existing communications forums |
| <p>Step 2 – Analysis</p> <ul style="list-style-type: none">• Determine available and acceptable communication media• Determine communication culture and define acceptable approach• Determine existing knowledge of subject in the environment |
| <p>Step 3 – Identification</p> <ul style="list-style-type: none">• Determine key interest groups related to the subject of the campaign• Determine communication objectives per interest group• Determine the key messages from each interest group's perspective |
| <p>Step 4 – Definition</p> <ul style="list-style-type: none">• Select the most appropriate media for communication from:<ul style="list-style-type: none">○ Direct Media – such as workshops, Focus Group discussions, or individual presentations○ Indirect Media – such as the Intranet, lectures or newsletters |
| <p>Step 5 – Planning</p> <ul style="list-style-type: none">• Define a plan that links important points in the subject of the communication (e.g. milestones in a project) to communication activities, and media• Determine the communication audience and resources• Determine the review criteria for successful communication• Obtain formal management support for the plan |
| <p>Step 6 – Implementation</p> <ul style="list-style-type: none">• Perform communication activities as per plan• Manage the plan and safeguard it• Ensure production and distribution of materials is effective and as per plan• Continually gauge reaction to the approach and messages |
| <p>Step 7 – Evaluation</p> <ul style="list-style-type: none">• Monitor reactions to the communication approach throughout the delivery of the plan and adjust the plan if necessary• Determine during the effects of the campaign using the review criteria established in step 5 |

The following types of communication are available:

| Communication Type | Examples of usage |
|----------------------|---|
| Escalations | To initiate (or trigger) actions To gain required resources (people, information, budget etc.) |
| Notifications | To communicate operational process information To promote team awareness |
| Controlled Documents | To communicate process descriptions/instructions To communicate reports |

Each of the above types of communication can be delivered via one or more of the following mediums:

| Communication Medium | Examples of Usage | Communication Type |
|-------------------------|--|---------------------------------------|
| Email | <ul style="list-style-type: none"> • Individual email messages • Group email messages | Notification Escalations Reports |
| Verbal | <ul style="list-style-type: none"> • Formal and informal meetings • Presentations • Telephone calls | Notifications Escalations |
| Documentation | <ul style="list-style-type: none"> • Updated process documents • Issued Project documentation • Implementation and back-out plans | Controlled Documents |
| Reports | <ul style="list-style-type: none"> • Test results • Development progress | Controlled Documents Notifications |
| Service Management tool | <ul style="list-style-type: none"> • Escalation • Status changes | Automated Notification |

APPENDIX 10 - IMPACT MATRIX

| APPENDIX 10 - IMPACT MATRIX | | |
|------------------------------------|------------|--|
| Impact 1 (Extensive/Widespread) | Definition | Major Business Impact: Outage with no workaround resulting in complete loss of core business systems to customer. |
| | Example | <ul style="list-style-type: none"> • Operating system unavailable. • Production system component failure resulting in loss of system availability. • Telephone switch unavailable. • Inter- and intra-site communication links not functioning. • Critical applications and databases (i.e., Lawson, SAP, CATIA) not functioning. • Critical network component (core router or switch supporting enterprise services) not functioning. • E-PoP connectivity and/or component failure resulting in a loss of access to Internet (i.e., firewall, Internet connection, proxy, etc). |
| Impact 2 (Significant/Large) | Definition | Significant Business Impact: Outage with no workaround resulting in significant loss or degraded system services to customer; however, operations can continue in a restricted mode. |
| | Example | <ul style="list-style-type: none"> • Production system components unavailable impacting batch and online schedules • Failure or system degradation in any of the following areas: cluster controller, hub, router, servers, data switch, server application, data-link failure with an alternate route, video services, voice mail system • Significantly degraded response from critical applications and databases. |
| Impact 3 (Moderate/Limited) | Definition | Batch/on-line/hardware problems resulting in minimal impact to system and system availability. |
| | Example | <ul style="list-style-type: none"> • Batch job/on-line transaction not requiring immediate contact |
| Impact 4 (Minor/Localized) | Definition | Single points of failure resulting in impact to: <ul style="list-style-type: none"> • Single customers • Single devices • Non-critical peripherals. |
| | Example | <ul style="list-style-type: none"> • Personal computer (PC), workstation, and terminal • Printer, plotter, scanner • Telephone • End-user software (e.g., LAN access, password resets, etc.) • Network services warnings. |

APPENDIX 11 – URGENCY MATRIX

| | | |
|-------------------------|------------|--|
| Urgency 1 (Critical) | Definition | Restoration is critical and time is of the essence. (Note: Detail definition updated when Service Level Management is implemented) |
| | Example | <ul style="list-style-type: none"> • User(s) are completely unable to perform their job functions • Experiments are off-line and the lab is unable to function |
| Urgency 2 (High) | Definition | Restoration requirement is high and time is of the essence. (Note: Detail definition updated when Service Level Management is implemented) |
| | Example | <ul style="list-style-type: none"> • User(s) can function in a limited capacity or a work-around is available. |
| Urgency 3 (Medium) | Definition | Restoration requirement is medium but time is less critical. (Note: Detail definition updated when Service Level Management is implemented) |
| | Example | <ul style="list-style-type: none"> • User(s) can function and perform their duties but in a degraded state. • User(s) may request that the full restoration take place at a later time. • System may require a Change that can wait until non-production time. |
| Urgency 4 (Low) | Definition | Restoration requirement is low or not required. (Note: Detail definition updated when Service Level Management is implemented) |
| | Example | <ul style="list-style-type: none"> • How to questions • Single customers and job functionality is not impacted • Requests • Personal computer (PC), workstation, and terminal • Printer, plotter, scanner • Telephone • End-user software (e.g., LAN access, password resets, etc.) • Network services warnings. |

| INCIDENT MANAGEMENT ESCALATION TABLE | | | | | | | | | | |
|--|-------------|-----------------|-------------|---------------|------------|---|----------------------------|-------------------------------------|--------------------------|--|
| F U N C T I O N A L E S C A L A T I O N ← | Tier | Priority | | | | Hierarchical Escalation | | | | |
| | | Critical | High | Medium | Low | Help Desk | Incident Management | Critical Incident Management | Senior Management | |
| | 1 | 10 Mins. | 30 Mins. | 2 Hrs. | 12 Hrs. | <i>Reviews Incident Summary and Action Plans, evaluates and responds to requested actions by email to Incident Owner; Initiates new actions to Incident Owner and/or escalates as needed; Incident Owner updates Incident Record; Escalates to tier 2 based upon automated triggers via the Incident Management tool; Incident owner updates Incident Summary, link to Incident Record and details actions for each appropriate tier 2 stakeholder.</i> | | | | |
| | 2 | 1 Hr. | 2 Hrs. | 12 Hrs. | 24 Hrs. | <i>Reviews Incident Summary and Action Plans; evaluates and responds to requested actions by email to Incident Owner; Initiates new actions to Incident Owner; Incident Owner updates Incident Record; Escalates to tier 3 based upon automated triggers via the Incident Management tool.</i> | | | | |
| | 3 | 2 Hrs. | As Needed | As Needed | As Needed | <i>Reviews Incident Summary and Action Plans; evaluates and responds to requested actions by email to Incident Owner; Incident Owner updates Incident Record.</i> | | | | |