APPENDIX A

INCIDENT MANAGEMENT PROCESS

Process Document

Incident Management

Published:	7/10/2013
Document Location:	P:\penndot shared\ITSM\ProcessDocuments\Incident_Management.pdf
Summary:	This document outlines the incident management process, procedures and work instructions

Table of Contents

1. Mission

The mission of the Incident Management process is to restore normal service operation as quickly as possible, in a prioritized fashion 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.

1.1 Objectives

Provide a consistent process to track incidents that ensures:
- Incidents are properly logged
- Incidents are properly routed
- Incident status is accurately reported
- Queue of unresolved incidents is visible and reported
- Incidents are properly prioritized and handled in the appropriate sequence
- Resolution provided meets the requirements of the SLA for the customer

2. Scope

Incident management includes any event which disrupts, or which could disrupt, a service. This includes events which are communicated directly by customers, either through the service desk or through an interface from event management to incident management tools.

Although both incidents and service requests are reported to the service desk, this does not mean that they are the same. Service requests do not represent a disruption to agreed service, but are a way of meeting the customer's needs and may be addressing an agreed target in an SLA. Service requests are dealt with by the request fulfillment process

The scope of the Incident Management process is limited to the incident types listed in the table below.

Incident Type	Description
User Service Restoration	Any unplanned interruption to an IT service or a reduction in the quality of an IT service. Failure of a component of an IT service that has not yet impacted the service itself is also an incident.
	Note: In addition to being reported by the customer or end-user, incidents can also be logged by technical staff (if, for example, they notice something alarming with a hardware or network component, they may report an incident).
User Service Request	Request from a customer for creating, modifying, adding, moving, or removing some or all service functionality, access, or infrastructure components. This incident type is also used for requests for information or simple questions.
	Note: Examples of User Service Requests include: a request to change/reset a password; a request to

Incident Type	Description
	install additional software onto a particular workstation; a request to relocate some items of desktop equipment; request for copying data; request to run an ad-hoc batch job and; a request for "how to" information.
Infrastructure Restoration	Use this incident type if the incident request is more focused on the restoration of infrastructure service. Typically, these types of incident requests are reported by system management tools (for example, if an incident is detected on a piece of network infrastructure by system monitoring software).
Infrastructure Event	Use this incident type when a system management tool registers an event that does not require infrastructure restoration.

Incident Management interfaces with the following ITSM modules:
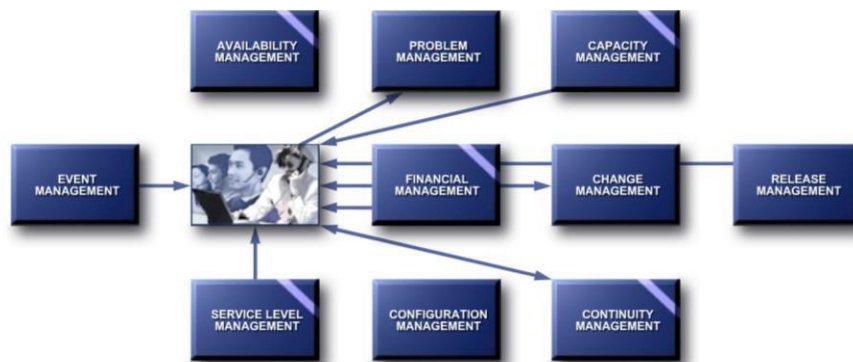
3. KPIs

The table below lists the critical success factors and associated key performance indicators (KPIs) that have been selected for tracking the success of the Incident Management process.

Critical Success Factors	Key Performance Indicators
Resolve incidents as quickly as possible minimizing impacts to the business.	• Mean time to resolution, broken down by incident type and priority • Number and percentage of incidents resolved by Service Desk via first call resolution • Number and percentage of open incidents, broken down by each status (e.g. ASSIGNED, IN PROGRESS, PENDING, RESOLVED, etc.)

Increase visibility and communication of incidents to business and IT support staff.	• Number and percentage of incidents not updated in the past 5 days • Number and percentage of incidents in PENDING status, broken down by timeframe (10, 30, 60, 90, over 90 days) • Top ten (10) operation and product categories utilized
Maintain quality IT services.	• Total numbers of incidents, broken down by incident type • Number and percentage of incidents with an Outage/Degradation operational categorization • Number and percentage of service restoration incidents, broken down by priority

4. Owner

The owner of the Incident Management process is the Service Management CAB

The Service Delivery Manager chairs the Service Management CAB and the CAB is responsible for reviewing, and subsequently approving or rejecting, requests for improvement of the Incident Management process and its supporting functionality in the service management application.

The Service Management CAB is comprised of a representative from each of the following areas:

• Technical management
• Application management
• IT Service Desk
• IT Service Management (ITSM) tool administrator

5. Roles

The table below lists the different roles that are involved in the Incident Management process, along with their respective responsibilities.

Role	Responsibility
Customer	• Requests support when necessary and provide the required information to help resolve the requests. The requests are submitted by contacting the service desk. • Validates the incident is resolved to his/her satisfaction.
Support Group Lead	• Distributes incident requests that have been assigned to his/her group among the group's support technicians and change coordinators, taking into account the skills, availability and access rights of the individual support technicians and the services for which the change coordinators are responsible. • Ensures that incident requests, which are assigned to his/her group, are resolved within the completion targets

Role	Responsibility
	dictated by the SLAs. This is done by ensuring that SLA escalations are followed up in an effective and timely fashion.
	• Escalates service outages to the service owner of the affected service when they have not been resolved within the available resolution time dictated by the related SLA.
	• Reviews and accepts or rejects solutions that have been proposed for general use after having received a solution approval notification.
	• Oversee support group membership.
Incident Owner	• The Incident Owner is the Support Group ultimately accountable for ensuring that an assigned Incident is satisfactorily completed through its lifecycle and that any service requirements are met. The Incident Owner is responsible for confirming customer satisfaction for assigned incidents and closing the incident. The Incident Owner is independent of the assigned Support Group for an incident request. Typically, the IT Service Desk will serve as the Incident Owner.
Service Desk Analyst (SDA)	• SDAs communicate between the customer and ISTO support service staff. This ensures that all incidents are recorded, prioritized, resolved, documented, and communicated in an efficient and controlled manner within the agreed OLAs and SLAs.
	• Identify what services customers require.
	• Efficiently obtaining accurate and complete information from the customer when creating the incident.
	• Ensuring incidents are assigned to the most appropriate support group for resolution with the most efficient means possible.
	• Escalating incidents either hierarchically (i.e., assigning incidents to another Tier or management for input) or functional (i.e., assigning incidents to a different support group within a Tier) in compliance with the escalation process.
	• Validating incident resolutions with customers.
	• Ensuring the overall completeness and accuracy of incidents prior to closing.
Service Owner	• Decides whether an escalated incident needs to be resolved by implementing an emergency change, by recovering the affected service at its continuity site, or by continuing the resolution of the incident within the Incident Management process.
Support Technician	• Updates and resolves incidents with relevant information and status changes through the ITSM system.
	• Communicating with SDAs regarding incidents as necessary.

| Role	Responsibility
	• Recording all details of how an incident is resolved in the work details tab. • Resolving incidents within the most efficient means possible. • Escalating incidents in compliance with the escalation process. • Receiving notifications of incidents assigned to the support group and escalations.

6. Description

The Incident Management Process consists of seven procedures for handling requests from customers.

1. **Incident Request Registration** – This procedure is used by service desk analysts when they register incident requests for customers.

2. **Incident Request Assignment** – It is used by service desk analysts and support group leads to assign incident requests to the appropriate support technicians or change coordinators for resolution or implementation.

3. **Incident Request Tracking** – It is used by support group leads when they are dealing with reassignment notifications or SLA escalations.

4. **Incident Request Resolution** – It is used by support technicians when resolving incident requests that have been assigned to them.

5. **Incident Escalation** – After an incident has been escalated, the service owner of the affected service uses this procedure to determine how the incident can be resolved in the most efficient manner.

6. **Incident Request Closure** – This procedure is used by an incident owner when an incident request is marked resolved and by requesters when they review incident requests that have been completed for them.

7. **Solution Approval** – This procedure is used by support group leads when their approval has been requested for a solution that has been proposed for general use.

Additional details about these procedures and graphical representation of the process is provided in the Process Flow section.

7. Process Flow

The following sections describe the process and procedure flows for Incident Management.

Incident Management Process
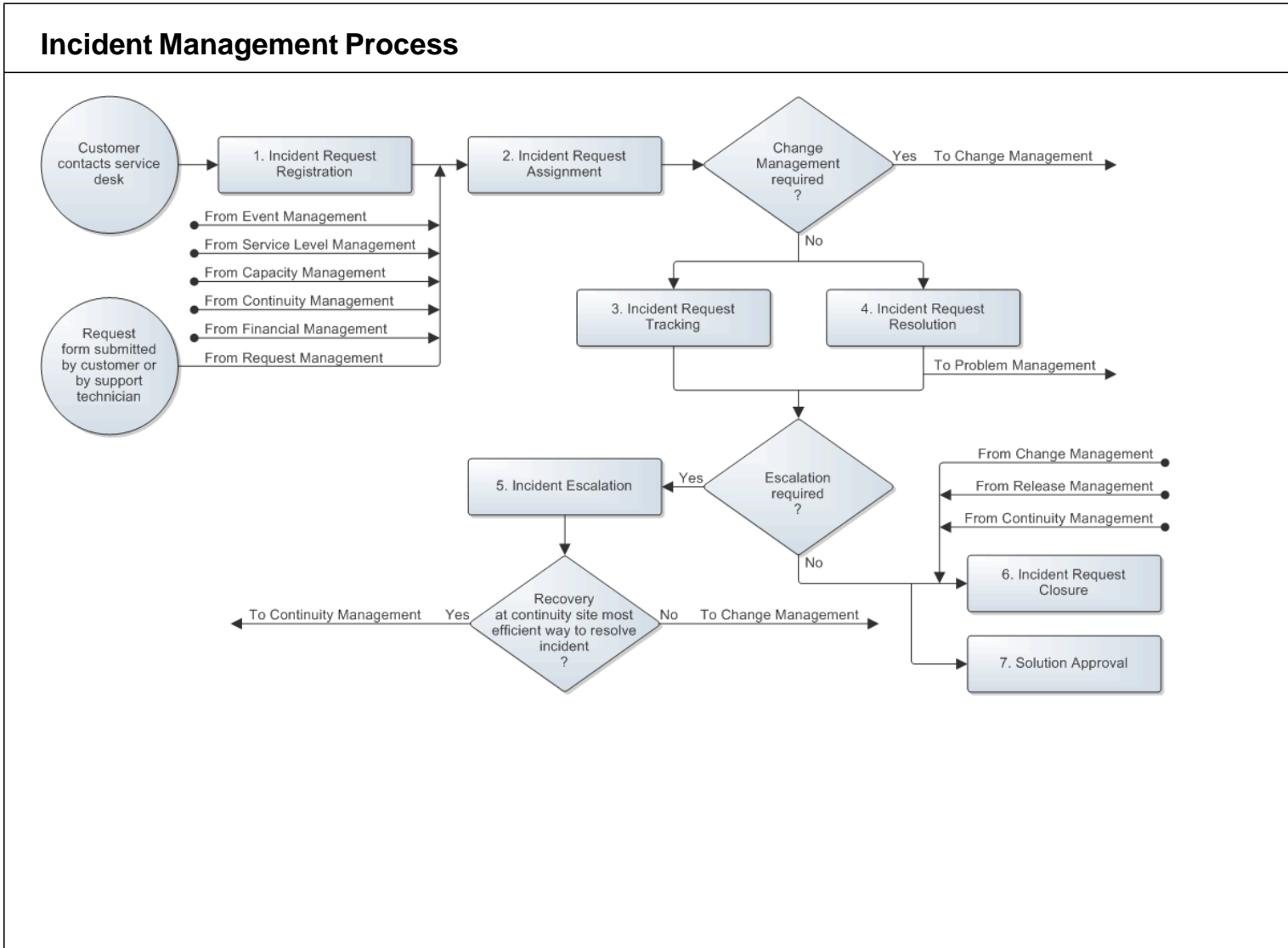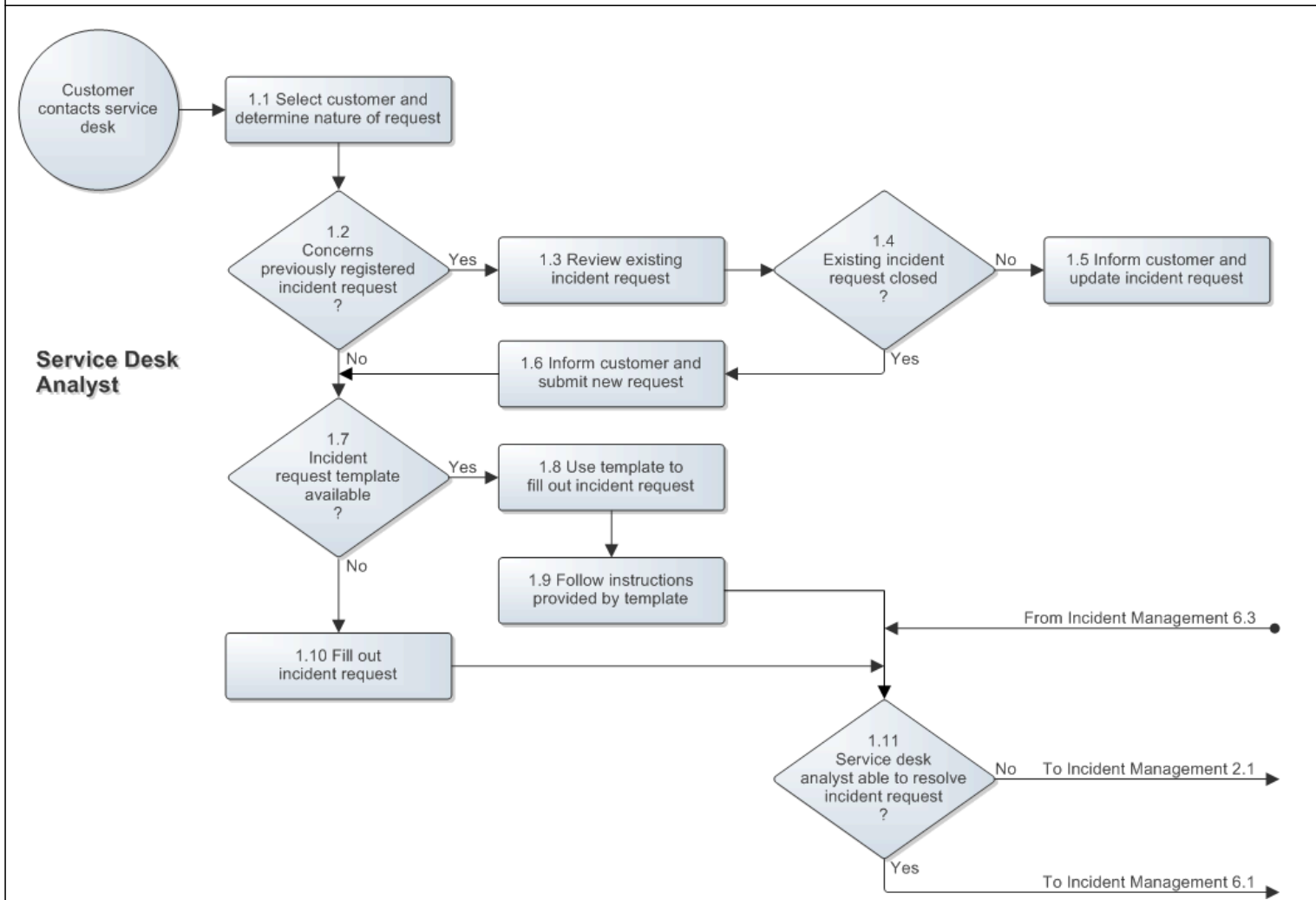
7.1   Incident Request Registration

When a customer contacts the service desk, the service desk analyst finds out how the customer can be assisted.

If the customer contacted the service desk about a previously registered incident request (regardless of whether it is already resolved or not), the service desk analyst looks up this incident request and takes the necessary actions (e.g. provides the customer with a status update).

If the customer contacted the service desk to submit a new request, the service desk analyst registers the request as a new incident request. If the service desk analyst is able to resolve the request (in terms of skills, access rights, and time considerations), he/she goes to Procedure 6, Incident Request Closure. However, if the service desk analyst is not able to resolve the incident request, he/she continues in Procedure 2, Incident Request Assignment.

The *Incident Request Registration* procedure is presented on the next page.

pennsylvania
DEPARTMENT OF TRANSPORTATION

Procedure 1, Incident Request Registration

Customer contacts service desk

Service Desk Analyst

1.1 Select customer and determine nature of request

1.2 Concerns previously registered incident request ?

Yes — 1.3 Review existing incident request

1.4 Existing incident request closed ?

No — 1.5 Inform customer and update incident request

1.6 Inform customer and submit new request

Yes

No

1.7 Incident request template available ?

Yes — 1.8 Use template to fill out incident request

1.9 Follow instructions provided by template

From Incident Management 6.3

No

1.10 Fill out incident request

1.11 Service desk analyst able to resolve incident request ?

No — To Incident Management 2.1

Yes — To Incident Management 6.1

Procedure 1 Steps	Work Instructions

1.1 Select customer and determine nature of request Service Desk Analyst	1.1.1 Open a new incident request and select the customer in the Customer×+ field.
	1.1.2 If you have the customer on the telephone, or if the customer visited the service desk in person, ask the customer how you may be of assistance.
	1.1.3 Use the information that the customer has provided you with (regardless of whether this information was obtained over the telephone, in an email, or otherwise) to determine if the customer has contacted the service desk about a previously registered incident request, or if the customer wants to submit a new incident request.
	1.1.4 If the customer is submitting a new request, continue by determining the nature of the customer's request, and ask for any additional information that could help resolve the request.
1.2 Concerns previously registered incident request ?	1.2.1 If the customer contacted the service desk about a previously registered incident request, regardless of whether it has already been closed or not, continue with 1.3.1. Otherwise, if the customer contacted the service desk to submit a new request, go to 1.7.1.
1.3 Review existing incident request Service Desk Analyst	1.3.1 Open the incident request that the customer has contacted the service desk about.
	Note: Use the Customer's Incidents quick action to look up the open incident requests for the customer.
	1.3.2 Review the incident request's information and its status. Pay specific attention to its progress, which is documented in the Work Info History table.
1.4 Existing incident request closed ?	1.4.1 Go to 1.6.1 if the status of the incident request is "Closed". Otherwise, if the customer contacted the service desk to provide additional information about the incident request he/she submitted earlier, or to ask for an update on its status, continue with 1.5.1.
	1.5.1 If the customer has provided additional information that is relevant to the resolution of the incident request, add this

| 1.5 Inform customer and update incident request

Service Desk Analyst	information to the Work Info History table of the incident request. Use this new work info entry to attach any related files to the incident request. Contact the specialist to whom the incident request is assigned and inform this person of the information that you have added to the incident request.
	1.5.2 Provide the customer with an update on the status of the incident request.
	Note: If it concerns an incident request that has not been updated recently, contact the specialist to whom it is assigned to obtain a status update. Pass this information on to the customer.
	1.5.3 Add a work info entry to the Work Info History table and use it to provide a summary of your actions and the information that you provided to the customer.
1.6 Inform customer and submit new request

Service Desk Analyst | 1.6.1   Inform the customer that the incident request is "Closed" and, if requested, provide Work Info History details. |
| | 1.6.2   Continue to 1.7 if the customer is experiencing continued or similar symptoms or wishes to submit a new incident request. |
| 1.7 Incident request template available ? | 1.7.1   Continue with 1.8.1 if an incident request template is available for the type of request that the customer has contacted the service desk about. Otherwise go to 1.10.1. |
| 1.8 Use template to fill out incident request

Service Desk Analyst | 1.8.1   Select the appropriate incident request template in the Template+ field. The service management application will use the template's information to populate the fields of the new incident request. |
| | 1.8.2   Select the customer for whom the incident request has been submitted in the Customer✗+ field and adjust the text in the Summary✗ field as needed. |
| | 1.8.3   Manually complete the registration of the incident request by following the field utilization guidelines for the Incident Request form. |
| 1.9 Follow instructions provided by template

Service Desk Analyst | 1.9.1   Read the instructions that were copied from the incident request template into the Notes field of the new incident request to determine which information needs to be collected from the customer and how the incident request will need to be resolved. |

	1.9.2	Collect the required information from the customer and add this to the incident request as per the instructions in the Notes field.	

1.10 Fill out incident request Service Desk Analyst	1.10.1	Fill out the new incident request by following the field utilization guidelines for the Incident Request form.
	Note:	If you need more information to be able to provide sufficient detail in the incident request so that it can be resolved, and if you are not currently in contact with the customer (e.g. if the customer contacted the service desk by email), contact the customer by telephone or email and request the additional information that is needed. Register the new incident request and assign to self while this information is being obtained.
	1.10.2	Any information that could facilitate the resolution of the incident request should be entered in the Notes field and a short but meaningful description of the incident request should be entered in the Summary× field.
	1.10.3	Ensure that the appropriate options are selected in the Impact×, Urgency×, Incident Type× and Reported Source fields.
	1.10.4	Ensure that the appropriate Operational and Product Categorizations are selected. To help select the appropriate Product Categorization, use the search function 🔍.
	Note:	If the correct categorization data is not available, categorize the incident with best possible data and continue processing the customer's incident request. After completing the customer's request, open a new incident, using the template requesting the correct categorization data be added to the ITSM tool.
	1.10.5	Use the Incident Matching quick action to determine if the incident request concerns the same issue as another, previously registered incident request that has not yet been resolved. If you see such an identical incident request, select the relationship type "Duplicate of" on the Incident Matching screen to relate the incident request that you are working on (the duplicate) to this identical incident request that was registered earlier (the original). After this, the Status× field of the duplicate incident request will automatically be set to "Pending" and its Status Reason field will be set to the special field option "Pending Original". No further action needs to be taken on the duplicate incident request, as it will automatically be updated by the original to which you related it.
	1.10.6	If you set the Incident Type× field to "User Service Restoration", check the service management application to see which changes, implemented during the past 24 hours, could have caused the incident. If you find a

	change that appears to have caused the incident, link it to the incident request on the Relationships tab. Enter the unique change ID in the Notes field and specify why you suspect the incident to have been caused by the implementation of this change.
1.11 Service desk analyst able to resolve incident request ?	**1.11.1** If the incident request can be resolved by the service desk analyst (with the assistance of other service desk analysts if necessary), go to 6.1.1. Otherwise continue with 2.1.1. **Note:** Click on the Incident Matching quick action and review the solution database entries to see whether any solutions are already available for the incident request's classification. Also review the problem investigations that the Incident Matching quick action found in the database. The workaround information, which can be found in the Workaround field of these problem investigations, may be used to resolve the support request if it concerns an incident that was caused by a previously identified problem. The workaround information could allow you to resolve the incident request without the help of a specialist. **Note:** The service desk may not be able to resolve incident requests due to access restrictions, time limitations, and/or insufficient knowledge. If a solution or workaround was found, but it is not possible for the service desk to implement it, specify where the solution or workaround instructions can be found in the Notes field of the incident request.

7.2   Incident Request Assignment

Having filled out a new incident request or having received a service request, the service desk analyst saves it to ensure that the service management application applies the automatic routing rules to automatically assign it to the most appropriate support group.

The support group lead, or delegate of the group to which the incident request has been assigned then reviews it. He/she sends it back to the service desk if information is missing but required for an efficient resolution, and/or if it was assigned to the wrong group. This will help the service desk analysts to understand what information needs to be collected from customers for such incident requests and to which group manually assigned incident requests are to be assigned.
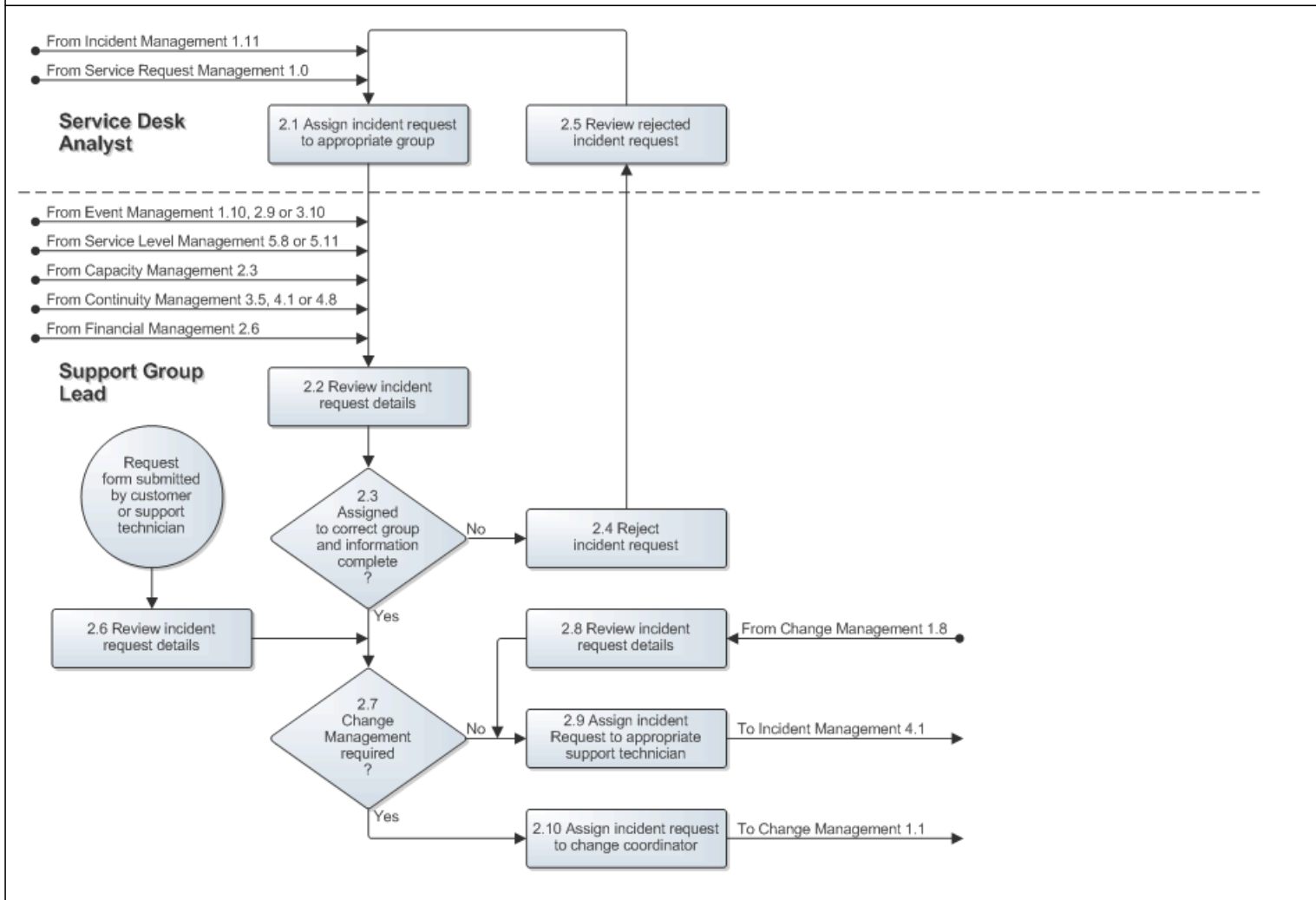
If the incident request contains the necessary information and has been assigned to the correct group, the support group lead, or delegate determines whether or not it needs to be resolved through the Change Management process. An incident request may not be resolved without Change Management when its resolution will cause:

- a service to become unavailable or degraded during service hours,
- the functionality of a service to become different, or
- the CMDB to require an update.

The support group lead assigns incident requests that require Change Management to the change coordinator of the concerned service. On the other hand, if an incident request does not require Change Management the support group lead assigns it to the most appropriate support technician within his/her group based on skills, availability and access rights.

The *Incident Request Assignment* procedure is presented on the next page.

Procedure 2, Incident Request Assignment

From Incident Management 1.11

From Service Request Management 1.0

Service Desk Analyst

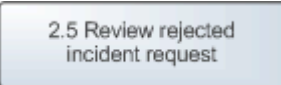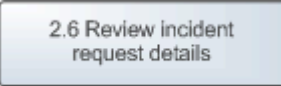2.1 Assign incident request to appropriate group

2.5 Review rejected incident request

From Event Management 1.10, 2.9 or 3.10

From Service Level Management 5.8 or 5.11

From Capacity Management 2.3

From Continuity Management 3.5, 4.1 or 4.8

From Financial Management 2.6

Support Group Lead

2.2 Review incident request details

Request form submitted by customer or support technician

2.3 Assigned to correct group and information complete ?

No → 2.4 Reject incident request

Yes

2.6 Review incident request details

2.8 Review incident request details ← From Change Management 1.8

2.7 Change Management required ?

No → 2.9 Assign incident Request to appropriate support technician → To Incident Management 4.1

Yes → 2.10 Assign incident request to change coordinator → To Change Management 1.1

Procedure 2 Steps	Work Instructions

2.1 Assign incident request to appropriate group

Service Desk Analyst

2.1.1 If you are completing the registration of a new incident request, leave its Assigned Group×+ field empty to ensure that the service management application applies the automatic routing rules to set the group assignment when the incident request is saved.

If you are dealing with an incident request that was rejected by a support group lead, select the appropriate assignment group manually.

Note: Always leave the Assignee+ field of the incident request empty. It is up to the group to decide who will work on which assignments.

2.1.2 Ensure that the Status× field of the incident request is set to "Assigned".

2.1.3 If it concerns an incident that must be dealt with as soon as possible (e.g. in case of a virus attack), telephone or page the support group lead of the group to which the incident request has been assigned to ensure that he/she is aware of the urgency. Do the same when it is currently after the group's normal office hours and it is important that a support technician already starts to work on the incident request.

2.2 Review incident request details

Support Group Lead

2.2.1 Examine the information in the incident request.

2.2.2 Determine if the incident request has been assigned to the appropriate support group.

2.2.3 Determine if the incident request contains all information that should have been provided in order to be able to resolve it.

2.2.4 Check the open incident requests that have already been assigned to a support technician within your group to ensure that the incident request is not a duplicate. If it is, go to its Relationships tab and link it to the identical incident request that is already assigned to a specialist (the original) using the relationship type "Duplicate of".
After this, the Status× field of the duplicate incident request will automatically be set to "Pending" and its Status Reason field will be set to the special field option "Pending Original". No further action needs to be taken on the duplicate incident request, as it will automatically be updated by the original to which you related it.

2.3.1 Continue with 2.4.1 if the incident request was not assigned to the appropriate support group or if it does not contain all information that should have been provided in order to be able to resolve it. Otherwise go to 2.7.1.

2.3 Assigned to correct group and information complete ?	
2.4 Reject incident request Support Group Lead	2.4.1 Select the service desk in the Assigned Group✗+ field of the incident request. Add a work info entry to the Work Info History table and use it to specify why you are rejecting the incident request. Also ensure that the Status✗ field of the incident request is set to "Assigned".
	Note: The service desk will subsequently ensure that the missing information is collected and/or that the incident request is assigned to the correct support group.
2.5 Review rejected incident request Service Desk Analyst	2.5.1 Determine why the incident request has been rejected by reviewing the information in its Work Info History table. If information is missing, collect this from the customer (or another source) and add a work info entry with this information to the Work Info History table of the incident request.
2.6 Review incident request details Support Group Lead	2.6.1 Examine the information in the incident request that was registered after a customer or support technician filled out and submitted the Request form.
	2.6.2 Ensure that the information in the incident request is complete and that it is correctly filled out by following the field utilization guidelines for the Incident Request form.
2.7 Change Management required ?	2.7.1 Go to 2.10.1 if it concerns an incident request that will need to be handled by Change Management. Otherwise continue with 2.9.1.
	Note: An incident request must be coordinated by Change Management if its implementation will cause:
	• a service to become unavailable or degraded during service hours,
	• the functionality of a service to become different, or
	• the CMDB to require an update.
	Note: If it concerns an incident request with its Incident Type✗ field set to "User Service Restoration" or "Infrastructure Restoration", a support technician will first need to determine in 4.2.1 how it is to be resolved in order to establish whether or not Change Management will be required to resolve it. So, in case of an incident, go to

	2.9.1.

	2.8.1	Examine the information in the incident request to gain an understanding of what has been requested and why the change coordinator of the related service has determined that the incident request can be completed within the Incident Management process.

2.8 Review incident request details

Support Group Lead

	2.9.1	Select the most appropriate support technician (in terms of skills, availability and access rights) in the Assignee+ field of the incident request.

2.9 Assign incident request to appropriate specialist

Support Group Lead

	2.9.2	Ensure that the Statusx field of the incident request is set to "Assigned".
	2.9.3	If it concerns an incident that must be dealt with as soon as possible (e.g. in case of a virus attack), telephone or page the support technician to whom the incident request has been assigned. Do the same if it is important that the support technician starts to work on the incident request even though the support technician is currently not expected to be checking for new assignments (e.g. because it is after office hours).

2.10 Assign incident request to change coordinator

Support Group Lead

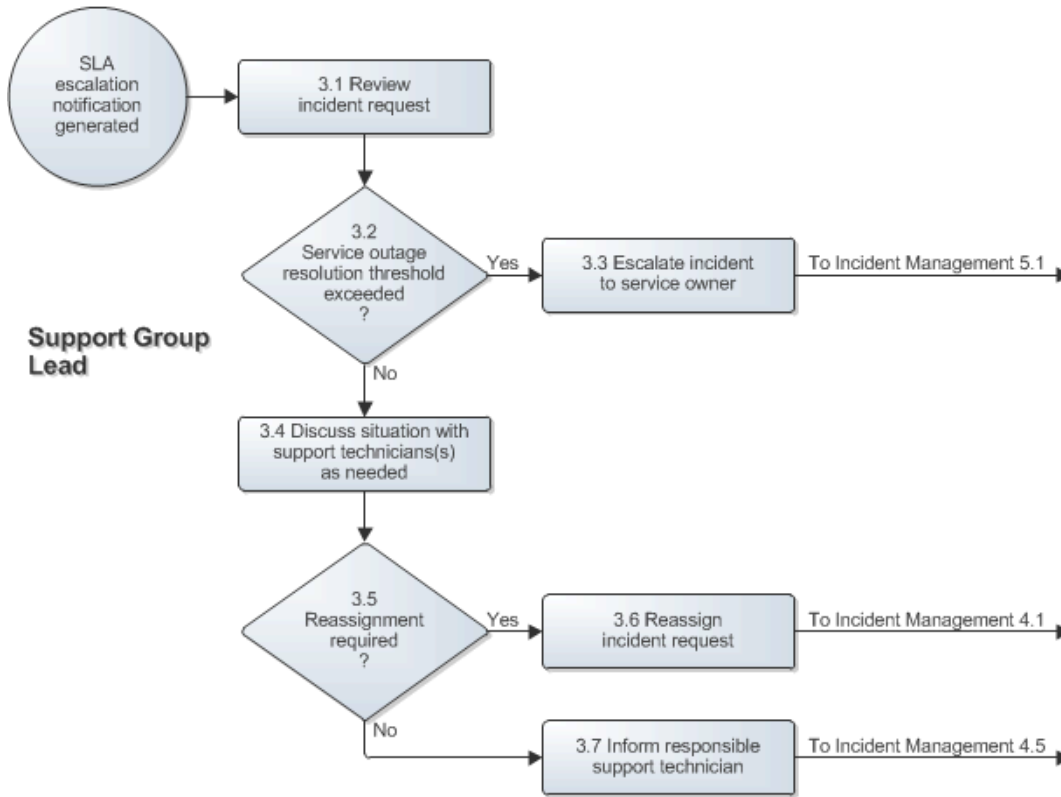|	2.10.1	Determine for which service the change has been requested.
	2.10.2	Select the change coordinator of this service in the Assignee+ field of the incident request.
	2.10.3	Ensure that the Statusx field of the incident request is set to "Assigned".

7.3 Incident Request Tracking

After an SLA has escalated an incident request, the support group lead reviews the notification that has been sent to him/her for this. If the incident request concerns a service outage which resolution threshold (as dictated by the SLA that generated the notification) has been exceeded, the support group lead contacts the service owner of the affected service and escalates the incident request to him/her.
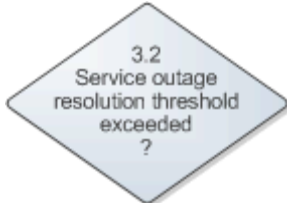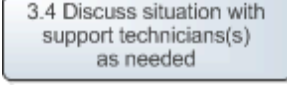
If the notification was not sent because the resolution threshold of a service outage has been exceeded, the support group lead determines who had best continue to work on the resolution of the incident request. He/she obtains the advice from support technicians within the group as needed to determine whether the incident request should be reassigned to another support technician, or should be resolved by the support technician to whom the incident request is currently assigned.

If the incident request should be reassigned, the support group lead does this by assigning it to a support technician who is in a better position (in terms of skills, availability and/or access rights) to resolve it. If the support group lead has decided not to reassign the incident request, he/she informs the support technician to whom the incident request is currently assigned, that the incident request needs to be resolved quickly to avoid or minimize SLT violations.

The *Incident Request Tracking* procedure is presented on the next page.

Procedure 3, Incident Request Tracking

Procedure 3 Steps	Work Instructions
3.1 Review incident request Support Group Lead	**3.1.1** After having received a notification informing you that an incident request has been escalated to you by one of the service level agreements registered in the service management application, review the incident request.
3.2 Service outage resolution threshold exceeded ?	**3.2.1** If a service level agreement that is registered in the service management application generated the notification for you because a service outage has not been resolved within the available resolution time, continue with 3.3.1. Otherwise go to 3.4.1.
3.3 Escalate incident to service owner Support Group Lead	**3.3.1** Contact the service owner of the affected service and inform him/her of the situation. Explain that the service is still unavailable, even though the available resolution time for the incident has already been exceeded. Be specific about the fact that the incident has now been escalated to him/her and that it needs to be handled in accordance with Procedure 5, Incident Escalation Handling. **3.3.2** Add a work info entry to the Work Info History table of the incident request. Use it to specify that you have escalated the incident to the service owner because the service is still unavailable, even though the available resolution time for the incident has already been exceeded.
3.4 Discuss situation with support technicians(s) as needed Support Group Lead	**3.4.1** If further clarification is required, contact the support technician who has been working on the resolution of the incident request and discuss the situation with him/her. Also consult with other support technicians as needed. **3.4.2** Determine whether or not it would be better to reassign the incident request if another support technician is in a better position (in terms of skills, availability and/or access rights) to resolve it.
3.5 Reassignment required ?	**3.5.1** Continue with 3.6.1 if the incident request had better be reassigned to another support technician. Otherwise, if the incident request should be resolved by the support technician to whom it is currently assigned, go to 3.7.1.

3.6 Reassign incident request Support Group Lead	3.6.1	Select the support technician to whom the incident request should be reassigned in the Assignee+ field.
	Note:	The support technician to whom the incident request is now assigned is automatically notified of the assignment.
	3.6.2	Inform the support technician to whom the incident request was assigned before to inform him/her that the incident request has been reassigned.
3.7 Inform responsible support technician Support Group Lead	3.7.1	Contact the support technician to whom the incident request is currently assigned. Inform this person that you received an SLA escalation and that it is very important that the incident request is resolved quickly to avoid or minimize SLT violations.

7.4   Incident Request Resolution

After an incident request has been passed to a specific support technician, the support technician reviews its information and determines how it should be resolved.

The support technician escalates the incident request to the service owner of the affected service when it concerns an incident that cannot be resolved without Change Management because its resolution will cause:

- a service to become unavailable or degraded during service hours,
- the functionality of a service to become different, or
- the CMDB to require an update.

If the support technician has decided that the incident request should not be escalated, he/she resolves it. Having resolved the incident request, he/she updates its information in the service management application to ensure that the requester is notified.

If the support technician believes that the solution information he/she entered in the incident request could help requesters, service desk analysts and/or support technicians to resolve future cases that are similar, he/she proposes it for general use. Finally, if the incident request was resolved using a workaround, and the support technician believes that the incident for which the workaround was provided is likely to recur, he/she informs the problem coordinator of the affected service to ensure that action is taken to prevent future occurrences.

The *Incident Request Resolution by Support technician* procedure is presented on the next page.

Procedure 4, Incident Request Resolution

From Incident Management 2.9, 3.6 or 6.8

Support Technician

4.1 Review and update incident request

4.2 Determine how to resolve incident request

4.3 Change Management required to resolve incident ?

Yes → 4.4 Escalate incident to service owner

To Incident Management 5.1

No

From Incident Management 5.5

From Incident Management 3.7

4.5 Resolve incident request → 4.6 Complete incident request

To Incident Management 6.6

To Incident Management 7.1

To Problem Management 1.1

pennsylvania
DEPARTMENT OF TRANSPORTATION

Procedure 4 Steps	**Work Instructions**
4.1 Review and update incident request Support Technician	4.1.1 Set the Status✗ field to "In Progress" as soon as you are ready to work on the incident request. 4.1.2 Examine the information in the incident request to find out what is requested. Note: As the support technician gains additional insight or makes progress in resolving the incident request, the support technician must add a work info entries to the Work Info History table of the incident request to document the steps taken. 4.1.3 If the incident request concerns the same issue as an incident request that you received earlier, go to the Relationships tab. Link the duplicate incident request to the one that you received earlier (the original) using the relationship type "Duplicate of". After this, the Status✗ field of the duplicate incident request will automatically be set to "Pending" and its Status Reason field will be set to the special field option "Pending Original". No further action needs to be taken on the duplicate incident request, as it will automatically be updated by the original to which you related it.
4.2 Determine how to resolve incident request Support Technician	4.2.1 Determine how best to resolve the incident request. Note: Click on the Incident Matching quick action and review the solution database entries to see whether any solutions are already available for the incident request's classification. Also review the problem investigations that the Incident Matching quick action found in the database. The workaround information, which can be found in the Workaround field of these problem investigations, may be used to resolve the support request if it concerns an incident that was caused by a previously identified problem. 4.2.2 If you determined that another support technician within your support group had better resolve the incident request, add a work info entry to the Work Info History table and use it to specify the reason. Subsequently, select the identified support technician within your support group (or you may enter your support group lead) in the Assignee+ field, and set the Status✗ field back to "Assigned". 4.2.3 If you have determined that the incident request needs to be resolved by another group, add a work info entry to the Work Info History table and use it to specify the reason and desired support group. Route the incident request back to the service desk for re-assignment. Select "IT Service Desk" in the Assigned Group✗+ field, and set the Status✗ field back to "Assigned". Do not select a specific service desk analysis in the Assignee+ field of the incident

request.

4.3
Change Management required to resolve incident ?

4.3.1 Continue with 4.4.1 if you have determined that the incident request concerns an incident which resolution may only be implemented through the Change Management process. Otherwise go to 4.5.1.

Note: The resolution of the incident must be coordinated by Change Management if its implementation will cause:

- a service to become unavailable or degraded during service hours,

- the functionality of a service to become different, or

- the CMDB to require an update.

4.4 Escalate incident to service owner

Support Technician

4.4.1 Contact the service owner of the affected service and inform him/her of the situation. Be specific about the fact that the incident has now been escalated to him/her and that it needs to be handled in accordance with Procedure 5, Incident Escalation.

4.4.2 Add a work info entry to the Work Info History table of the incident request. Use it to specify that you have escalated the incident to the service owner because the solution you propose for the incident may only be implemented through the Change Management process.

4.5 Resolve incident request

Support Technician

4.5.1 Resolve the incident request. If necessary, request support from other support technicians, external suppliers/vendors, or even the customer.

Note: Set the Status× field to "Pending" and select the most applicable option in the Status Reason field if the work cannot continue for a while (e.g. because you are waiting for a spare part or for information from a supplier). Add a work info entry to the Work Info History table of the incident request. Use it to specify what you are waiting for and enter an estimated time at which you expect the incident request to be resolved. If you have submitted a request with a supplier, add a work info entry containing both the vendor name and vendor ticket number, if available, to the Work Info History table.

Note: If you have completed your work on the incident request, but further action is still required to get it resolved, add a work info entry to the Work Info History table. Use it to specify what you have done, the reason for reassignment and the desired support group or support technician. If the additional work needs to be done by a specific member within your group, select this person in the Assignee+ field. On the other hand, if the additional work needs to be done by another group, Route the incident request back to the service desk for re-assignment. Select "IT Service Desk" in

			the Assigned Group×+ field, and set the Status× field back to "Assigned". Do not select a specific service desk analysis in the Assignee+ field of the incident request.
4.6 Complete incident request Support Technician	4.6.1	If you found the solution for the incident request using the Incident Matching quick action, select this solution and click on the Relate With Solution button. This causes the solution information to be entered in the Resolution field of the incident request. Edit this text as needed to provide an accurate account of how the incident request was resolved. If you did not use a proposed solution to resolve the incident request, use the Resolution field to provide a concise, step-by-step account of how the incident request was resolved. Also fill out or edit the text in the Resolution field as needed to provide detailed solution instructions (e.g. if the customer needs to adjust a setting), to provide the answer to a request for information, or to describe why the incident request cannot be resolved if it is not possible to provide a solution or a workaround.	
	4.6.2	If you have manually entered the solution information, and if you believe that the solution information could help customers, service desk analysts and/or specialists to resolve future incident requests that are similar, propose your solution for general use. Do this by clicking on the Relationships tab, selecting the "Solution Database" option in the Request Type field and clicking on the Create button. Ensure that the Status field of the solution is set to "Inactive" and that its View Access× field is set to "Internal".	
	4.6.3	Select the appropriate CI in the CI+ field of the incident request if this has not been done yet, or if the wrong CI was selected before.	
	4.6.4	Set the Status× field of the incident request to "Resolved" and select the most appropriate option in the Status Reason field.	
	4.6.5	Perform a final review of the incident request to ensure that its information is accurate and complete.	
	4.6.6	If you have resolved the incident request by providing a workaround, and you believe that incidents similar to this one are likely to occur if the root cause is not removed quickly, contact the problem coordinator of the affected service. Give him/her the incident ID so that he/she can easily find the incident request in the service management application.	

7.5   Incident Escalation

After a support group lead or support technician has escalated an incident to the owner of the affected service, the service owner talks to the support technician(s) who have been dealing with the incident to get an understanding of the current situation and to determine how the incident had best be resolved. If the recovery of the affected service at its continuity site is the most efficient and reliable way to resolve the incident, the service owner escalates the incident and alerts the necessary support group lead(s) to get the service recovery started.

In most cases, however, the recovery of a service at its continuity site is either not going to fix the incident (e.g. when the incident is caused by a bug), or the implementation of a fix within the service's current infrastructure is going to be more efficient and reliable. In such cases, the service owner continues by determining whether the resolution of the incident needs to be coordinated by Change Management. Change Management is required when the resolution of the incident will cause:

- a service to become unavailable or degraded during service hours,
- the functionality of a service to become different, or
- the CMDB to require an update.

If Change Management is not required, the service owner ensures that the most appropriate support technician(s) continue to resolve the incident within the Incident Management process.

On the other hand, if Change Management is required, the service owner consults with the support technician(s) to gain an understanding of the risks that could cause the implementation of the change to fail and the impact of the implementation on customers. Together, they figure out the best way to keep the risk and impact of the change implementation at an acceptable level. After they have established how the change should be implemented, the service owner asks the support technician(s) to perform the implementation as an emergency change.

Note that the role of service owner is performed by the on-duty manager when the service owner of the affected service is not available.

The *Incident Escalation Handling* procedure is presented on the next page.

Procedure 5, Incident Escalation

From Incident Management 3.3 or 4.4

From Change Management 8.3

Service Owner

5.1 Determine best way to resolve incident

5.2 Recovery at continuity site most efficient way to resolve incident ?

Yes → 5.3 Escalate incident → To Continuity Management 2.1

No

5.4 Change Management required to resolve incident ?

Yes → 5.6 Analyze risk & impact of change to resolve incident

No

To Incident Management 4.5 ← 5.5 Request resolution within Incident Management

5.7 Request implementation of emergency change → To Change Management 7.1

Procedure 5 Steps	Work Instructions
5.1 Determine best way to resolve incident Service Owner	5.1.1 Discuss the situation with the support technician(s) who have been working on the resolution of the incident. 5.1.2 If the service is degraded, but not completely unavailable to the affected customers, consider whether the service will need to be taken down in order to resolve the incident. Also determine if other, currently unaffected, services are going to become unavailable when the incident is being resolved. Note: This step is very important in situations where, for example, a reboot of a server, on which multiple services are running, is required to complete the implementation of the change that will resolve the incident. 5.1.3 Decide, with the help of the support technician(s), how the incident had best be resolved.
5.2 Recovery at continuity site most efficient way to resolve incident ?	5.2.1 Continue with 5.3.1 when it is clear that the resolution of the incident is going to take a long time and that the recovery of the affected service at its continuity site is the most efficient and reliable way to resolve the incident. If this is not the case, go to 5.4.1. Note: The recovery of the service at its continuity site should not be considered when it is possible to resolve the incident by: • Improving security measures (e.g. updating virus definitions, applying a security patch, etc.), • Restoring a backup or a previous software release at the production site (e.g. in case of data corruption or an application change implementation that was unsuccessful), or by • Replacing hardware that has failed in order to continue service delivery from the production site.
5.3 Escalate incident Service Owner	5.3.1 Contact the appropriate support group to apprise of the current situation. Be specific about the fact that the incident has now been escalated to the support group because a service recovery is required in order to get the incident resolved in a timely fashion. 5.3.2 Add a work info entry to the Work Info History table of the incident request. Use it to specify that you have escalated the incident to the appropriate support group because the service needs to be recovered at its continuity site in order to get the incident resolved in a timely fashion.
	5.4.1 Go to 5.6.1 if the resolution of the incident needs to be

5.4 Change Management required to resolve incident ?		handled by the Change Management process. Otherwise continue with 5.5.1.
	Note:	The resolution of the incident must be coordinated by Change Management if its implementation will cause:
		• a service to become unavailable or degraded during service hours,
		• the functionality of a service to become different, or
		• the CMDB to require an update.
5.5 Request resolution within Incident Management Service Owner	5.5.1	Ask the most appropriate support technician(s) to complete the resolution of the incident by continuing to follow Procedure 4, Incident Request Resolution.
	5.5.2	Continue to monitor the progress of the incident's resolution. If necessary start again at 5.1.1 to determine whether the incident should be resolved in a different manner.
5.6 Analyze risk & impact of change to resolve incident Service Owner	5.6.1	Discuss the implementation of the change that is expected to resolve the incident with the support technician(s). Identify the risks that could cause the implementation to fail, as well as the impact of the implementation on customers.
	5.6.2	Discuss the back out possibilities with the support technician(s) and figure out how to keep the risk and impact of the change implementation at an acceptable level.
	5.6.3	If the affected service needs to be recovered on a different infrastructure at the production site, find out whether a continuity plan is available. If this is the case, select the checklists of the plan that should be followed by the support technician(s) during the change implementation to help minimize the risk of failure.
5.7 Request implementation of emergency change Service Owner	5.7.1	Ask the most appropriate support technician(s) to implement the change by following the Emergency Change Management procedures.
	5.7.2	Take enough time to ensure that the support technician(s) understand how the change is to be implemented to avoid unnecessary risk of failure and impact on customers. This includes specifying which continuity plan checklists are to be used, if a continuity plan can be used to help minimize the risk of failure.
	5.7.3	Contact the support technician(s) to confirm that you have approved the use of the Emergency Change Management procedures for the resolution of this incident.

7.6   Incident Request Closure

When a service desk analyst is able to resolve an incident request (in terms of skills, access rights, and time considerations), he/she resolves it and updates the incident request accordingly. The service desk analyst closes the incident request if the customer is still in contact with the service desk analyst and was already able to verify the solution.

If the service desk analyst believes that the solution information he/she entered in the incident request could help requesters, service desk analysts and/or support technicians to resolve future cases that are similar, he/she proposes it for general use.

After a customer has received an incident request resolution notification, he/she reviews the resolution information of his/her incident request. In addition to the resolution notification generated by the tool, the service desk will promote customer satisfaction by attempting personal contact to have the customer verify the solution. If the customer considers the solution acceptable, he/she does not need to take any further action and the incident request will be closed. If the solution is not acceptable, the deficiency(ies) will be noted the Work Info History table of the incident request and reassigned.

The *Incident Request Closure* procedure is presented on the next page.

pennsylvania
DEPARTMENT OF TRANSPORTATION

Procedure 6, Incident Request Closure

To Incident Management 1.11

From Incident Management 1.11

Service Desk Analyst

6.1 Resolve incident request

6.2 Customer able to verify solution immediately ?

Yes

6.3 Customer accepts solution ?

No

Yes

6.4 Close incident request

To Incident Management 7.1

To Request Management

No

6.5 Complete incident request

6.8 Reject Resolution & reassign incident request

To Incident Management 4.1

From Incident Management 4.6

From Change Management 6.8 or 8.4

From Release Management 4.9

From Continuity Management 3.8

User

6.6 Review incident request completion notification

6.7 Solution acceptable ?

No

Yes

Procedure 6 Steps	Work Instructions
6.1 Resolve incident request Service Desk Analyst	**6.1.1** Resolve the incident request. If necessary, ask the customer and/or your colleagues at the service desk for assistance. **6.1.2** If you found the solution for the incident request using the Incident Matching quick action, select this solution and click on the Relate With Solution button. This causes the solution information to be entered in the Resolution field of the incident request. Edit this text as needed to provide an accurate account of how the incident request was resolved. If you did not use a proposed solution to resolve the incident request, use the Resolution field to provide a concise, step-by-step account of how the incident request was resolved. Also fill out or edit the text in the Resolution field as needed to provide detailed solution instructions (e.g. if the customer needs to adjust a setting) or to provide the answer to a request for information. **6.4.3** If you have manually entered the solution information, and if you believe that the solution information could help customers, service desk analysts and/or specialists to resolve future incident requests that are similar, propose your solution for general use. Do this by clicking on the Relationships tab, selecting the "Solution Database" option in the Request Type field and clicking on the Create button. Ensure that the Status field of the solution is set to "Inactive" and that its View Access× field is set to "Internal". **6.1.4** If you still have the customer on the telephone, or if you are able to quickly contact the customer, ask him/her to verify the solution.
6.2 Customer able to verify solution immediately ?	**6.2.1** If the customer who submitted the incident request has already verified the solution, continue with 6.3.1. Otherwise go to 6.5.1.
	6.3.1 If the customer who submitted the incident request has indicated that he/she is satisfied with the solution, continue with 6.4.1. Otherwise return to 1.11.1. **Note:** The Status× field of the incident request will automatically change from "Resolved" to "Closed" after seven (7) days.

6.3
Customer accepts solution ?

6.4 Close incident request

Service Desk Analyst

6.4.1   Set the Statusx field of the incident request to "Closed".

6.4.2   Capture any customer comments by adding a work info entry to the Work Info History table of the incident request.

6.4.3   Perform a final review of the incident request to ensure that its information is accurate and complete.

6.5 Complete incident request
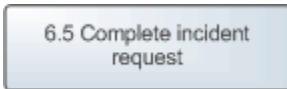
Service Desk Analyst

6.5.1   Set the Statusx field of the incident request to "Resolved" and select the most appropriate option in the Status Reason field.

6.5.2   Contact the customer via phone to review the incident request completion.

6.6 Review incident request completion notification

User

6.6.1   After having received an email notification informing the customer that his/her incident request has been resolved. Review its solution information in the Resolution field.

Note: In addition to the email notification, the service desk will make three (3) attempts, one (1) business day apart, to contact the customer by phone. If unsuccessful speaking to the customer, on the last attempt the service desk analyst will leave a voicemail for the customer.

6.6.2   Verify the solution to make sure that is acceptable.

6.7 Solution acceptable ?

6.7.1   If the solution provided for the incident request is acceptable, go to 6.9.1. Otherwise continue with 6.8.1.

Note: The Statusx field of the incident request will automatically change from "Resolved" to "Closed" after seven (7) days.

6.8 Reject Resolution & reassign incident request

Service Desk Analyst

6.8.1   Determine why the incident request has been rejected and use the "Add Work Info" option on the navigation pane to specify why the customer is not satisfied with the solution of the incident request.

Note: This information will be added to the Work Info History

		table of the incident request.
	6.8.2	Confirm that the assignment group in the Assigned Group×+ field is accurate.
	6.8.3	Change the Status× field of the incident request to "Assigned".

7.7 Solution Approval

After a support group lead has received a notification that a new solution has been proposed, he/she reviews the proposed solution information. If the support group lead agrees that the proposed solution could help customers, service desk analysts and/or support technicians to resolve future incident requests that are similar, he/she activates it (after having improved the solution information if this was deemed necessary). This makes the solution available for general use.

On the other hand, if the support group lead does not believe that the proposed solution provides any benefit, he/she ensures that it does not become available for general use.

The *Solution Approval* procedure is presented on the next page.

pennsylvania
DEPARTMENT OF TRANSPORTATION

Procedure 7, Solution Approval

From Incident Management 4.6, 6.4 or 6.5 → 7.1 Review new solution

Support Group Lead

7.2 Should solution be made available for general use ?

Yes → 7.4 Activate new solution

No → 7.3 Leave new solution inactive
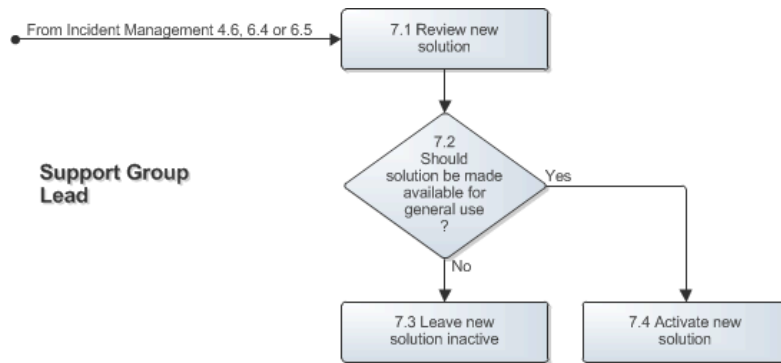
Procedure 7 Steps	Work Instructions	
7.1 Review new solution Support Group Lead	7.1.1 Note:	After having received a notification requesting the approval for a proposed solution, open it and review the solution information for completeness and accuracy. Contact the specialist who proposed the solution if you do not understand the solution or the need to make it available for general use.
7.2 Should solution be made available for general use ?	7.2.1	If the proposed solution appears to be accurate and complete, and if it could help customers, service desk analysts and/or specialists to resolve future incident requests with the same categorization, go to 7.4.1. Otherwise continue with 7.3.1.
7.3 Leave new solution inactive Support Group Lead	7.3.1	Specify the reason for not wanting to make this solution available for general use on the Work Info tab of the solution and fill out the current date and time in its Expiry Date field. Leave the Status field of the solution set to "Inactive".
7.4 Activate new solution Support Group Lead	7.4.1 7.4.2	Edit the solution information as needed to perfect it. Change the value in the Status field of the solution from "Inactive" to "Active" to make it available for general use.

8. Forms

Within the ITSM tool, a form is defined as a collection of fields in which information is entered and displayed. The collection of fields represents a record of information in the ITSM tool. Within the ITSM tool, fields assist users in navigating through the system and identifying mandatory fields when completing requests. For example:

- **Bold** fields with an asterisk (*) are mandatory fields and must be completing before submitting or updating the form
- Fields with a plus sign (+) indicate that the field is searchable or has predictive text functionality

8.1   Incident Request Form

The Incident Request form organizes the fields most commonly used for creating, resolving, and updating incident requests. You can access additional, less frequently used functionality from the tabbed sections of the form or from the links in the Navigation pane.

The table below lists fields for the Incident Request form and provides a description for each field.

Incident Details	
Field	**Description**
Incident ID	This field displays the unique incident request identifier automatically after the incident request has been saved for the first time. This ID number can be used as a reference for searching.
Company	Use this field to select the company of the customer for whom the incident request is to be resolved. Transportation is pre-populated in this field.
Customer	This field requires users to select a customer by typing the last name or using the search icon.
Contact	This field requires users to select a contact by typing the last name or using the search icon. **Note:** *Contact names are only required when someone is logging the incident on behalf of someone else.*
Template	Select the Template by placing the cursor in the field and selecting enter. A list of templates appears in a new screen.
Summary	This is a free text field for a user to enter a brief description of the incident.

Notes	This is a free text field to enter details about the incident. This field has unlimited character functionality.
Configuration Item (CI)	The CI field provides a place to indicate to which piece of infrastructure the incident pertains. This field is currently not in use.
Impact	Identify the impact of the incident by selecting the appropriate level from the drop-down list: • **Extensive/Widespread** – Majority or all customers, statewide, regardless of location, district and/or bureau. • **Significant/Large** – Numerous customers in most locations, districts and/or bureaus. • **Moderate/Limited** – Several customers within a couple locations, districts and/or bureaus. • **Minor/Localized** – Single customer or small group of customers at a single location, district and/or bureau.
Urgency	Identify the urgency of the incident by selecting the appropriate level from the drop-down list: • **Critical** - Immediate impact with no workaround • **High** - Immediate impact with workarounds available • **Medium** - Approaching impact with or without workarounds • **Low** - Distant impact or for planning purposes
Priority	The incident priority is automatically set by the application based upon the Impact and Urgency that is selected. Priority values include: • Critical • High • Medium • Low
Incident Type	Use this field to select the incident type. The available options include:: • **User Service Restoration** - Use this service type for typical service restoration requests (for example, a request to restore printing services). • **User Service Request** - Use this service type if the incident request is a simple question or a request for information (for example, a request for how to" information). • **Infrastructure Restoration** - Use this service type if the incident request is more focused on the restoration of infrastructure service. Typically, these types of incident requests are reported by system management tools (for example, if an incident is detected on a piece of network infrastructure by system monitoring software). • **Infrastructure Event** - Use this service type when a system management tool registers an event that does not require infrastructure restoration.

Reported Source	Records how the customer reported the incident. Use this field to select the source of the incident request. The available options are: • Direct Input • Email • External Escalation • Fax • Self Service • Systems Management • Phone • Voice Mail • Walk In • Web • Other • BMC Impact Manager Event
Assigned Group	Select the Support Group to be assigned the incident from the drop-down list or by filling out (part of) the group's name and selecting the correct group.
Assignee	Select the individual assignee from the drop-down list to specify who the incident request is to be assigned.
Owner Group	Displays the Support Group the user who created the request is associated with.
Owner	Displays the owner of the incident.
Status	Use this field to select the status of the incident request. The available options are: • New — The incident request has not yet been saved. • Assigned — The responsibility for the resolution of the incident request has been assigned to a specific group or group member. • In Progress — The incident request is currently being resolved. • Pending — It is temporarily not possible to make any further progress in the resolution of the incident request. The reason for this is specified in the Status Reason field. • Resolved — The work on the resolution of the incident request has come to an end because of the reason specified in the Status Reason field. • Closed — The incident request has been closed because the customer has accepted the solution, or because of the reason specified in the Status Reason field.

	• Cancelled The incident request has been cancelled because the customer has withdrawn the request.
Status Reason	Select a status reason when an incident is in one of the following: Pending, Resolved, Cancelled or Closed. The available options for the status "Pending" are: • Approval • Client Hold • Parts • Scheduled Date • Client Action Required • Testing • Support Contact Hold • Local Site Action Required • Purchase Order Approval • Registration Approval • Supplier Delivery • Third Party Vendor Action Reqd • Infrastructure Change • Request • Monitoring Incident • Future Enhancement The available options for the status "Resolved" are: • Automated Resolution Reported • Customer Follow-up Required • Temporary Corrective Action • Future Enhancement • Monitoring Incident • No Further Action Required • No Trouble Found The available options for the status "Closed" are: • Infrastructure Change Created • Automated Resolution Reported • No Further Action Required • No Trouble Found • Resolution Successful The available options for the status "Cancelled" are: • By User Request • Issue Resolved Itself • Training Issue

Cause	This field is required when resolving an incident. Select an option from the drop down list below: • Application Error • Application Performance • Configuration Error • Data Change • Education Required • Facilities Issue • Hardware Failure • Infrastructure Issue • Network Outage • Network Performance • No Issue/Trouble Found • Power Failure • Service Call/Warranty Work • Software Version Not Compatible • Third-Party/Vendor Issue/Outage • User Request • Virus/Malware
Resolution	Free text field to note the resolution details of the incident.

Tab – Categorization

Field	Description
Company	This field defaults to Transportation.
Operational Categorization	
Tier 1	This mandatory field is used to identify the operational categorization that is most relevant to the incident request. To easily identify, use the search icon to the right.
Tier 2	This mandatory field is used to select the second tier of the operational categorization that is most relevant to the incident request.
Tier 3	This field is not in use.
Product Categorization	
Tier 1	Mandatory field that identifies the item request. This field contains the search icon, which opens a new window when selected. The window displays all product categorization tiers. When a selection is made starting in Tier 1, the table below provides a list of possible matches.

Tier 2	This mandatory field is used to select the second tier of the product categorization that is most relevant for the incident request.
Tier 3	This mandatory field is used to select the third tier of the product categorization that is most relevant for the incident request.
Product Name	Use this field to select the product name of the product categorization that is most relevant to the incident request.
Model/Version	Use this field to select the model or version of the product categorization that is most relevant for the incident request.
Manufacturer	This field automatically populates the manufacturer of the product selected in the Product Name field.
Service	This field is currently not in use.
Customer	
Device Name	Work station used by the customer.

Tab – Work Detail	
Field	**Description**
Work Info History	This table shows the work info entries for the incident request. Add an entry that provides a detailed description of the actions performed in Notes Section and Click Add button.
Preferences	Allows users to add or remove columns to the tables.
Refresh	Refresh the work details displayed within the table.
Notes	This is a free text field to enter details about the incident.
Attachment	Documents associated with the incident may be attached here for reference. **Note:** Up to three documents can be attached for each work entry.
Work Info Type	Provides a drop down list for users to select the type of service they provided.
Locked	To ensure the work info is modifiable, ensure the field is marked No.

View Access	Choose the type of view access: • Public: This is the preferred option as it allows the customer to see the work information entry. • Internal: The customer will not be able to see the work information entry.

Tab – Relationships

Field	Description
Relationships	This table lists the records that are linked to the incident request.
Show Related	Use this field to select one of the following options to indicate which type of related record you would like to see displayed in the table below: • ALL • CI Unavailability • Configuration Item • Incident • Infrastructure Change • Known Error • Problem Investigation • Release • Solution Database • Work Order
Search	Use this field to select one of the following options to indicate which type of record you would like to search for or create: • CI Unavailability • Configuration Item • Incident • Infrastructure Change • Known Error • Problem Investigation • Release • Solution Database • Work Order After having selected the appropriate option, click on the Search or

	Create button to either start the search or to open a new record that will be linked to this incident request when it is saved. When a search is performed, the records in the search result can subsequently be linked to this incident request.
Tab – Date/System	
Field	**Description**
Date Information	
Reported Date	Use this field to specify the date and time at which the incident request was reported. Do this by filling out (part of) the Reported Date and subsequently pressing the Enter key or use the Find as you type feature.
Required Resolution Date Time	This identifies the date in which the incident must be resolved.
Target Date	Use this field to enter the date on which the incident request is estimated to be resolved.
Responded Date	This field displays the date and time at which the incident request was first responded to. Do this by filling out (part of) the Responded Date and subsequently pressing the Enter key or use the Find as you type feature.
Closed Date	This field is automatically set to the current date and time when the status of the incident request is set to "Closed".
System Information	
Submitter	This field is automatically set to the unique login name of the person who registered the incident request.
Submit Date	This field is automatically set to the date and time at which the incident request was registered.
Last Modified By	This field is automatically set to the unique login name of the person who last modified the incident request.
Last Modified Date	This field is automatically set to the date and time at which the incident request was last modified.
Tab – Hardware Service Call	

Field	Description
PennDOT Asset Tag	Tag placed on all assets at PennDOT (e.g., P000027879). If the asset tag is known and the user hits enter, Remedy searches for the data and automatically populates the following fields if found • Device Type • Make • Model • Serial Number • Location • Site • Floor • Cube • OA Site • Warranty Date or Maintenance Date
Device Information	
Device Type	Denotes the type of device (e.g., Monitor, Printer, Laptop).
Make	Manufacturer (e.g., Dell, HP, Lexmark).
Model	Specific version of the device (e.g., Latitude).
Serial Number	Identification number on the device.
Equipment Status	Status of the device (e.g., Lease, Warranty, Third Party Maintenance).
Service Provider	Company or manufacturer (e.g., Dell, Pomeroy, Lexmark) providing the service for the device.
Vendor Group	This field is not in use.
Vendor Ticket Number	Maintenance ticket number (e.g., OA Ticket number, Pomeroy Ticket number or Verizon ticket number).
Location	
On-Site Contact Name	Contact person for any questions about the device. This field has the capability to search by last name.
Contact Telephone	This field is auto populated when a search is performed for the on-site contact name. If the telephone is not available, one can be manually entered.
Device Name	This field gives the name of the device.
Location of Device	Building where the device is located (e.g., Keystone building, District Office, ROC)
Site Name	Address of the "Location of Device" (i.e., Street address, City, State, Zip)

Floor	Floor where the device is located.
Cube	Cube number where the device can be found.
OA Site Name	The name of the PennDOT facility used by the Office of Administration (OA).
Lifecycle	
Warranty End Date	If the device has a manufacturer warranty, the relevant date is displayed.
Maintenance Start Date	If the device is covered by a third party maintenance contract, the relevant date is displayed.