

White Paper: BMC Service Management Process Model 7.6
BMC Best Practice Flows



October 2009

Contacting BMC Software

You can access the BMC Software website at <http://www.bmc.com>. From this website, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

United States and Canada

Address	BMC SOFTWARE INC 2101 CITYWEST BLVD HOUSTON TX 77042-2827 USA	Telephone	713 918 8800 or 800 841 2031	Fax	713 918 8000
----------------	--	------------------	---------------------------------	------------	--------------

Outside United States and Canada

Telephone	(01) 713 918 8800	Fax	(01) 713 918 8000
------------------	-------------------	------------	-------------------

If you have comments or suggestions about this documentation, contact Information Design and Development by email at doc_feedback@bmc.com.

© Copyright 2009 BMC Software, Inc.

BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners.

BMC Software considers information included in this documentation to be proprietary and confidential. Your use of this information is subject to the terms and conditions of the applicable End User License Agreement for the product and the proprietary and restricted rights notices included in this documentation.

Restricted rights legend

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Section 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time. Contractor/Manufacturer is BMC Software, Inc., 2101 CityWest Blvd., Houston, TX 77042-2827, USA. Any contract notices should be sent to this address.

Customer Support

You can obtain technical support by using the Support page on the BMC Software website or by contacting Customer Support by telephone or email. To expedite your inquiry, please see “Before Contacting BMC Software.”

Support website

You can obtain technical support from BMC Software 24 hours a day, 7 days a week at <http://www.bmc.com/support>. From this website, you can:

- Read overviews about support services and programs that BMC Software offers.
- Find the most current information about BMC Software products.
- Search a database for problems similar to yours and possible solutions.
- Order or download product documentation.
- Report a problem or ask a question.
- Subscribe to receive email notices when new product versions are released.
- Find worldwide BMC Software support center locations and contact information, including email addresses, fax numbers, and telephone numbers.

Support by telephone or email

In the United States and Canada, if you need technical support and do not have access to the Web, call 800 537 1813 or send an email message to customer_support@bmc.com. (In the Subject line, enter *SupID: yourSupportContractID*, such as *SupID: 12345*.) Outside the United States and Canada, contact your local support center for assistance.

Before contacting BMC Software

Have the following information available so that Customer Support can begin working on your issue immediately:

- Product information
 - Product name
 - Product version (release number)
 - License number and password (trial or permanent)
- Operating system and environment information
 - Machine type
 - Operating system type, version, and service pack
 - System hardware configuration
 - Serial numbers
 - Related software (database, program, and communication) including type, version, and service pack or maintenance level
- Sequence of events leading to the problem
- Commands and options that you used
- Messages received (and the time and date that you received them)
 - Product error messages
 - Messages from the operating system, such as `file system full`
 - Messages from related software



License key and password information

If you have a question about your license key or password, contact Customer Support through one of the following methods:

- E-mail customer_support@bmc.com. (In the Subject line, enter SupID: *yourSupportContractID*, such as SupID: 12345.)
- In the United States and Canada, call 800 537 1813. Outside the United States and Canada, contact your local support center for assistance.
- Submit a new issue at <http://www.bmc.com/support>.

Contents

Preface	7
<hr/>	
Chapter 1 Availability Management	9
<hr/>	
Procedure 1, Service Infrastructure Design	10
Procedure 2, Availability Tracking	12
Chapter 2 Capacity Management	15
<hr/>	
Procedure 1, Capacity Utilization Threshold Setting	16
Procedure 2, Capacity Warning Handling	17
Procedure 3, Capacity Tracking	19
Chapter 3 Change Management	21
<hr/>	
Procedure 1, Request for Change Review	22
Procedure 2, Change Planning	24
Procedure 3, Change Approval	25
Procedure 4, Infrastructure Change Implementation	28
Procedure 5, Application Change Implementation	29
Procedure 6, Planned Change Closure	30
Procedure 7, Emergency Change Implementation	31
Procedure 8, Emergency Change Closure	33
Chapter 4 Configuration Management	35
<hr/>	
Procedure 1, CI Requisition	36
Procedure 2, Supplier Information Maintenance	38
Procedure 3, CI Registration	39
Procedure 4, CI Update	40
Procedure 5, Contract Administration	41
Chapter 5 Continuity Management	43
<hr/>	
Procedure 1, Disaster Notification Handling	44
Procedure 2, Service Recovery	46
Procedure 3, Return to Production	47
Procedure 4, Service Recovery Testing	49
Procedure 5, Continuity Manual Maintenance	51
Procedure 6, Continuity Plan Maintenance	53

Chapter 6	Event Management	55
<hr/>		
Procedure 1, Event Handling		56
Procedure 2, Event Review		57
Procedure 3, Outage Review		58
Chapter 7	Financial Management	61
<hr/>		
Procedure 1, Accounting & Charging		62
Procedure 2, Financial Review		63
Procedure 3, Budgeting		64
Chapter 8	Incident Management	67
<hr/>		
Procedure 1, Incident Request Registration		68
Procedure 2, Incident Request Assignment		69
Procedure 3, Incident Request Tracking		71
Procedure 4, Incident Request Resolution by Specialist		72
Procedure 5, Incident Escalation Handling		73
Procedure 6, Incident Request Closure		75
Procedure 7, Solution Approval		76
Chapter 9	Problem Management	79
<hr/>		
Procedure 1, Incident Request Review		80
Procedure 2, Root Cause Analysis		81
Procedure 3, Analysis Review		82
Procedure 4, Problem Closure		84
Chapter 10	Release Management	85
<hr/>		
Procedure 1, Request for Change Handling		86
Procedure 2, Release Definition		87
Procedure 3, Business Justification		88
Procedure 4, Release Coordination		90
Chapter 11	Service Level Management	93
<hr/>		
Procedure 1, Service Catalog Maintenance		94
Procedure 2, Service Activation		96
Procedure 3, Customer Information Maintenance		98
Procedure 4, Service Termination		99
Procedure 5, SLA Review and Request Handling		100

Preface

This white paper provides a high-level overview of the service management processes that make up the BMC Service Management Process Model (BMC SMPM).

Each section starts with a high-level overview of a different BMC SMPM process, which is followed by a detailed description of the related procedures. Each section also contains flow diagrams that show where the procedures fit into the process and the individual steps that make up each procedure.

The following list describes additional process information that comes bundled with the BMC SMPM application. It is included with each process description:

- **Work instructions** – Each procedure step has a related work instruction describing how to perform the step, which you can view from the BMC SMPM interface.
- **Field use guidelines** – A set of field use guidelines is available for each of the BMC Remedy IT Service Management forms used to support the process.

NOTE

You can configure BMC SMPM to open from within the BMC Remedy IT Service Management (BMC Remedy ITSM) applications – starting with BMC Remedy ITSM version 7.5.00. This makes the work instructions, when combined with the field use guidelines, a useful training tool and reference guide.

- **Roles and responsibilities** – A list of the roles needed to complete each process (Group Coordinators, Service Desk Analysts, and so on). The list also describes the responsibilities of each role.
- **Key Performance Indicators (KPIs)** – A list of the KPIs used for tracking how successfully you are performing each process.
- **Links** – Each procedure is hyperlinked to the next so that you can see how the procedures flow into one another and how they are related.

Availability Management

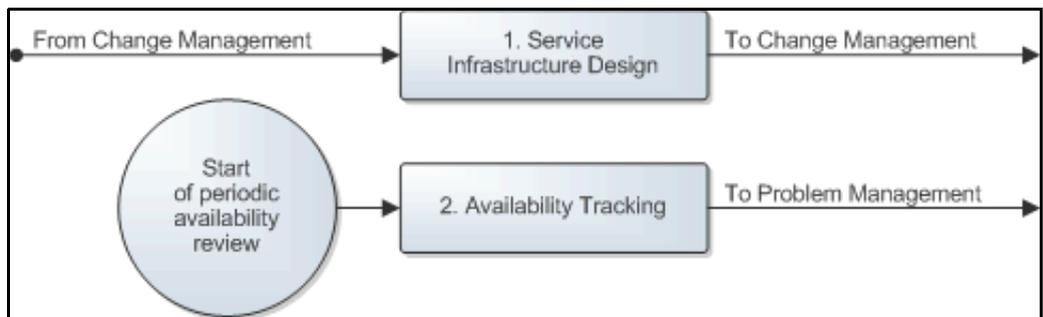
The Availability Management process consists of two procedures.

The first procedure is called "Service Infrastructure Design". This procedure is used by availability managers when they design new service infrastructures or when they adjust the design of existing service infrastructures.

The second procedure is called "Availability Tracking". It is used by availability managers when they track the availability and reliability of the services which availability they are responsible for.

A graphical representation of the process is provided below. Each procedure is described in more detail in the sections that follow this diagram.

Figure 1-1: Availability Management process



Procedure 1, Service Infrastructure Design

A change coordinator requests the design of a new service infrastructure when he/she is planning a change to build a new service infrastructure. Similarly, a change coordinator requests the adjustment of an existing service infrastructure design when he/she believes that an adjustment might be necessary to satisfy the requirements for which he/she is planning the change. These requests are sent by email to the availability manager who is responsible for the availability of the service for which the change was requested.

Such a request is subsequently reviewed by the availability manager who determines if a new service infrastructure is to be built or if an existing service infrastructure needs to be altered.

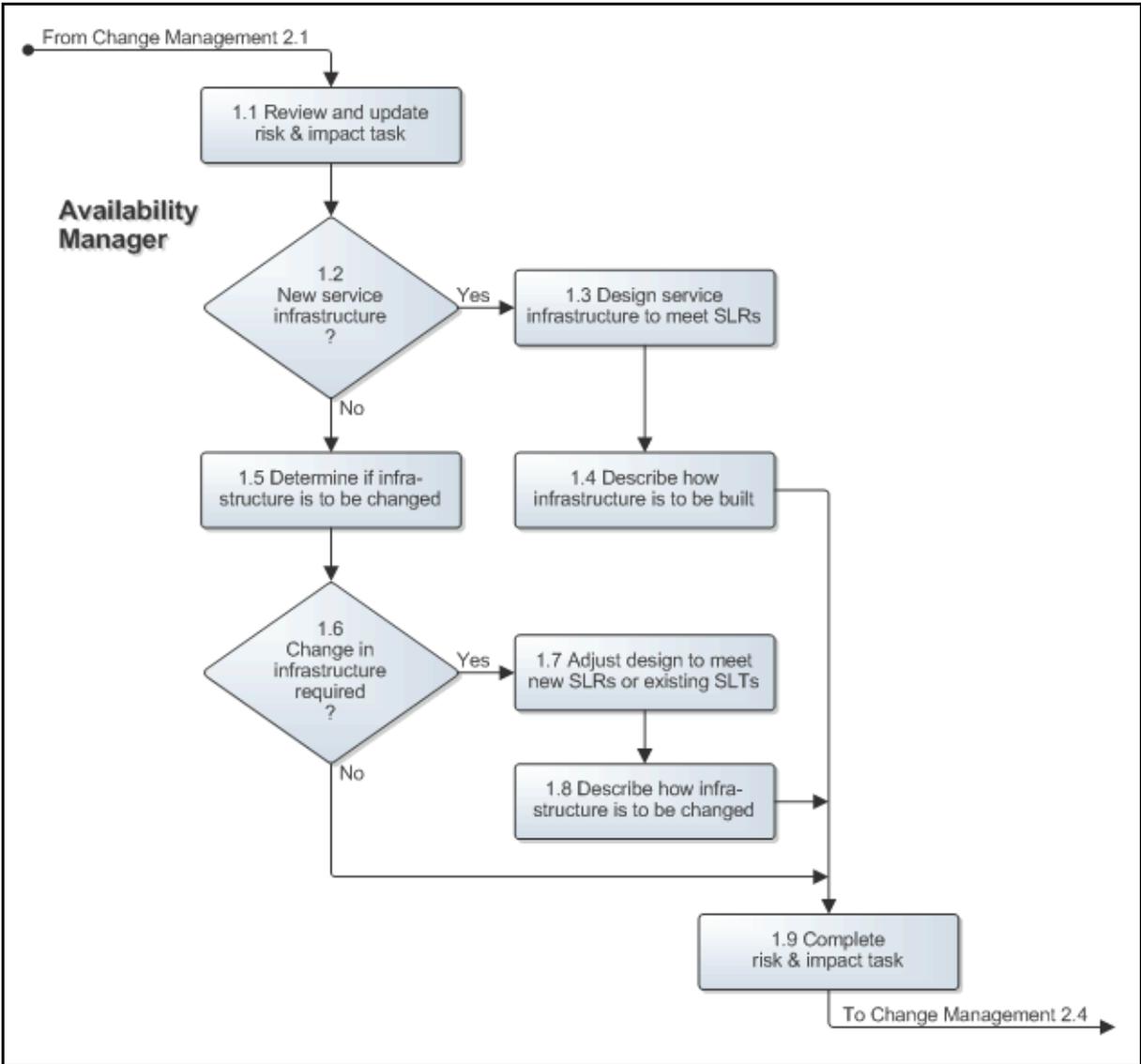
If a new service infrastructure is to be built, the availability manager designs it in such a way that it will be capable of meeting the SLRs set by the service level manager. The availability manager specifies the SLTs that the proposed service infrastructure will be able to meet.

If an existing service infrastructure needs to be altered, the availability manager adjusts the design of the existing service infrastructure in such a way that the existing SLTs of the service will be met after the change has been implemented and the service infrastructure has been adjusted. However, if (one of) the objective(s) of the change is to adjust the existing SLTs, the availability manager adjusts the existing design of the service infrastructure to ensure that it will be capable of meeting the new SLRs.

After the new design has been prepared, the availability manager describes how it is to be built. The availability manager subsequently sends this information back to the change coordinator so that he/she can finalize the risk & impact analysis and plan the change accordingly.

The Service Infrastructure Design procedure diagram is presented on the next page.

Figure 1-2: Service Infrastructure Design



Procedure 2, Availability Tracking

At the end of an availability tracking period, the availability manager finds out what the availability and reliability has been over the past period. He/she does this for every SLA that has been signed, and is still active, for the service(s) which availability he/she is responsible for. The availability manager then updates and publishes the availability tracking overview(s) of these service(s).

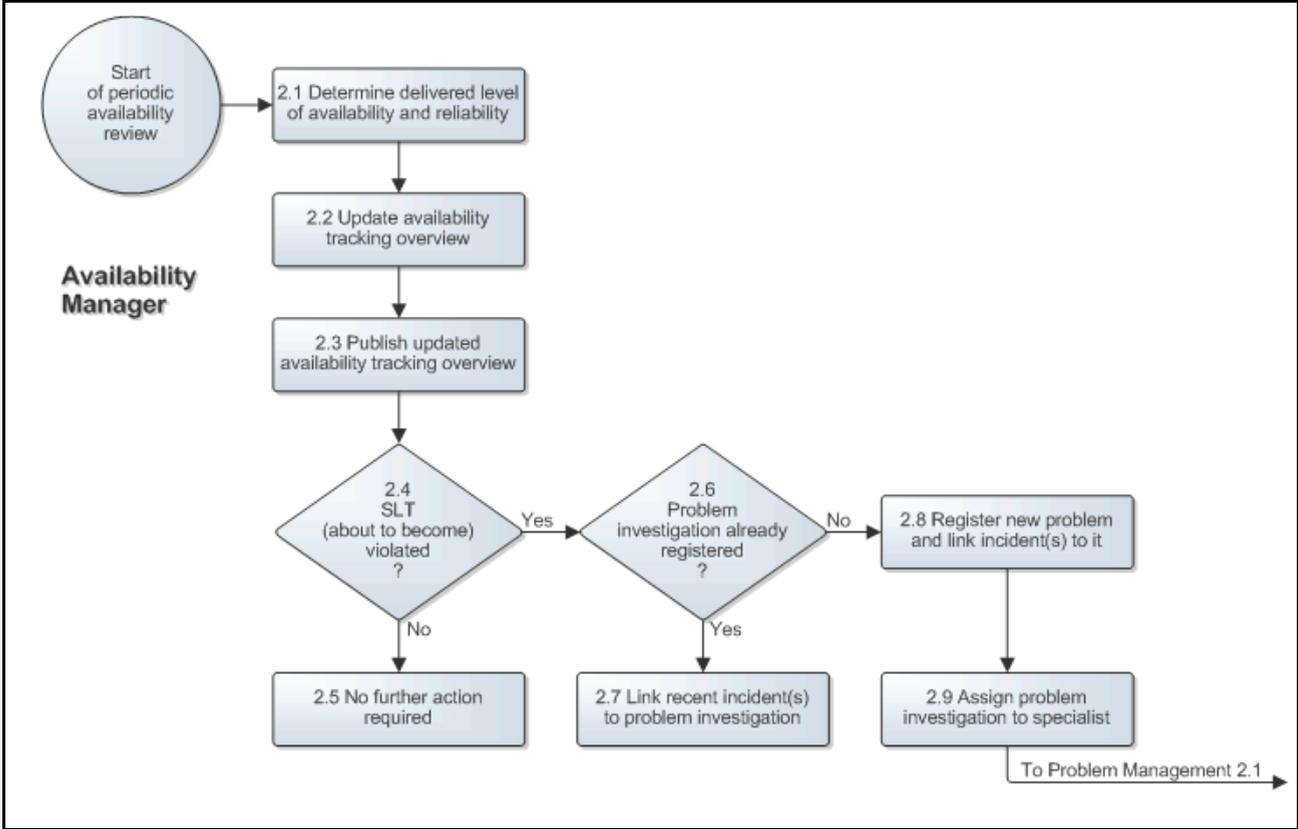
If the availability manager found out that the availability or reliability target of one or more SLAs is in danger of being violated, or if it has already been violated, he/she checks to find out if a problem investigation has already been registered for this. If this is the case, the availability manager ensures that the incident requests that have been caused by this problem during the past availability tracking period are linked to the problem investigation.

If multiple problem investigations have already been registered, because there are several root causes that are causing the availability and/or reliability targets to be(come) violated, the availability manager links the incident requests that appear to have been caused by these problems to the appropriate problem investigation.

If one or more incident requests appear to have been caused during the past availability tracking period by a root cause for which a problem investigation has not yet been registered, the availability manager registers a new problem investigation. He/she links the related incident request(s) to the new problem investigation and assigns it to the most appropriate specialist (in terms of skills, availability and access rights) for analysis.

The Availability Tracking procedure diagram is presented on the next page.

Figure 1-3: Availability Tracking



2 Capacity Management

The Capacity Management process consists of three procedures.

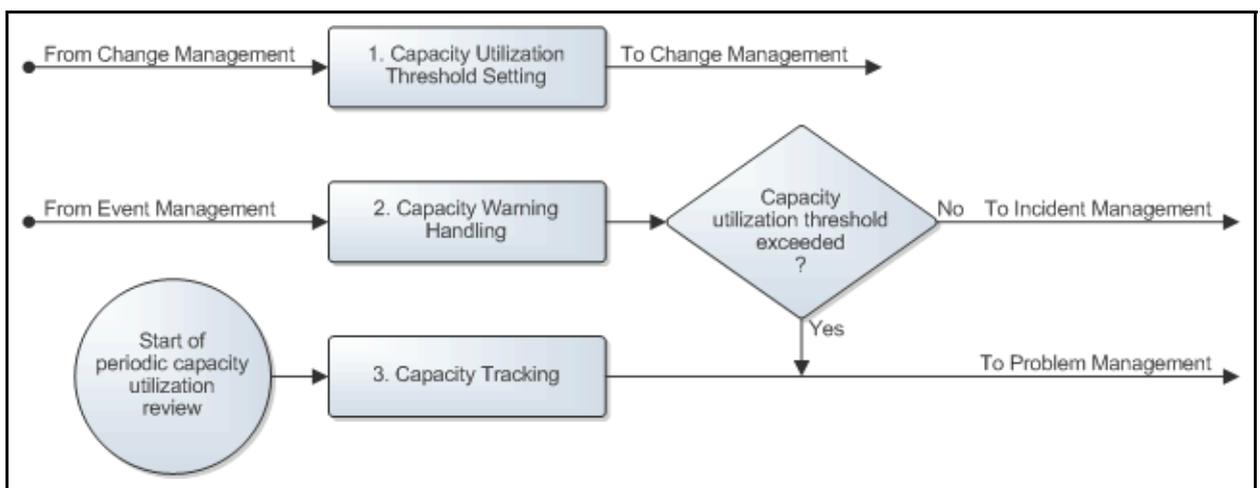
The first procedure is called "Capacity Utilization Threshold Setting". This procedure is used by capacity managers to set up a new capacity tracking overview after a new service infrastructure has been built, or to update an existing capacity tracking overview after the capacity of a service infrastructure has been changed.

The second procedure is called "Capacity Warning Handling". Capacity managers follow this procedure after an incident request that warns of an impending capacity shortage has been assigned to them by an operator.

The third procedure is called "Capacity Tracking". It is used by capacity managers when they track the capacity of the infrastructures of the services which capacity they are responsible for.

A graphical representation of the process is provided in the following diagram. Each procedure is described in more detail in the sections that follow this diagram.

Figure 2-1: Capacity Management process



Procedure 1, Capacity Utilization Threshold Setting

A change coordinator assigns a task for the creation of a new capacity tracking overview after a new service infrastructure has been built. Similarly, a change coordinator assigns a task for the update of an existing capacity tracking overview after the capacity of an existing service infrastructure has been altered. These tasks are assigned to the capacity manager who is responsible for the capacity of the service for which the change was requested.

Such a task is subsequently reviewed by the capacity manager who determines if a new capacity tracking overview is to be created or if an existing capacity tracking overview needs to be updated.

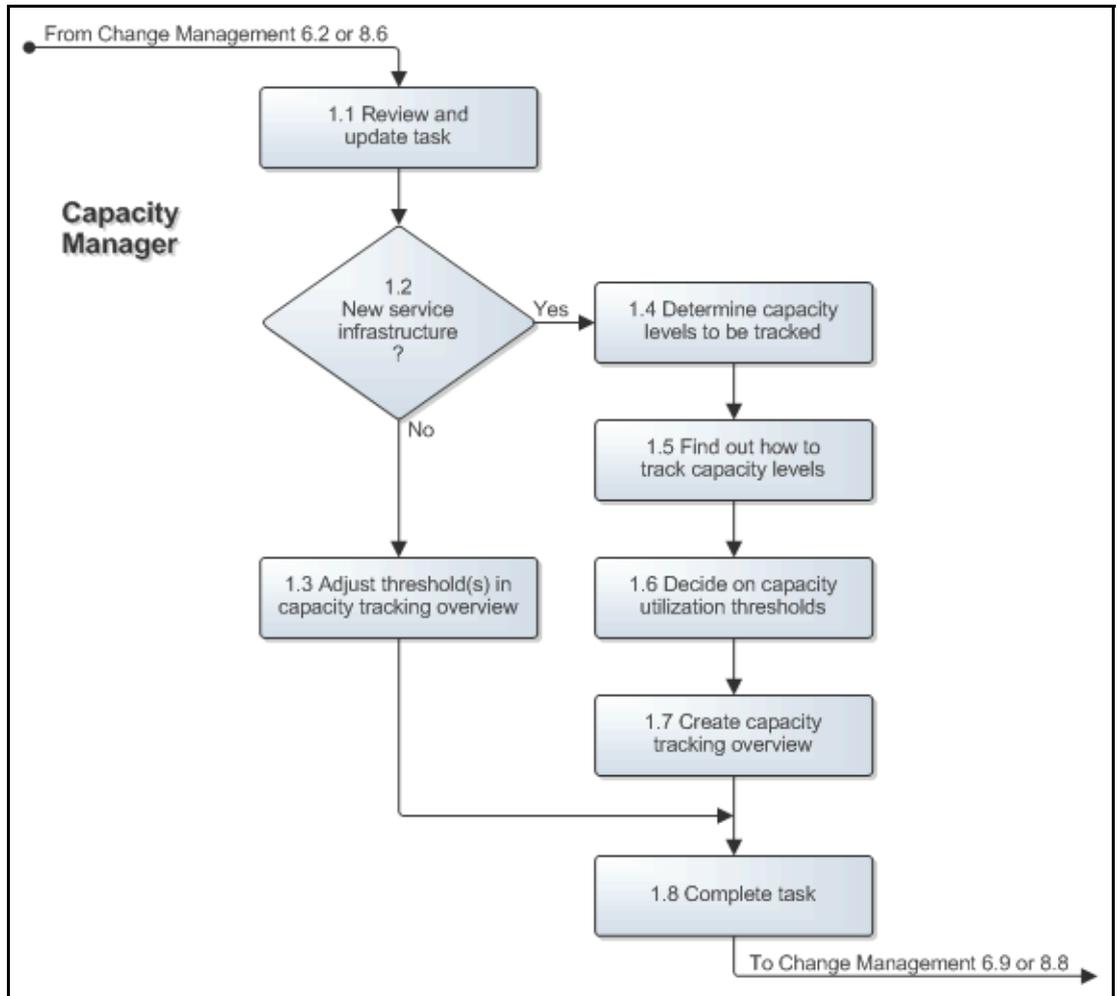
If a new capacity tracking overview is to be created, the capacity manager decides which capacity levels are to be tracked, finds out how to track them in an efficient fashion, decides on a practical frequency for updating the capacity tracking overview, and sets reasonable capacity utilization thresholds. With this, the capacity manager creates the new capacity tracking overview for the new service infrastructure.

If the capacity of an existing service infrastructure has been updated, the capacity manager updates the capacity tracking overview for this service infrastructure.

After the creation of a new, or the update of an existing, capacity tracking overview, the capacity manager describes in the task which values were put into the capacity tracking overview, before closing the task.

The Capacity Utilization Threshold Setting procedure diagram is presented on the next page.

Figure 2-2: Capacity Utilization Threshold Setting



Procedure 2, Capacity Warning Handling

After an incident request that warns of an impending capacity shortage has been assigned to a capacity manager by an operator, the capacity manager looks up the capacity utilization level at which the event, for which this incident request was created, had been generated. Knowing the capacity utilization level, the capacity manager opens the capacity tracking overview spreadsheet of the service that consumes the capacity. In the capacity tracking overview spreadsheet, he/she looks up the specific service infrastructure that would become affected by the impending capacity shortage and determines if the utilization level exceeds one of its capacity utilization thresholds.

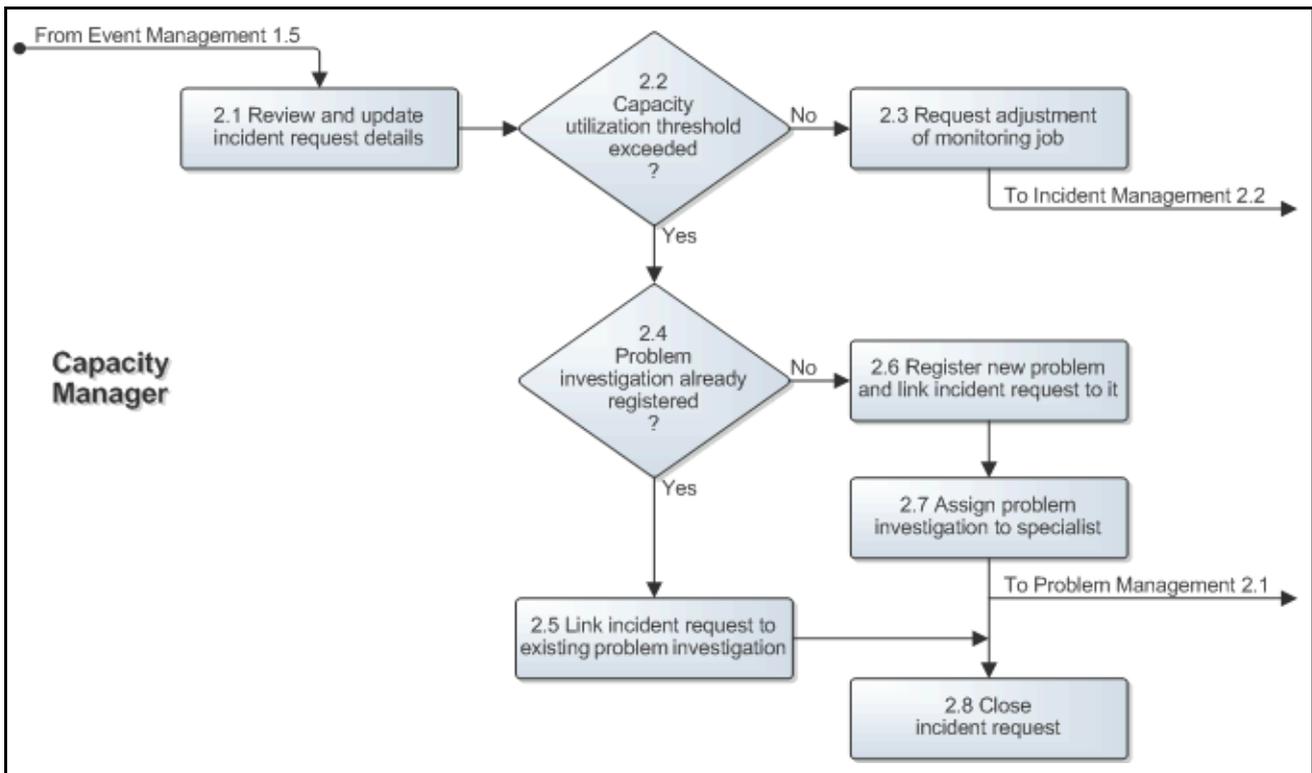
If the utilization level does not exceed one of these thresholds, the capacity manager requests an adjustment of the monitoring job that generated the event to prevent such events from being generated in the future.

On the other hand, if the utilization level did exceed a threshold specified in the capacity tracking overview spreadsheet, the capacity manager determines whether or not a problem investigation has already been registered for this. If a problem investigation has already been registered, the capacity manager simply links the incident request to this problem investigation. The capacity manager registers a new problem investigation if a problem investigation has not yet been registered for this impending capacity shortage. He/she subsequently links the incident request to the new problem investigation and assigns it to the most appropriate specialist (in terms of skills, availability and access rights) to find out how incidents had best be avoided (e.g. by freeing up some of the utilized capacity or by adding more capacity to the service infrastructure).

The capacity manager closes the incident request after it has been linked to an existing or a new problem investigation.

The Capacity Warning Handling procedure diagram is presented below.

Figure 2-3: Capacity Warning Handling



Procedure 3, Capacity Tracking

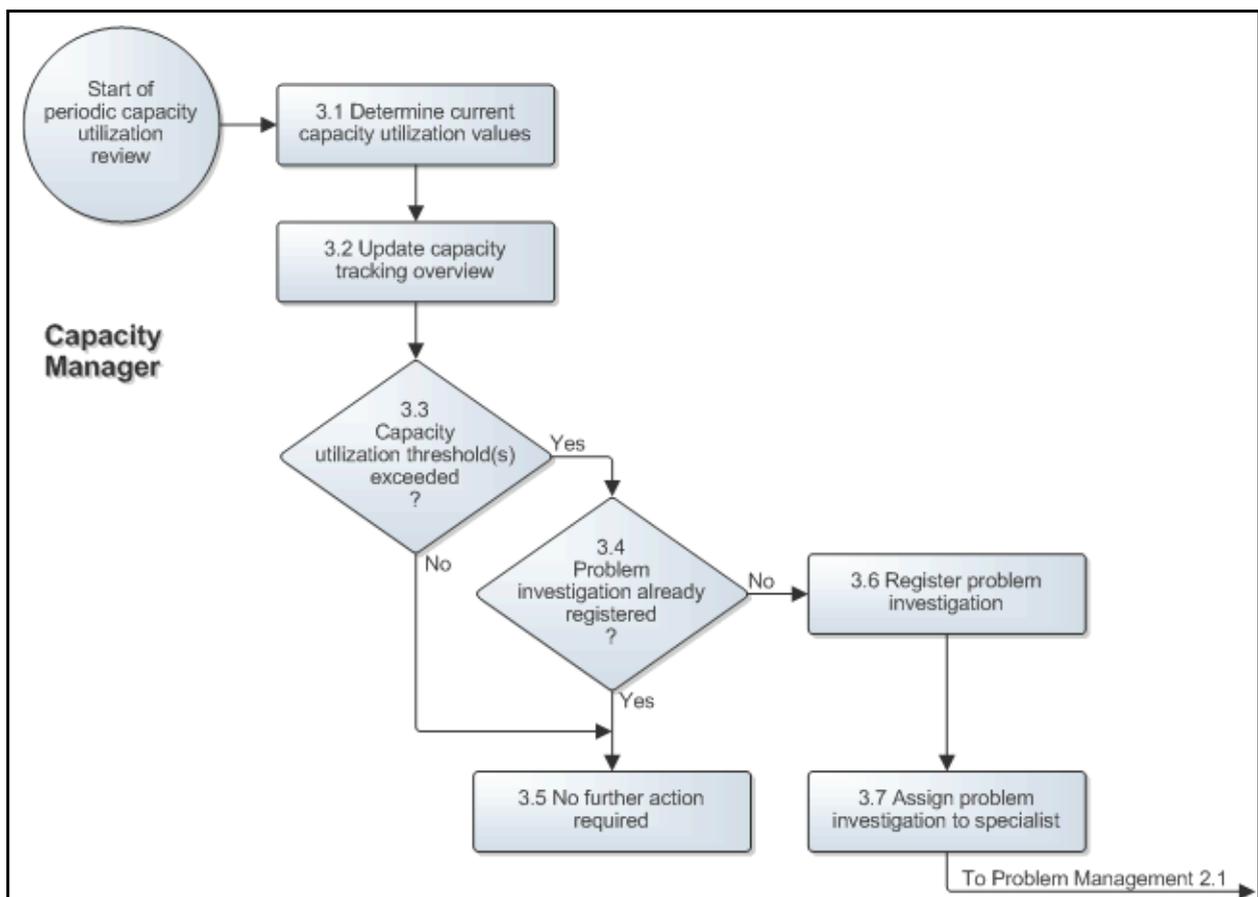
At the end of a capacity tracking period, the capacity manager determines the capacity utilization value for each capacity level that is to be tracked for the different service infrastructures of the service(s) which capacity he/she is responsible for. The capacity manager then updates the capacity tracking overview(s) of these service(s).

If one or more capacity utilization thresholds have been exceeded, the capacity manager checks for each threshold violation whether or not a problem investigation has already been registered for it. The capacity manager registers a new problem investigation for every threshold violation for which a problem investigation has not yet been registered.

Each new problem investigation is then assigned to the most appropriate specialist (in terms of skills, availability and access rights) to find out how incidents had best be avoided (e.g. by freeing up some of the currently utilized capacity, or by adding more capacity to the service infrastructure).

The Capacity Tracking procedure diagram is presented below.

Figure 2-4: Capacity Tracking



Change Management

The Change Management process consists of eight procedures: six for implementing planned changes, and two for implementing emergency changes.

The first procedure is called "Request for Change Review". This procedure is used by change coordinators when they are dealing with requests for change.

The second procedure is called "Change Planning". It is used by change coordinators and specialists to prepare the implementation plans for changes.

The third procedure is called "Change Approval". It is used by the change manager and approvers (i.e. customer representatives and service owners) to approve planned changes.

The fourth procedure is called "Infrastructure Change Implementation". It is used by specialists to implement infrastructure changes.

The fifth procedure is called "Application Change Implementation". It is used by specialists, release administrators, customer representatives and change coordinators to implement application changes.

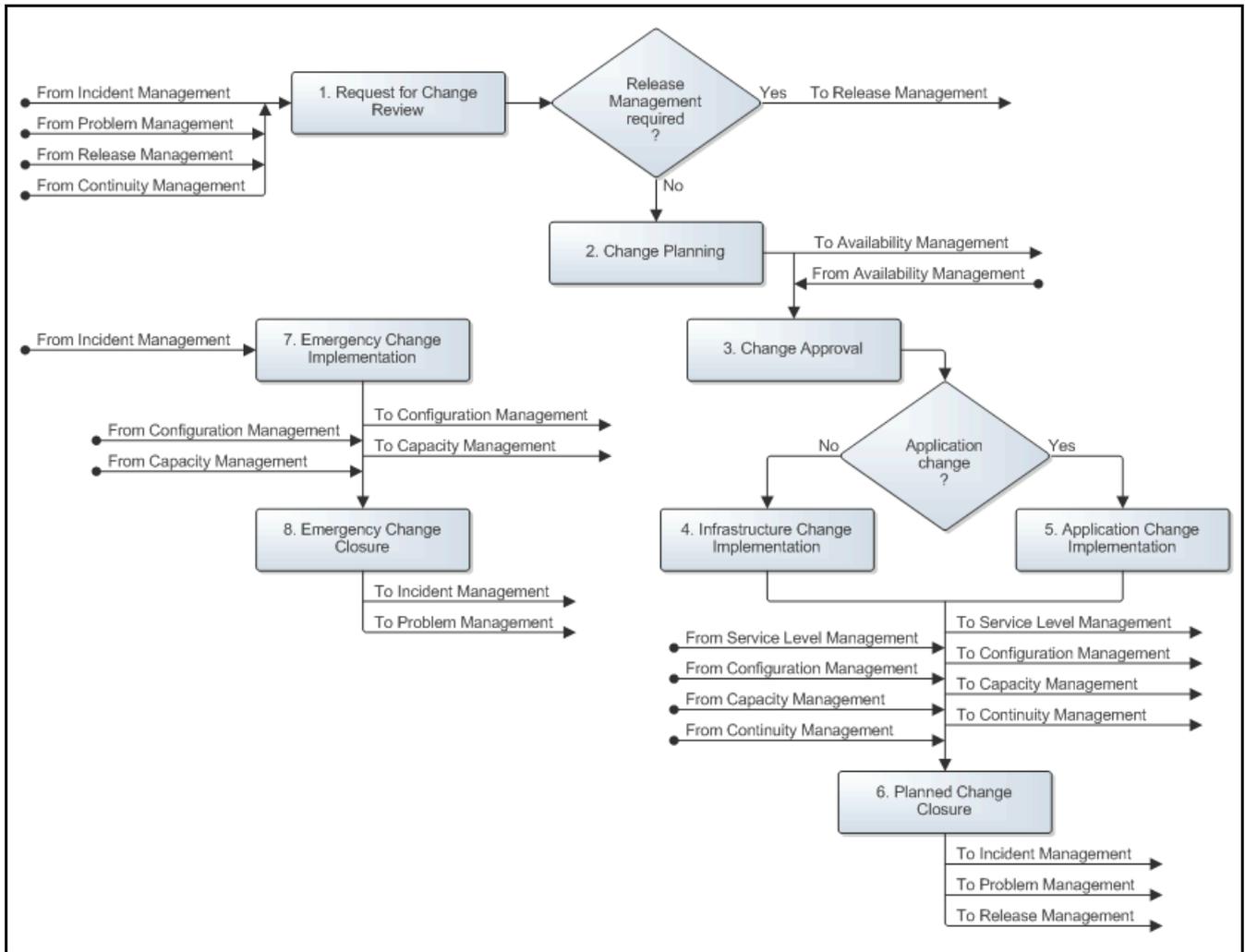
The sixth procedure is called "Planned Change Closure". It is used by specialists when they perform production tests after changes have been implemented and by change coordinators when they close out changes.

The seventh procedure is called "Emergency Change Implementation". This procedure is used by specialists and release administrators to implement changes to resolve incidents.

The eighth and last procedure is called "Emergency Change Closure". This procedure is used by specialists and change coordinators to complete and close out emergency changes.

A graphical representation of the process is provided on the next page. Each procedure is described in more detail in the sections that follow this diagram.

Figure 3-1: Change Management process



Procedure 1, Request for Change Review

The change coordinator receives the requests for change for the service(s) that he/she coordinates the change for. The requests for change can originate from the following five sources:

- Incident Management, in the form of incident requests which resolutions need to be implemented by Change Management.
- Incident Management, in the form of changes that were generated upon the submission of the Request form.
- Problem Management, in the form of known errors.

- Release Management, in the form of documents that detail the change requirements.
- Continuity Management, in the form of return-to-production requests from service owners following the recovery of service infrastructures at their continuity sites.

Upon receiving a request for change from Problem Management, the change coordinator determines if it can be added to a change that was already prepared earlier. If this is the case, the change coordinator links the new request for change to the existing change to optimize efficiency.

If the request for change asks for the implementation of a standard change, the change coordinator uses the appropriate change template to prepare the change.

If the request for change is not a request for a standard change, the change coordinator checks the request to ensure that it does not conflict with internal standards or policies. If it does conflict, the request for change is rejected and the requester is informed of the internal standard or policy that the request for change conflicts with.

If there is no conflict, the change coordinator determines whether the change implementation really needs to be coordinated by Change Management. This is only necessary when the implementation will cause:

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

If the change can be implemented without the involvement of Change Management, the change coordinator rejects the request for change and informs the requester that Change Management is not required.

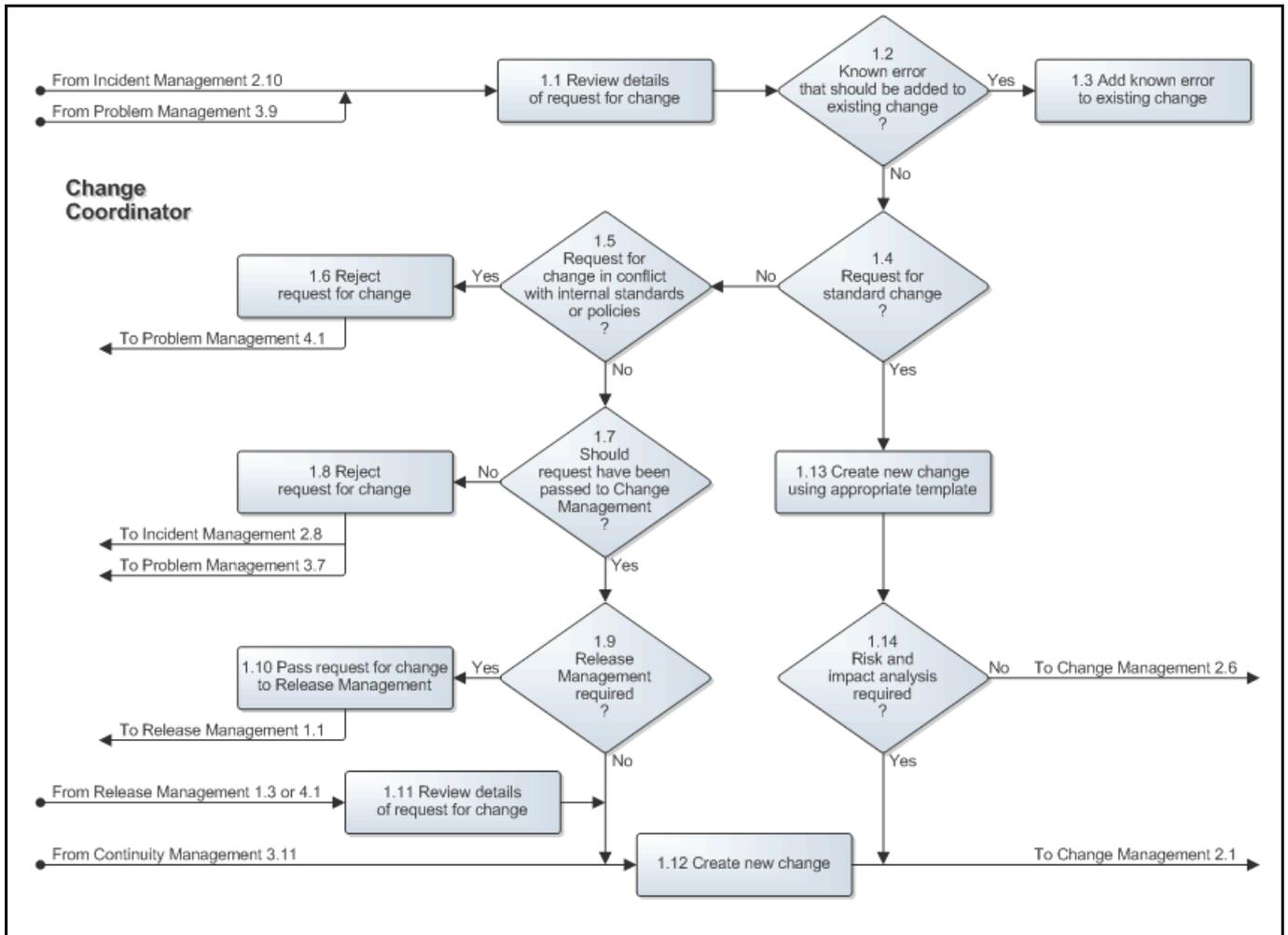
If it has been determined that Change Management is required for the implementation of the requested change, the change coordinator determines whether the request for change should be passed on to Release Management. Release Management is not required if the request for change asks for the prevention or fix of a problem, provided that:

- the change implementation can be coordinated by a single change coordinator.
- the implementation will not cause the functionality of the service to become different.
- no additional funding is required to complete the implementation.

If Release Management is not required, or if the request for change originated from Release or Continuity Management, the change coordinator selects the most appropriate change template and/or task (group) template(s) to register the change. All other requests for change are assigned to Release Management.

The Request for Change Review procedure diagram is presented on the next page.

Figure 3-2: Request for Change Review



Procedure 2, Change Planning

After having registered a new change, the change coordinator starts the risk & impact analysis phase by gathering the necessary information so that a change implementation plan can be created that minimizes both the risk of failure and the impact on user(s).

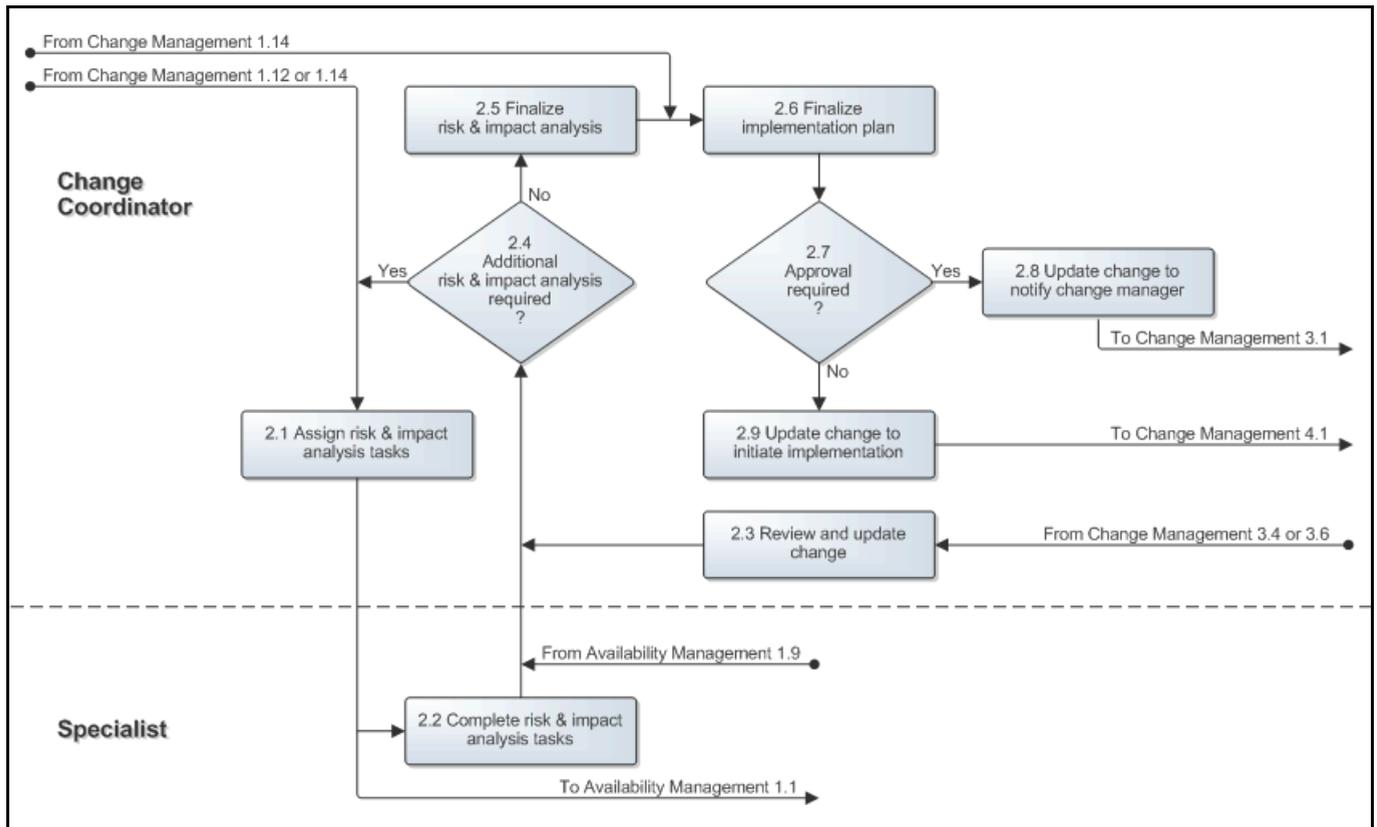
The change coordinator consults other specialists as needed to obtain this information. If a new service infrastructure is to be built, or if an existing service infrastructure is likely to require a modification in order to satisfy the change requirements, the change coordinator also requests the assistance from the availability manager for the creation of a new, or the modification of an existing, service infrastructure design.

Having gathered all the risk & impact information, the change coordinator finalizes the planning for the change implementation ensuring that the risk of failure and the impact on the user(s) is minimized.

If the change is a standard change for which the approval phase can be skipped, the change coordinator initiates the implementation of the change. On the other hand, if approval is required, the change coordinator asks the change manager to initiate the collection of the necessary approvals.

The Change Planning procedure diagram is presented below.

Figure 3-3: Change Planning



Procedure 3, Change Approval

After a change coordinator has informed the change manager that a change is ready for approval, the change manager reviews the change. If the change manager finds the change to be in conflict with internal standards or policies, he/she informs the change coordinator that the change cannot be implemented.

If the change is not in conflict with any internal standards or policies, the change manager reviews the risk assessment and the implementation plan. The change manager checks the plan to ensure that appropriate precautions have been planned to minimize both the risk of failure and the impact on the user(s), and that the timing of the implementation does not conflict with other planned changes or planned events.

If the risk & impact analysis is found to be insufficient, the change manager requests additional analysis from the change coordinator. Similarly, if the planning does not adequately address the risk of failure or the impact on the user(s), or if the planning conflicts with other planned changes or events, the change manager requests an adjustment of the implementation plan from the change coordinator.

On the other hand, if the risk & impact analysis and the planning of the implementation appear to be in order, the change manager ensures that the necessary approvals will be collected for the change.

Approval is required from the representatives of customers who will be affected by the change implementation, if it will cause:

- a service to become unavailable or degraded during service hours.
- the functionality of a service to become different.

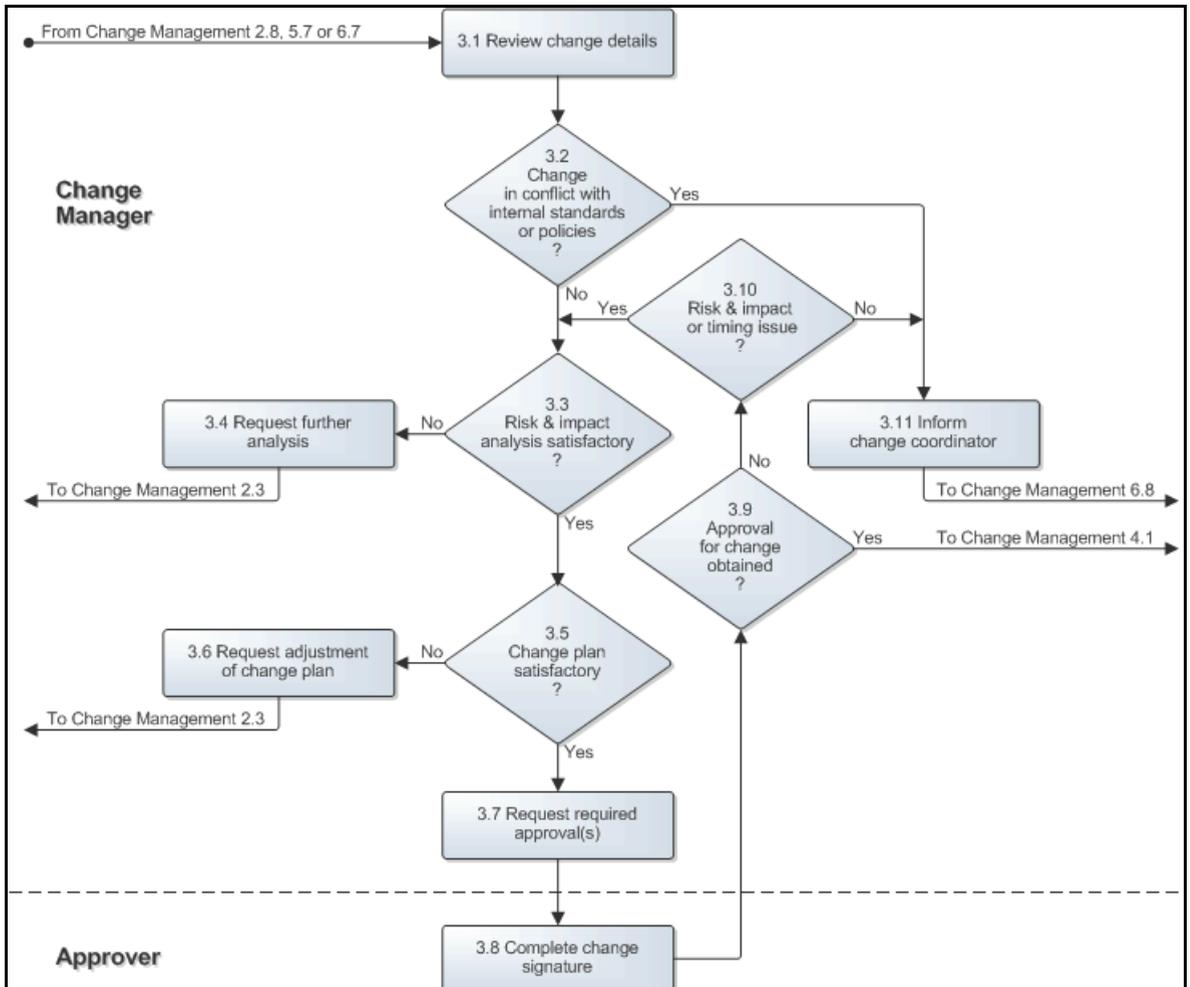
Approval from the service owner is sufficient if these conditions do not apply to the planned implementation.

If the change is rejected by an approver, the change manager finds out why. The change manager asks the change coordinator to perform additional risk & impact analysis or to adjust the planning if that was the reason why the change was rejected.

If the change was rejected for any other reason, the change manager informs the change coordinator that the change cannot be implemented.

The Change Approval procedure diagram is presented on the next page.

Figure 3-4: Change Approval



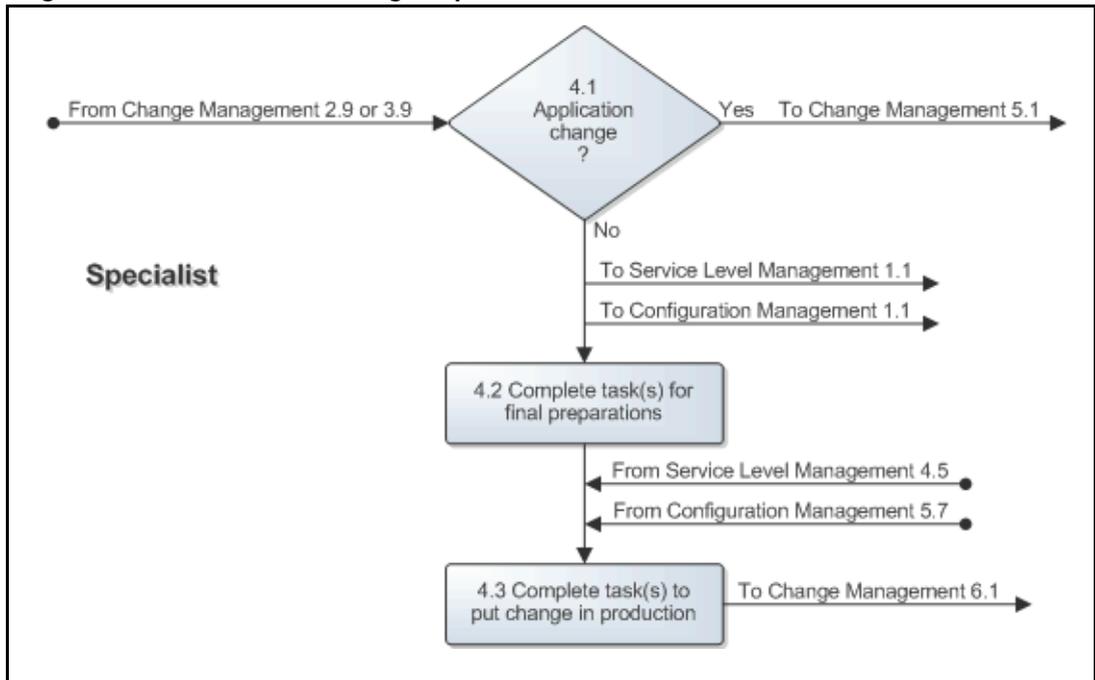
Procedure 4, Infrastructure Change Implementation

If the change concerns an application change, the implementation continues in Procedure 5, Application Change Implementation. The first task(s) of an infrastructure change, however, are assigned to the specialist(s) for the preparation of the implementation (i.e. to ensure operational readiness). This can involve ordering hardware, configuring a test environment, performing tests, etc.

When everything is ready, the specialist(s) receive and complete the task(s) for the actual implementation of the change.

The Infrastructure Change Implementation procedure diagram is presented below.

Figure 3-5: Infrastructure Change Implementation



Procedure 5, Application Change Implementation

After the first implementation task(s) of the application change have been assigned, one or more specialists develop the new release in the development environment. The new release is tested by the specialist(s) to ensure that the change requirements have been met. This is done in a separate test environment if one has been made available for this purpose. Otherwise, the tests are performed in the development environment. The (automated) scripts for regression testing are also updated and run by the specialist(s) if such scripts are available for the application. The specialist(s) fix any errors that were encountered during the tests in the development environment.

Once the specialist(s) have confirmed that the change requirements have been met and that no new bugs have been introduced, the release administrator transfers the new release to the test environment where the customer representative(s) ensure that it gets tested.

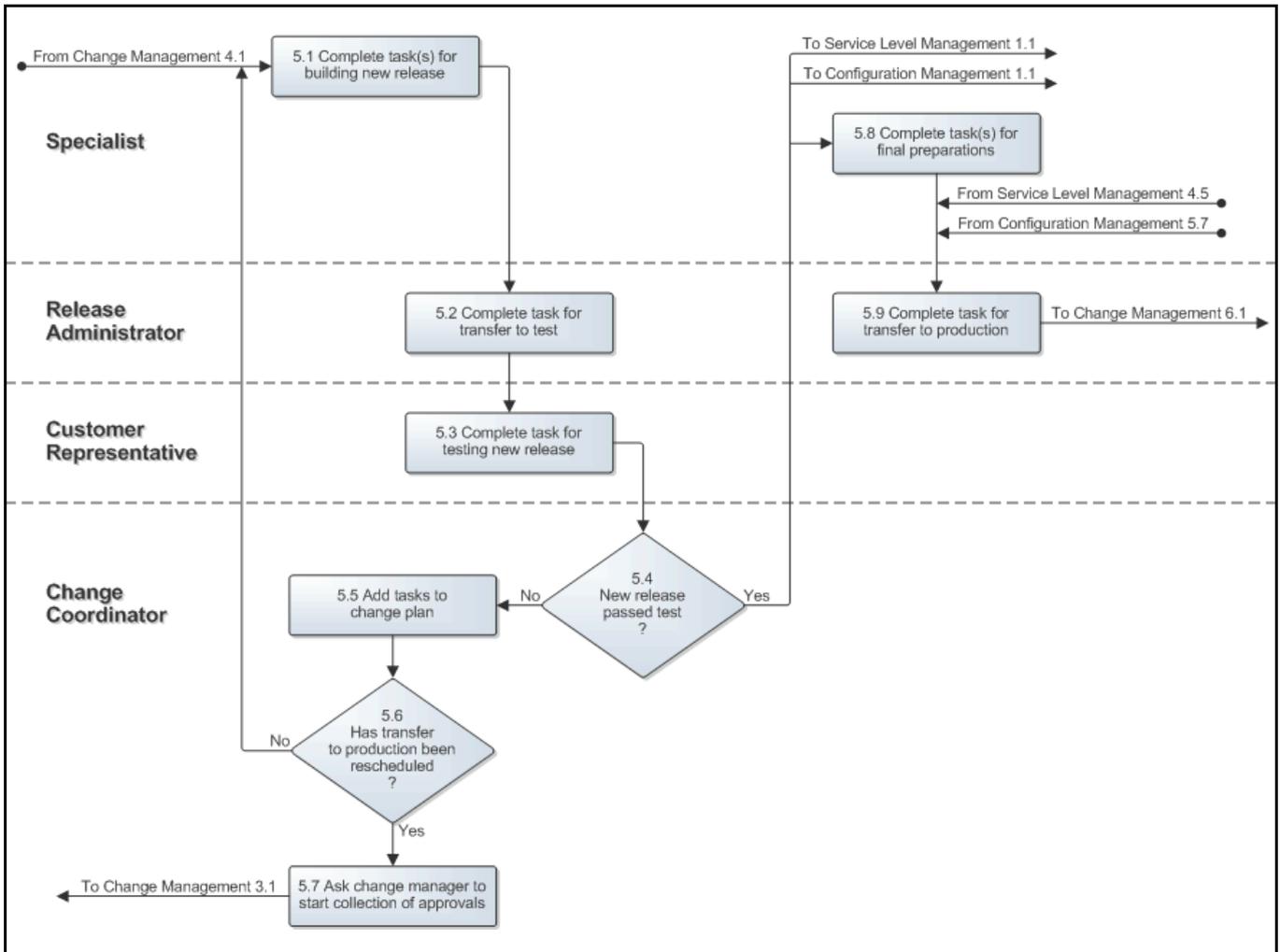
The change coordinator creates and assigns additional tasks if the new release did not pass customer testing, so that the new release can be corrected. If these additional tasks caused the transfer to production to be rescheduled, the change will need to be approved again.

Once the new release has passed customer testing, the specialist(s) ensure that everything is ready to take the new release into production (i.e. ensure operational readiness). This could involve user training, the addition of storage capacity to the production and continuity environments, ordering additional software licenses, etc.

Finally, the release administrator transfers the new release into production.

The Application Change Implementation procedure diagram is presented on the next page.

Figure 3-6: Application Change Implementation



Procedure 6, Planned Change Closure

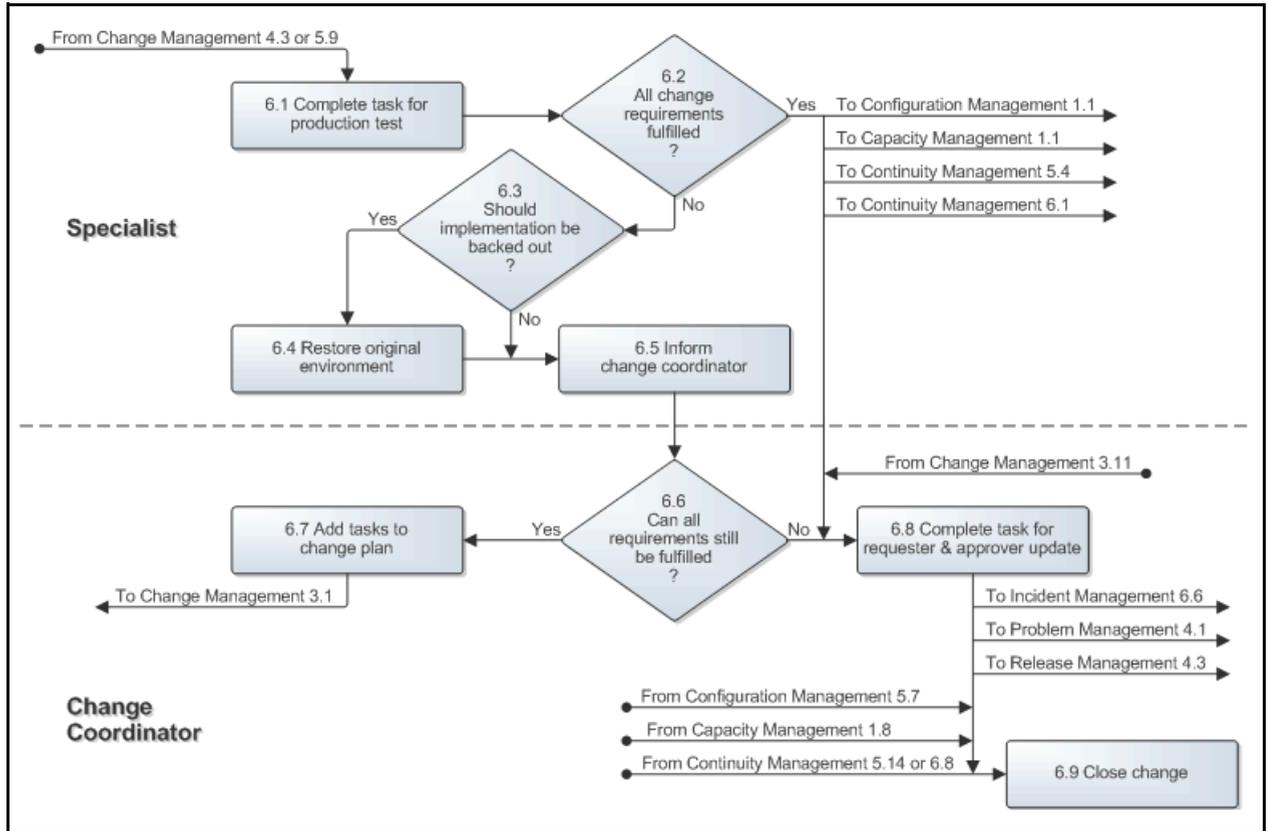
After the change has been put into production, a specialist (with the help of a user if the specialist does not have sufficient access rights) performs the production test to verify the success of the implementation. The CMDB, the Capacity Management and the Continuity Management information is updated as needed after the specialist has determined that all the requirements of the change have been met.

If all change requirements have not been fulfilled, however, the specialist who performed the production test determines if the change implementation should be backed out. The change is backed out if its implementation does not provide an improvement over the previous situation, or causes a security or data integrity risk. If the unsuccessful change implementation can still be made into a success, the change coordinator creates and assigns the necessary additional tasks.

Before closing a change, the change coordinator ensures that its requesters and approvers are informed.

The Planned Change Closure procedure diagram is presented below.

Figure 3-7: Planned Change Closure



Procedure 7, Emergency Change Implementation

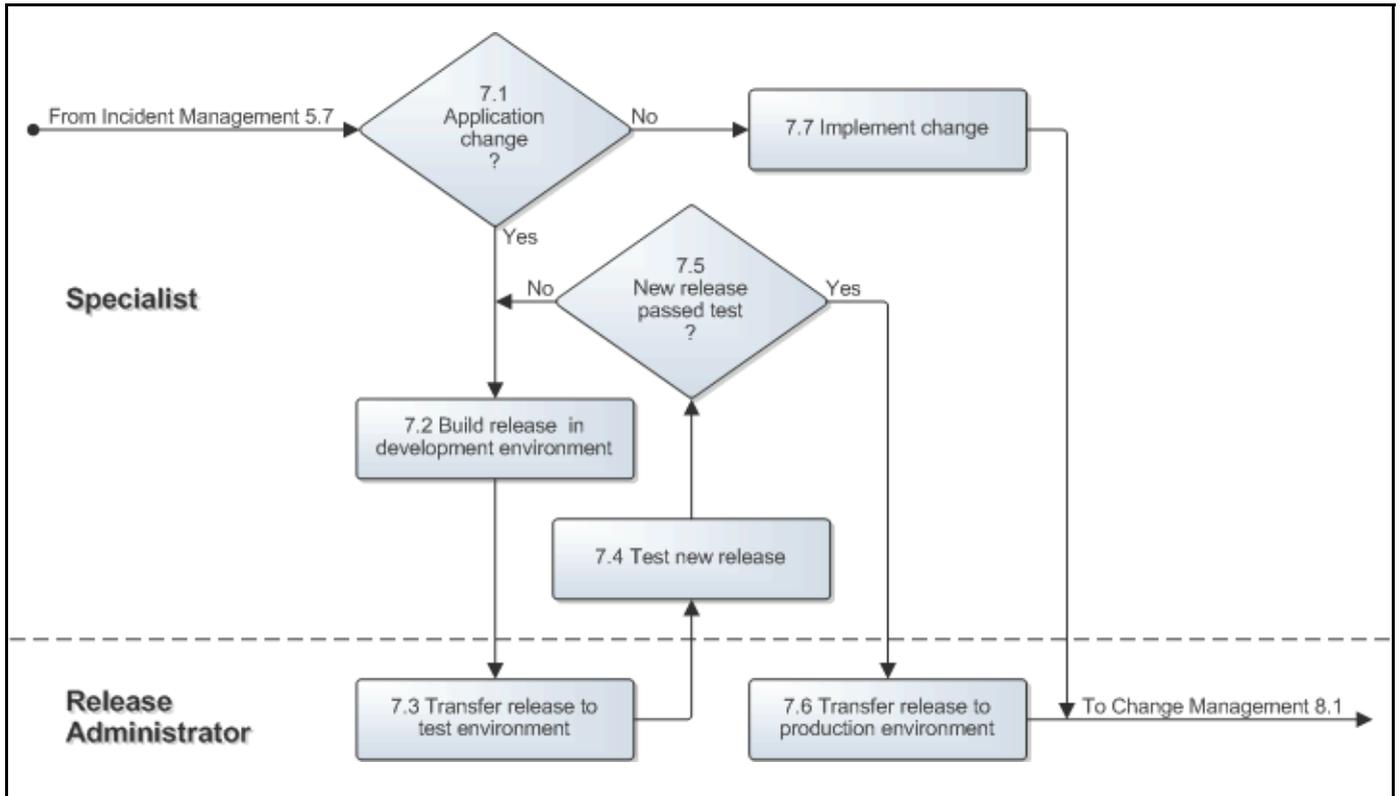
After the service owner (or on-duty manager if the service owner was not available) has asked a specialist to resolve an incident by implementing an emergency change, the specialist starts to work on the implementation. If the emergency change concerns an infrastructure change, the specialist performs the implementation as if completing a normal incident request.

Alternatively, if the emergency change is an application change, the specialist first builds a new release in the development environment and makes sure that it will fix the incident without introducing new bugs. The specialist subsequently asks a release administrator to transfer the new release to the test environment. In the test environment, the specialist tests the new release.

If the new release did not pass the test, the specialist goes back to the development environment to correct it. On the other hand, if the new release passed the tests, the specialist asks the release administrator to transfer it to the production environment.

The Emergency Change Implementation procedure diagram is presented below.

Figure 3-8: Emergency Change Implementation



Procedure 8, Emergency Change Closure

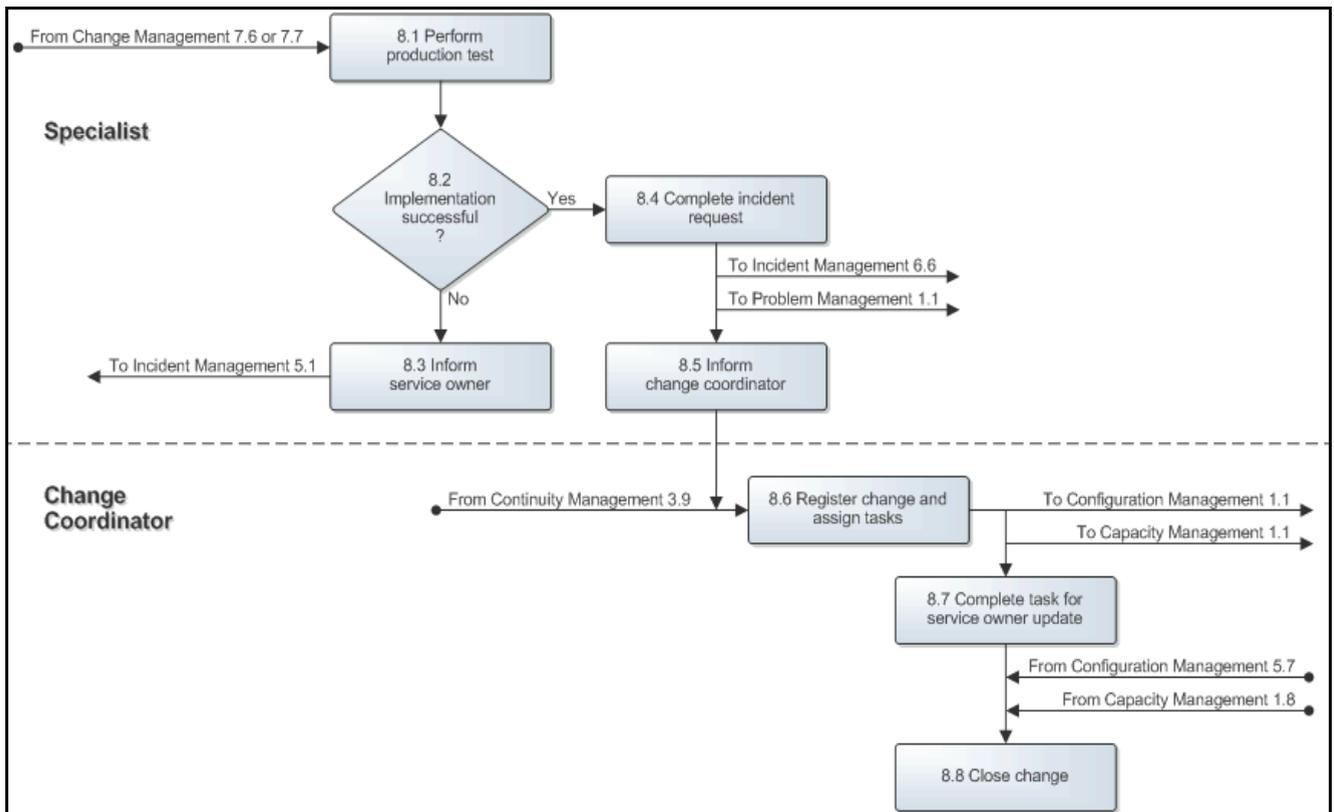
The specialist performs the production test (with the help of a user if the specialist does not have sufficient access rights) after the implementation has been completed. If the implementation turns out to be unsuccessful, the specialist informs the service owner (or on-duty manager if the service owner is not available) to discuss the situation.

Conversely, if the specialist has determined that the implementation is successful, he/she completes the incident request. In addition, the specialist asks the change coordinator of the affected service to register a change in the service management application for the emergency change that he/she just implemented.

The change coordinator registers the change and, if required, ensures that the CMDB and the Capacity Management information are updated. Before closing the change, the change coordinator informs the service owner (and the on-duty manager if he/she approved the emergency change implementation) via email that the emergency change has been implemented successfully.

The Emergency Change Closure procedure diagram is presented on the next page.

Figure 3-9: Emergency Change Closure



Configuration Management

The Configuration Management process consists of five procedures.

The first procedure is called "CI Requisition". It is used by configuration administrators, purchasing agents and approvers to order new CIs.

The second procedure is called "Supplier Information Maintenance". Configuration administrators use this procedure when they register new suppliers and when they update the contact details of previously registered suppliers.

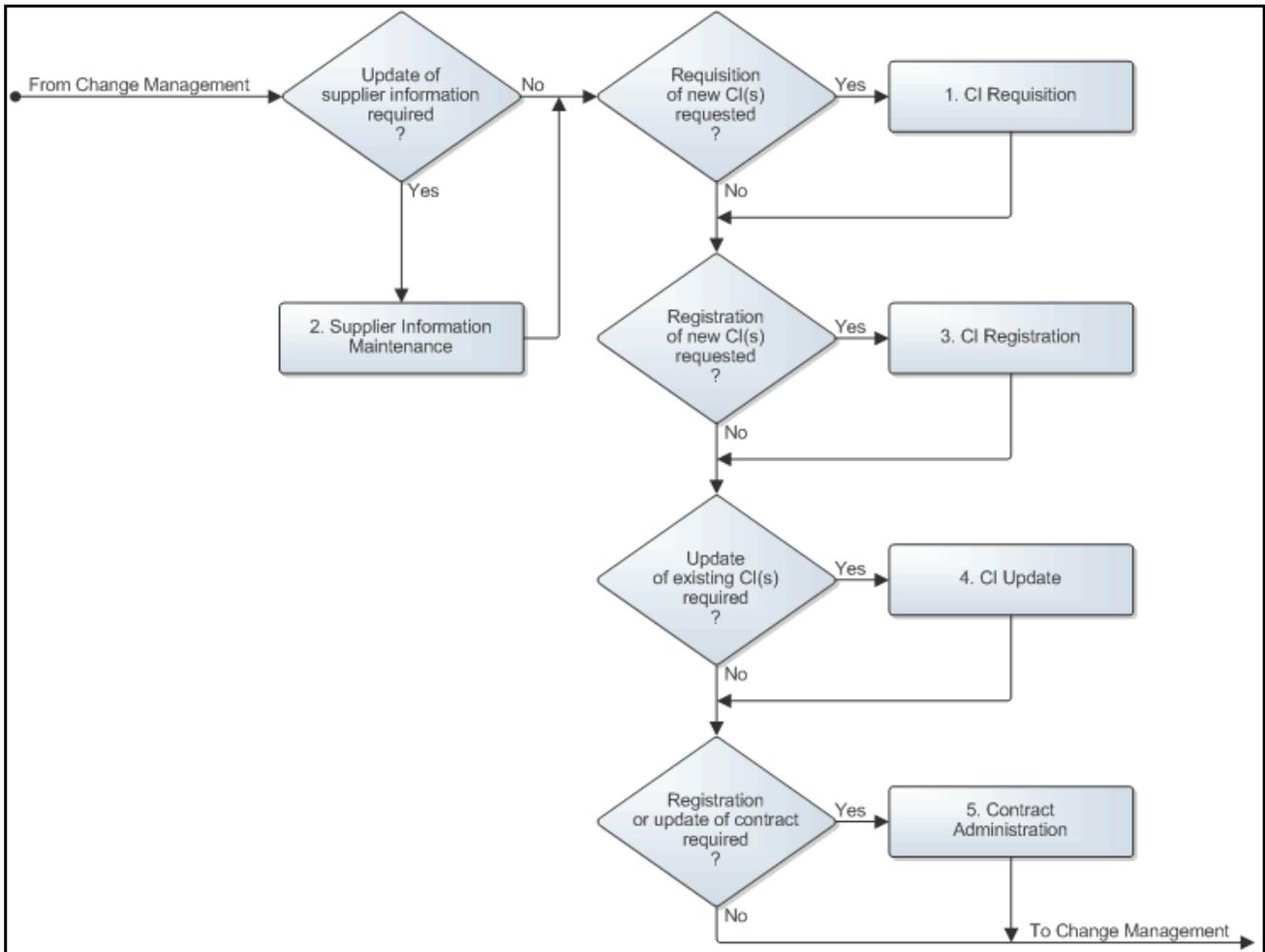
The third procedure is called "CI Registration". This procedure is used by configuration administrators and purchasing agents when they register new CIs in the CMDB.

The fourth procedure is called "CI Update". It is used by configuration administrators when they update the attributes and/or relations of CIs that were already registered in the CMDB.

The fifth procedure is called "Contract Administration". It is used by configuration administrators when they register or update the contracts for the CIs registered in the CMDB.

A graphical representation of the process is provided on the next page. Each procedure is described in more detail in the sections that follow this diagram.

Figure 4-1: Configuration Management process description



Procedure 1, CI Requisition

Tasks for CI requisition or for the update of the CMDB are assigned to configuration administrators by change coordinators when new CIs need to be ordered, when the information concerning existing CIs needs to be updated, or when a contract or license certificate needs to be added or updated.

After such a task has been assigned to a configuration administrator, he/she reviews its details. The configuration administrator goes directly to Procedure 3, CI Registration if the task does not request the requisition of one or more CI(s).

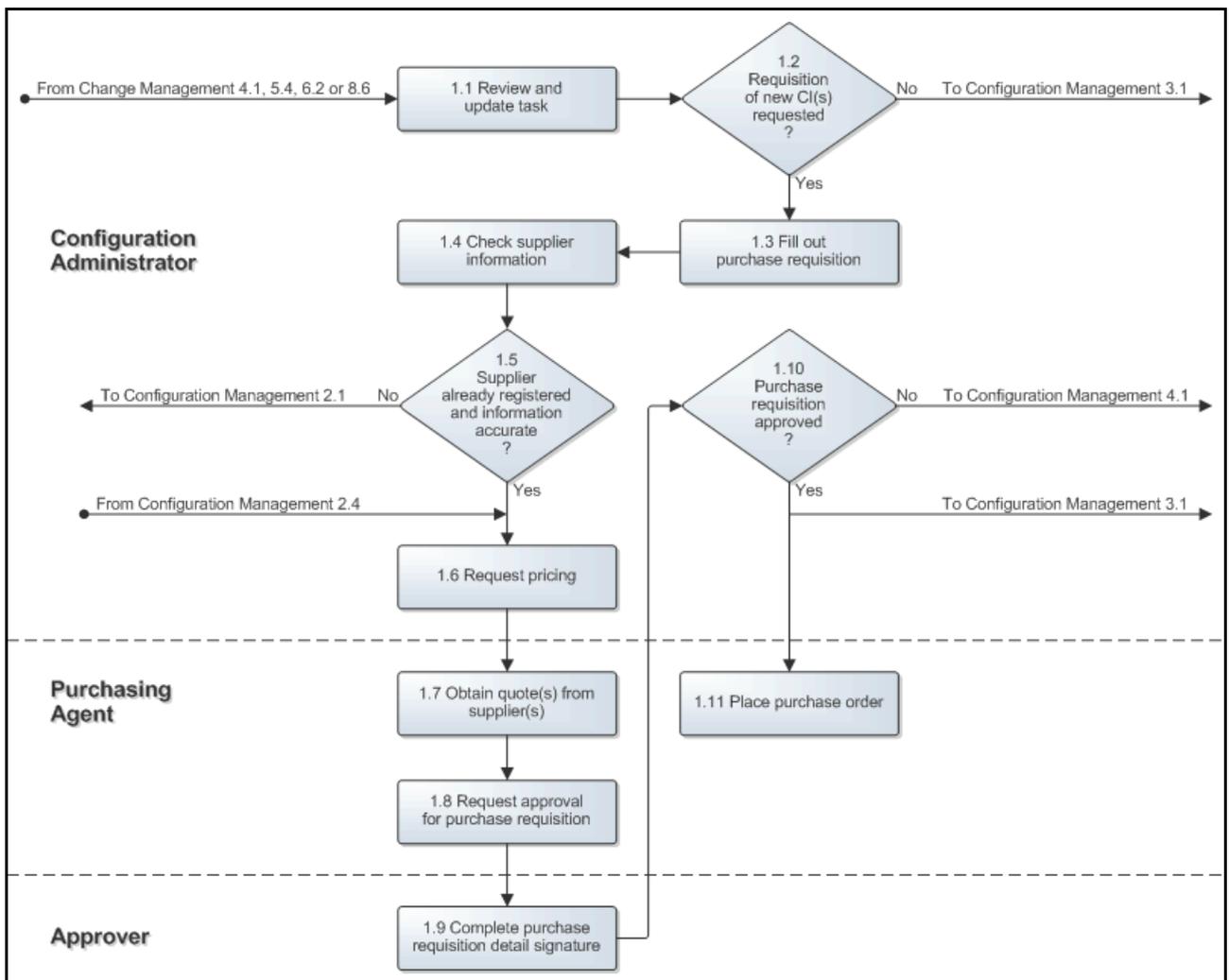
If new CI(s) are to be ordered, however, the configuration administrator fills out a purchase requisition. He/she also checks the service management application to see if the contact details of the suppliers, which should be asked to submit quotes, are up-to-date. If a supplier has not yet been registered, or if its contact details are no longer up-to-date, the configuration administrator ensures that the supplier information is registered or updated in Procedure 2, Supplier Information Maintenance.

Having ensured that the supplier contact details are up-to-date, the configuration administrator submits the purchase requisition, thereby requesting pricing from purchasing. A purchasing agent then obtains the necessary quotes from suppliers. After the quotes have been received, he/she requests approval for the purchase requisition.

The approvers review the purchase requisition and either reject or approve it. If it is approved, the purchasing agent orders the requested CI(s). If the purchase requisition is rejected, however, the configuration administrator continues in Procedure 4, CI update to determine whether the task also requested existing CI information to be updated.

The CI Requisition procedure diagram is presented on the next page.

Figure 4-2: CI Requisition



Procedure 2, Supplier Information Maintenance

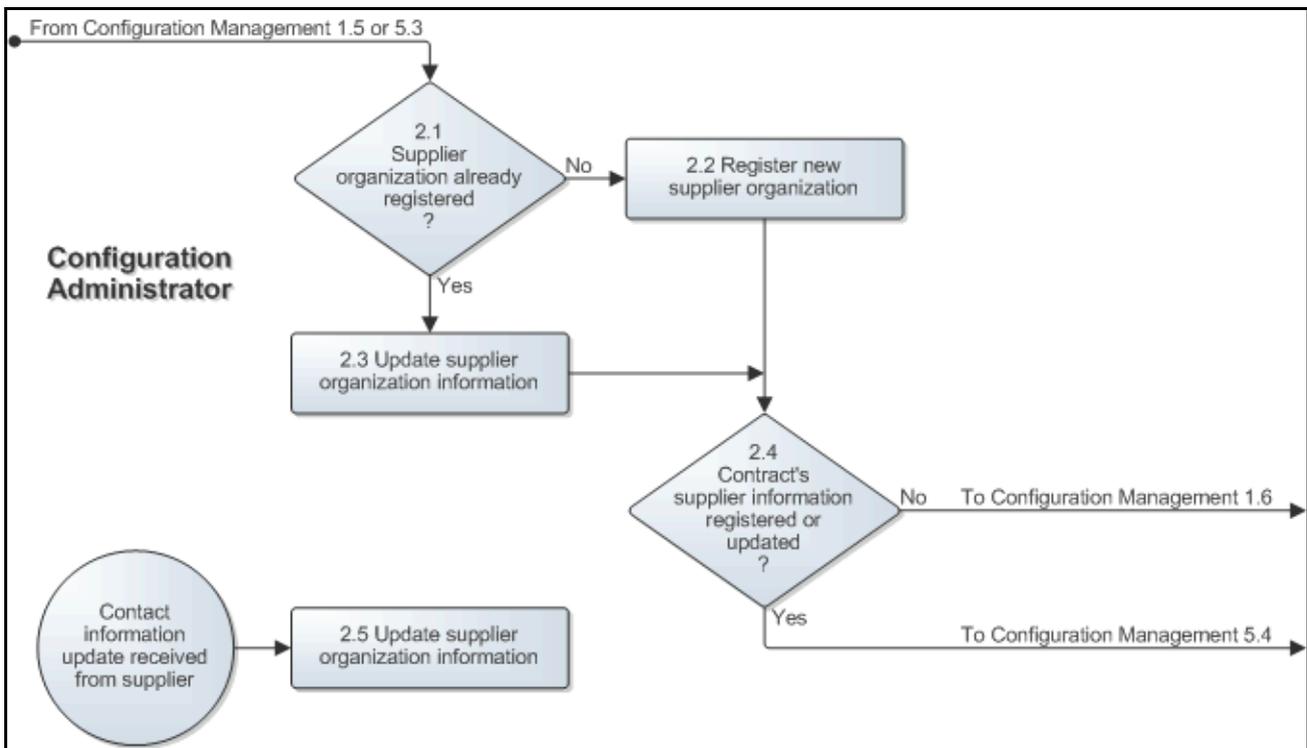
The configuration administrators are responsible for registering and updating the information of organizations that supply configuration items and/or support to the service provider organization.

A configuration administrator performs the supplier information maintenance tasks as needed while filling out purchase requisitions, before registering or updating contracts, and whenever updated contact information has been received from an existing supplier.

If a supplier organization is not already registered, the configuration administrator adds it. If the supplier organization already exists in the service management application, the configuration administrator updates its contact details as needed. This is done in accordance with the field utilization guidelines for the supplier information forms that are available in the service management application for maintaining the contact details of supplier organizations and persons who work for these companies.

The Supplier Information Maintenance procedure diagram is presented below.

Figure 4-3: Supplier Information Maintenance



Procedure 3, CI Registration

If the task from Change Management does not require any new CIs to be added to the CMDB, the configuration administrator goes directly to Procedure 4, CI Update.

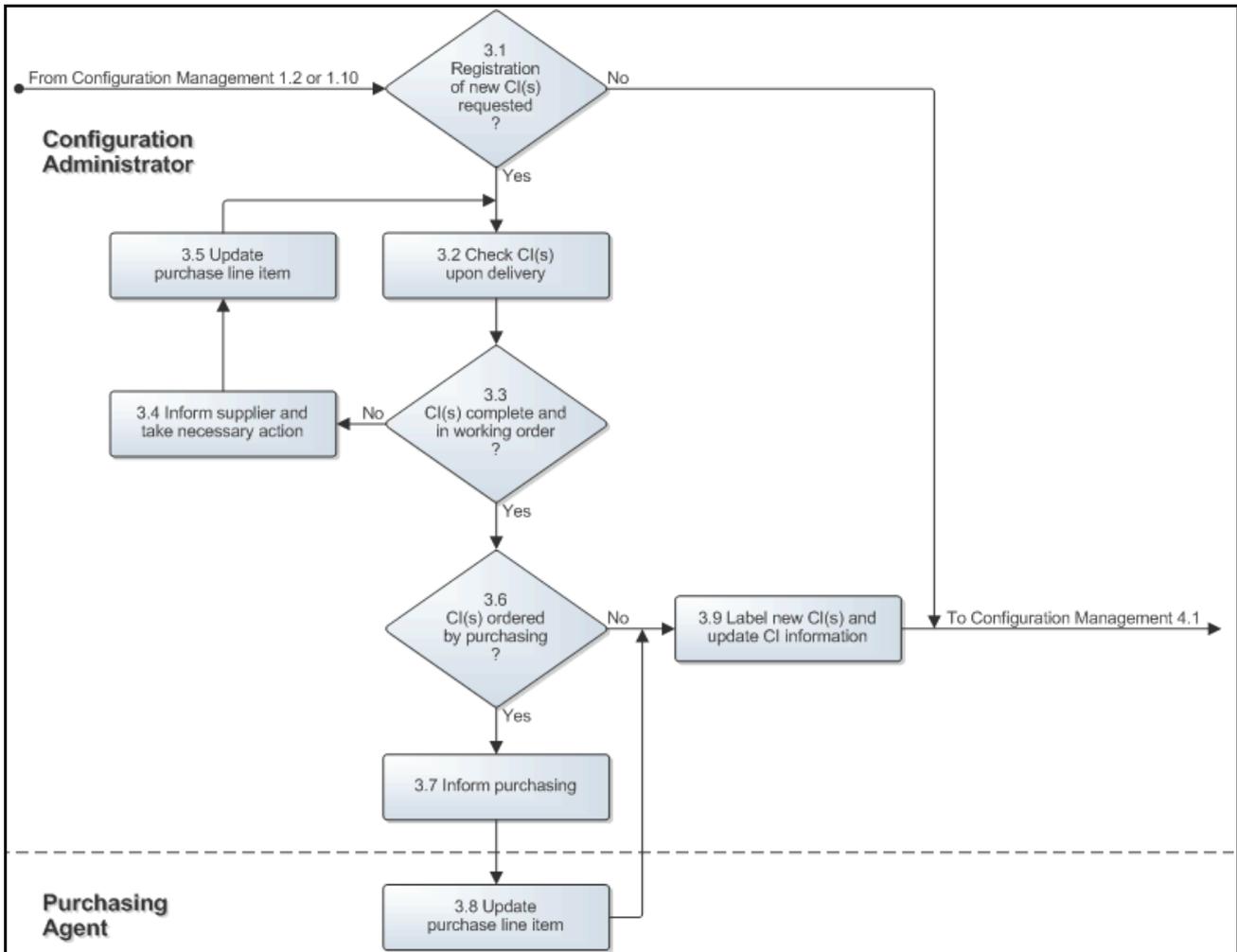
On the other hand, if the task requests the registration of one or more CIs for which a formal purchase requisition was not submitted (e.g. in the case of internally developed software), or if one or more new CIs were ordered in Procedure 1, CI Requisition, the configuration administrator first checks the CI(s) after they have been delivered. He/she does this to ensure that the correct hardware, software and/or software licenses have been received, that no items are missing, and that the CI(s) are not damaged. If the delivery is not whole, the configuration administrator informs the supplier and subsequently informs the change coordinator of the delay by updating the purchase line item associated with the ordered CIs.

Conversely, if the CI(s) were ordered by purchasing and have been received in good condition, the configuration administrator informs the purchasing agent who then updates the purchase line item to ensure that the CIs are registered in the CMDB. If a formal purchase requisition was not submitted, and the CI(s) have been received in good condition, the configuration administrator registers the new CI(s).

The configuration administrator ensures that the necessary attributes (e.g. the serial number) are specified for each new CI and that it is related to other CI records, services and users as needed. All this is done in accordance with the field utilization guidelines for the forms that are available in the service management application for maintaining the CMDB.

The CI Registration procedure diagram is presented on the next page.

Figure 4-4: CI Registration



Procedure 4, CI Update

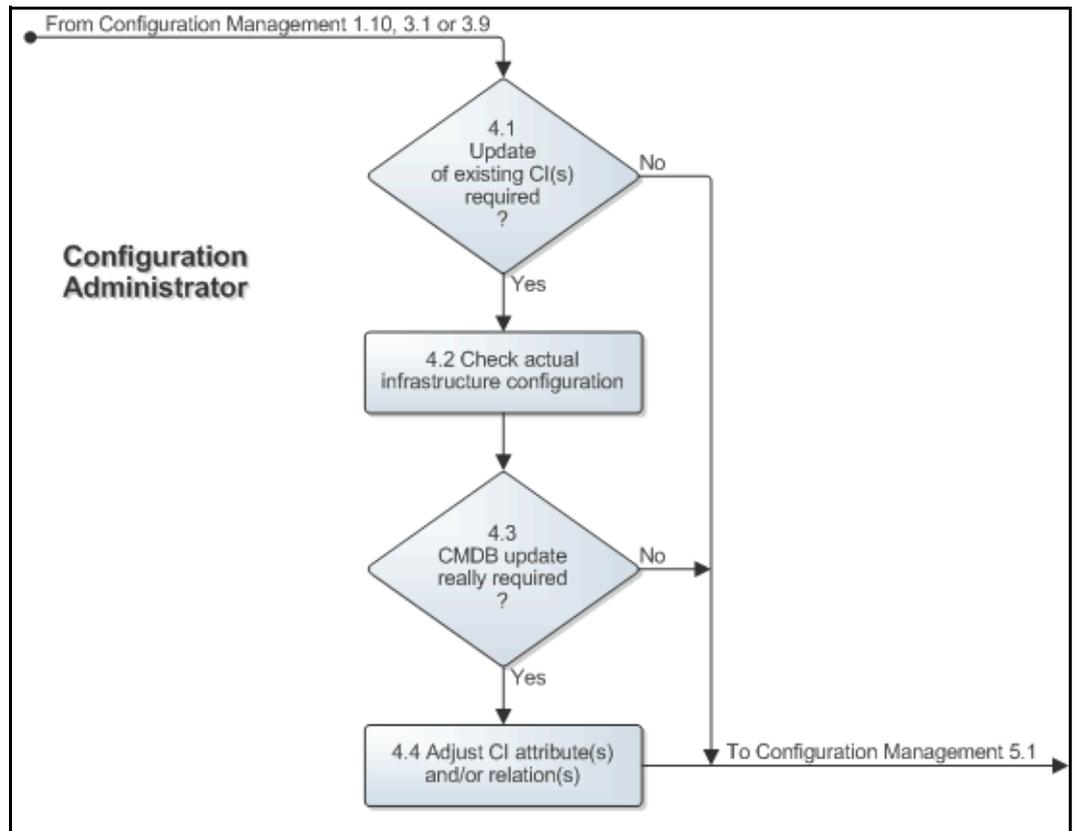
When the configuration administrator is dealing with a task requesting the update of CI attributes and/or relations, he/she checks the actual configuration of the infrastructure to confirm that the requested CMDB modifications are really required to bring the CMDB back up-to-date.

If it turns out that the CMDB should be updated, the configuration administrator performs the update of the necessary CI attributes and/or relations. This is done in accordance with the field utilization guidelines for the forms that are available in the service management application for maintaining the CMDB.

After having updated the CMDB, or if it turned out that the CMDB did not need to be updated, the configuration administrator moves on to Procedure 5, Contract Administration.

The CI Update procedure diagram is presented below.

Figure 4-5: CI Update



Procedure 5, Contract Administration

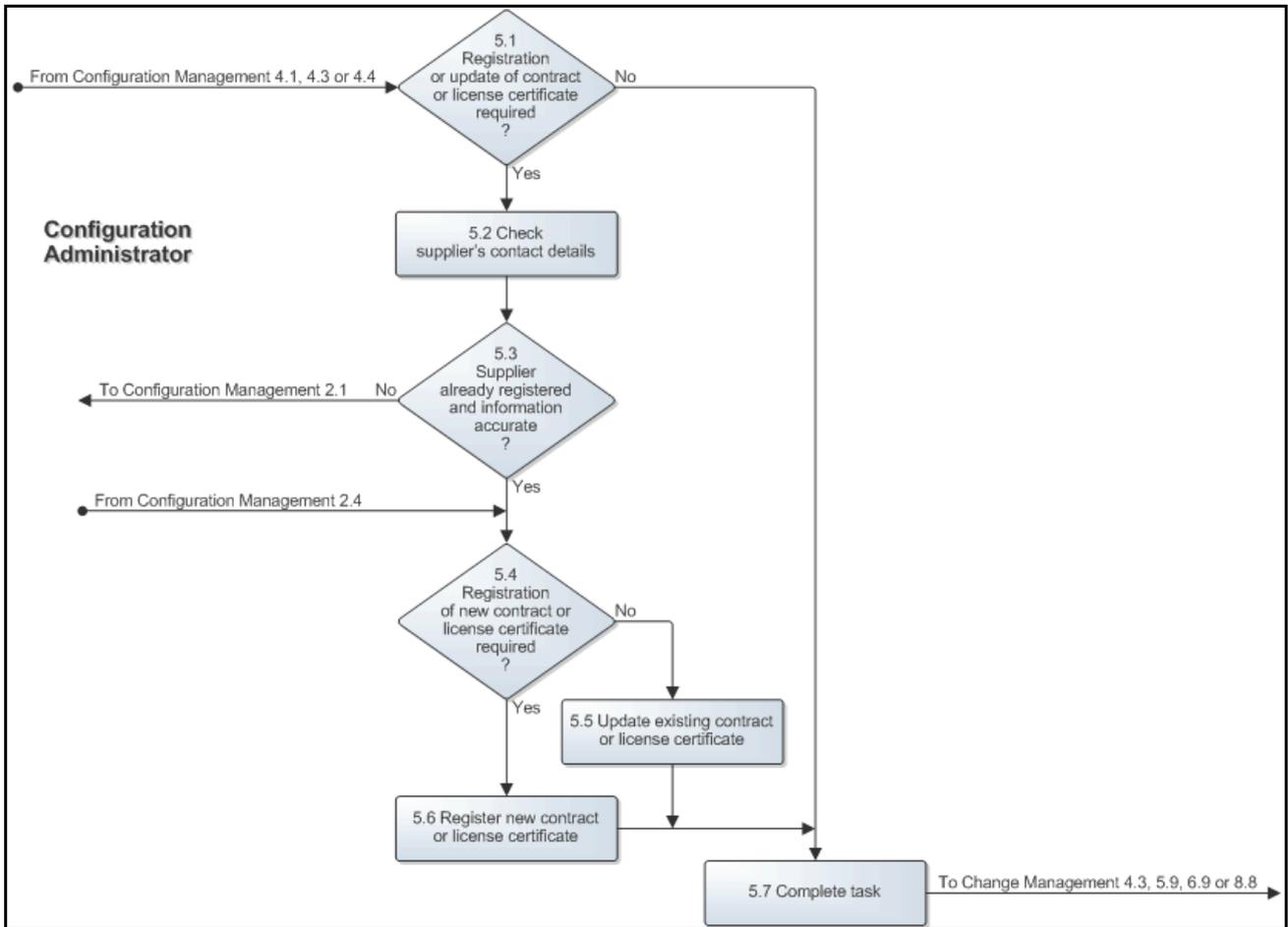
Before registering a new, or updating an existing, contract or license certificate, the configuration administrator first ensures that the contact details of its supplier exist. If the supplier organization of the contract or license certificate has already been registered, the configuration administrator checks the registered contact details to see if they are still up-to-date. If the supplier has not yet been registered, or if its contact details are no longer up-to-date, the configuration administrator ensures that the supplier information is registered or updated by following Procedure 2, Supplier Information Maintenance.

Having ensured that the contact details of the supplier are registered and up-to-date, the configuration administrator registers or updates the contract or license certificate in accordance with the field utilization guidelines for the contracts forms that are available in the service management application.

After the contract or license certificate information has been updated, or if the task does not request the registration or update of contracts or license certificates, the configuration administrator closes the task.

The Contract Administration procedure diagram is presented on the next page.

Figure 4-6: Contract Administration



Continuity Management

The Continuity Management process consists of six procedures.

The first procedure is called "Disaster Notification Handling". When the on-duty manager is notified of an (impending) disaster, he/she uses this procedure and the situation assessment checklist to determine whether or not services are to be recovered at their respective continuity sites.

The second procedure is called "Service Recovery". It is used by the on-duty manager and the recovery teams for the recovery of services at their respective continuity sites.

The third procedure is called "Return to Production". After the successful completion of a service recovery, this procedure is used by the continuity manager, service recovery team members, service owners and change coordinators of the recovered services. They follow this procedure to initiate the return of the service delivery from a continuity mode back to the normal production mode.

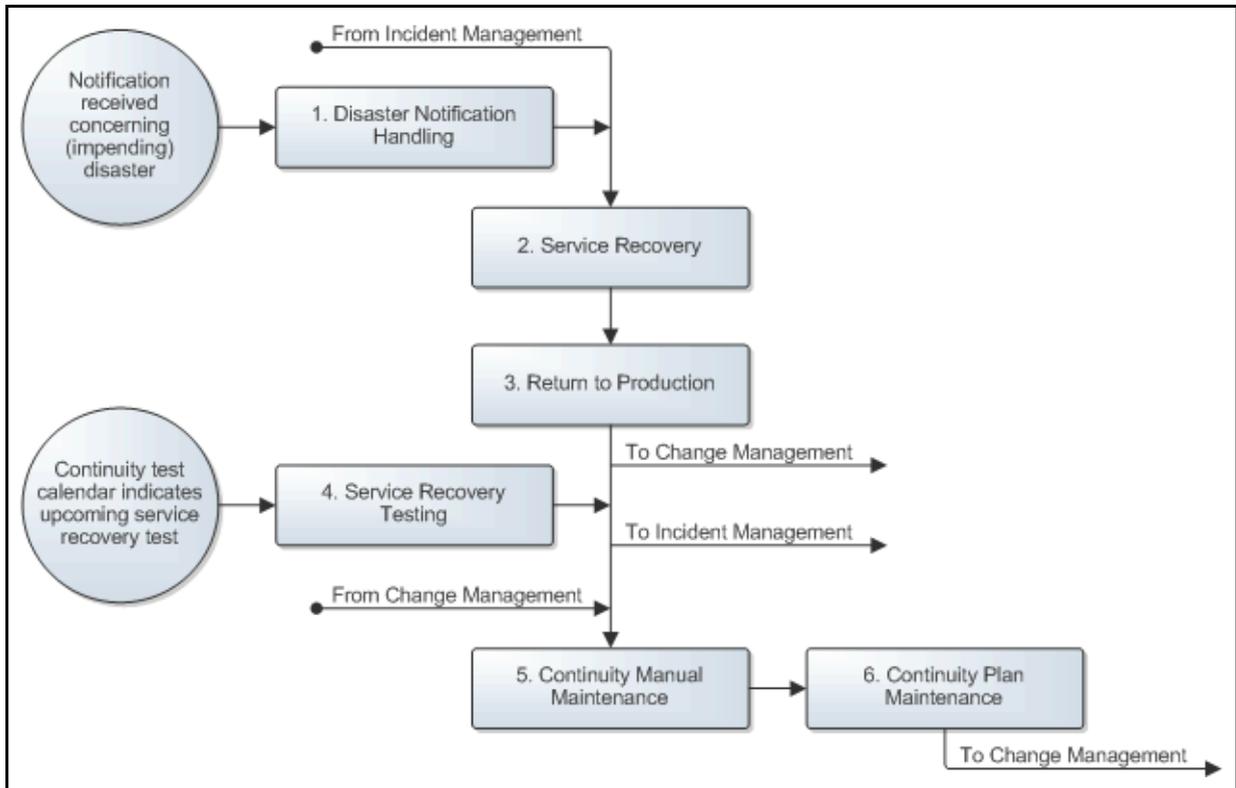
The fourth procedure is called "Service Recovery Testing". It is used by the continuity manager to ensure that the instructions in the continuity manual and the continuity plans can be relied on for the recovery of services at their respective continuity sites.

The fifth procedure is called "Continuity Manual Maintenance". This procedure is used by the continuity manager to maintain the continuity manual, and to distribute new versions of this manual and continuity plans after they have been approved.

The sixth and last procedure is called "Continuity Plan Maintenance". This procedure is used by continuity planners to prepare and maintain the continuity plans for the service infrastructures that are covered by a continuity target specified in an active SLA.

A graphical representation of the process is provided on the next page. Each procedure is described in more detail in the sections that follow this diagram.

Figure 5-1: Continuity Management process description



Procedure 1, Disaster Notification Handling

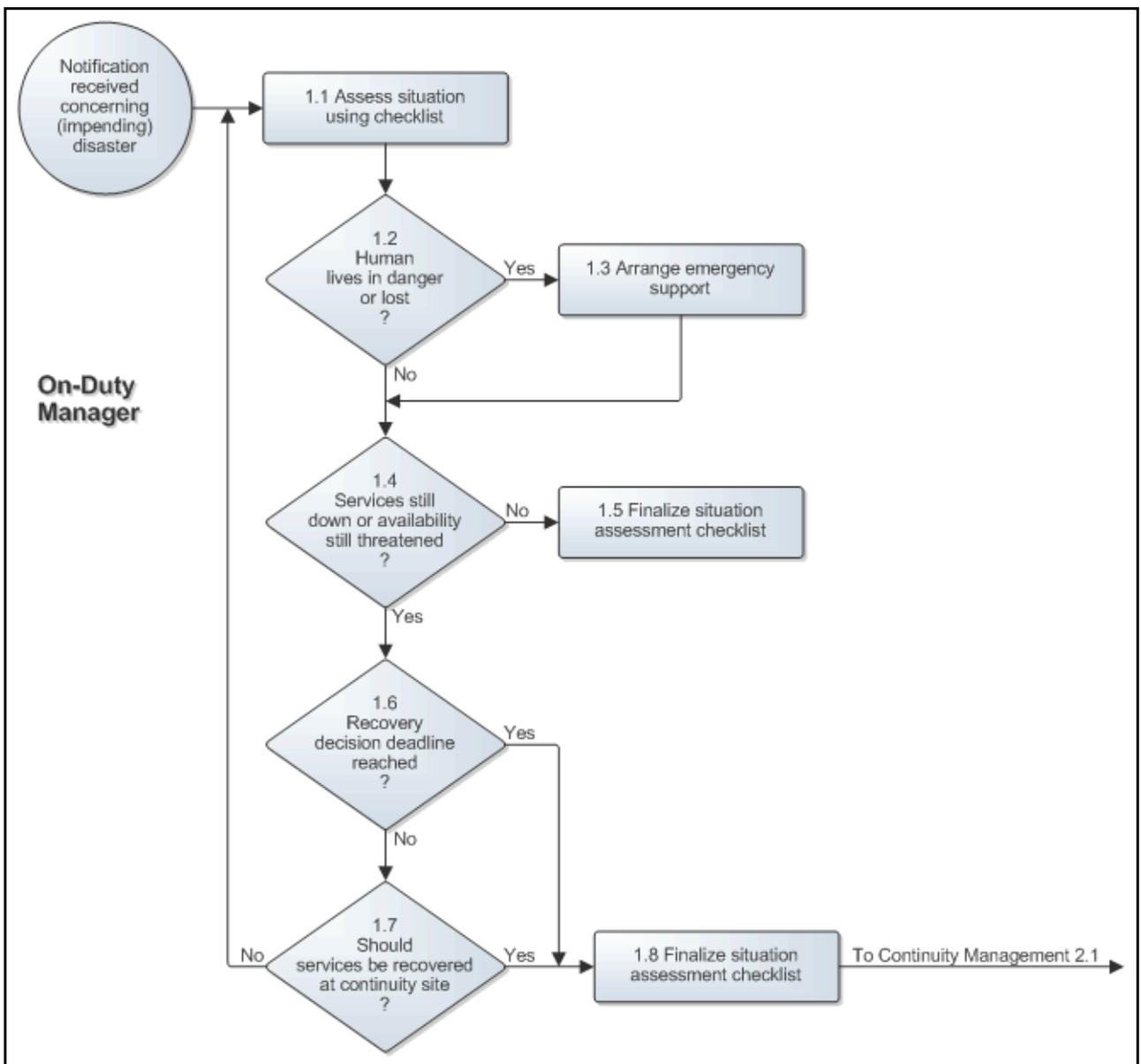
The on-duty manager takes out a copy of the Situation Assessment Checklist after someone has informed him/her that a disaster has struck, or is about to strike. Using the situation assessment checklist, the on-duty manager first determines whether people are in danger, have been injured, or have lost their lives. If this is the case, the on-duty manager makes sure that emergency support is provided (e.g. by calling security).

If emergency support is not required, or once this has been arranged, the on-duty manager finds out whether any services have become unavailable, or could go down, due to the disaster. If the (impending) disaster has not caused any service outages, and is not threatening the availability of any services (e.g. in case of a false alarm), the on-duty manager completes the situation assessment checklist by filling out why this conclusion was drawn.

On the other hand, if services are down or threatened because of the disaster, the on-duty manager uses the situation assessment checklist to decide whether a service recovery needs to be initiated. This needs to be done right away if the disaster has already caused one or more services to be down for so long that the recovery decision deadline has been reached. If the recovery decision deadline has not yet been reached, the situation assessment checklist guides the on-duty manager towards the decision to either re-evaluate the situation, or to initiate a service recovery. In the latter case, the on-duty manager writes down why he/she decided that a service recovery is required, and thereby completes the situation assessment checklist.

The Disaster Notification Handling procedure diagram is presented below.

Figure 5-2: Disaster Notification Handling



Procedure 2, Service Recovery

After the decision has been made to initiate a service recovery, the on-duty manager determines the appropriate number of people required for each team to perform the recovery in an efficient manner. The on-duty manager uses the contact details listed in the continuity manual to call these people out to the recovery control room from which the service recovery will be coordinated. As the members of the teams arrive in the recovery control room, the on-duty manager assigns them the tasks that need to be performed.

The members of the customer liaison team ensure that the following people are kept up-to-date on the progress of the service recovery:

- the representatives of the affected customer(s).
- the owners of the affected service(s).
- the service level manager(s) of the affected customer(s).
- the service desk analysts.
- the operators.

The recovery support team members make sure that everyone working on the service recovery receives the supplies they need and that they are taken care of in terms of meals, travel, accommodation, etc.

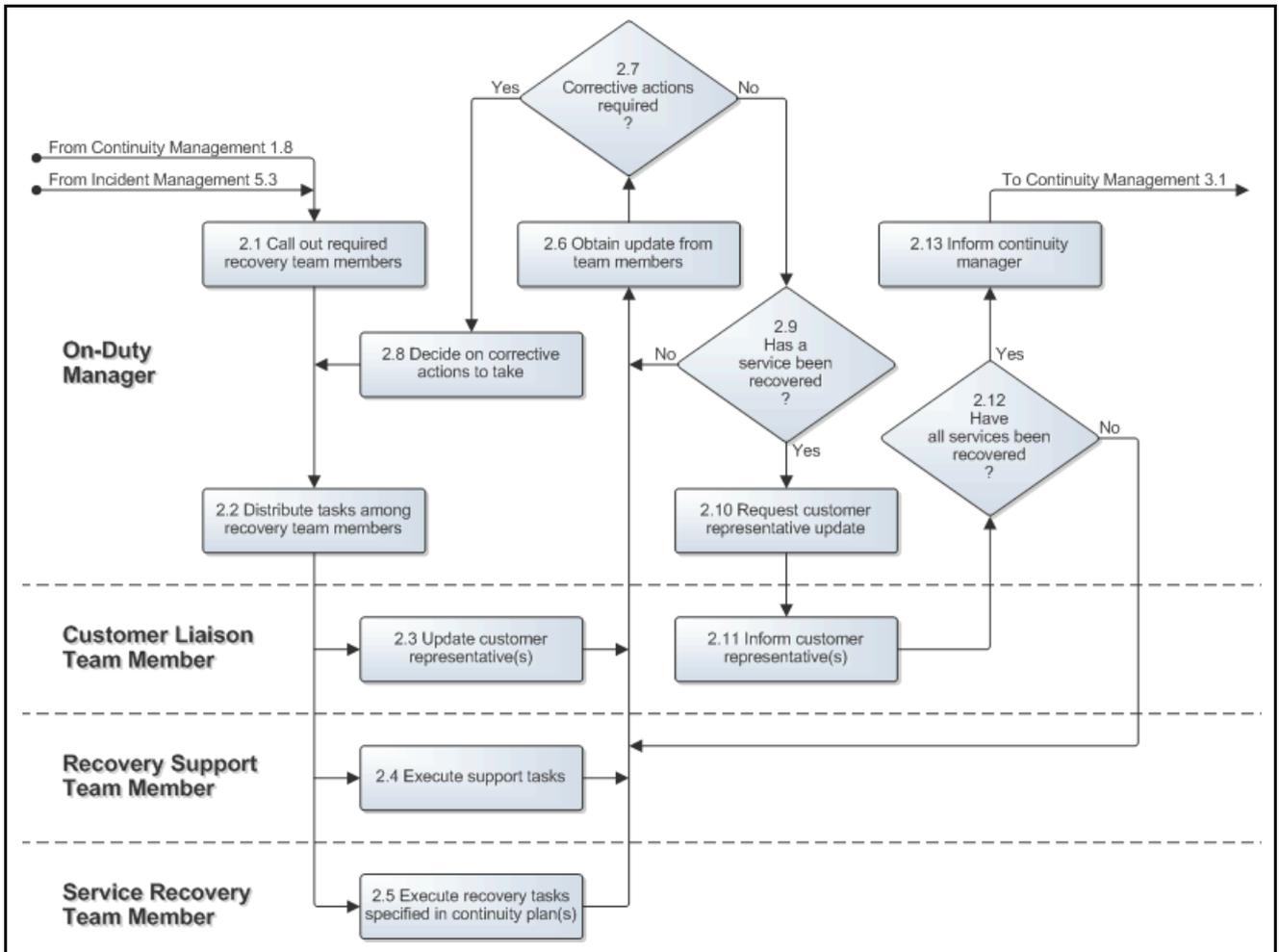
The members of the service recovery team(s) complete the continuity plan checklists that the on-duty manager has asked them to complete.

The on-duty manager keeps track of the service recovery by frequently obtaining updates from the different team members. Whenever corrective actions are required to deal with unforeseen circumstances, the on-duty manager distributes these tasks among the team members.

Every time a service has been recovered, the on-duty manager asks the customer liaison team to inform the representative(s) of the customer(s) that rely on the service, as well as the other people that they have been keeping up-to-date on the progress of the service recovery. Naturally, if only one service had to be recovered, this only happens once.

The Service Recovery procedure diagram is presented on the next page.

Figure 5-3: Service Recovery



Procedure 3, Return to Production

After the recovery of the service(s) has been completed, the continuity manager asks the people who worked together to perform the service recovery to attend the post-recovery meeting. The continuity manager also invites the continuity planner(s) and the service owner(s) of the recovered service(s) to this meeting. During the meeting, the continuity manager reviews the entire recovery with the attendees and collects all ideas for improvement.

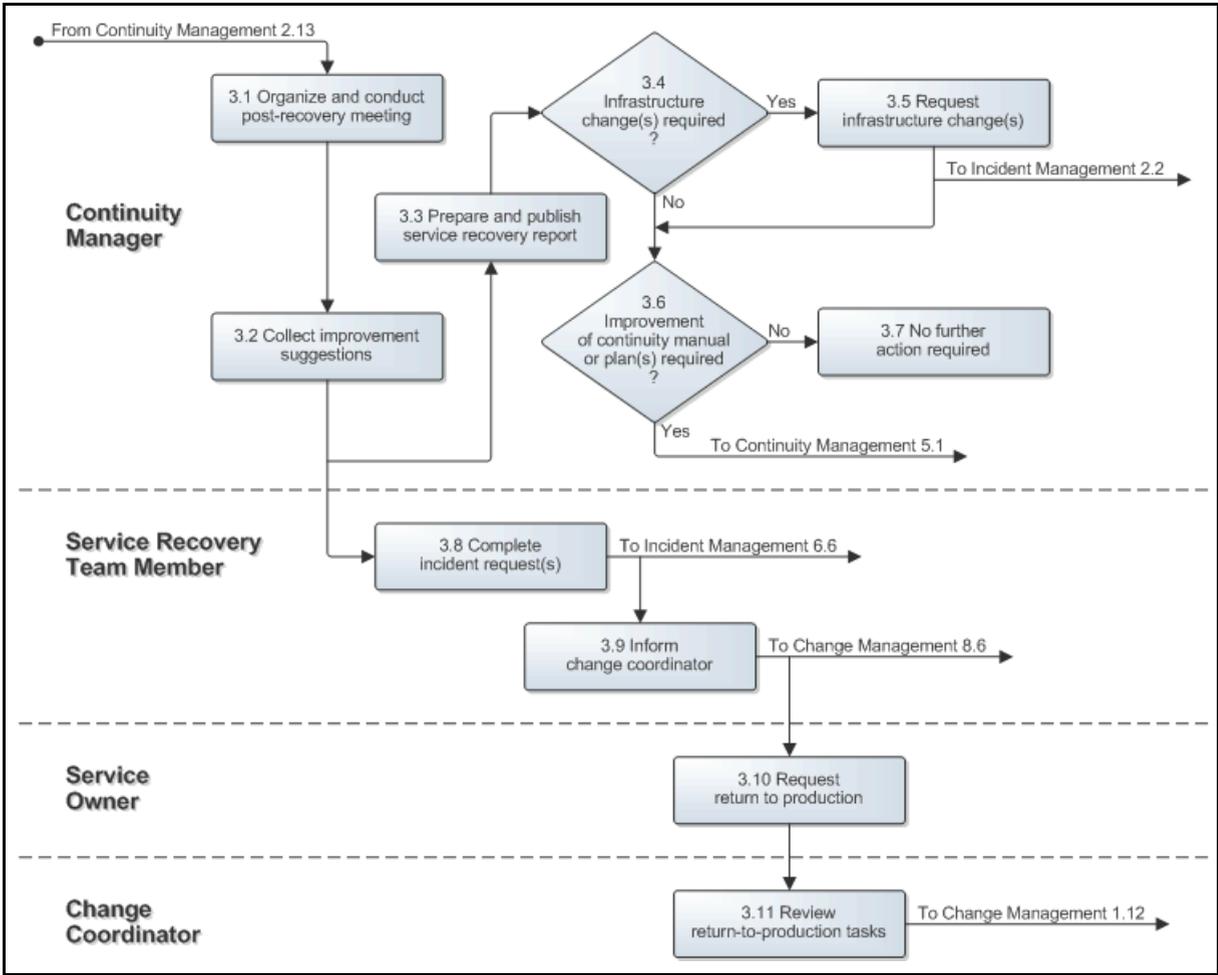
The continuity manager uses the improvement suggestions collected during the post-recovery meeting to register an incident request for every proposed infrastructure change. In Procedure 5, Continuity Manual Maintenance the continuity manager also registers one change for all proposed continuity manual and/or continuity plan modifications. Before registering these incident requests and this change, however, the continuity manager prepares the service recovery report. He/she publishes this written account of the service recovery (in digital format if possible) to ensure that everyone in the service provider organization can access it.

Meanwhile, one member of the service recovery team (or a member of each service recovery team, if there were multiple) ensures that the incident requests are updated if any were registered for the outage(s) of the recovered service(s) before the service recovery was finished. This service recovery team member also updates the change coordinator of the service that he/she helped to recover. In the update the service recovery team member specifies, for each recovered service infrastructure, how it has changed from its previous state (when it was still running at its production site), to its current state (where it is being delivered from its continuity site). The change coordinator(s) of the recovered service(s) subsequently use this information to ensure that the CMDB gets updated.

As soon as all site requirements have been met to return a recovered service infrastructure back to its normal production state, the responsible service owner orders its return to production. This prompts the change coordinator of the service to review the return-to-production tasks that are specified in the continuity plan of the service infrastructure. The change coordinator does this to prepare for the return to production that he/she will coordinate.

The Return to Production procedure diagram is presented on the next page.

Figure 5-4: Return to Production



Procedure 4, Service Recovery Testing

When the continuity test calendar indicates that a service recovery test is coming up, the continuity manager checks which services are to be included in the test. He/she submits an incident request for each service, asking the change coordinator of the service to register a change for the service's recovery test. Registering such changes for service recovery tests ensures that the change manager is able to identify potential conflicts with other planned changes and planned events. In addition, these changes ensure that the owners of the services that are to be included in the service recovery test, as well as the representatives of the affected customer(s), are informed.

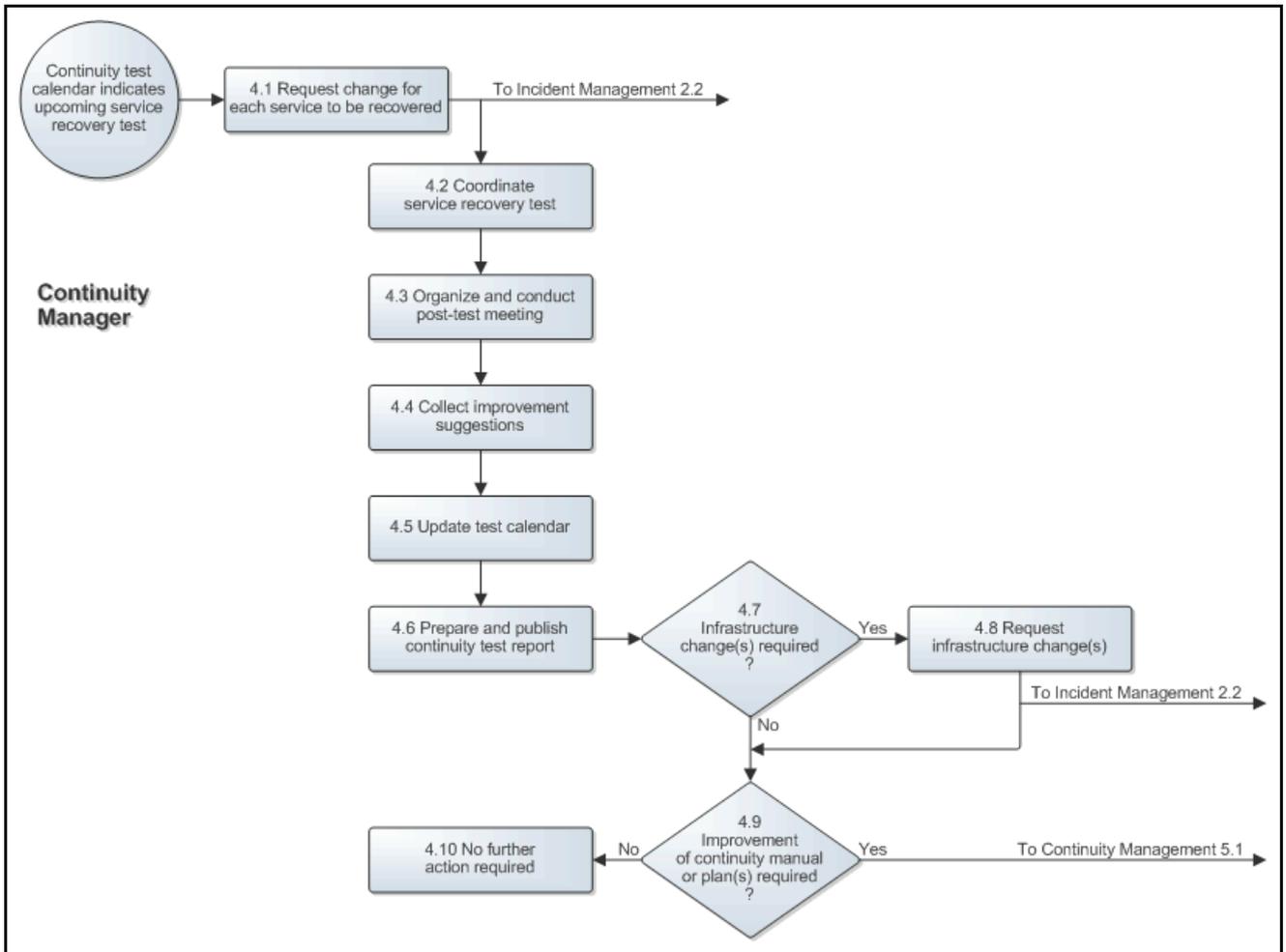
The continuity manager is the person who coordinates the actual service recovery test. After the test has been completed, the continuity manager asks all team members who participated in the test to attend the post-test meeting. The continuity manager also invites the continuity planner(s) and the service owner(s) of the service(s) that were recovered during the test to this meeting. During the meeting, the continuity manager reviews the entire service recovery test with the attendees and collects all ideas for improvement.

The continuity manager uses the improvement suggestions collected during the post-test meeting to register an incident request for every proposed infrastructure change. In Procedure 5, Continuity Manual Maintenance the continuity manager also registers one change for all proposed continuity manual and/or continuity plan modifications. Before registering these incident requests and this change, however, the continuity manager prepares the continuity test report. He/she publishes this written account of the service recovery to ensure that everyone in the service provider organization can access it.

Finally, the continuity manager schedules an additional test in the continuity test calendar. This is done in such a way that the service provider organization's target of the number of tested continuity plans will be met.

The Service Recovery Testing procedure diagram is presented on the next page.

Figure 5-5: Service Recovery Testing



Procedure 5, Continuity Manual Maintenance

If improvement suggestions for the continuity manual and/or the continuity plans were gathered during a post-test or post-recovery meeting, the continuity manager registers a new change. The continuity manager adds tasks to this change for the update of continuity plans as needed. Such tasks are assigned to the continuity planners who are responsible for maintaining the continuity plans that are to be updated. The continuity manager also adds a task to the change for him/herself when an update of the continuity manual is required. Finally, he/she ensures that a task is included and assigned to him/herself for the distribution of the updated continuity management documents.

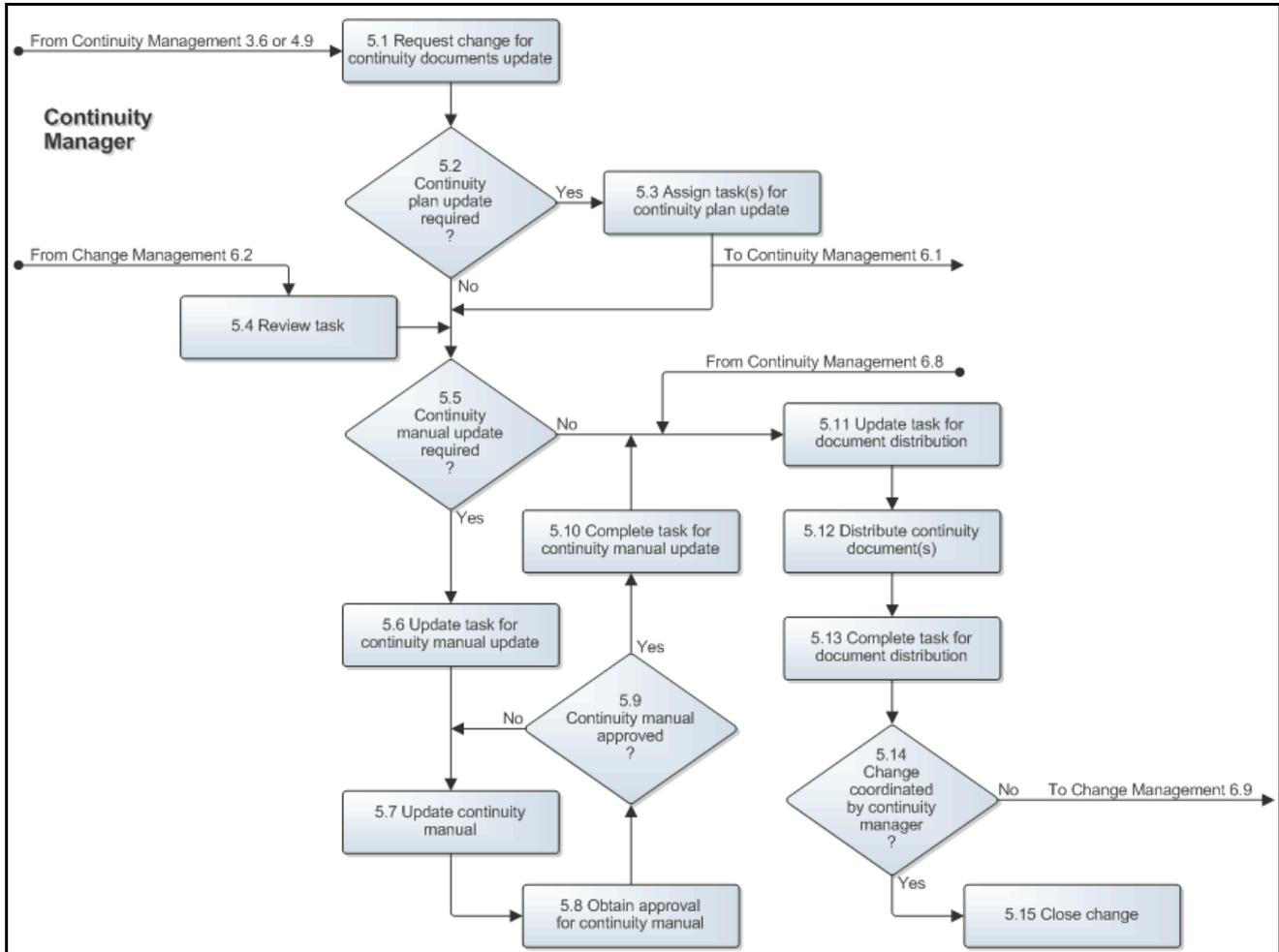
If this change, or a change that is managed by one of the change coordinators, includes a task for the update of the continuity manual, the continuity manager prepares the new version of the manual. Once the new version is ready, the continuity manager asks the on-duty manager (the one who is on-duty at that moment) to approve it.

When all new versions of the continuity documents, which had to be prepared for a specific change, are approved, the continuity manager distributes a copy of each new version. At the same time, the continuity manager collects the older versions and ensures that these are destroyed.

After the distribution has been completed, and if the change is coordinated by the continuity manager, the continuity manager closes the change.

The Continuity Manual Maintenance procedure diagram is presented below.

Figure 5-6: Continuity Manual Maintenance



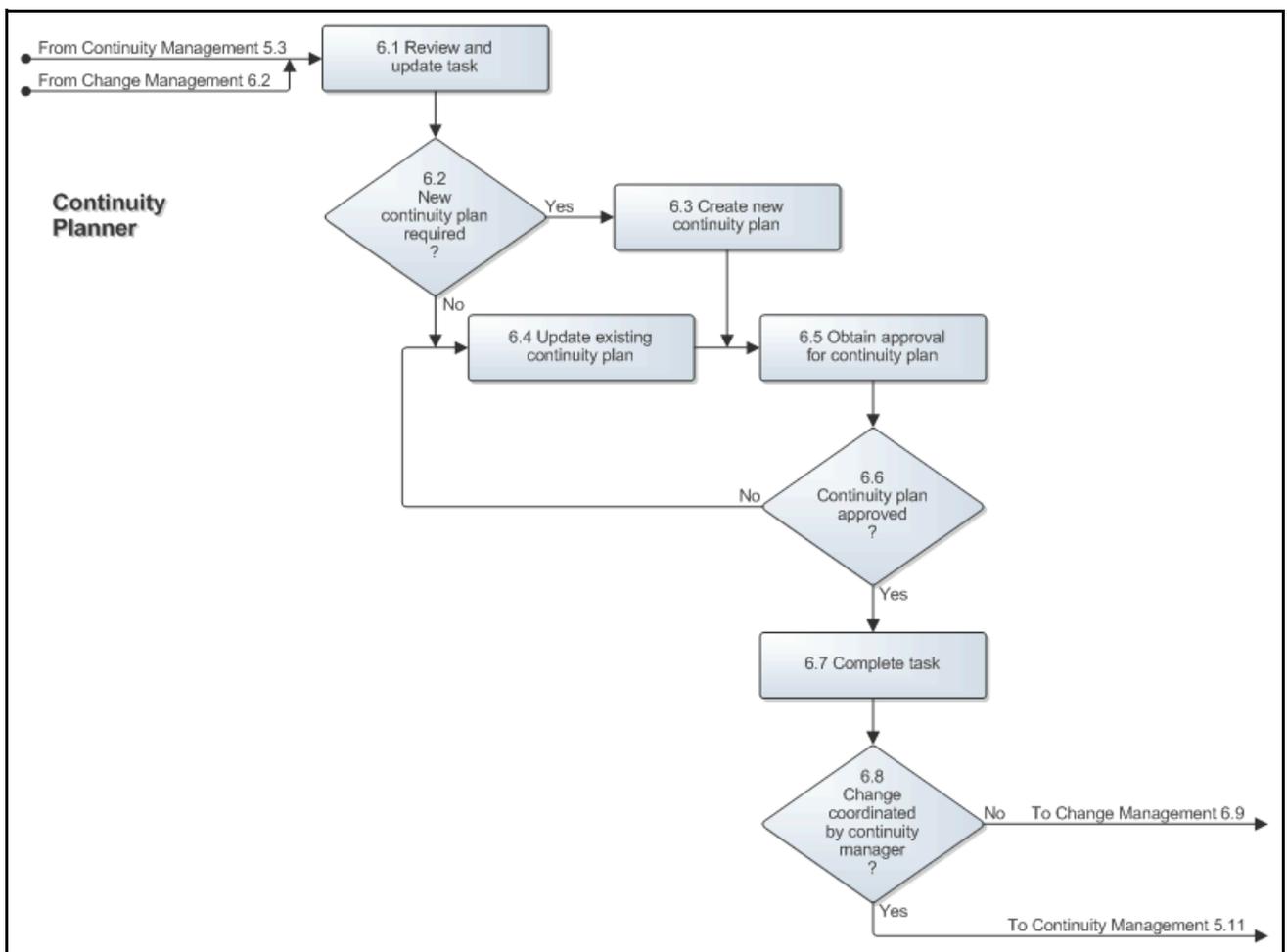
Procedure 6, Continuity Plan Maintenance

When a continuity planner receives a task for the creation of a new continuity plan, he/she creates the new continuity plan using the current version of the Continuity Plan Template. Similarly, when a continuity planner receives a task for the update of an existing continuity plan, he/she prepares the new version.

When the new continuity plan has been prepared, or after the existing continuity plan has been updated, the continuity planner obtains the approval for the plan from both the responsible service owner as well as the continuity manager. Having obtained both approvals, he/she closes the task that requested the new or updated continuity plan.

The Continuity Plan Maintenance procedure diagram is presented below.

Figure 5-7: Continuity Plan Maintenance



6 Event Management

The Event Management process consists of three procedures.

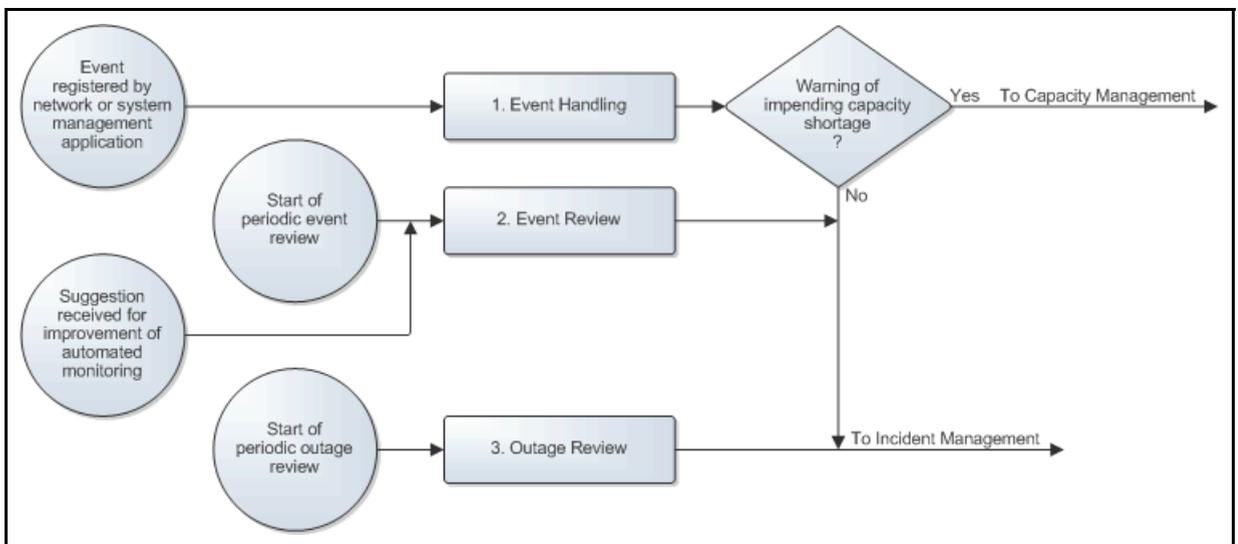
The first procedure is called "Event Handling". It is used by operators when they deal with events raised by network and system management applications.

The second procedure is called "Event Review". This procedure is used by the operations manager to identify opportunities for improvement of the efficiency with which events are handled.

The third and last procedure is called "Outage Review". The operations manager follows this procedure to identify weaknesses in the monitoring of the services by periodically reviewing the information about service outages that affected multiple users.

A graphical representation of the process is provided on the next page. Each procedure is described in more detail in the sections that follow this diagram.

Figure 6-1: Event Management process description



Procedure 1, Event Handling

After the registration of a new event by a network or system management application, the operator reviews its information to determine which configuration item (CI) has failed, or is about to fail, and to find out the apparent cause of the event.

Next, the operator reviews the other recently generated events to ensure that the event was not raised because the network or system management application could no longer accurately determine the CI's status due to the failure of another CI elsewhere in the infrastructure. In addition, the operator checks if the event is the result of a planned change or planned event.

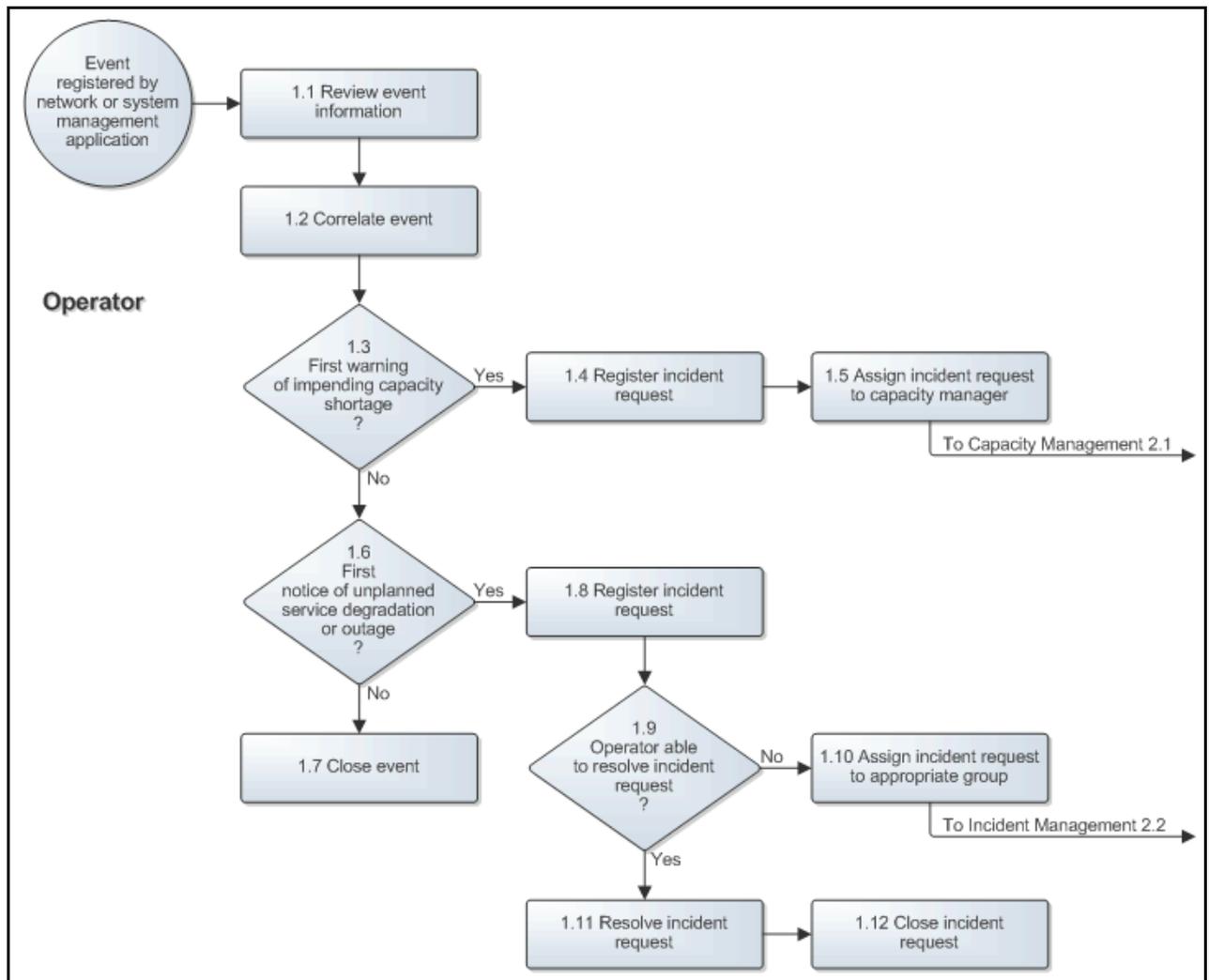
If the event represents the first warning of an impending capacity shortage (e.g. because a capacity threshold has been exceeded), the operator registers a new incident request to prevent this imminent incident. The operator sets the service type to "Infrastructure Event" and ensures that the CI and the service infrastructure it supports are linked to the incident request. The operator assigns the incident request to the capacity manager of the service infrastructure to which the CI is linked.

If the event represents the first notification of an unplanned service outage or degradation, the operator registers a new incident request of the service type "Infrastructure Restoration" for it. The operator ensures that the incident request is linked to the affected CI and service infrastructure. If the operator is able to resolve this incident request (in terms of skills, access rights and time restrictions), he/she resolves and closes it. If not, the operator ensures that the incident request gets assigned to the appropriate group. The operator closes the event after he/she has either resolved it, or assigned the incident request that he/she registered for it. Closing the event ensures that it is removed from the list of open events.

The operator also closes the event if it was not the first event that was generated for a current or future incident (i.e. when an incident request had already been registered for this), or if the event represents a service degradation or outage that was planned.

The Event Handling procedure diagram is presented on the next page.

Figure 6-2: Event Handling



Procedure 2, Event Review

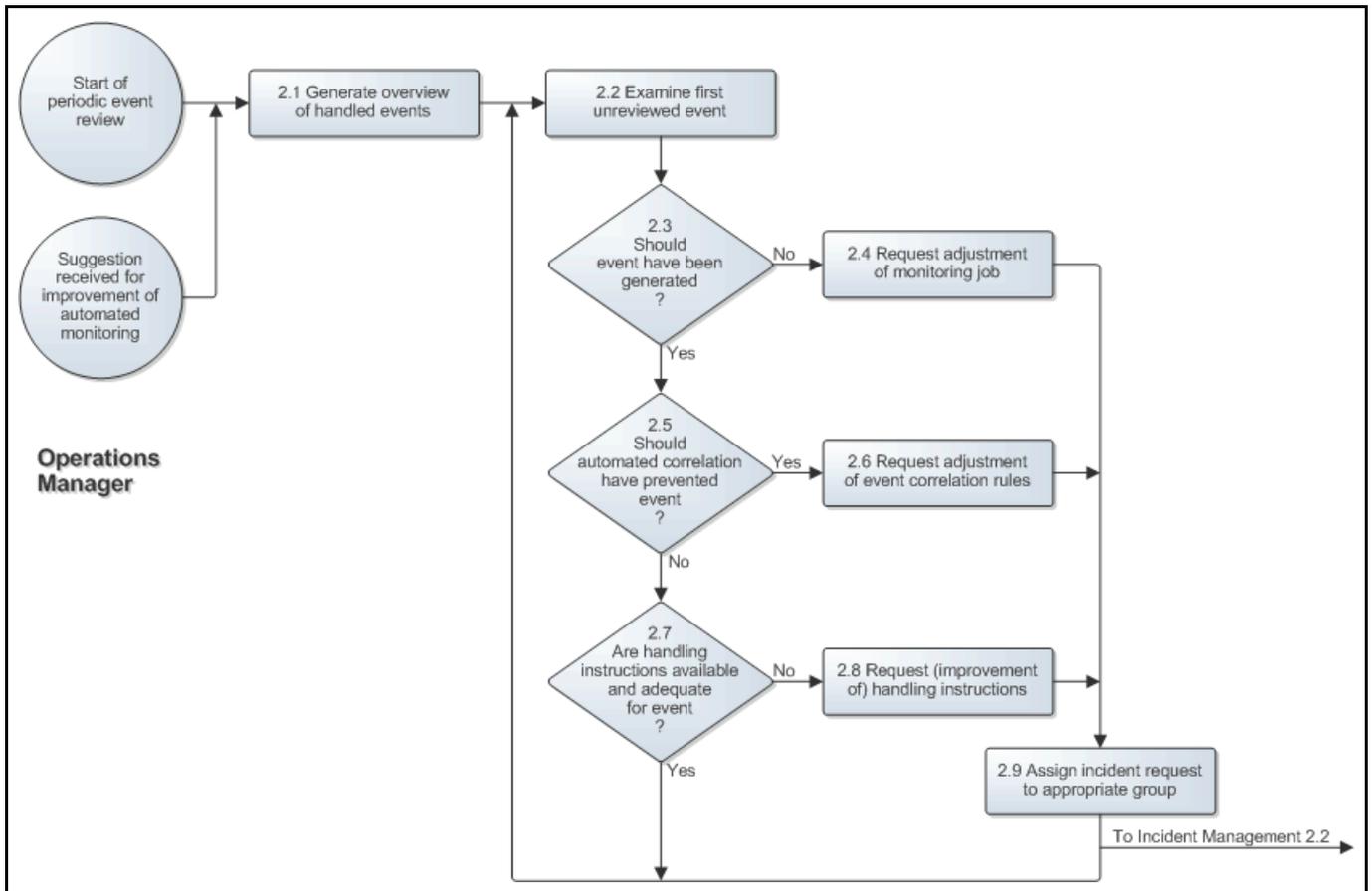
The operations manager regularly reviews all events that have been handled by the operators. He/she also considers suggestions offered by operators and specialists for the improvement of the manner in which the service infrastructures are being monitored by the network and system management applications. The operations manager does this in order to identify:

- monitoring jobs that generate unnecessary events.
- missing or ineffective automated event correlation rules.
- missing or inadequate event handling instructions for the operators.

When the operations manager has identified an improvement opportunity, he/she opens a new incident request and explains what should be changed. Having filled out the new incident request, the operations manager ensures that it gets assigned to the group that will be responsible for implementing the requested improvement.

The Event Review procedure diagram is presented below.

Figure 6-3: Event Review



Procedure 3, Outage Review

The operations manager periodically reviews all high-impact incident requests (i.e. all service outages that affected multiple users). For each of these incident requests, the operations manager first determines whether or not an event was generated to notify the service provider organization of the outage.

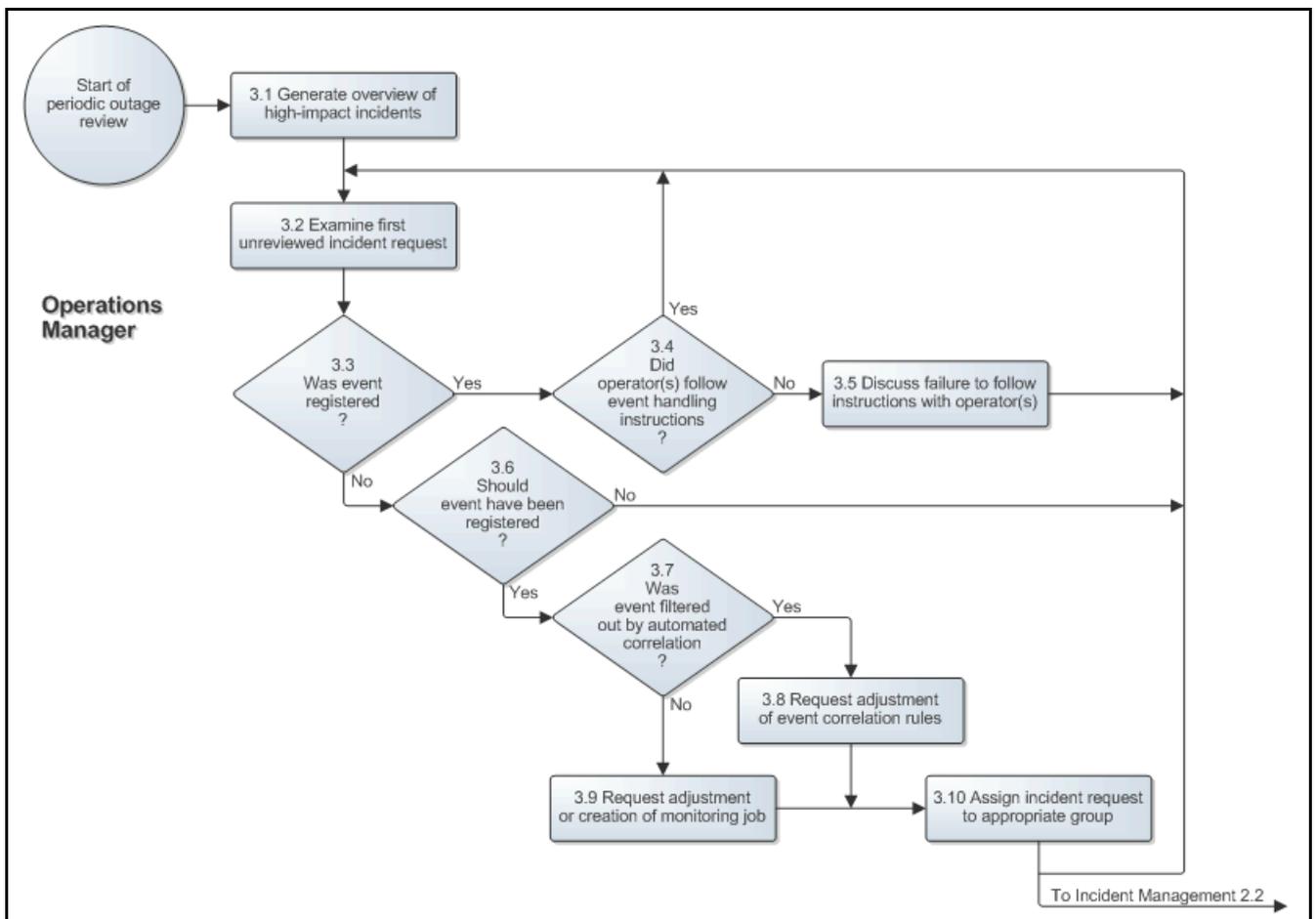
If an event was generated, the operations manager finds out whether or not the operator(s) followed the event handling instructions correctly. If this was not the case, the operations manager collects the information for review with the operators.

If an event was not generated for the service outage, this might be correct (e.g. because it has been decided that it is too expensive to automatically monitor the service infrastructure that was affected). If an event should have been registered, however, the operations manager finds out whether this was prevented by the automated correlation rules, or because a monitoring job needs to be created or adjusted. The operations manager subsequently registers a new incident request to request a correction in the automated correlation rules or the configuration of a monitoring job.

After completing the review of a high-impact incident request, the operations manager reviews the next one until all of the high-impact incident requests that were resolved during the past review period have been reviewed.

The Outage Review procedure diagram is presented below.

Figure 6-4: Outage Review



Financial Management

The Financial Management process consists of three procedures.

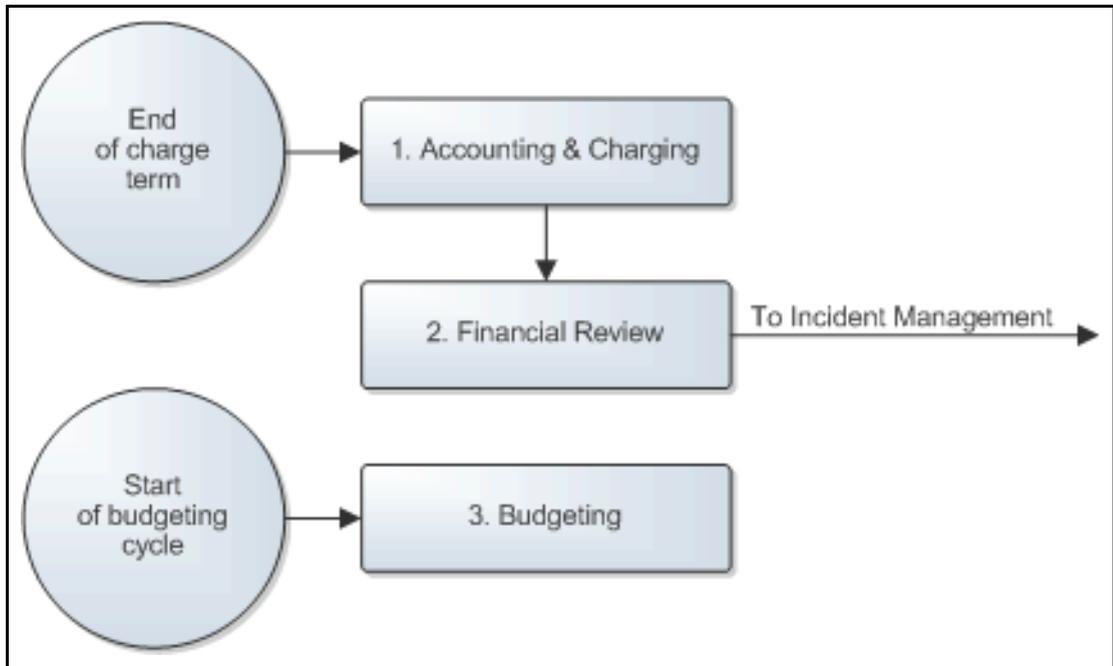
The first procedure is called "Accounting & Charging". It is used by the service level administrator at the end of a charge term when the actual service utilization overview and the cost overview of each service is prepared. The IT controller uses this procedure to ensure that all costs have been attributed to the different services and to charge the customers for their use of the services.

The second procedure is called "Financial Review". This procedure is used by the service owners to evaluate the costing and charging data and to identify opportunities to reduce service costs.

The third and last procedure is called "Budgeting". The service owners follow this procedure to propose a budget and charges for each service for the next budget period. The financial manager uses this procedure to formalize the new service budgets and charges. This procedure is also used by the service level administrator to update the service catalog and SLAs with the new service charges. The service level managers use this procedure to inform the affected customers of the new service charges.

A graphical representation of the process is provided below. Each procedure is described in more detail in the sections that follow this diagram.

Figure 7-1: Financial Management process description



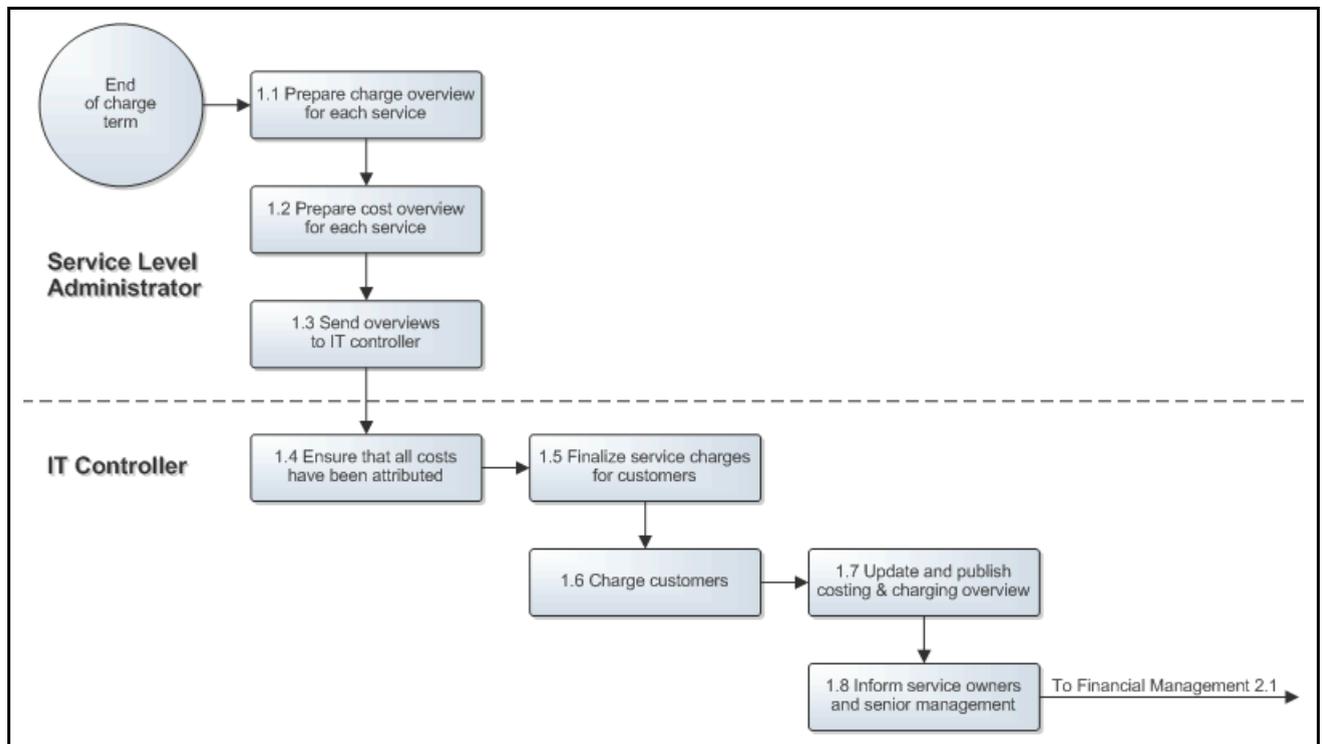
Procedure 1, Accounting & Charging

At the end of a charge term, the service level administrator prepares an overview that lists the actual utilization of each service by customers. The service level administrator also prepares an overview that lists the actual costs of each service over the past charge term. The service level administrator sends these overviews to the IT controller who ensures that all costs that were incurred by the service provider organization during the past charge term have been attributed. After this, the IT controller ensures that the customers get charged for the usage of the services during the past charge term.

Having charged the customers, the IT controller updates the costing & charging overview. He/she then publishes the updated costing & charging overview on the organization's intranet and informs all senior managers and service owners that the updated overview is available online.

The Accounting & Charging procedure diagram is presented on the next page.

Figure 7-2: Accounting and Charging



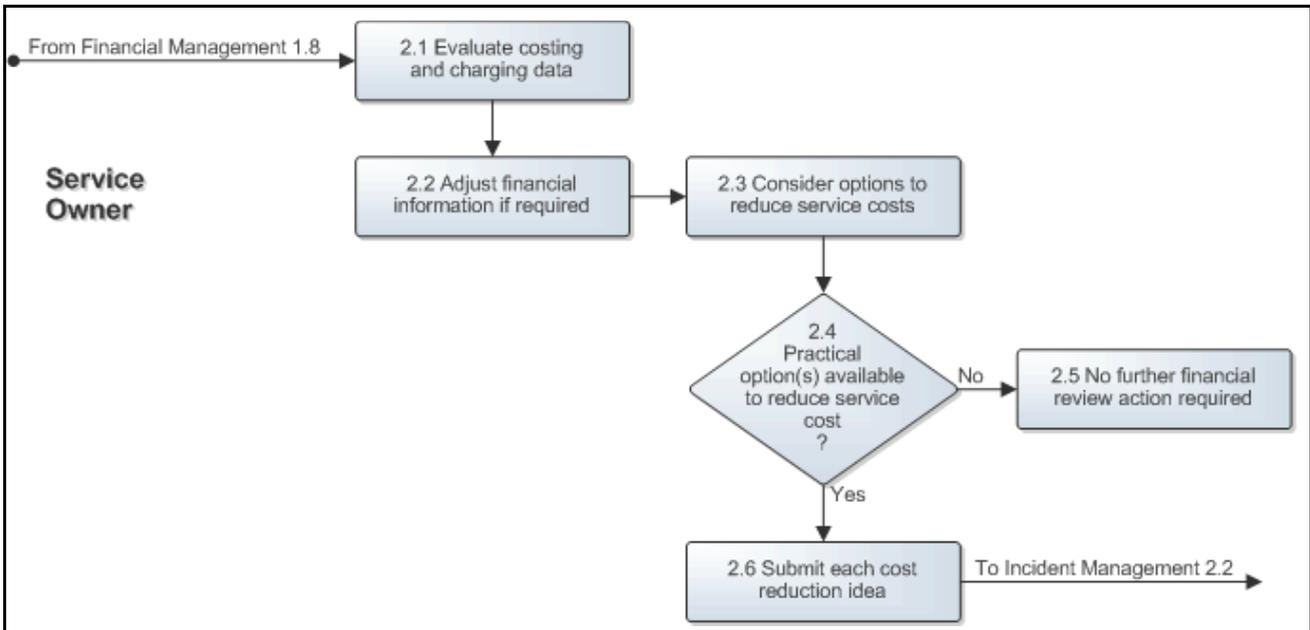
Procedure 2, Financial Review

Having received the notification from the IT controller that the updated costing & charging overview has been published, each service owner evaluates the numbers for their respective service(s). Each service owner subsequently ensures that the financial information in the service management application is corrected as requested by the IT controller in the notes of the updated overview.

Using the updated costing & charging overview, the service owners then try to find ways to reduce the costs of their service(s). They submit an incident request for each cost reduction opportunity that they have identified.

The Financial Review procedure diagram is presented on the next page.

Figure 7-3: Financial Review



Procedure 3, Budgeting

At the start of a new budgeting cycle, the service owners extrapolate the historical utilization trends of the services for which they are responsible to forecast the service utilization during the next budget period. They subsequently correct these utilization forecasts by taking the impact of planned releases and projects into account. The service owners also forecast the service costs for the next budget period in a similar fashion. Using the utilization forecasts and the cost forecasts, the service owners calculate the required service budgets and propose service charges for the next budget period. The service owners submit their forecasts, proposed budgets and proposed service charges to the IT director for review.

The IT director adjusts the proposed service budgets and service charges for the next budget period as needed before submitting a consolidated proposal to the financial manager.

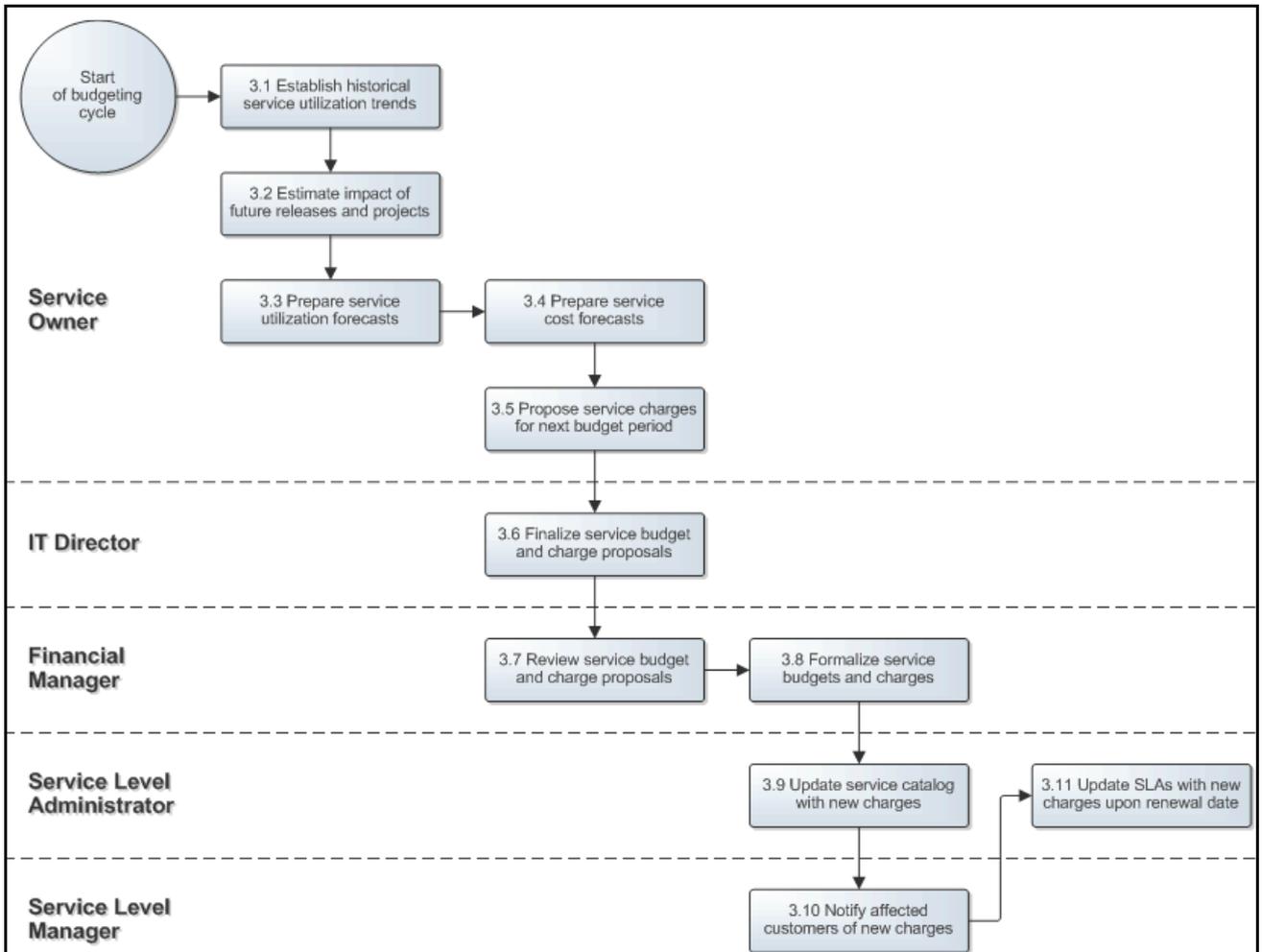
The financial manager reviews the consolidated proposal for the service provider organization's budget and service charges. He/she adjusts the proposed numbers as needed before approving them and ensures that the IT director, the IT controller and the service level administrator are informed of the approved service budgets and service charges for the next budget period.

The service level administrator adds the service charges for the next budget period to the service catalog, after which the service level managers inform their customers.

Just before the start of the new budget period, the service level administrator updates the SLAs with the new service charges.

The Budgeting procedure diagram is presented on the next page.

Figure 7-4: Budgeting



Incident Management

The Incident Management process consists of seven procedures.

The first procedure is called "Incident Request Registration". This procedure is used by service desk analysts when they register incident requests for users.

The second procedure is called "Incident Request Assignment". It is used by service desk analysts and group coordinators to assign incident requests to the appropriate specialists or change coordinators for resolution or implementation.

The third procedure is called "Incident Request Tracking". It is used by group coordinators when they are dealing with reassignment notifications or SLA escalations.

The fourth procedure is called "Incident Request Resolution by Specialist". It is used by specialists when resolving incident requests that have been assigned to them.

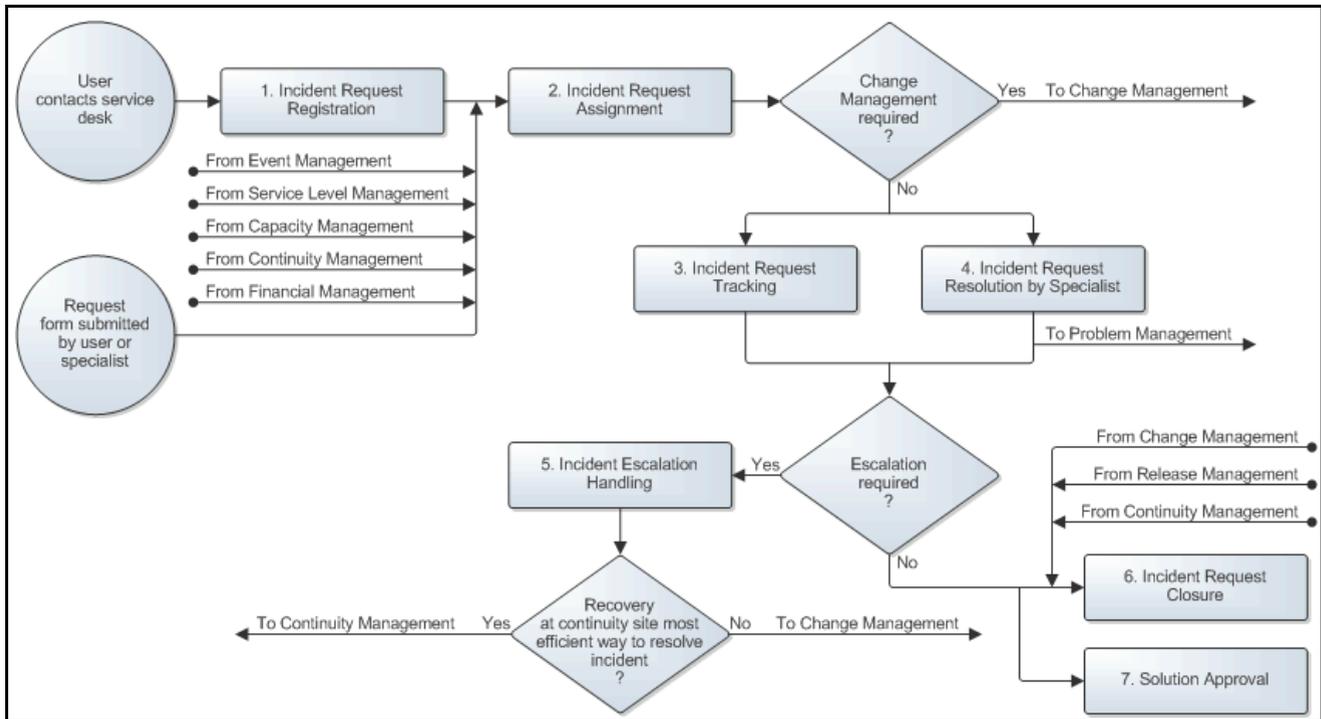
The fifth procedure is called "Incident Escalation Handling". After an incident has been escalated, the service owner of the affected service uses this procedure to determine how the incident can be resolved in the most efficient manner.

The sixth procedure is called "Incident Request Closure". This procedure is used by service desk analysts when they resolve incident requests, and by requesters when they review incident requests that have been completed for them.

The seventh and last procedure is called "Solution Approval". This procedure is used by group coordinators when their approval has been requested for a solution that has been proposed for general use.

A graphical representation of the process is provided on the next page. Each procedure is described in more detail in the sections that follow this diagram.

Figure 8-1: Incident Management process description



Procedure 1, Incident Request Registration

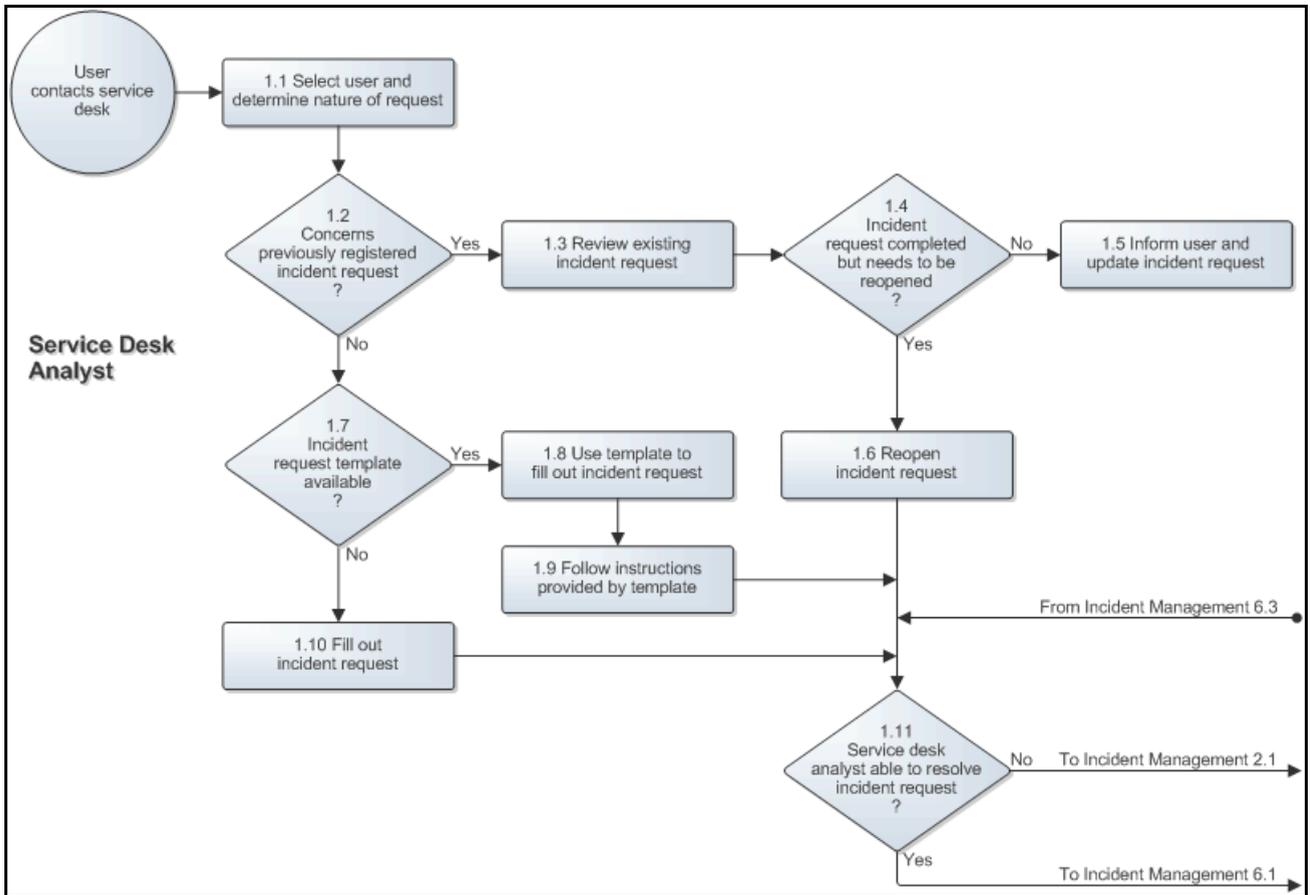
When a user contacts the service desk, the service desk analyst finds out how the user can be assisted. This is done by asking the user how he/she can be helped, if the user contacted the service desk by phone or in person. Alternatively, if the user contacted the service desk in writing (e.g. with an email) the service desk analyst determines the nature of the request by reading through the information.

If the user 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 user with a status update or reopens it if the previously provided solution does not work).

If the user 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 diagram is presented on the next page.

Figure 8-2: Incident Request Registration



Procedure 2, Incident Request Assignment

Having filled out a new incident 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 group.

If the service desk analyst reopened an existing incident request, he/she manually selects the most appropriate assignment group.

The group coordinator 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 users 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 group coordinator determines whether or not it needs to be resolved through the Change Management process.

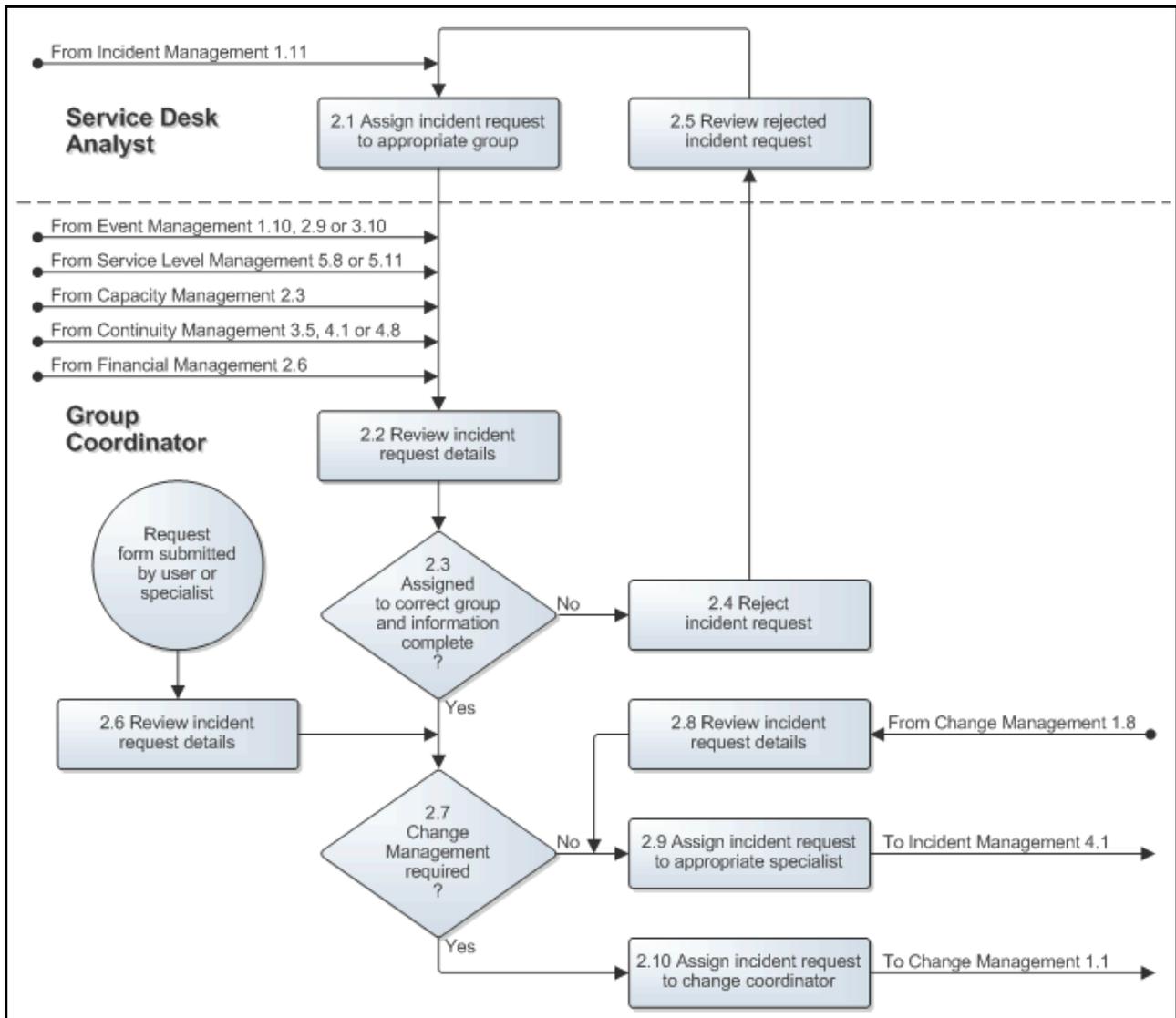
An incident request may not be resolved without Change Management when its resolution will cause:

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

The group coordinator 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 group coordinator assigns it to the most appropriate specialist within his/her group based on skills, availability and access rights.

The Incident Request Assignment procedure diagram is presented below.

Figure 8-3: Incident Request Assignment



Procedure 3, Incident Request Tracking

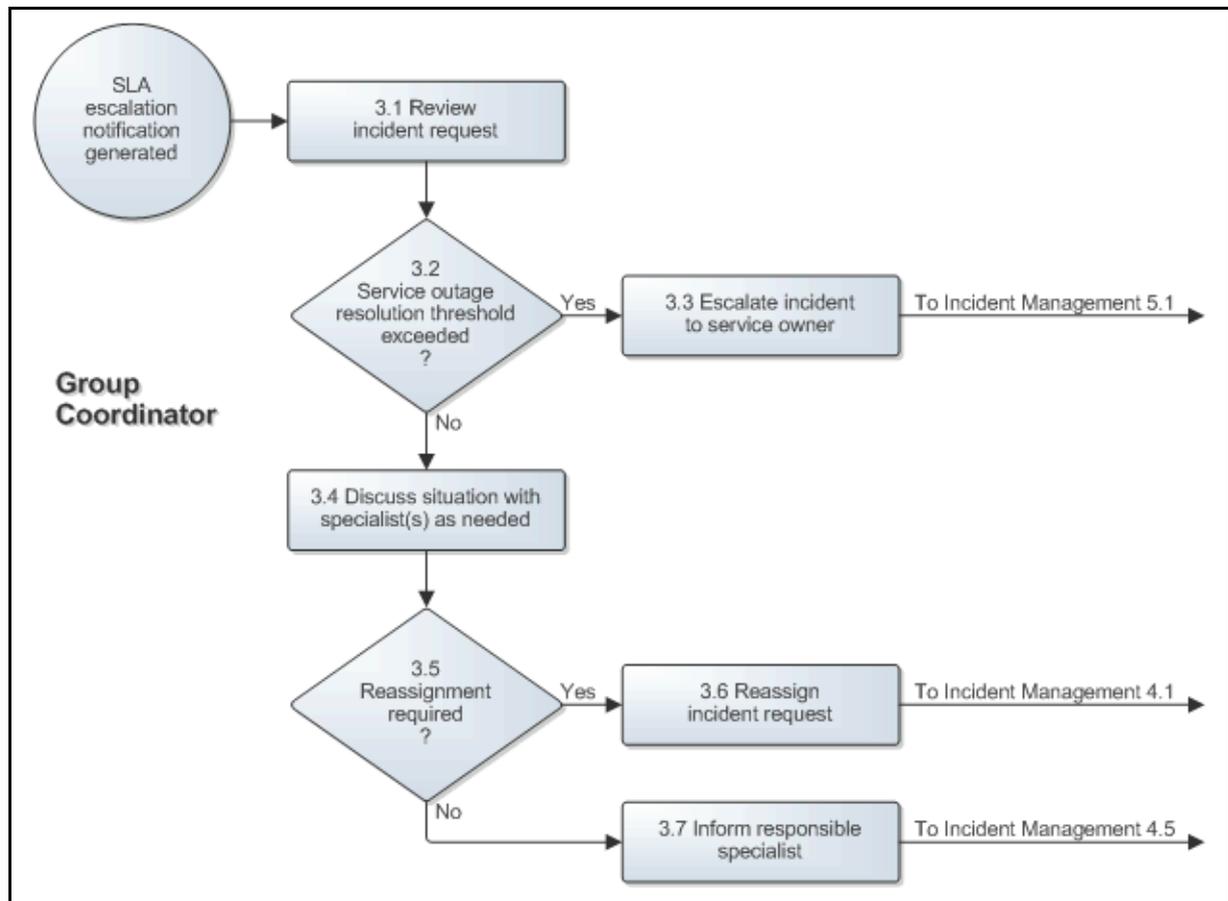
After an SLA has escalated an incident request, the group coordinator reviews the notification that has been sent to him/her for this. If the incident request concerns a service outage which resolution threshold (as dictated by the SLA that generated the notification) has been exceeded, the group coordinator 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 group coordinator determines who had best continue to work on the resolution of the incident request. He/she obtains the advice from specialists within the group as needed to determine whether the incident request should be reassigned to another specialist, or should be resolved by the specialist to whom the incident request is currently assigned.

If the incident request should be reassigned, the group coordinator does this by assigning it to a specialist who is in a better position (in terms of skills, availability and/or access rights) to resolve it. If the group coordinator has decided not to reassign the incident request, he/she informs the specialist 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 diagram is presented on the next page.

Figure 8-4: Incident Request Tracking



Procedure 4, Incident Request Resolution by Specialist

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

The specialist 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:

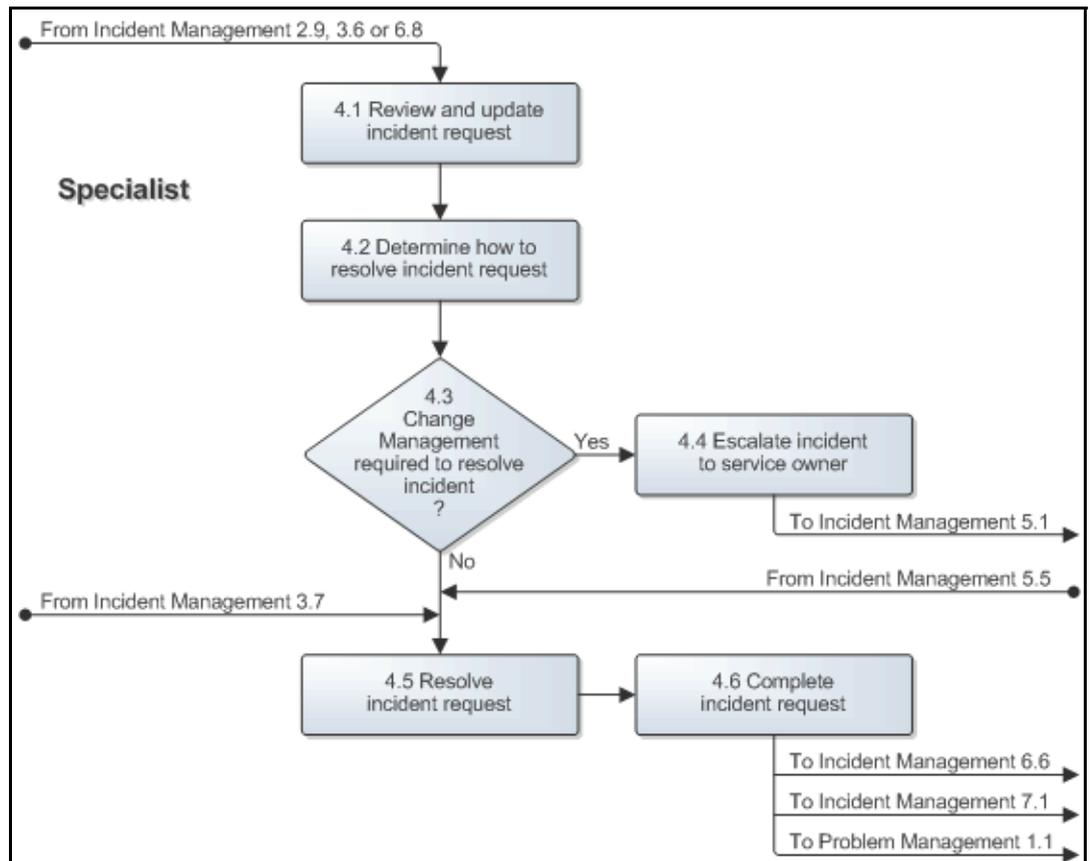
- a service to become unavailable or degraded during service hours.
- the functionality of a service to become different.
- the CMDB to require an update.

If the specialist 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 specialist believes that the solution information he/she entered in the incident request could help requesters, service desk analysts and/or specialists 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 specialist 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 Specialist procedure diagram is presented below.

Figure 8-5: Incident Request Resolution by a Specialist



Procedure 5, Incident Escalation Handling

After a group coordinator or specialist has escalated an incident to the owner of the affected service, the service owner talks to the specialist(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 to the on-duty manager 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.
- the CMDB to require an update.

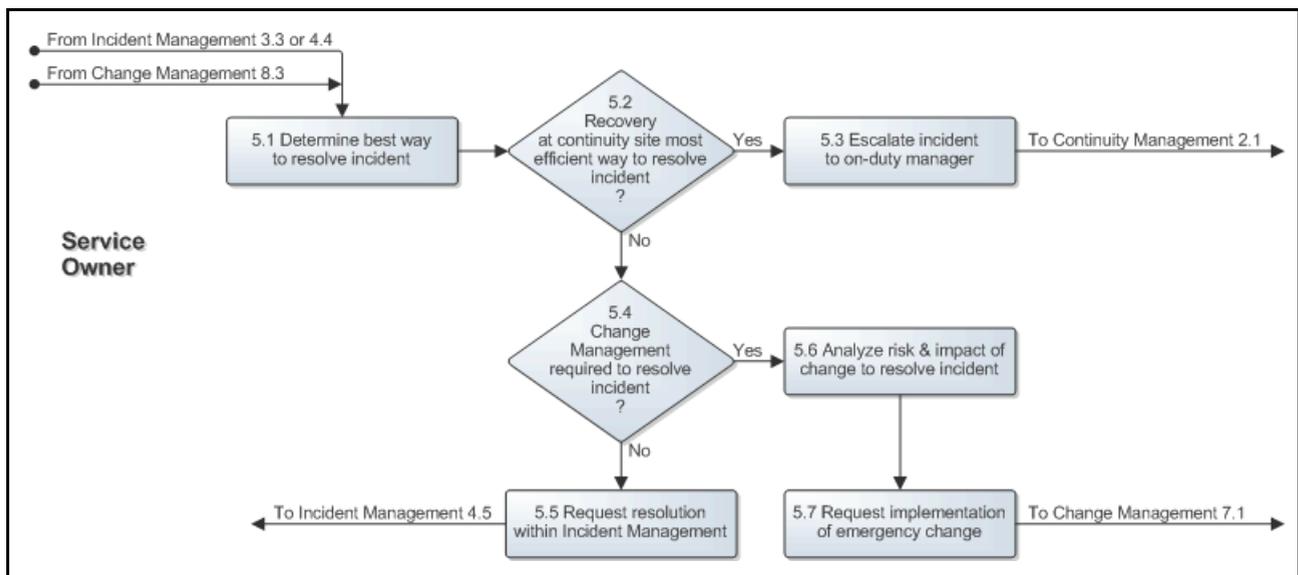
If Change Management is not required, the service owner ensures that the most appropriate specialist(s) continue to resolve the incident within the Incident Management process.

On the other hand, if Change Management is required, the service owner consults with the specialist(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 users. 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 specialist(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 diagram is presented below.

Figure 8-6: Incident Escalation Handling



Procedure 6, Incident Request Closure

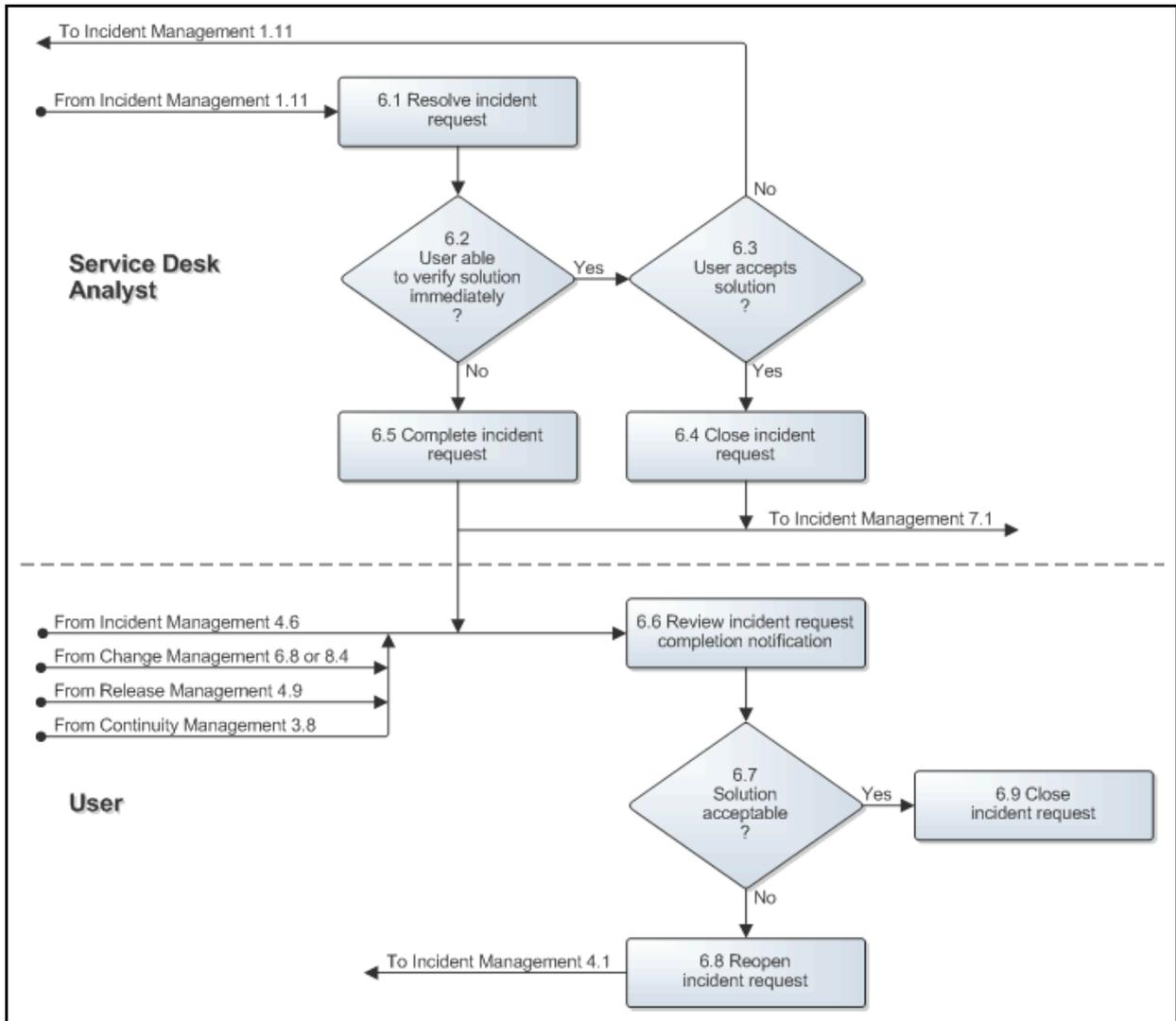
When a service desk analyst is able to resolve an incident request (in terms of skills, access rights, and time considerations), he/she resolves it and updates the incident request accordingly. The service desk analyst closes the incident request if the user is still in contact with the service desk 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 specialists to resolve future cases that are similar, he/she proposes it for general use.

After a user has received an incident request completion notification, he/she reviews the solution information of his/her incident request. The user then tries to verify the solution. If the user considers the solution acceptable, he/she does not need to take any action. If the solution is not acceptable, however, the user reopens the incident request, thus requesting a better solution.

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

Figure 8-7: Incident Request Closure



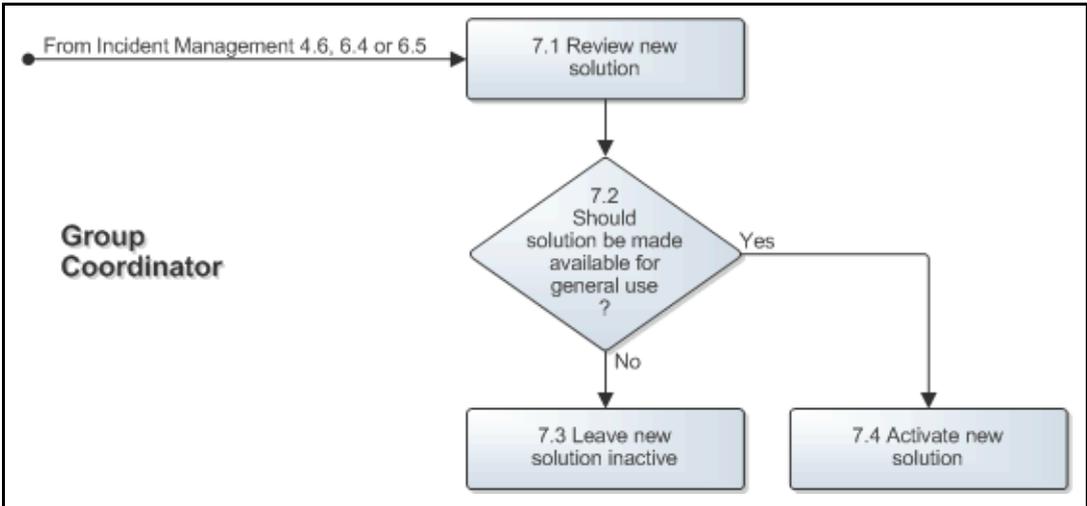
Procedure 7, Solution Approval

After a group coordinator has received a notification that a new solution has been proposed, he/she reviews the proposed solution information. If the group coordinator agrees that the proposed solution could help users, service desk analysts and/or specialists 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 group coordinator 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 diagram is presented on the next page.

Figure 8-8: Solution Approval



9 Problem Management

The Problem Management process consists of four procedures.

The first procedure is called "Incident Request Review". This procedure is used by problem coordinators when they review incident requests to identify problems within the services they are responsible for.

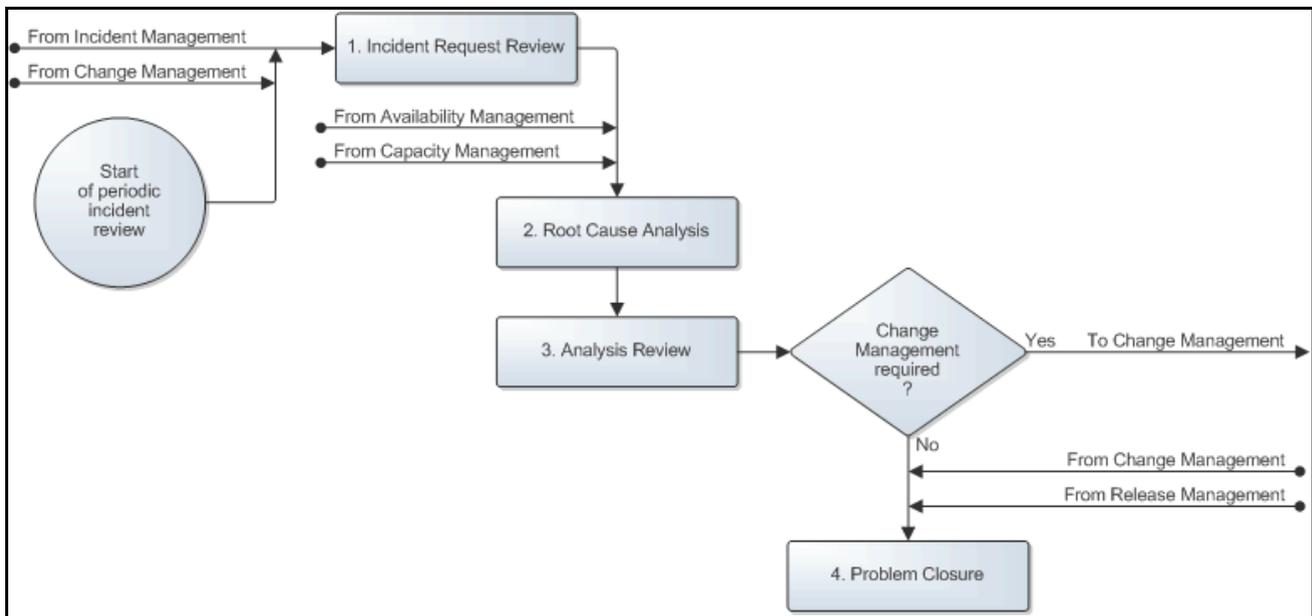
The second procedure is called "Root Cause Analysis". It is used by specialists when they analyze a problem.

The third procedure is called "Analysis Review". It is followed by problem coordinators when they review the results of a root cause analysis performed by a specialist.

The fourth and final procedure is called "Problem Closure". Problem coordinators use it when they close out problems.

A graphical representation of the process is provided on the next page. Each procedure is described in more detail in the sections that follow this diagram.

Figure 9-1: Problem Management process description



Procedure 1, Incident Request Review

The problem coordinator uses incident request information to identify problems in the service(s) he/she is responsible for. A specialist can also draw the attention of a problem coordinator to certain incident requests that, in the opinion of the specialist, have been caused by a problem.

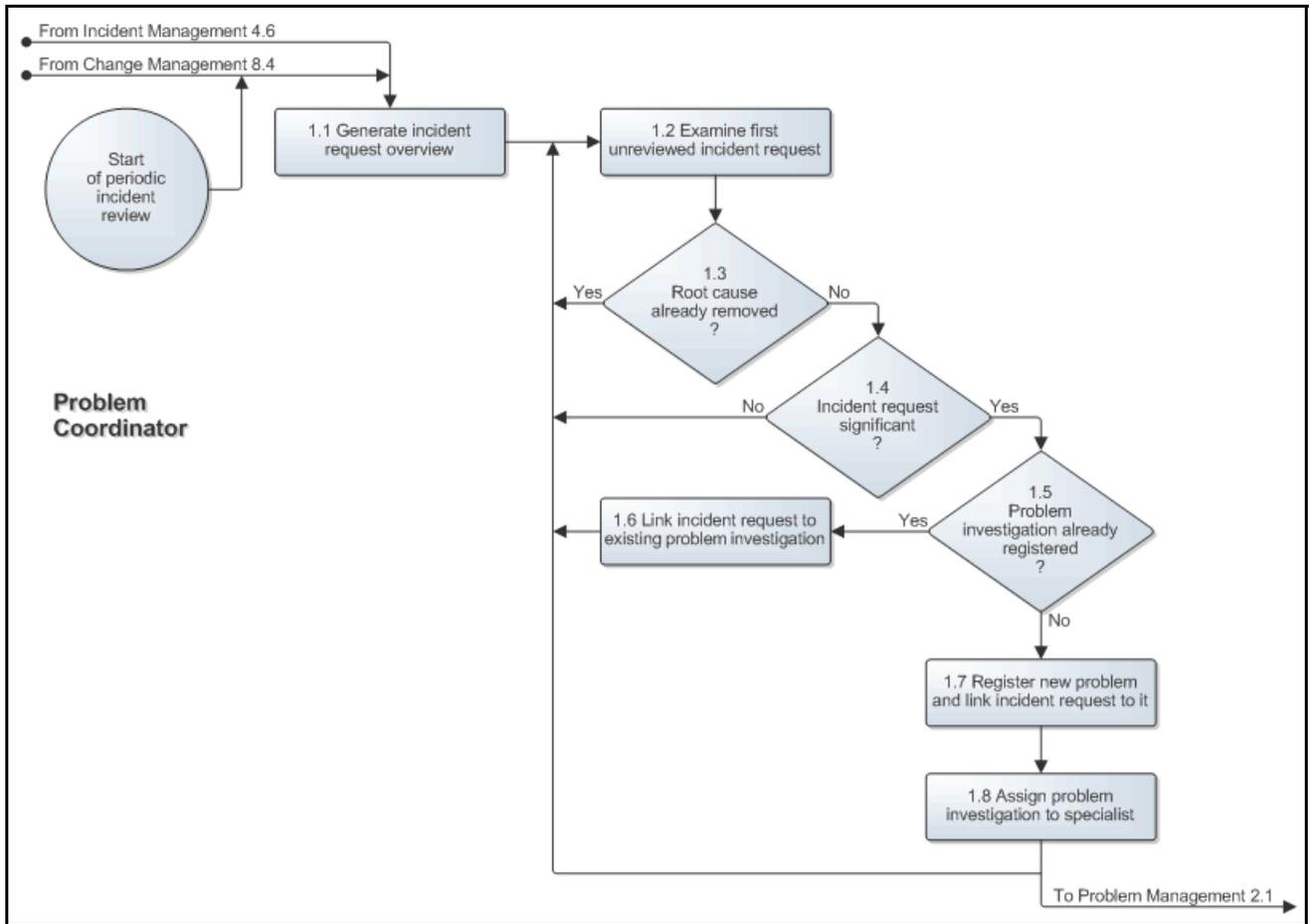
After the identification of a problem, the problem coordinator registers a new problem investigation in the service management application. The problem coordinator subsequently links the incident requests that were caused by the problem to it.

The problem coordinator then assigns the new problem investigation to the most appropriate specialist (in terms of skills, availability and access rights) for analysis.

When the problem coordinator finds incident requests that have not yet been linked to a problem investigation, but which were caused by a previously identified problem, he/she links these incident requests to the problem investigation.

The Incident Request Review procedure diagram is presented on the next page.

Figure 9-2: Incident Request Review



Procedure 2, Root Cause Analysis

After a problem investigation has been assigned to a specialist for analysis, the specialist reviews the details of the problem. If the problem was identified after one or more incidents were already caused by it, the specialist attempts to provide a temporary workaround. The information about the workaround, and specifically how to implement it, is added to the problem investigation. This workaround can be used to resolve future incidents caused by the problem until a structural solution has been found and implemented.

The specialist subsequently starts to track down the root cause of the problem. Having found the root cause, the problem investigation is updated with its description.

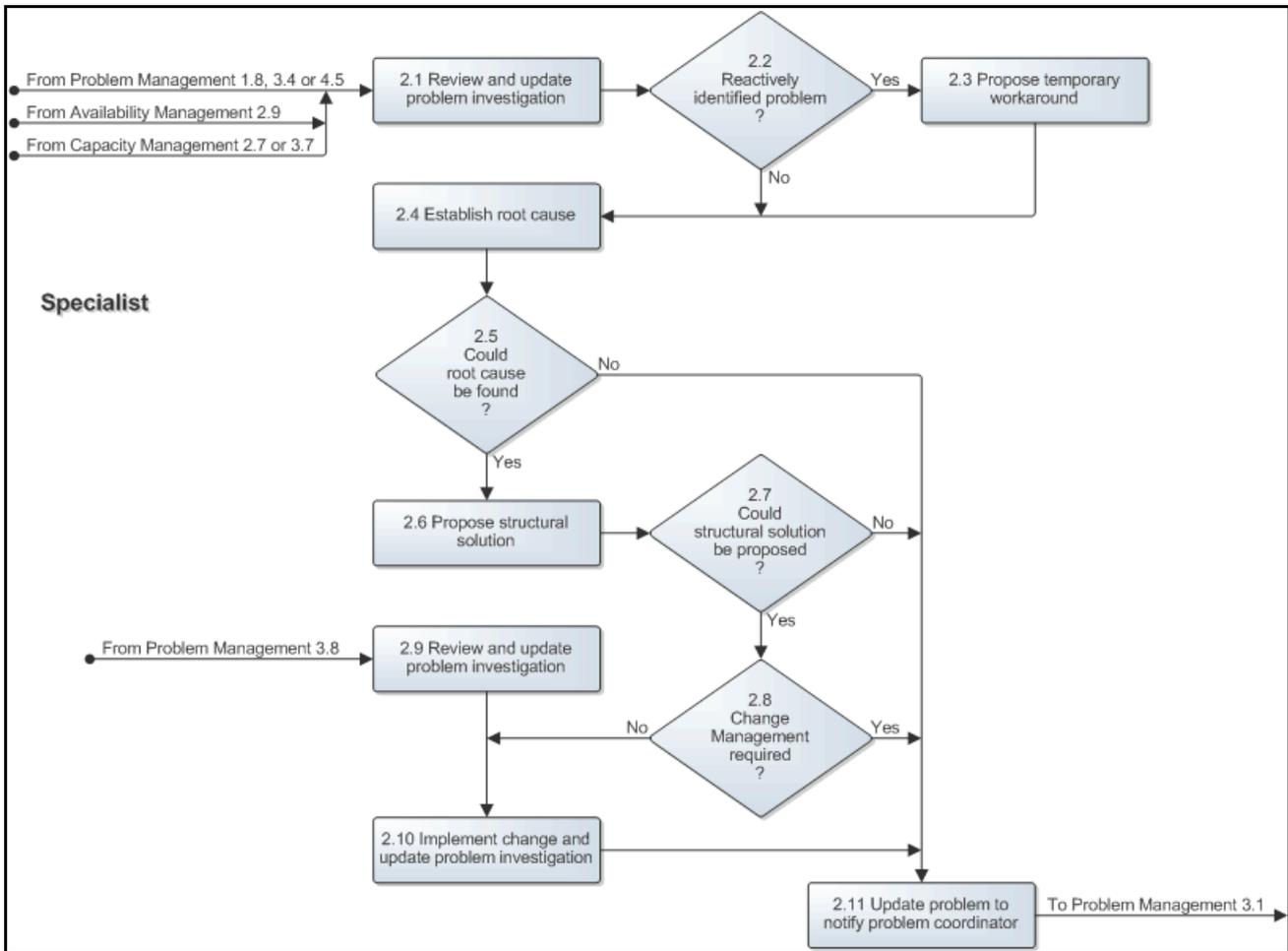
Next, the specialist considers possible structural solutions and evaluates them. A description of each option is added to the problem investigation along with the recommendation for the preferred structural solution.

If Change Management is not required to permanently work around or remove the root cause, the specialist implements the preferred structural solution.

If the specialist is not able to find the root cause or is not able to propose a structural solution, he/she specifies the reason for this in the problem investigation. Regardless of whether a structural solution was proposed or even already implemented, the specialist informs the problem coordinator that his/her work has been completed.

The Root Cause Analysis procedure diagram is presented below.

Figure 9-3: Root Cause Analysis



Procedure 3, Analysis Review

After a specialist has completed the root cause analysis of a problem, the problem coordinator reviews the results to determine if a structural solution has been proposed or has been implemented already. If the specialist has already fixed the problem because Change Management was not required to coordinate the implementation of the structural solution, the problem coordinator goes directly to Procedure 4, Problem Closure.

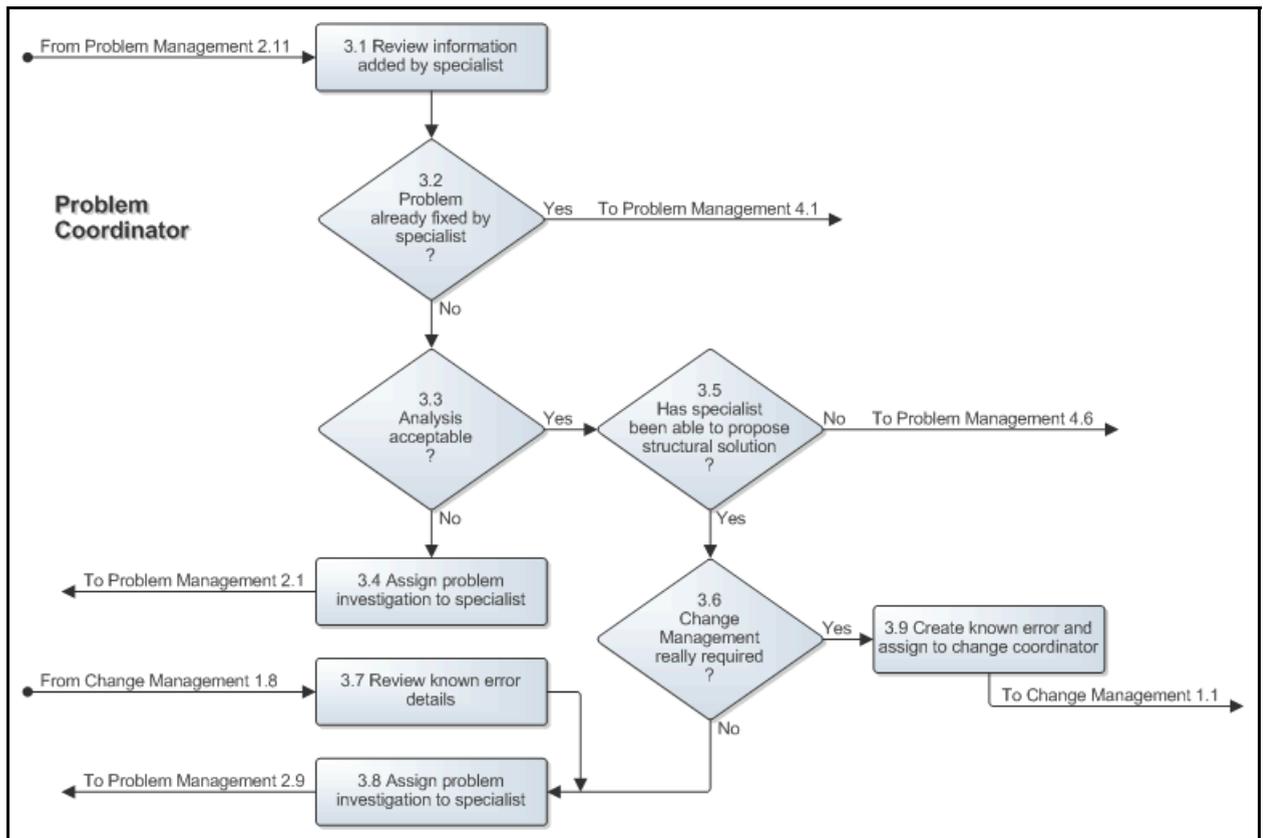
The problem coordinator also goes to Procedure 4, Problem Closure if the specialist performed a good analysis but was not able to propose a practical structural solution.

If the specialist proposed a practical structural solution, but did not implement it because he/she believed Change Management to be required, the problem coordinator checks to see whether Change Management is really needed. If this is not the case, the problem management assigns the problem investigation to the most appropriate specialist to get the problem fixed. If Change Management is really required, the problem coordinator generates a known error and passes it to the change coordinator of the affected service.

If the analysis of the specialist is not acceptable, however, the problem coordinator reassigns the problem investigation to the same or another specialist for a better analysis.

The Analysis Review procedure diagram is presented below.

Figure 9-4: Analysis Review



Procedure 4, Problem Closure

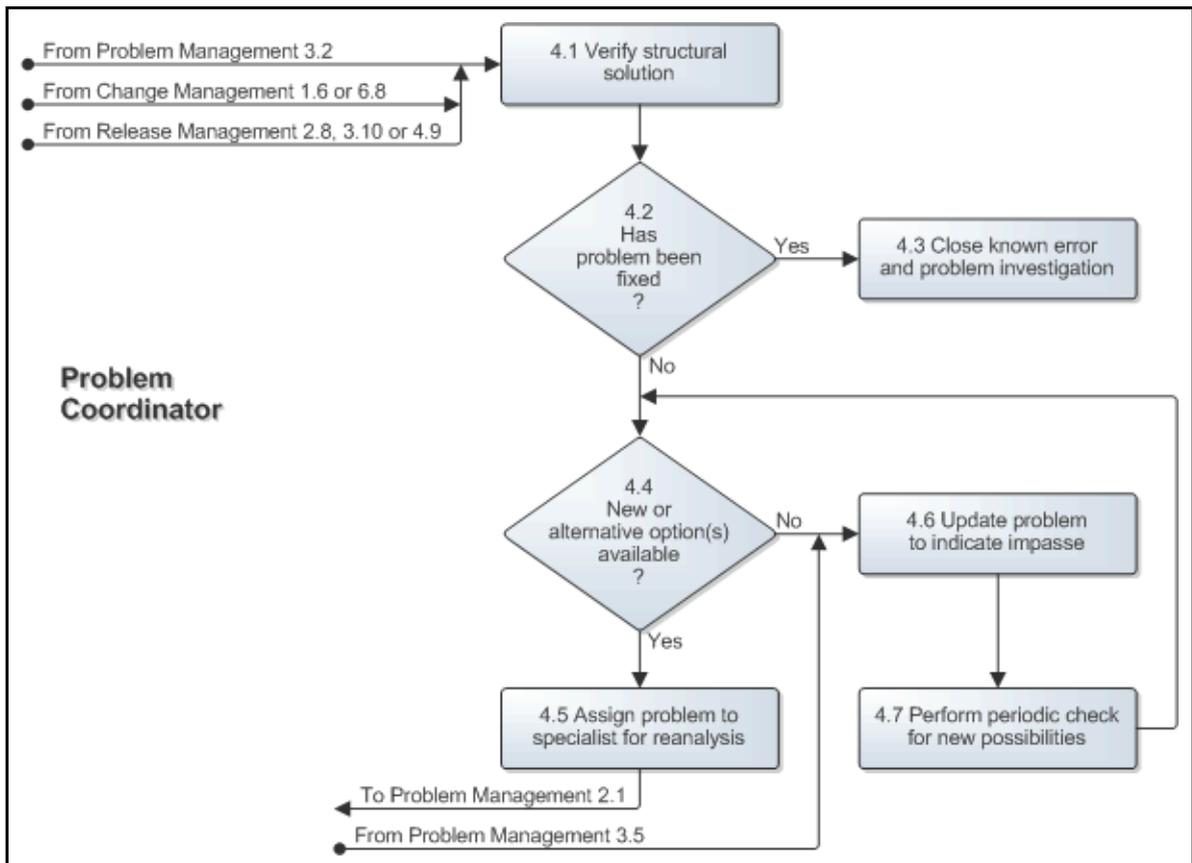
After a change has been implemented to provide a structural solution for the problem, the problem coordinator verifies whether or not the change has actually solved the problem.

If the implementation appears to have solved the problem, the problem coordinator closes it. On the other hand, if the change was not implemented, or if the implementation did not fix the problem, the problem coordinator determines if it might be possible to propose a different structural solution for the problem. If this might be possible, the problem coordinator reassigns the problem investigation to a specialist within his/her group.

Alternatively, if it is clear that there is currently no practical means available to permanently work around or remove the root cause, the problem coordinator updates the problem investigation to indicate the impasse. Periodically, the problem coordinator will then check for new possibilities and will ask for another analysis when it is likely that a new or different approach or technology could provide a practical structural solution.

The Problem Closure procedure diagram is presented below.

Figure 9-5: Problem Closure



Chapter 10 Release Management

The Release Management process consists of four procedures.

The first procedure is called "Request for Change Handling". It is used by the release coordinators to review the requests for change that have been passed to Release Management.

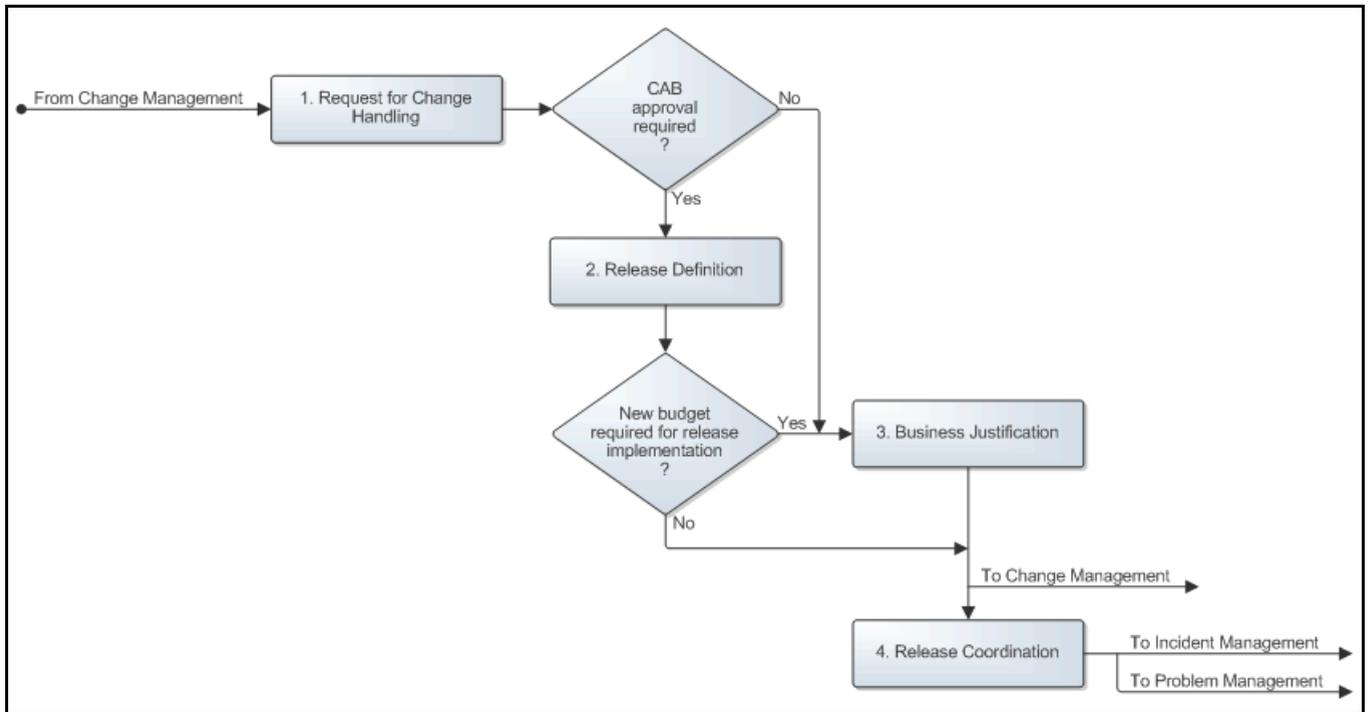
The second procedure is called "Release Definition". This procedure is used by release coordinators to organize CAB meetings and by CAB members when they decide which of the requests for change that have been collected for CAB review should be fulfilled by the next release. Release coordinators also use this procedure to split the requirements of releases into logical groups that can be handled efficiently by change coordinators.

The third procedure is called "Business Justification". It is used by the release coordinators when additional funding needs to be obtained for the implementation of a release.

The fourth procedure is called "Release Coordination". Release coordinators use this procedure to initiate the implementation of releases and to decide on corrective actions as needed.

A graphical representation of the process is provided on the next page. Each procedure is described in more detail in the sections that follow this diagram.

Figure 10-1: Release Management process description



Procedure 1, Request for Change Handling

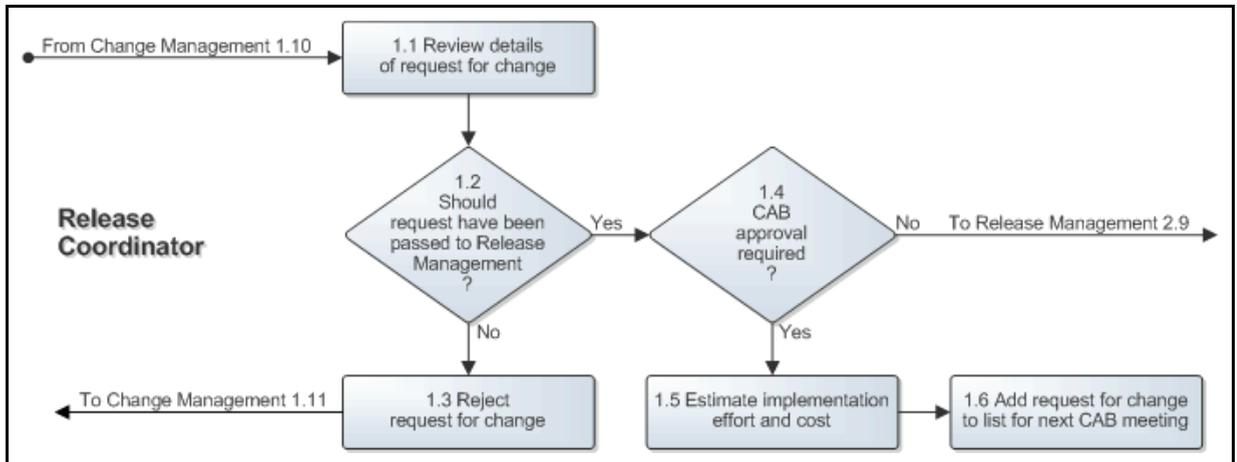
After a change coordinator of a service has passed a request for change to the release coordinator of the service, the release coordinator reviews the request for change to gain an understanding of its requirements. The release coordinator passes the request for change back to the change coordinator if it does not require the involvement of Release Management. Only requests for change that ask for the implementation of a non-standard change must be handled by Release Management, with the exception of requests for change that have been submitted for the prevention or fix of a problem, provided that their implementation:

- can be coordinated by a single change coordinator.
- will not cause the functionality of a service to become different.
- does not require any additional funding.

If the request for change does require the involvement of Release Management, the release coordinator checks to see if it requires CAB approval. The CAB does not need to review the change if it asks for the implementation of a change to prevent or fix a problem and if this change will not cause the functionality of a service to become different. If CAB approval is required, however, the release coordinator estimates the implementation effort and cost, and adds the request for change to the list that will be reviewed during the next meeting of the service's CAB.

The Request for Change Handling procedure diagram is presented on the next page.

Figure 10-2: Request for Change Handling



Procedure 2, Release Definition

When the next CAB meeting for a service is due, the release coordinator of the service sends out the invitations to the service's CAB members. In the invitation, the release coordinator specifies the deadline until which requests for change can be submitted for review during the next CAB meeting. After the request for change submission deadline has passed, the release coordinator finalizes the list of requests for change that will be reviewed during the next CAB meeting and sends it to the CAB members so that they can discuss the requests for change internally before the meeting.

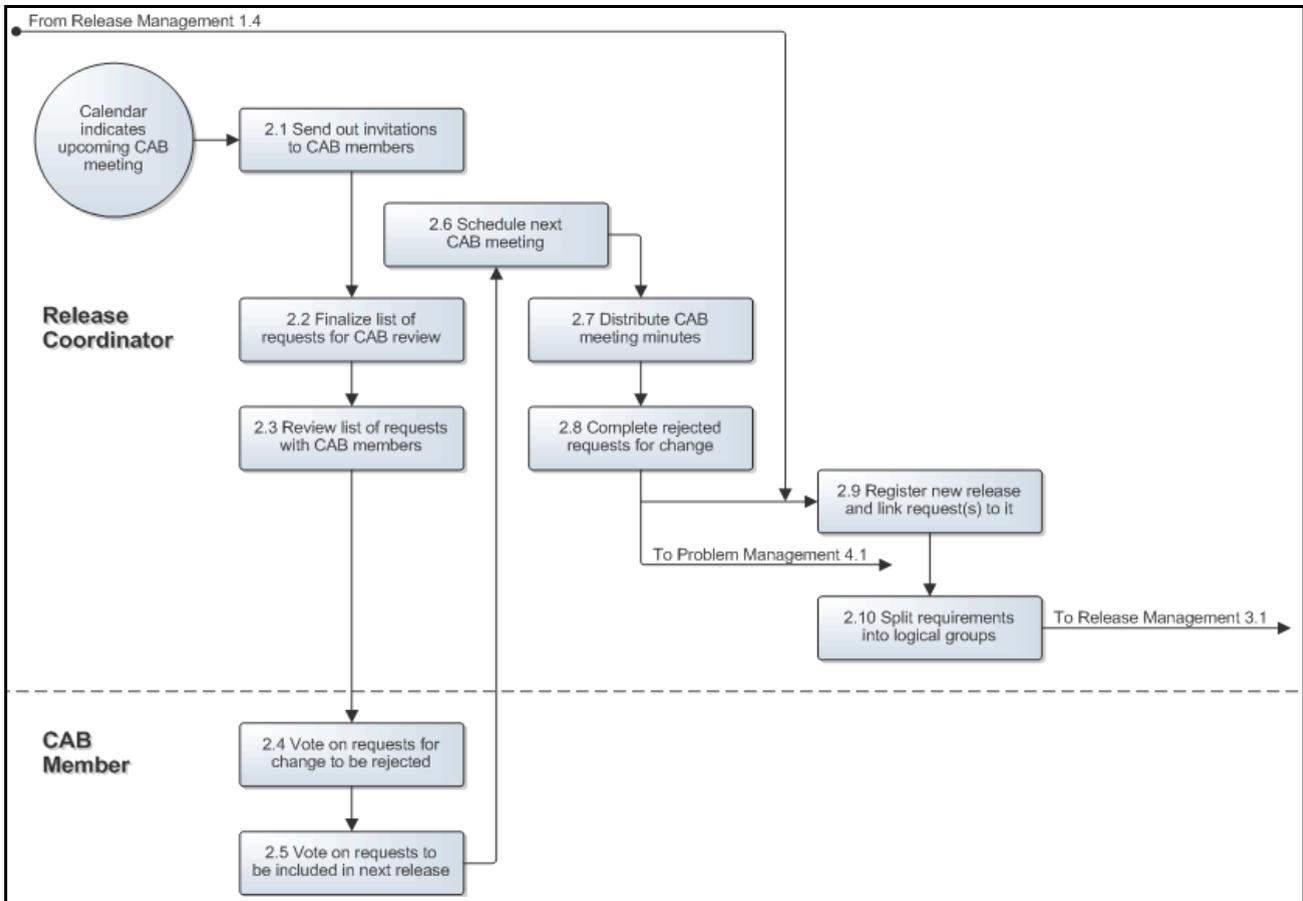
The finalized list of requests for change is reviewed during the meeting. After all requests for change have been reviewed, each CAB member lets the release coordinator know which requests for change he/she would like to see rejected and which requests for change he/she would like to see included in the next release. A request for change is rejected when at least two-thirds of the CAB members agree that it should be rejected. Similarly, a request for change is included in the next release when two-thirds or more of the CAB members have asked for it to be included. Requests for change that are neither rejected nor included in the next release will be reviewed again during the next CAB meeting. Before closing the CAB meeting, the CAB members agree on the date, time and location of the next CAB meeting.

After the CAB meeting, the release coordinator closes the rejected requests for change and ensures that the requesters are informed. Having done this, the release coordinator publishes the minutes of the CAB meeting and registers the new release. To this release he/she links the requests for change that are to be included in the release.

The release coordinator then reviews these requests for change with the change coordinator of the service for which the release is to be implemented and the change coordinators of the supporting services that will also need to be changed. Together they divide the requirements of the different requests for change amongst them and they draft a high-level implementation plan that indicates the duration of each change, as well as the dependencies between these changes.

The Release Definition procedure diagram is presented below.

Figure 10-3: Release Definition



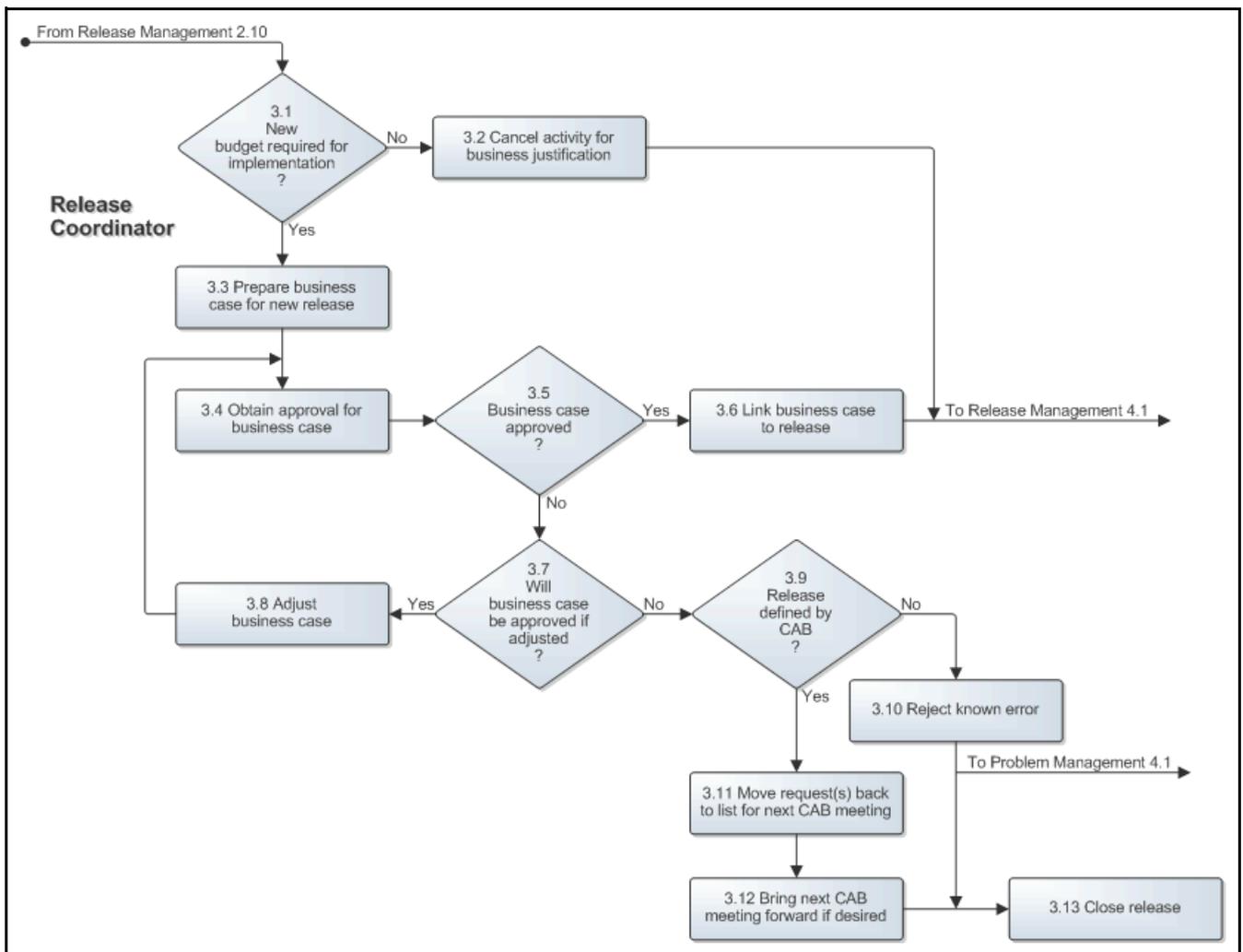
Procedure 3, Business Justification

If an approved business case is not required for the release, the release coordinator cancels the business justification activity that is part of the release. On the other hand, if the next release cannot be implemented using the budget(s) already available to the service owner, the release coordinator prepares a business case to justify the release. Having prepared the business case, the release coordinator requests approval for the business case to ensure that a budget will be made available for the implementation of the new release.

If the business case was rejected, the release coordinator adjusts it if an adjusted business case for the release could still get the necessary approvals. If it is not possible to get the business case approved, the release coordinator lets the requesters of the release know that the business case for the release has been rejected. If the release was defined by the CAB, the release coordinator moves the requests for change that are linked to the release back to the backlog release that acts as the placeholder for requests for change that are to be reviewed during the next CAB meeting. Before closing the release, the release coordinator also contacts the CAB members to inform them that the business case for their release has been rejected and gives them the option to bring the next CAB meeting forward.

The Business Justification procedure diagram is presented below.

Figure 10-4: Business Justification



Procedure 4, Release Coordination

The release coordinator prepares a document for each change coordinator that details the release requirements that the change coordinator will be responsible for. The release coordinator sends the requirement documents to the change coordinators and ensures that the requested changes are registered and linked to the release.

When a change coordinator has notified the release coordinator that one of the release's changes has been completed, the release coordinator enters a short update in the release.

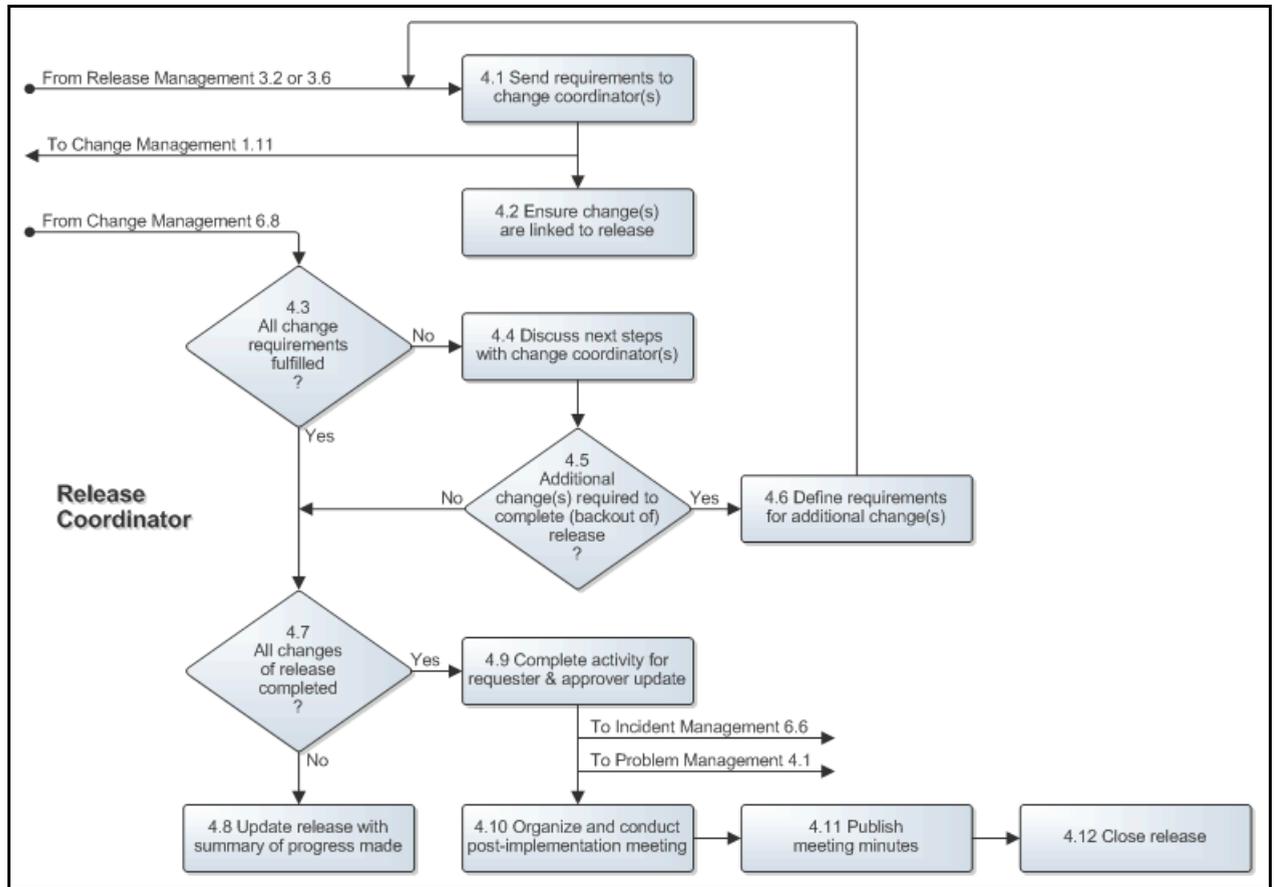
If the requirements of the change could not all be fulfilled, the release coordinator works with the change coordinators that have been asked to coordinate changes for the release to determine how the (partial) failure of the change implementation affects the overall implementation of the release. If it is still possible to implement one or more additional changes to ensure that all or most requirements of the release are fulfilled, or if one or more additional changes are required to ensure that the black-out of the release is completed, the release coordinator documents the requirements for the additional change(s) before passing them to the appropriate change coordinator(s).

After the last change that a change coordinator was asked to get implemented for the release has been completed, the release coordinator ensures that the requesters are informed whether or not their requirements were fulfilled by the release implementation. If the release was defined by the CAB, the release coordinator moves any requests for change which requirements were not fully met back to the backlog release that acts as the placeholder for requests for change that are to be reviewed during the next CAB meeting. The release coordinator also informs the CAB members (if the release was defined by them) and the approvers of the business case (if one had to be prepared for the release).

Having updated the requesters and approvers of the release, the release coordinator continues by organizing and conducting the post-implementation meeting. During this meeting, the release coordinator reviews the entire lifecycle of the release with the service owner of the service for which the release was implemented and the change coordinators who coordinated one or more of the release's changes. After the meeting, the release coordinator publishes the improvement suggestions and decisions that were agreed on by the attendees of the meeting. Finally, the release coordinator closes the release.

The Release Coordination procedure diagram is presented on the next page.

Figure 10-5: Release Coordination



Chapter 11

Service Level Management

The Service Level Management process consists of five procedures.

The first procedure is called "Service Catalog Maintenance". It is used by service level administrators when a change coordinator has asked for a new catalog item to be registered.

The second procedure is called "Service Activation". This procedure is followed by service level administrators after a customer has selected a catalog item and has decided to subscribe to the service at the level specified by this catalog item.

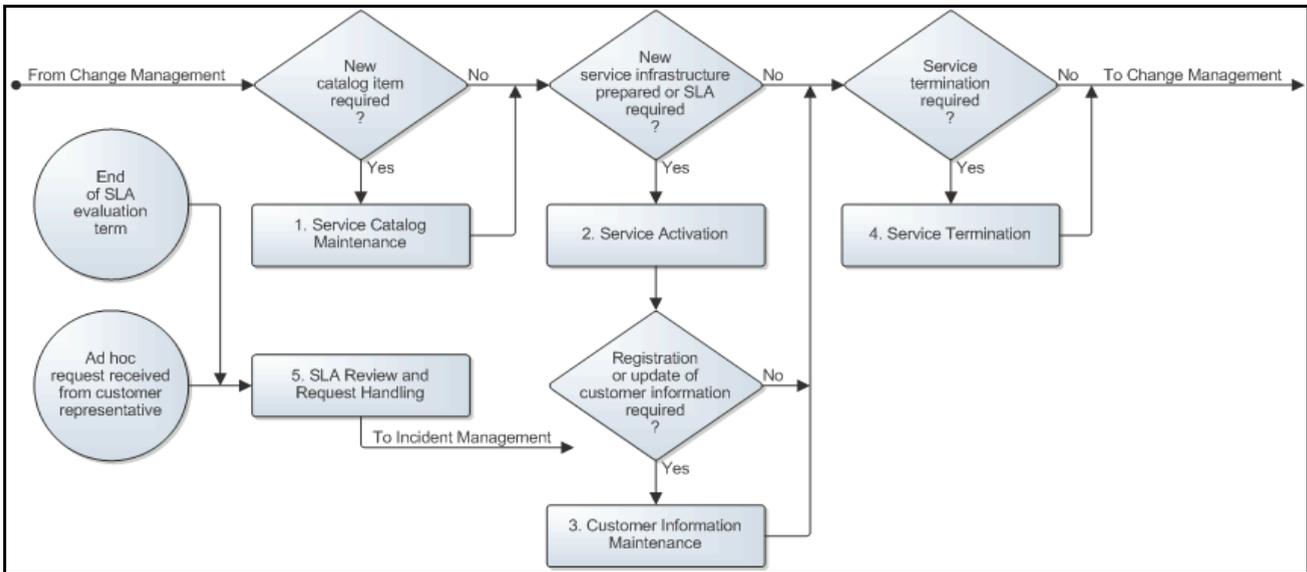
The third procedure is called "Customer Information Maintenance". This procedure is used by service level administrators when they register new customers of the service provider organization. They also use this procedure when they update the contact information that has been registered for these customers.

The fourth procedure is called "Service Termination". It is used by service level administrators when a service, catalog item and/or SLA is discontinued.

The fifth procedure is called "SLA Review and Request Handling". This procedure is used by service level managers when reviewing SLAs at the end of their respective evaluation terms. The service level managers also use this procedure when customer representatives contact them to submit requests.

A graphical representation of the process is provided on the next page. Each procedure is described in more detail in the sections that follow this diagram.

Figure 11-1: Service Level process description



Procedure 1, Service Catalog Maintenance

Changes that cause the Service Level Management information to require an update include a task that is assigned to the service level administrator requesting this update to be performed.

When the service level administrator receives such a task, he/she determines whether a new catalog item is required. If this is not the case, the service level administrator skips the rest of this procedure and goes to Procedure 2, Service Activation. If a new catalog item is required, however, the service level administrator prepares it using the Catalog Item Template, or by copying a similar catalog item.

Having prepared the new catalog item, the service level administrator gets it approved by:

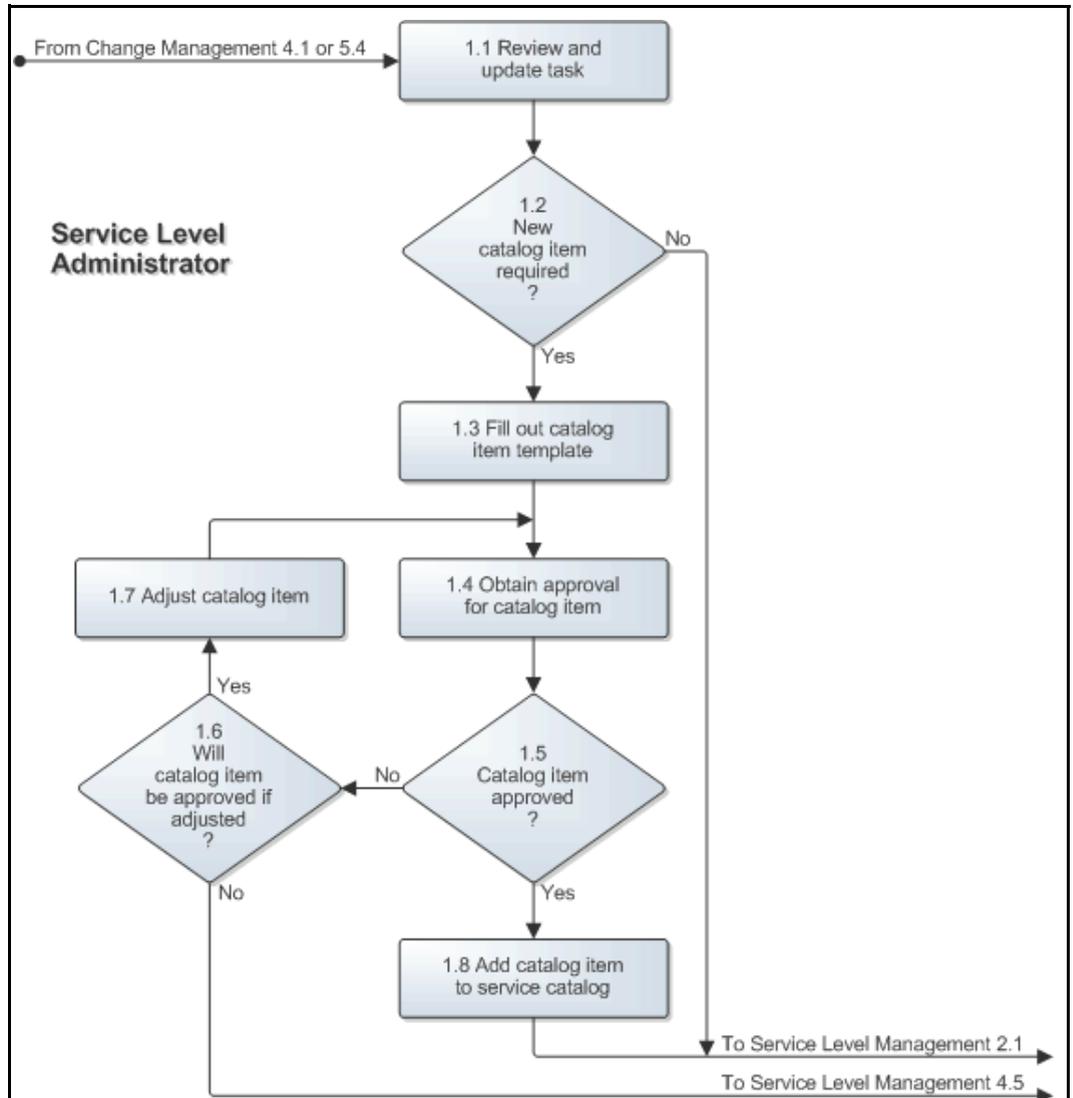
- the service owner who will be responsible for meeting the SLTs specified in the catalog item,
- the service level manager(s) of the customer organization(s) for which the catalog item has been prepared to ensure that the SLRs of the customer(s) are covered by the catalog item, and
- the financial manager of the service provider organization whose commitment is required for the financial aspects of the catalog item.

If the approvers require adjustments to be made before the new catalog item can be signed, the service level administrator adjusts the catalog item as needed until all approval signatures have been collected. If the approvers cannot reach an agreement, however, the service level administrator goes to Procedure 4, Service Termination to indicate in the task why the creation of the new catalog item has failed.

When the approvers have all signed the new catalog item, the service level administrator adds it to the service provider organization's web-based service catalog. If the new catalog item was prepared as a one off to meet the specific SLRs of one customer, the service level manager ensures that the published version of the new catalog item cannot be accessed by customers.

The Service Catalog Maintenance procedure diagram is presented on the next page.

Figure 11-2: Service Catalog Maintenance



Procedure 2, Service Activation

If the task for the Service Level Management information update requests the registration of a new service infrastructure the service level administrator does this by filling out the Business Service form in the service management application.

If the task requests the preparation of a new SLA, the service level administrator prepares the new SLA by filling out the Service Level Agreement Template, printing two copies, and attaching a printout of the relevant catalog item to each copy. The service level administrator then collects the signatures of both the customer representative and the service owner who will be responsible for meeting the SLTs specified in the SLA.

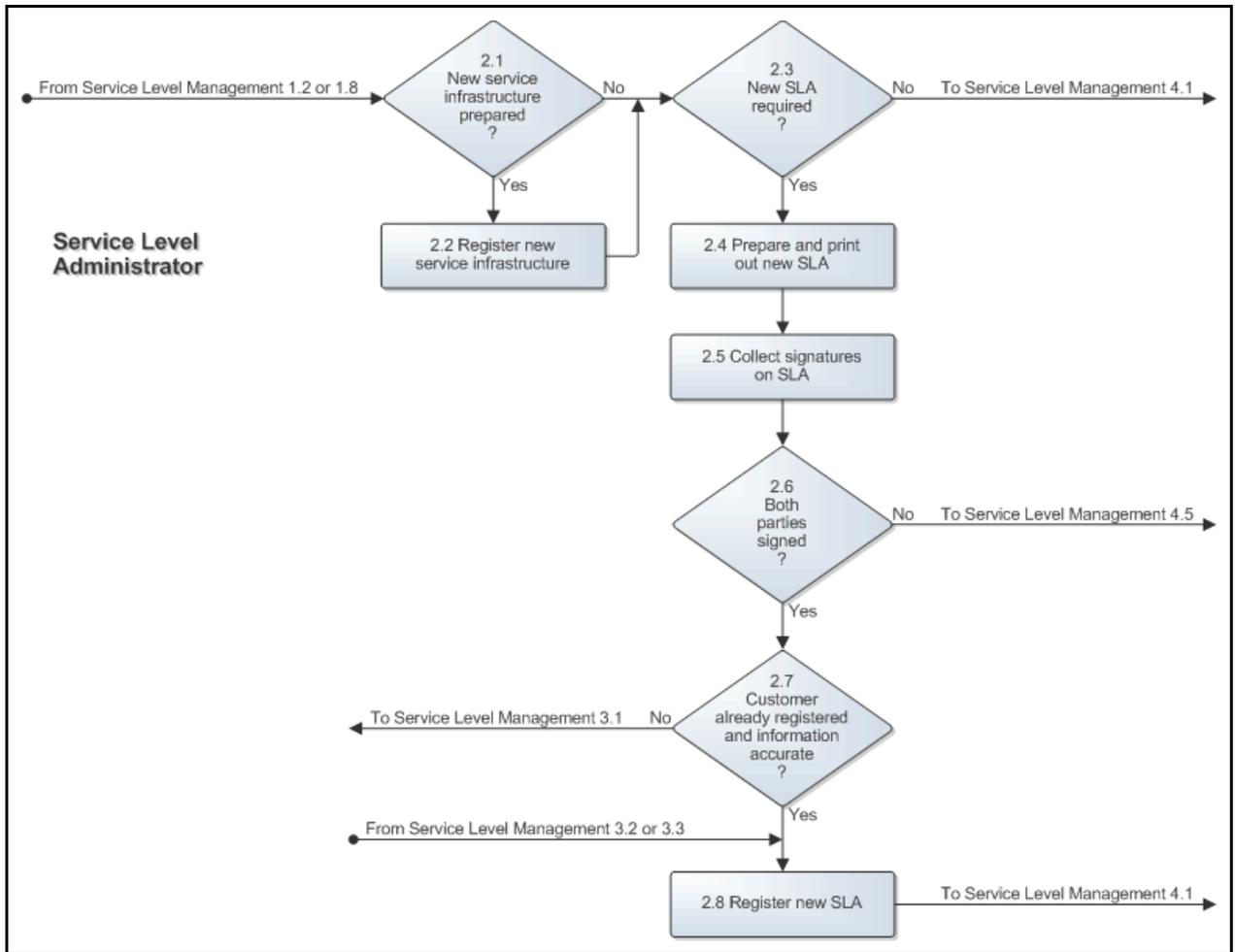
If either the customer representative or the service owner decided not sign the SLA, the service level administrator goes to Procedure 4, Service Termination to indicate in the task why the new SLA could not be established. On the other hand, if the new SLA was signed, the service level administrator files one copy of the signed SLA and returns the other to the customer representative for his/her files.

Before registering the new SLA, the service level administrator checks the service management application to see if the contact details of the customer are up-to-date. If the customer of the SLA has not yet been registered, or if the contact details of the customer are no longer up-to-date, the service level administrator ensures that the customer information is registered or updated in Procedure 3, Customer Information Maintenance.

When the customer's contact details are up-to-date, the service level administrator registers the new SLA in the service management application to ensure that the application monitors the SLTs to help avoid violations.

The Service Activation procedure diagram is presented on the next page.

Figure 11-3: Service Activation



Procedure 3, Customer Information Maintenance

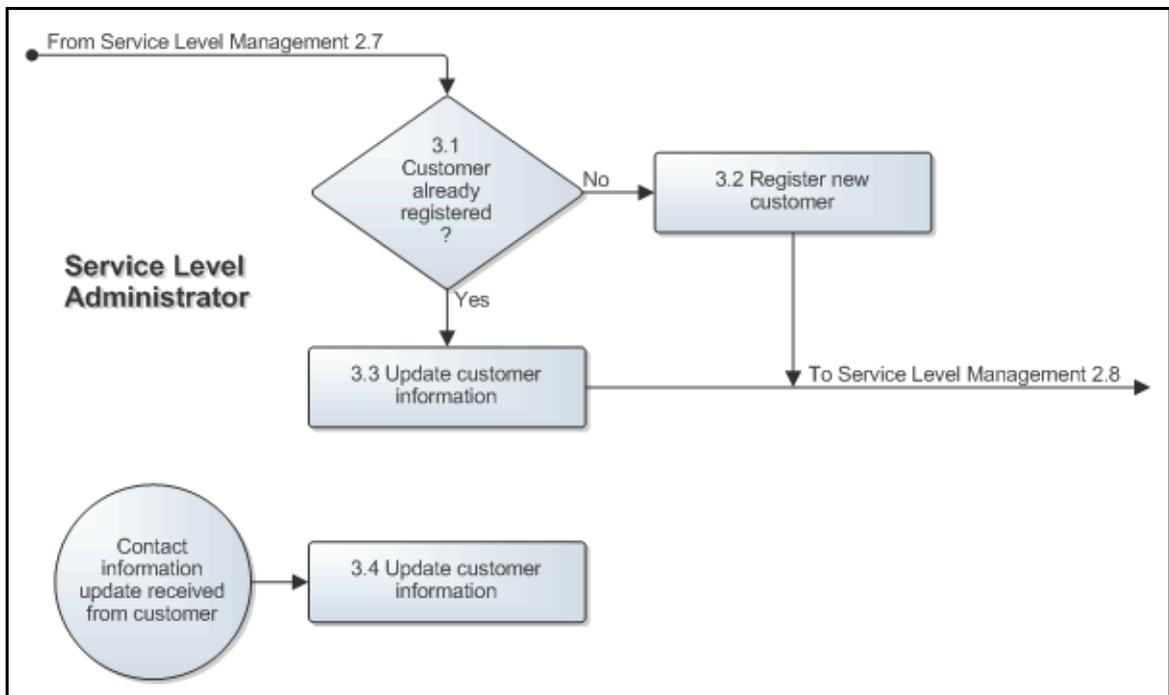
The service level administrators are responsible for registering and updating the contact details of the service provider organization's customers.

A service level administrator performs the customer information maintenance tasks when customers subscribe to one of the provider's services for the first time (i.e. before registering new SLAs) and whenever updated contact information has been received from an existing customer.

If an individual customer or a customer organization is not already registered, the service level administrator adds this customer. If the customer already exists in the service management application, the service level administrator updates the customer's contact information. All this is done in accordance with the field utilization guidelines for the Organization Update form when it concerns a customer organization. If it concerns an individual customer, a customer representative, or a person who works for the customer organization and must be supported by the service provider organization, the service level administrator follows the field utilization guidelines for the People form.

The Customer Information Maintenance procedure diagram is presented below.

Figure 11-4: Customer Information Maintenance



Procedure 4, Service Termination

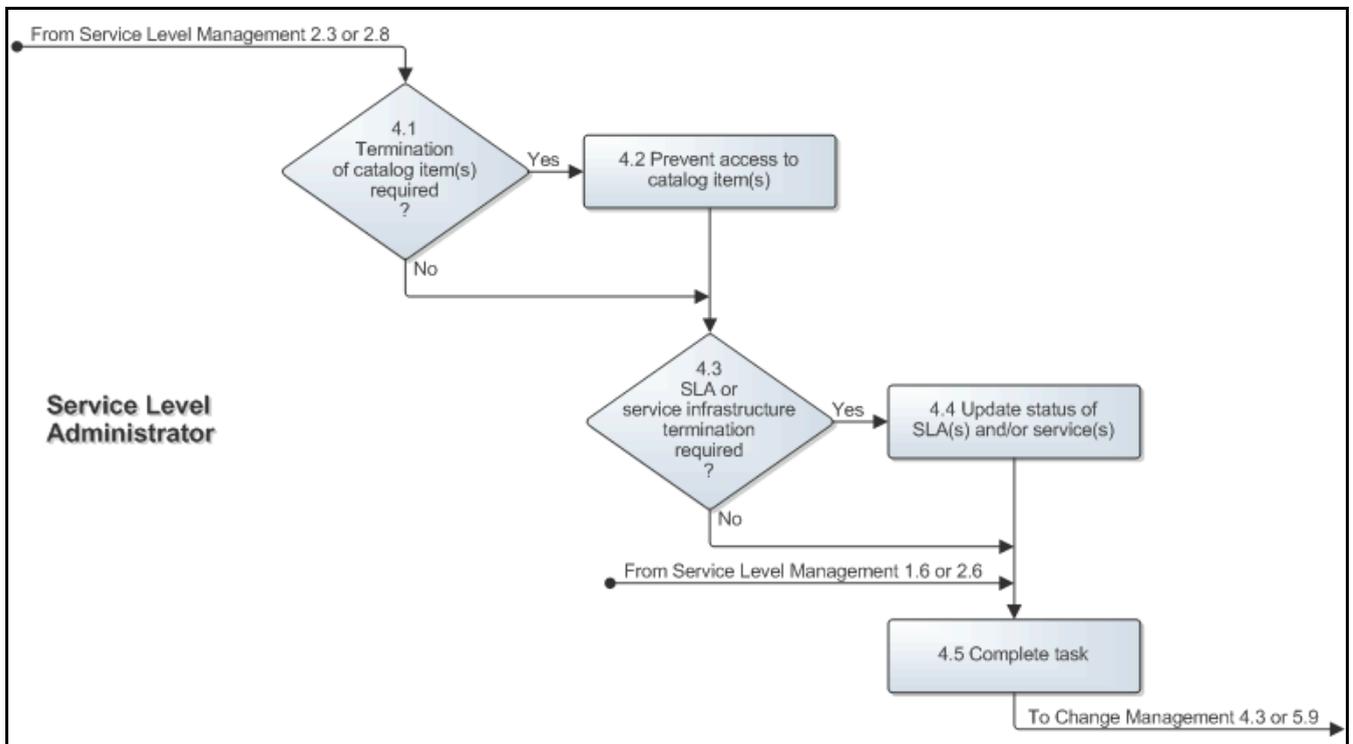
If the task for the Service Level Management information update requests the discontinuation of a catalog item, the service level administrator does this by ensuring that it can no longer be accessed from the service provider organization's web-based service catalog by customers.

If the task requests the termination of one or more SLAs, the service level administrator updates the SLA information in the service level management application to ensure that the SLTs are no longer monitored. In addition, the service level administrator indicates on the signed hardcopy version of such SLAs that they have been discontinued. Finally, the service level administrator checks if there are any active SLAs left for the service for which the SLA(s) were discontinued. If there are no more active SLAs left for this service, the service level administrator also discontinues the service by updating its status in the service management application.

When no further action is required from the service level administrator in terms of updating the Service Level Management information, he/she updates the task. He/she does this to inform the change coordinator that the task has either been performed successfully or failed (e.g. because the requested catalog item was not approved, or because the requested SLA was not signed).

The Service Termination procedure diagram is presented below.

Figure 11-5: Service Termination



Procedure 5, SLA Review and Request Handling

When the SLA(s) of one of the service level manager's customer organizations have reached the end of their evaluation term, he/she schedules a meeting with the representative for this customer. Next, the service level manager determines the actual level at which the service(s) have been provided over the past term to the customer of the SLA(s).

The service level manager subsequently compares the actual service levels with the service level targets (SLTs) specified in the SLA(s). If one or more SLTs were violated during the evaluation term, the service level manager contacts the responsible service owners to find out why the SLTs were violated and how the service owner will ensure that these SLTs will not be violated again. The service level manager uses all this information, along with his/her proactive improvement suggestions, to compile a detailed report for the customer representative.

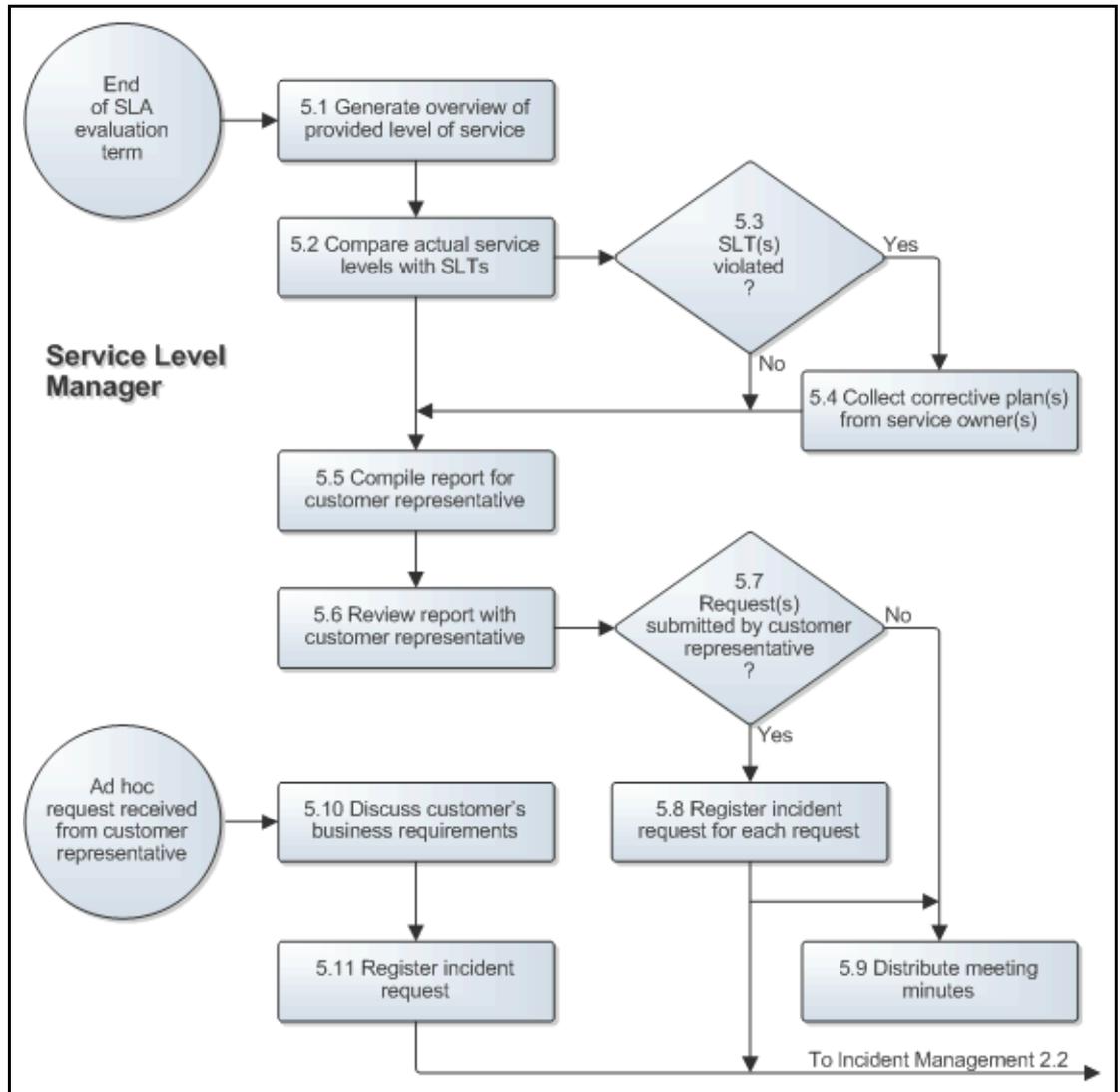
The service level manager reviews the report with the customer representative, preferably within one month after the end of the evaluation term. During the meeting the customer representative informs the service level manager of any requests from the customer organization that he/she represents.

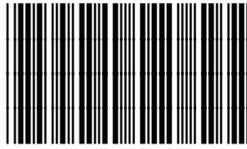
After the meeting the requests are registered as incident requests by the service level manager and passed to the most appropriate group. The service level manager then documents the minutes of the meeting and references the numbers of these incident requests. The minutes are distributed to the customer representative, the concerned service owner(s), and the manager of the service desk.

Ad hoc requests from customer representatives are also registered by the service level manager and passed to the most appropriate group.

The SLA Review and Request Handling procedure diagram is presented on the next page.

Figure 11-6: SLA Review and Request Handling





106430