[organization logo]

[organization name]

INCIDENT MANAGEMENT PROCESS

Code:	
Version:	
Date of version:	
Created by:	
Approved by:	
Confidentiality level:	

Comment [BV1]: All fields in this document marked by square brackets [ ] must be filled in.

Comment [BV2]: If you want to find out more about Incident Management process, see http://www.20000academy.com/Blog/May-2013/Incident-Management-in-ITIL-solid-foundations-of-operational-processes

Comment [BV3]: The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.

Change history

Date	Version	Created by	Description of change
xx/xx/2013	0.1	Branimir Valentic	Basic document outline

Table of contents

1. Purpose, scope and users

The aim of this document is to define the purpose, scope, principles and activities for the Incident Management process.

This document is applied to the entire IT organization.

Users of this document are all employees of [organization name], as well as all external parties who have a role in IT Service Management (ITSM).

Comment [BV4]: ***OPTION***
Replace this with "SMS" if you are implementing ISO 20000.

Comment [BV5]: ***OPTION***
Replace this with "SMS" if you are implementing ISO 20000.

2. Reference documents

- Incident Management Policy
- Incident Measurement and Metrics
- Problem Management Process
- Release and Deployment Management Process
- Service Asset and Configuration Management Process
- Service Level Agreement Management Process
- Information Security Management Process
- ISO/IEC 20000-1:2011, clause 8.1.
- ISO/IEC 20000-1:2011, clause 6.6.3.

Comment [BV6]: ***OPTION***
Delete this if you are implementing ITIL and not ISO 20000.

3. Process activities

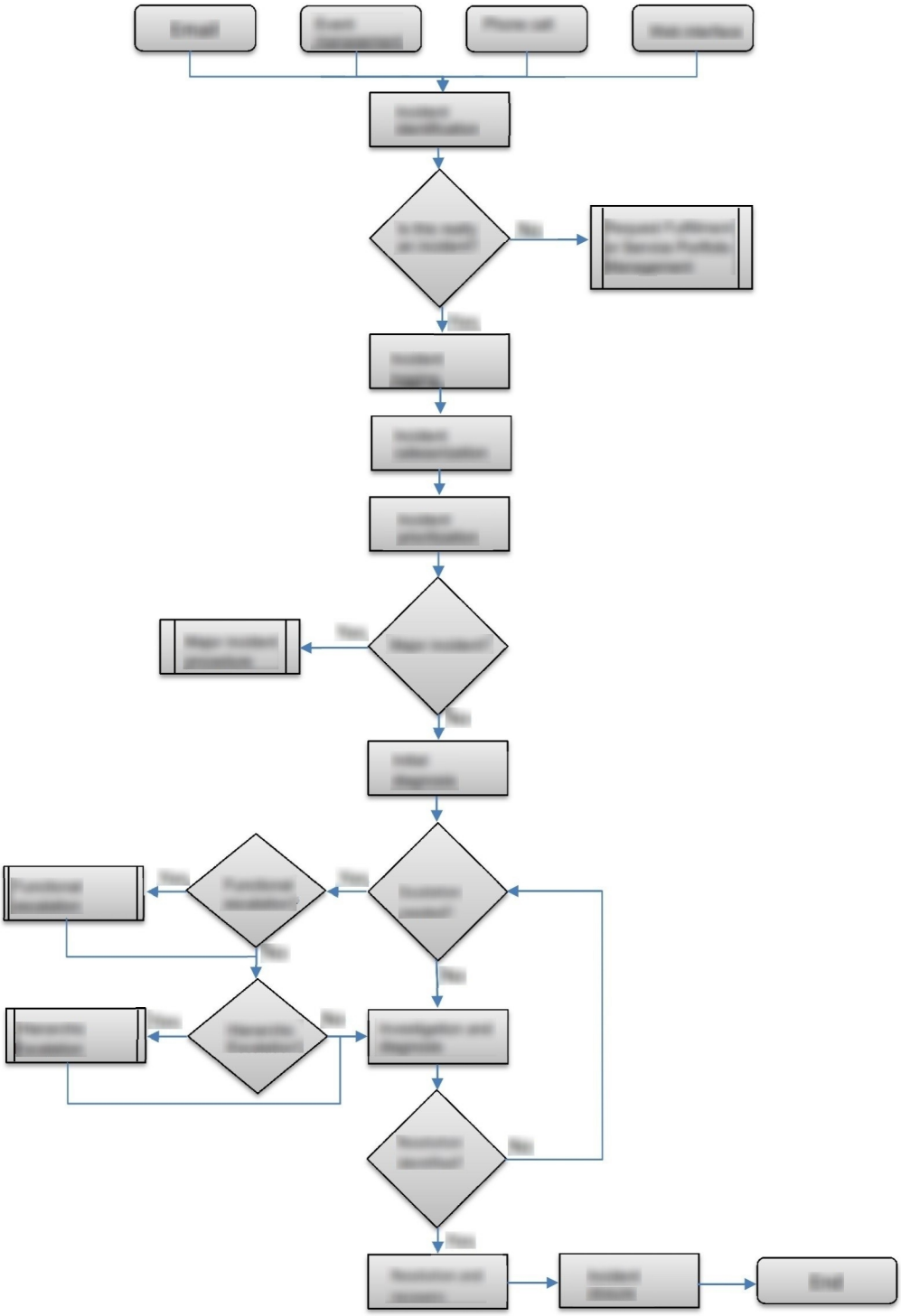

Figure: Incident Management process activities

Incidents can be detected by [illegible]

3.1. Incident identification

This is the stage where an Incident has been recognized. Sources of an Incident are:

Source	[illegible]
Web portal: [insert web or intranet address]	User
Phone: ○ [illegible] ○ [illegible]	Service Desk staff
E-mail [...]	[illegible]
[illegible]	Event Manager

[Service Desk staff] is responsible to pass [illegible] Request Fulfillment process by [...].

3.2. Incident logging

An incident can be logged by:

a) User
   - Using web portal, [insert web or intranet address]
   - E-mail [...]
   - Phone:
     - [illegible]
     - Outside agreed service hours: [...]

b) Event tool: [enter tool(s) name]

Organization uses [tool name] tool for Incident Management. [illegible] data.

Service Desk staff is responsible for entering [illegible] phone.

Mandatory data that need to be recorded are:

- Incident number – provided automatically
- [illegible]
- User name / department / location (if other than Requestor)
- [illegible]
- [illegible]
- Description

Incident assignees are responsible, as the incident progress to the resolution, for ensuring that every [illegible] resolution is available.

Comment [BV7]: Double-click to edit figure and adapt to your own requirements.

Comment [BV8]: ***OPTION*** Delete this figure if you are implementing ISO20000 and not ITIL.

Comment [BV9]: Delete redundant or [illegible] missing.

Comment [BV10]: ***OPTION*** Delete this section if you are implementing ISO20000 and not ITIL.

Comment [BV12]: Delete if Incidents cannot be opened by phone, i.e. change responsible function as needed.

Comment [BV11]: Insert phone number in appropriate format.

Comment [BV13]: Insert e-mail address which is used to open an Incident.

Comment [BV14]: Insert monitoring tools that are integrated with Incident Management tool.

Comment [BV15]: If tool is used to keep incident records – use tool [illegible] manually open new service request.

Comment [BV16]: Insert e-mail address which is used to open an Incident.

Comment [BV17]: Insert phone number in appropriate format.

Comment [BV18]: ***OPTION*** Delete this if you are implementing ITIL and not ISO20000.

Comment [BV19]: Insert Incident Management tool name.

Comment [BV20]: Insert Incident Management tool name.

Comment [BV21]: Delete if Incidents cannot be opened by phone, i.e. change responsible function as needed.

Comment [BV22]: Delete if not true.

Comment [BV23]: 2
- Support group/person to which the incident is allocated
- [illegible]
- Closure category
- Closure date and time

Comment [BV24]: Change if necessary. Example: 1st Level support, 2nd Level support, Service Desk staff...etc. This is done by person working on incident, i.e. incident assignee.

3.3. Incident categorization

During the logging phase, incidents are categorized. Service Desk staff categorizes incidents [illegible] Service Desk and can be re-categorized.

Categories are set in 3 levels as defined in the Incident Catalogue; see Incident Catalogue in Appendix.

3.4. Incident prioritization

[role description] is responsible for ensuring that every incident is prioritized. Priority consists of [illegible] has [illegible] based on the following table:

[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	1	2	3
[illegible]	[illegible]	[illegible]	4
[illegible]	[illegible]	[illegible]	[illegible]

Resolution time of an incident depends on its priority code and is calculated as follows:

[illegible]	Description	Target Resolution Time
1	Critical	[illegible]
2	[illegible]	[illegible]
3	[illegible]	[illegible]
4	[illegible]	[illegible]
5	Planned	24 hours

Impact – business impact [illegible] causes:

High	Medium	Low
[illegible]	30% - [illegible]	Less than 30% of users are affected
[illegible]	35 - [illegible]	Less than 35% of services are affected

Urgency – how [illegible] a resolution:

High	Medium	Low
[illegible] available	[illegible] workaround exists	[illegible] good workaround exists

Comment [BV25]: If you want to learn more about Incident categorization, i.e. classification, see http://www.20000academy.com/Blog/March-2013/All-About-Incident-Classification#

Comment [BV26]: ***OPTION*** If you are using this document for ISO 20000, replace "categorization" with "classification," which is more common in ISO 20000.

Comment [BV27]: [illegible]

Comment [BV28]: Change if needed. Examples of who can change category are: 1st Level technician, Service Manager, Service Desk Manager...etc.

Comment [BV29]: It is advisable to [illegible] groups.

Comment [BV30]: Service Desk is usually adequate.

Comment [BV31]: Can be adapted according to organization's needs.

Comment [BV32]: [illegible]

Comment [BV33]: This is an example. Change for particular service, insert it into SLA/OLA/UC and communicate to support staff.

Comment [BV34]: This is an example. Change for particular service, insert it into SLA/OLA/UC and communicate to support staff.

Comment [BV35]: [illegible]

Change of priority – [illegible] changed by the Service Desk or incident assignee.

VIP treatment – priority for VIPs is [...].

3.5. Initial diagnosis

Initial diagnosis is performed by [role description], with the goal being to resolve the incident without [illegible] diagnosis.

Matching of incidents to problems and known errors [illegible] as quickly as possible and/or save time needed for escalation.

To use existing information and knowledge, [incident assignee] has access to and uses the following resources:

- Known Errors – see Known Error in Appendix of Problem Management Process
- [illegible] Problem Record in Appendix of Problem Management Process
- [illegible] – see CMDB in Appendix of the Service Asset and Configuration Management Process
- Release report and Release plan – see Release and Deployment Planning in Appendix of the Release and Deployment Management Process

3.6. Escalation

There are two escalation possibilities:

- Functional escalation
- Hierarchical escalation

The Service Desk is responsible for the [illegible] This includes tracking progress, keeping users informed and incident closure.

3.6.1. Functional Escalation

Functional escalation is triggered by [role description]/[tool name]. Functional escalation of an incident is escalation to specialist group. The OLA (Operation Level Agreement) and UC (Underpinning Contract) define under which circumstances an incident will be escalated. The Service Desk is [illegible] resolution.

3.6.2. Hierarchical Escalation

Hierarchical escalation is triggered by [role description]/[tool name]. Hierarchical Escalation is used in the following situations:

- For high priority incidents – Service Level Manager is informed about such incident
- When resolution of an incident reaches [illegible]
- [illegible]

[role description] is responsible to [illegible] [role description].

Comment [BV36]: One of the [illegible] should be deleted.

Comment [BV37]: Delete if priority can't be changed or change role according to the real situation and add circumstances under which priority can be changed. Note: some organizations allow increasing of priority if Target Resolution Time is broken or almost achieved.

Comment [BV38]: Delete if not [illegible] recognized as an independent service option documented in Service Catalogue...etc.

Comment [BV39]: ***OPTION*** Delete this if you are implementing ISO 20000 and not ITIL.

Comment [BV40]: If you want to learn more about Incident diagnosis, see http://www.20000academy.com/Blog/June-2013/A-trip-of-1000-miles-begins-with-the-first-step-Initial-diagnosis-of-an-incident#

Comment [BV41]: Insert who performs initial diagnosis. Usually, that's Service Desk. Insert role description if some other role performs this task.

Comment [BV42]: Or any other Knowledge Base. If Knowledge Base or similar database doesn't exist, delete the whole paragraph.

Comment [BV43]: ***OPTION*** Delete this if you are implementing ITIL but not ISO 20000.

Comment [BV44]: Change if needed.

Comment [BV45]: SLA defines rules and handling of Incidents escalated to internal support group.

UC defines rules and handling of Incidents escalated to external support group.

Comment [BV46]: Change if needed.

Comment [BV47]: Change if needed.

Comment [BV48]: [illegible]

Comment [BV49]: Insert role. Usually this is handled by Service Level Manager.

Comment [BV50]: Insert role. Usually this is line manager.

[role description] [illegible] of Target Resolution time and if it is obvious that the SLA cannot be met.

Hierarchical Escalation is done by [Implemented tool] / [Incident Manager].

3.7. Investigation and diagnosis

[role description] ensures that [illegible] Resolution Time (see Service Level Agreement in Appendix of Service Level Management Process). [role description] is responsible for coordination of all activities, particularly [illegible]

3.8. Resolution and recovery

[role description] is responsible for the following:

- To define personnel responsible for resolution test and application
- To ensure [illegible]
- To coordinate activities [illegible]

When successfully resolved, the resolving group passes [illegible] Service Desk for closure action.

3.9. Incident closure

The Service Desk checks that the [illegible] and willing to agree that the incident can be closed.

When a resolution is implemented, the Service Desk changes the incident's status to "Resolved." The [illegible] "Closed" automatically.

3.10. Reopening

Incidents [illegible]

Reopening of an incident is defined in the Incident Policy.

3.11. Major incident

Major incidents are incidents with higher impact, resulting in significant disruption of services, and [illegible] SLA (see Service Level Agreement in Appendix of Service Level Management). [role description] is responsible for:

- Reporting to the [top management]
- Definition of major incident procedure (as part of SLA) that should define:
  - Declaration of major incident
  - Management, i.e. handling of major incidents
  - When and where to communicate during and following major incidents

Comment [BV51]: List all interested parties.

Comment [BV52]: Service Level Manager role on customer side.

Comment [BV53]: Adapt to your own requirements. This should be defined in SLA.

Comment [BV54]: ***OPTION*** Delete this section if you are implementing ITIL and not ISO 20000.

Comment [BV55]: Delete what is unnecessary.

Comment [BV56]: Insert role. Usually this is done by Incident Manager.

Comment [BV57]: If you want to learn more about Incident resolution and closure, see http://www.20000academy.com/Blog/July-2013/Incident-resolution-and-closure-waiting-for-the-fat-lady-to-sing#

Comment [BV58]: Insert role. Usually this is done by Incident Manager.

Comment [BV59]: Change if needed. Example: Incident Manager, Resolving Group Manager...etc.

Comment [BV60]: Service Desk is responsible for the whole lifecycle of an Incident. If no Service Desk in place – define role which will close the Incident.

Comment [BV61]: Service Desk is responsible for the whole lifecycle of an Incident. If no Service Desk in place – define role which will perform this action.

Comment [BV62]: Delete redundant.

Comment [BV63]: Delete this paragraph if:
[illegible]
This can be done for all Incidents or just for some of them, e.g. VIP Incidents or Major Incidents.

Comment [BV64]: ***OPTION*** Delete this section if you are implementing ISO 20000 and not ITIL

Comment [BV65]: [illegible]

Comment [BV66]: [illegible] conditions in SLA.

Comment [BV67]: This is, usually, Incident Manager.

Comment [BV68]: Insert correct function of top management. Exam ... [1]

Comment [BV69]: A clear trigger must [illegible] ... [2]

Comment [BV70]: To whom? E.g. Support group, Service Desk.

- [illegible] identify improvement opportunities and action plan for implementation
- The format, timing and participants of a major incident review

[role description] is [illegible] see Major Incident Report in Appendix

[top management function] appoints the Major Incident Manager.

Comment [BV71]: This is usually done by Business Relationship Manager.

Comment [BV72]: e.g. CIO, Board of Management…

4. Roles and responsibilities

4.1. Incident Manager

[role description] assigns the Incident Manager role.

Responsibilities of Incident Manager:

- Overall responsibility for carrying out activities within the scope of Incident Management
- [illegible]
- [illegible]
- Responsible for reporting and managing information
- Manages work of incident staff
- [illegible]
- Manages of incidents throughout first-, second- and third-line analysts

4.2. First-Line Analyst (1st Level)

[role description] assigns the First-Line Analyst role.

Responsibilities of First-Line Analyst:

- Incident recording
- [illegible]
- [illegible]
- Monitoring the status and progress of assigned incidents
- Closing of incidents
- [illegible]
- Updating Incident Record

Comment [BV73]: Delete if this is done by Service Desk only.

4.3. Second-Line Analyst (2nd Level)

Comment [BV74]: If Third Line or Nth Line exists, describe it here. Example: 3rd Line can be internal SW development or vendor.

[role description] assigns the Second-Line Analyst role.

Responsibilities of Second-Line Analyst:

- Same as First-Line Analyst, but with [illegible] incident resolution.

4.4. Service Desk

Service Desk is a [illegible] "Service Desk Function."

5. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Incident Record (in electronic form)	[tool name]	[role description]	Service Desk, 1st Level and 2nd Level have right to add to /change the record.	Incident Records are kept for [...].
Reports	[tool name]	[role description]	Incident Manager	Reports are kept for [...].
Customer Satisfaction Survey	[Service Knowledge Management System – SKMS]	[role description]	Incident Manager	Reports are kept for [...].
Reopened Incidents	[tool name]	[role description]	Reopening of Incident Record can be done only by [role description].	Reports are kept for [...].

Comment [BV75]: Overall responsibility for Incident Records. Usually Incident Manager.

Comment [BV76]: Change if needed.

Comment [BV77]: Overall responsibility for Incident Records. Usually Incident Manager.

Comment [BV78]: Change if needed.

Comment [BV79]: Example: for current year (YTD) – in [tool name], otherwise archived in [tool name or place of archive].

Comment [BV80]: Overall responsibility for Incident Records. Usually Incident Manager.

Comment [BV81]: Change if needed.

Comment [BV82]: Example: for current year (YTD) – in [tool name], otherwise archived in [tool name or place of archive].

Comment [BV83]: Overall responsibility for Incident Records. Usually Incident Manager.

Comment [BV84]: Change if needed.

Comment [BV85]: Example: for current year (YTD) – in [tool name], otherwise archived in [tool name or place of archive].

6. Validity and document management

This document is valid as of [date].

Owner of this document is [role description], who must [illegible] document at least once a year.

Comment [BV86]: ***OPTION*** Delete this if you are implementing ISO 20000 and not ITIL.

Comment [BV87]: This is only a recommendation; adjust frequency as appropriate.

7. Appendices

- Appendix 1: Incident Catalogue
- Appendix 2: Incident Record
- Appendix 3: Major Incident Report

[job title]

[name]

_____

[signature]

Comment [BV88]: Only necessary if the Procedure for Document Control prescribes that paper documents must be **signed.**

Page 8: [1] Comment [BV68]	Branimir Valentic	8/20/2013 9:30:00 PM

Insert correct function of top management. Example: IT manager, Board of Management, CEO, Company President…etc.

Page 8: [2] Comment [BV69]	Branimir Valentic	11/20/2013 11:02:00 PM

A clear trigger must be defined, when major incident procedure starts.