Monitor 24-7 inc.
service management solutions

Boost Service Desk Performance by Improved Categorization

Prepared by

Monitor 24-7 Inc.

November 19, 20154

Monitor 24-7 Inc, 335 Renfrew Dr., Suite# 301, Markham, ON, L3R 9S9, Canada, +1-416-410-2716
Monitor 24-7 Inc Europe, Zijlweg 142L, 2015 BH Haarlem, The Netherlands, +31-88-008-4600

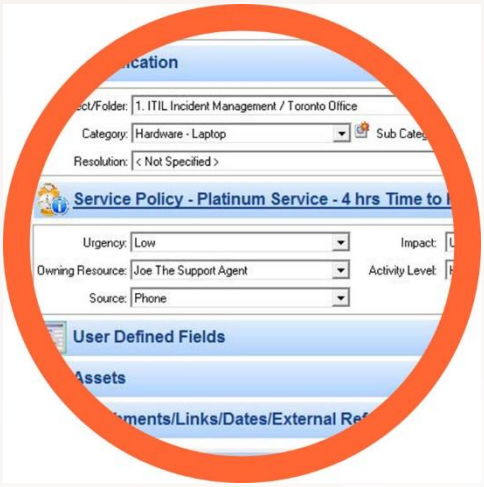
Categorization has an impact on your service desk performance

The correct categorization of new requests is key to your service desk performance and the support you provide to your customers. Incorrectly categorized incidents will skew your metrics, throw your SLAs times off and impact the real-time performance of your service desk.

Defining the categorization when implementing a service desk software solution and maintaining the classification when a service desk is growing is a challenge for all organizations.

In this document we share our thoughts about how you can organize your service desk tool using categorizations that matches your organization, and supports your SLAs and metrics.

A good approach is to combine Scope, Object, Action and SLA definitions



1. The **SCOPE** describes the aspect of the related product for which the action is requested. So for example if someone is requesting an update of software the action is not the computer on which the upgrade should be performed but it is upgrade of the software itself. So some actions can be Access Request, Software, Hardware or Service
2. The **OBJECT** is a subdivision of the scope. If possible, as abstract as possible so you can use it for multiple SCOPES. If a specific object is used in multiple scopes it will be easier for the service desk to use. E.g. the term Configuration can be applied to user access, as well as software.
3. The **ACTION** can be a third layer which can be good for reporting and filtering on open items. Action examples are Repair, Update, Delete, Question, etc…

4. The **SLA** is policy-based service management used to increase the performance of the service desk and improve overall business performance. The service desk works in line with the business. For example. A problem with the monitor or a notification that a backup failed doesn't have a significant impact on the business. An alert about a disk failure on a mission-critical server has a significant an impact on the business. This is important to keep in mind when defining the categorization. Sometimes we see that the category is Hardware and the sub category is Server with a linked SLA. Logging requests against this categorization goes from simple hardware failure to high impact incident.

Keep the categorization simple and clear. The challenge we see most often is when the service desk is growing. Often new categories are added to the scope which can make it more difficult to categorize and sometimes when you actually look at logged requests after a few months you often see that multiple categorizations are used for similar type of issues.

So what is the best approach to define what works for your organization?

There are a few steps to take in order to get the best result.

Collect Data

First thing to do is to collect around 3 months of historical requests. This should be enough to get a good understanding of the type of requests you get in.

What should you collect?

1. Request title or short description
2. Request summary
3. Current request classification
4. Actions taken to solve the issue
5. Assigned team/resource who solved the issue
6. Request Resolution

Analyze

Now try to see if there are common factors. What are the most critical items, how did they come in. Are there matching titles, matching actions taken to resolve, matching resolution.

Define the Scope Compared to your SLA

If you see that in the organization multiple software tools are critical, it could be that the highest level of a request classification can be some common factors for using the software solutions.

For example:

- Access
- Service
- Hardware
- Software

A question around access can apply to multiple software tools. For example someone requests access to a specific area in software X where someone else requests access in software Y. The main question here is not the software itself, but access to software. Access for a specific user to a software tool will have a completely different impact on the organization than if the software completely fails and no one can use the software. So a different SLA against this classification applies.

The take away here is that the company policies also applies on the categorization.

The high level classification should be clear and understandable for the users.

Define the Object

From the historical data you have now defined the highest level of your classification, the scope. Now let's look into the actual object.

This is the more detailed list which you can extract from the historical data of the last three months of requests. Try to list them as well just like you listed the scopes.

Examples can be:

- Application (or even main application names if you want. Though those can also be added via the Configuration Database!)
- Authentication
- Cancellation
- Connectivity
- Credentials
- Patch
- Password
- System
- Etc..

Cross Match Scope vs Object

Now cross match scope to the object and use the objects as sub categories of the scope. This will help to use similar type of subcategories below multiple categorizations. The idea behind this that you try to keep it as simple as possible with a low learning curve for your service desk staff. If you use a different naming/label for a subcategory in A as in B which actually has the same meaning it will be more difficult to understand and can cause confusion.

Example:

Type of Scopes	**Type of Object**
Access	Application
Service	Authentication
Hardware	Cancellation
Software	Connectivity
Question	Credentials
etc	Patch
	Password
	Upgrade
	etc

Result after combining scope / object

Category	Subcategory
Access	Application Authentication Cancellation Credentials Password
Software	Connectivity Upgrade Password Authentication
Question	Authentication Credentials
etc	

Add a Third Layer

A third layer for logging requests can be added to this list for reporting reasons. When a request comes in around Access or Software it could be pretty handy to know to which software tool or to which multiple software tools this applies. With IncidentMonitor we allow you the option to create a third layer. But what probably might be better is to start using the CMDB at this point. If you have a few standard CI's configured the third layer of logging the request is simply adding the CI to the request. For example an access request to application IncidentMonitor will be logged as:

Access > Application > CI IncidentMonitor.

If you don't want to work with a CMDB the module (sub sub categorization) can be activated.

Example:

	A	B	C
1	**Category**	**Sub category**	**sub sub category**
2	Access	application	IncidentMonitor
3			Exchange
4			Exact Accounting Software
5			Salesforce CRM
6			
7	Access	password reset	IncidentMonitor
8			Exchange
9			Exact Accounting Software
10			Salesforce CRM

A Final Word About IncidentMonitor™

IncidentMonitor enables you to easily adapt to the needs of your organization. With its configuration capabilities and unique project concept you are able to start with a simplistic linear request management system and grow this over time. We see many implementations start with a simplistic Incident Management approach which simply aggregates all of the out-of-band (i.e. e-mail, chat, web requests, etc.) and in-band data (service requests, incidents, change requests etc.) into a single system for reporting and statistics. Then as the organization matures (by organization we mean your service organization and your end user community) other aspects are turned on (or enabled).

A Final Word About Monitor 24-7 Inc.

Monitor 24-7 redefines service management by helping organizations improve their customer-facing functions. Monitor 24-7 provides simple solutions that tackle complex help desk processes -- right out of the box. Our goal is to help customers reduce running costs, manage change, implement a fully functional advanced software solution and lower the cost of ownership.

Monitor 24-7 is a Canadian software development organization focused on service management. The software is purely developed by Canadian and Dutch developers. Years of experience and many different customers have brought us where we are today. We believe we have proven ourselves and we are very proud of our flagship IncidentMonitor -- an enterprise service management solution which is being used in many different environments.

- 100% dedication to Service Management since 1999
- Over 250 customers, more than 10,000 licenses sold
- Active in 10 countries

Monitor 24-7 Inc Head Quarters
335 Renfrew Drive Suite # 301
Markham ON, L3R 9S9
Canada
Phone +1 416 410.2716 / +1 866 364.2757
sales@monitor24-7.com
www.monitor24-7.com

Monitor 24-7 Inc Europe
Zijlweg 142-L
2015 BH Haarlem
The Netherlands
+31 88 008 4601

eusales@monitor24-7.com
www.monitor24-7.com