The Essential Guide to Incident Categorization

by Julie L. Mohr

Inside

Introduction

Incident categorization is a challenge for IT organizations. Whether it is due to culture, politics, complexity, or an inability to agree, every organization at some point finds that the categorization of incidents is ineffective, out-of-control, or difficult to maintain. Why does it cause so much of a challenge?

There is no one right way to create a categorization. There's no template. Every organization is different. The products and services are different. The service levels are different. The customers are different, and the required information to track is different. Even the reports differ. These distinguishing factors impact how incidents are tracked and monitored. There is no master categorization to use because it is up to your organization to define what works for your environment.

There is no one right way to create a categorization. There's no template. Every organization is different.

What Is Categorization?

Categorization is an essential activity in both incident and problem management. Categorization is the process of arranging incidents and problems into classes or categories. The main objective is to understand what type of incident has occurred. Over time, if incidents are categorized similarly, the data is then used to identify trends and focus efforts on improving proactively. If the data is flawed due to poor categorization, then it makes it incredibly challenging to know what improvements are needed and how to prioritize those improvements.

Categorization is not just used in the management of transactional work within an IT organization. We use classification to arrange a vast array of datasets. Two examples are the Dewey Decimal System and a recipe box. Let's examine both in more detail.

The Dewey Decimal System. In most libraries around the world, the Dewey Decimal System is used to classify or categorize books. Essentially the goal is to organize knowledge into 10 main classes. Each main class is then further subdivided into 10 divisions. Each division is then further divided into 10 sections. Ultimately, the categorization system contains 10 main classes, 100 divisions, and 1000 sections. The Dewey Decimal System identifies the correct location to store and retrieve a book within the library's bookshelves. Additionally, books of a similar genre are stored on the same shelf and related works on shelves nearby.

A Recipe Box. A recipe box is also an example of a categorization scheme. However, with this categorization, there is no established standard to follow. For instance, you could store the recipes by food type (appetizers, beverages, bread, breakfast, cakes, candies…) or to make it easier to find a recipe based upon the food you have in your cupboard. you could store them based upon main ingredient (apples, bananas, beans, beef, berries…). Other categorizations could include ethnic identity (Asian, Chinese, European, French…), special occasion, or by unique classifications (6 ingredients or less, bread machine, casseroles, diabetic…). The options provide an extensive array of possibilities, but it also is an example similar to what happens in organizations with incident classification. Without standardization, recipes can be stored in more than one category and may make it difficult to find.

Why Is It Important?

Linking of Service Management Information. When incidents, problems, known errors, events, workarounds, and changes share a common or similar categorization scheme, it is much easier to link the related records. For example, a service owner can run a report and find all incidents, problems, events, known errors, workarounds, and changes related to a service.

Improved Root Cause Elimination. Trend analysis based upon categorization can help to identify faulty components and repetitive errors and assist with more accurate root cause analysis. Historical information related to services is only helpful when trends can be identified. If a problem or incident can be entered into the service management system in more than one way, trends can be missed or under-reported.

Improved Knowledge Searches. When an incident can only be categorized in one way, the search against previous knowledge is more effective. The analyst searches for knowledge in the form of incidents, problems, or known errors within the same categorization. The categorization provides the context for searching for related knowledge and narrows down the data to a much more manageable subset. If knowledge is not present, the categorization provides the context to begin gathering the necessary information to diagnosis and categorize the new knowledge.

Improved Process Efficiency. The activity of categorizing the incident speeds up the incident management process and creates greater efficiency within the process flow. If the issue cannot be solved, the categorization determines the appropriate incident escalation group. When the escalation group is tied to the categorization, the organization can eliminate errors in escalation and improve the efficiency of the incident management process.

Prioritization is also an important activity that identifies the importance of an issue related to business impact and urgency. In most environments, categorization will drive what is set for a priority. For example, a critical business application that is used by a vital business function may require faster response and resolution timeframes when setting the priority of an incident.

Service Improvements. Finally, another benefit to useful categorization is the ability to produce meaningful reports that help the organization to take a more proactive approach to manage services. The available information is used by the service manager along with continual service improvement to make informed decisions on how to improve the overall quality and delivery of services and possible ways to innovate services in meaningful ways for the business.

Why Is It So Challenging?

Organizations allocate resources to different functional units that require specific skills and experience to manage the infrastructure effectively and manage services for improvements in business outcomes. However, the functional units often have very different perspectives on what represents an appropriate categorization structure. Typically, one group wins the discussion, and the categorization is established by one group that will be used by all functional units. Another contributing factor to the difficulty of developing a single structure that works for the entire organization is that the infrastructure is complex, and it is difficult to determine a single structure that allows for tracking of incidents across such a variety of potential issues.

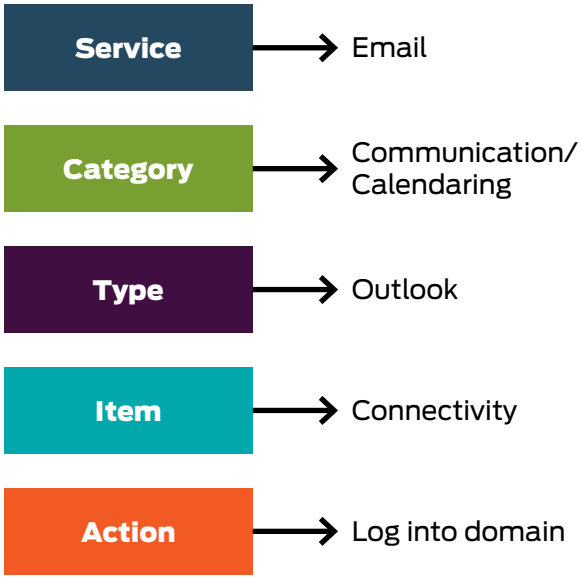
Often there are political pressures to make changes to the structure. For example, if a product or service is not listed explicitly in the categorization structure, it can be viewed as not being important enough to the organization. When this occurs, pressure is often used to get a product added to the categorization so that it gains visibility.

Also, as the organization goes through change, the categorization grows organically over time as products are added and released from the environment. The organic growth often results in a fragmented structure to the categorization. The fragmentation is worse in environments that have not established policies or standards on when and how to change the categorization structure.

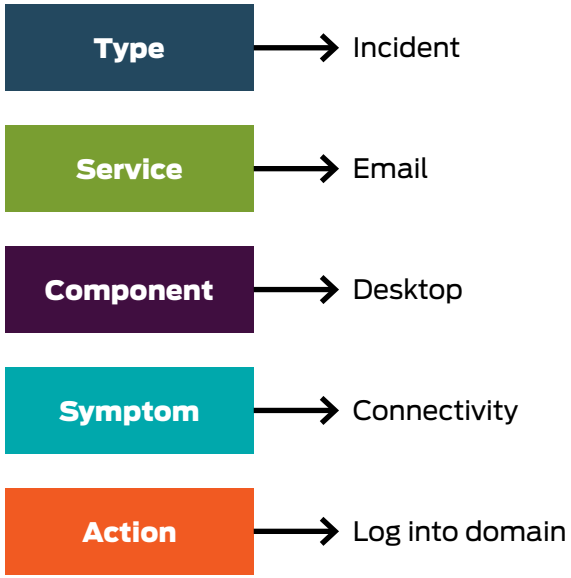
What Works in Categorization?

When developing a categorization scheme, it is helpful to have three to four hierarchical menus where lower types form part of the higher-level categories. For example, a family is comprised of parents, children, and issues. If you select a family, then the parents form part of the family. Once a parent is picked, the children belong to the selected parents, etc. From a service management perspective, typical categorizations schemes are Service/Category/Type/Item/Action; Type/Service/Component/Symptom; or Location/Service/System/Application.

Here are two sample structures with sample selections to help you understand how each is used as well as similarities and differences:



Ex. Service/Category/Type/Item



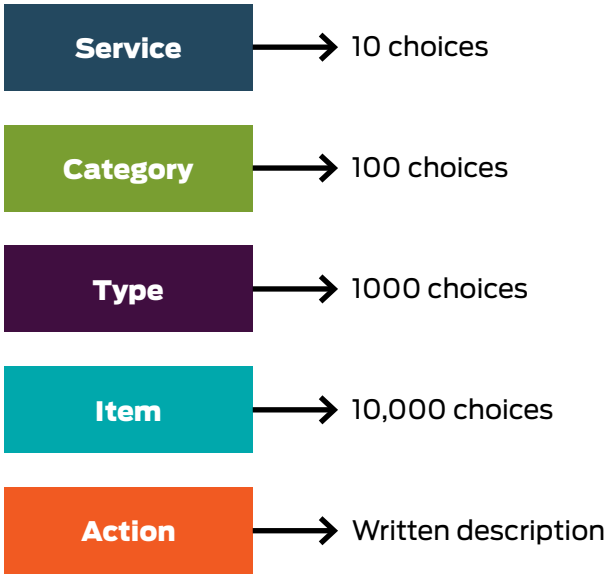
Ex. Type/Service/Component/Sympton

A carefully designed categorization scheme will simplify how incidents are entered into the system, reduce errors in miscategorization, and tie each unique category/type/item to a specific owner.

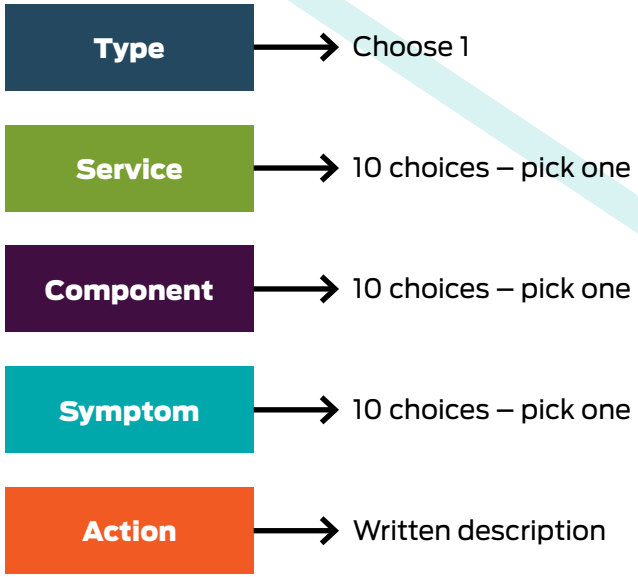
What Works in Categorization? *(continued)*

Hierarchy/Dependencies Required. An important factor in reducing errors is the use of a hierarchy. The choice in the first menu provides a subset of choices in the second menu. By using a hierarchy, users have a limited number of choices instead of trying to choose from all options.

The following graphic shows the difference between using a hierarchical structure and not using one:



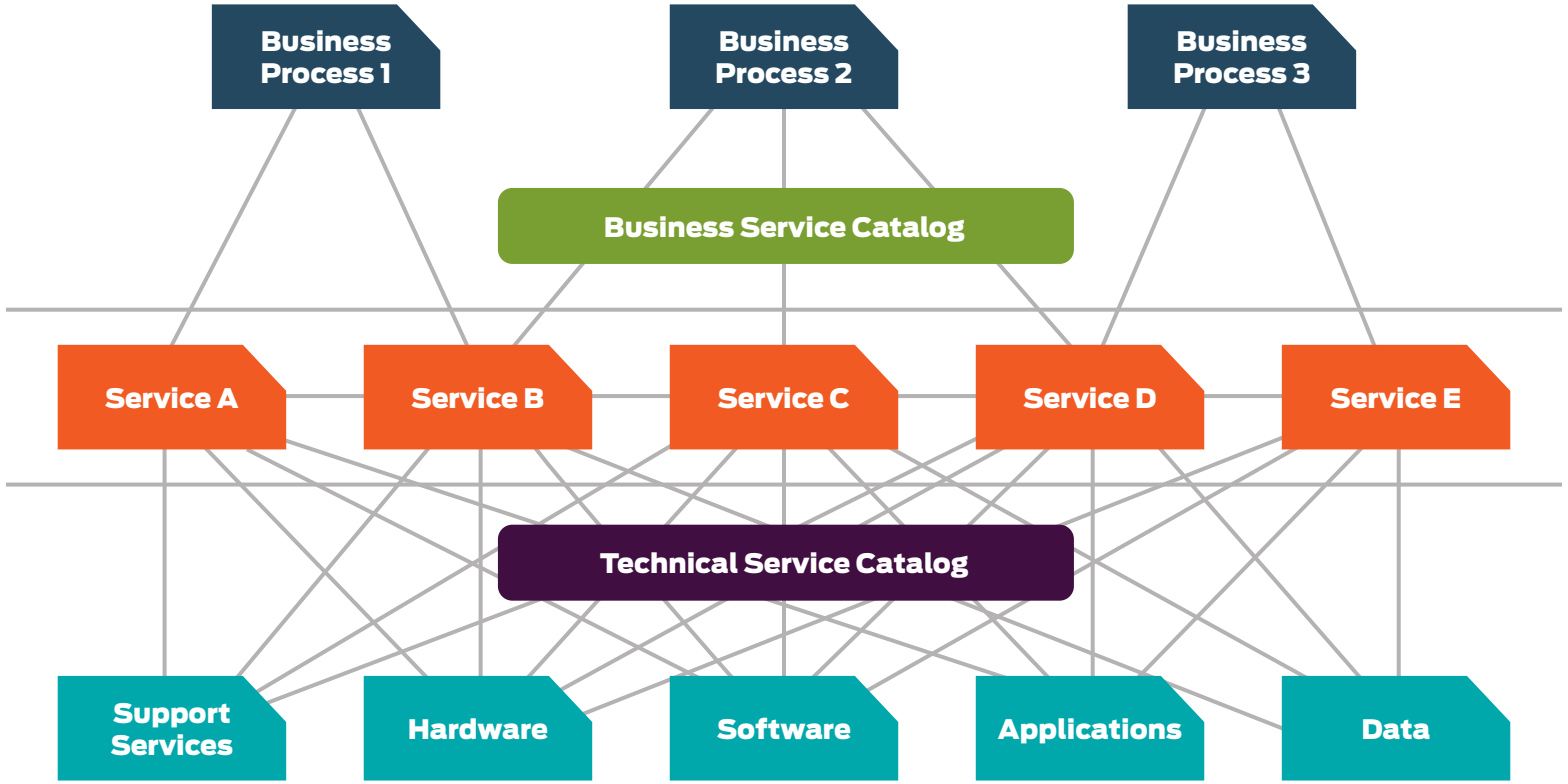
Ex. All the Possibilities



Ex. Limited Choices

What Works in Categorization? *(continued)*

Categorization Dependencies. In the overall service value system, there are other aspects of value delivery that are tied to the categorization. The **service catalog** provides a view of the services that are in the operational environment. The ability to put services into categories that make sense to our customers makes it easier for customers to find information about those services and how to request them. The categorization of incidents is directly related to the ability to categorize our services. All too often, organizations try to categorize incidents before they understand how to categorize services. Even worse, if you decide to categorize incidents without understanding what services are provided, then the categorization is likely to be technology-focused and cannot provide a view of the impacted service. This will limit proactive service management.



What Works in Categorization? *(continued)*

Incident management drives process improvement through the analysis of incidents to identify improvement opportunities. By using accurately categorized incident data, the overall customer experience can be analyzed to determine what is working well and where improvements can be made for the customers.

Career development also depends upon categorization. For each service in the service catalog, the organization needs to have a full understanding of the skills and level of experience required to support the offered products and services. When a new service is added to the service catalog, it is then entered in the incident categorization, and training and skills development requirements should then be identified. Additionally, management can use the identified skills and experience requirements to develop training and career development plans for analysts.

KNOWLEDGE REQUIRED	LEVEL
Advanced knowledge/experience in all aspects of the product or activity with understanding of planning and implementation requirements.	5.00
Advanced knowledge/experience in all aspects of the product or activity with understanding of the interactions and requirements for effective utilization.	4.00
Thorough knowledge/experience in most aspects of the product or activity.	3.00
General knowledge/experience in most aspects of the product or activity.	2.00
Minimal or basic knowledge/experience of the product or activity.	1.00
No knowledge/experience of the product or activity.	0.00

NAME:	ASSESSMENT					
	0.00	1.00	2.00	3.00	4.00	5.00
SKILLS REQUIRED FOR POSITION						
TECHNICAL SKILLS:						
PC Office Systems						
MS Office						
Word						
Excel						
Powerpoint						
Project						
Access						
Visio or any flowchart tool						
Lotus Notes						
Laptop Remote Connectivity						

What Works in Categorization? *(continued)*

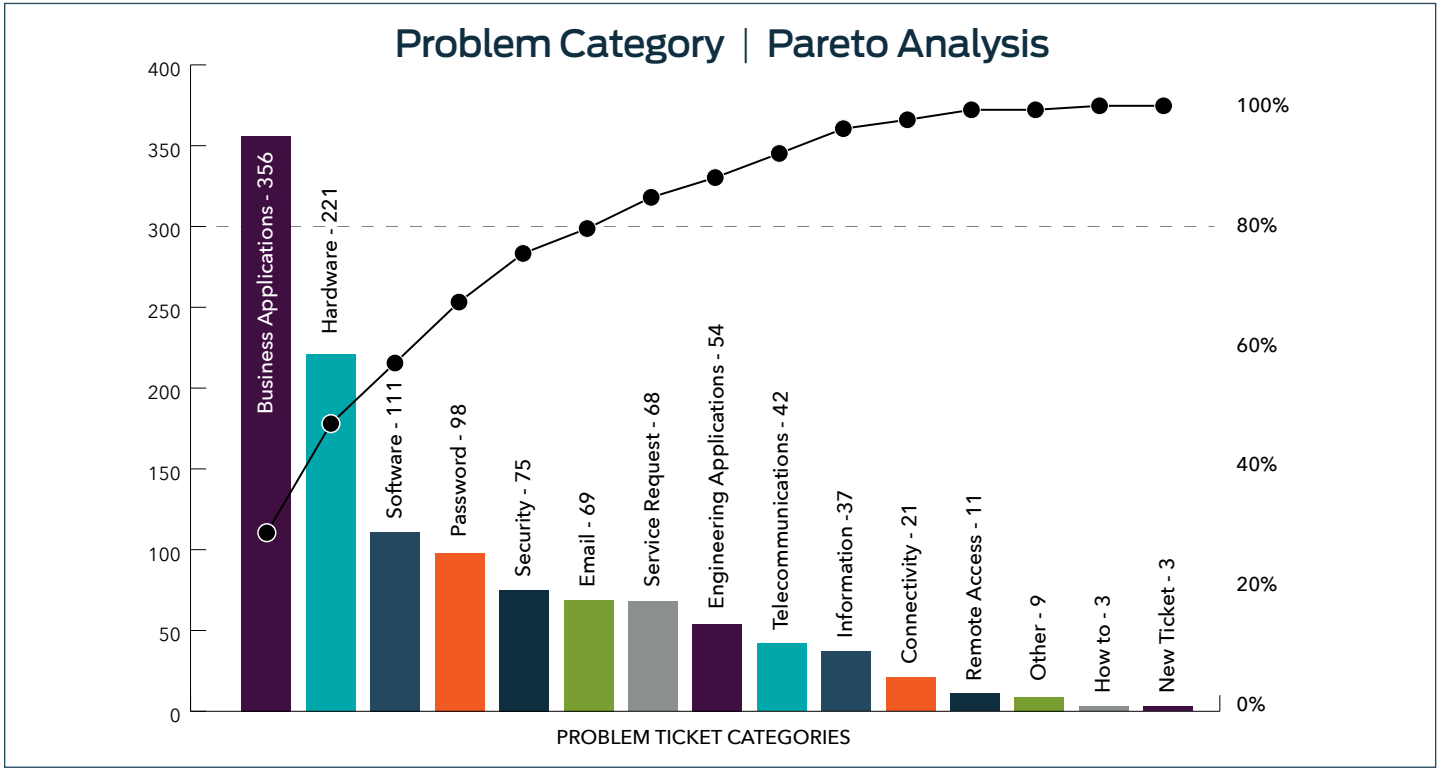
Categorization is also critical to establishing expectations when the organization develops **operational level agreements**. What is solved at the service desk before it is escalated to level 2? The organization needs a core understanding of the types of incidents related to services, the level of support provided at the service desk, and what support is provided by level 2 and beyond.

Category: Business Applications				
Type	**User Base**	**Priority**	**Technical Support Partner**	**Level of Support**
Acquire	Small	High	HR/Organizational Dev.	Log & Escalate
Lotus Notes	Small	Medium	Argent Marketing Dept	Log & Escalate
Category: Hardware				
Type	**User Base**	**Priority**	**Technical Support Partner**	**Level of Support**
Printers	Large	Medium	IS Field Services	Troubleshoot
Workstations	Large	High	Desktop Engineering	Troubleshoot
Category: Desktop Operating Systems and Software				
Type	**User Base**	**Priority**	**Technical Support Partner**	**Level of Support**
Adobe Acrobat	Large	Medium	Desktop Engineering	Functionality
MS Office	Large	Medium	Desktop Engineering	Functionality
Windows 7	Small	Medium	System Engineering	Functionality

What Works in Categorization? *(continued)*

Event management also has a direct dependency on incident categorization. The ability to build automation that supports filtering and correlation of events to determine the appropriate control action is vital to the success of the process.

Proactive problem management is nearly impossible to do without useful categorization. Imagine trying to run a report that provides visibility into all incidents and problems related to a specific service, type of issue, or component if the analyst can log a single incident in five or six different categorizations. There will be no ability to conduct trend analysis.

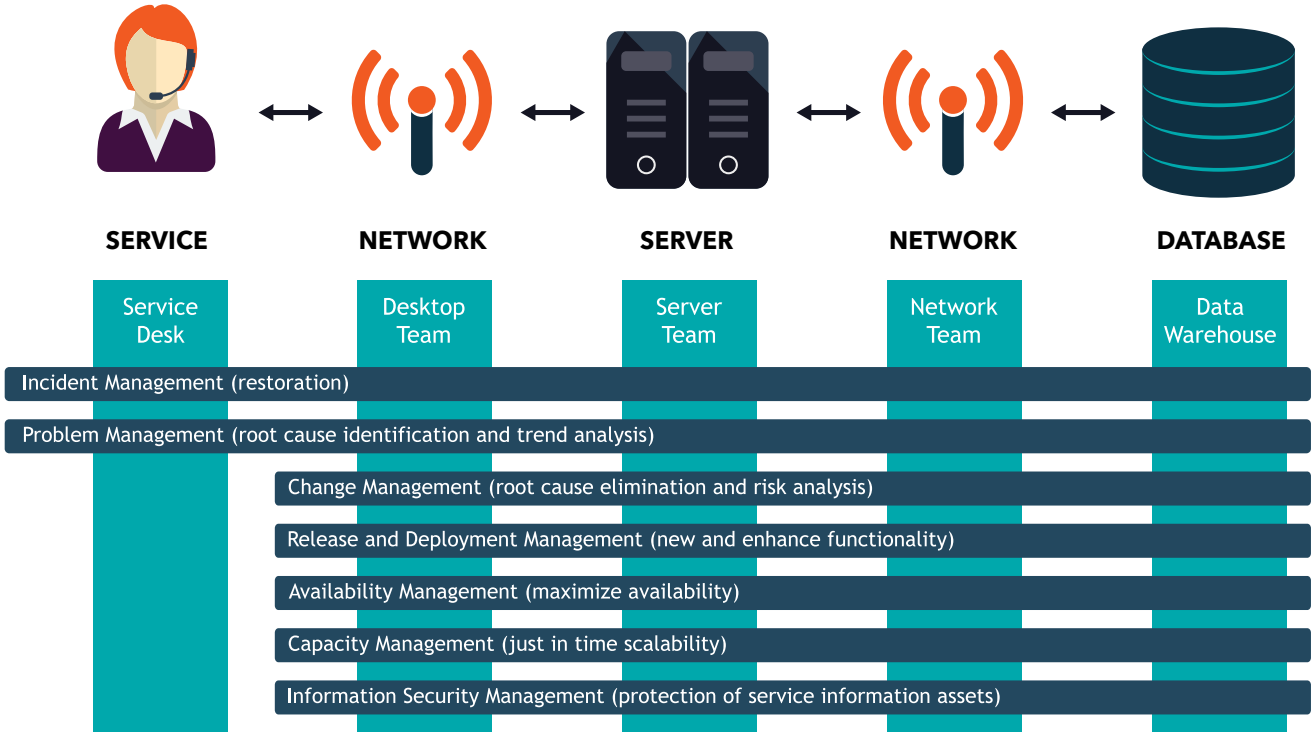


What Works in Categorization? *(continued)*

A report may find some similarities between incidents and problems. But without the full picture, we may not. Service improvement and error elimination opportunities are much easier to identify with a working categorization that is used in both the problem and incident management processes.

Overall, the information captured within the ITSM system represents the knowledge needed across the service value stream to understand what and how to improve service delivery.

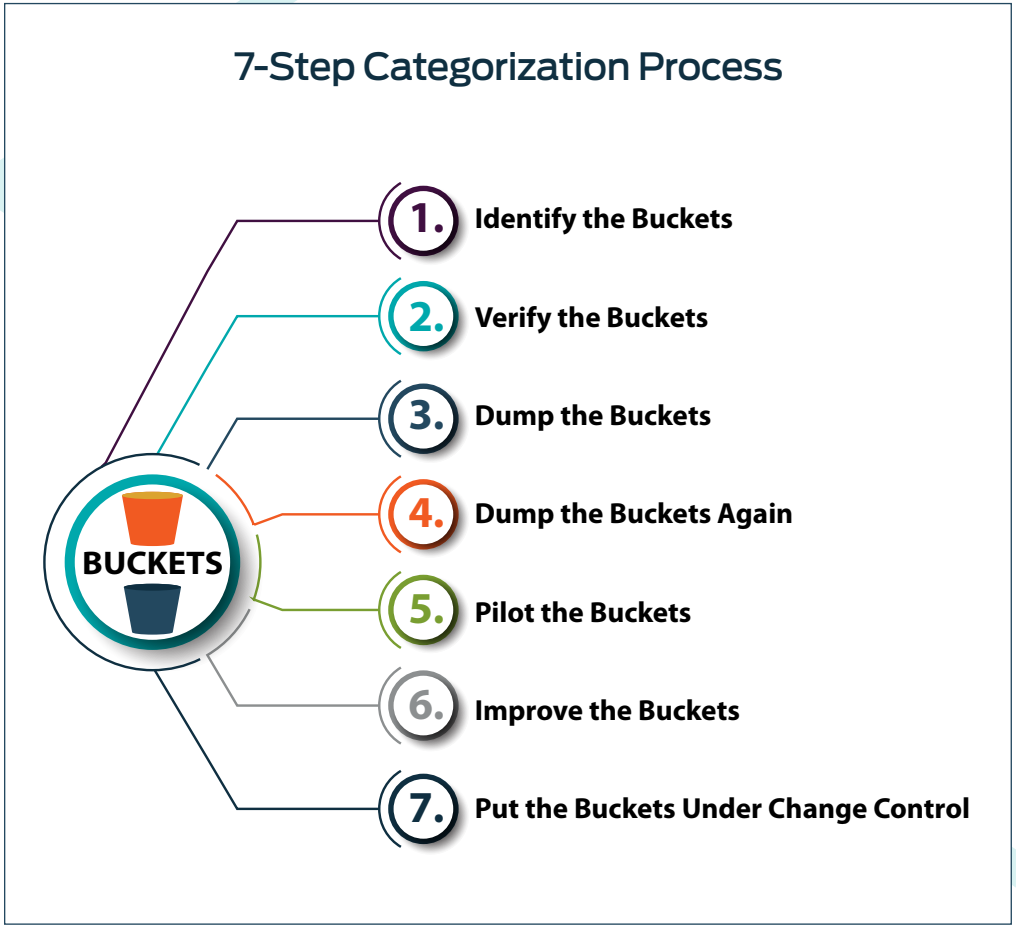
It is no wonder why an accurate and usable categorization scheme is challenging to do. With so many dependencies and requirements, how do we create a categorization scheme that works?



7 Steps to Incident Categorization

Next, let's explore how to create a categorization that works for capturing incidents within your service management system. I will walk you through, step-by-step, how to create a new categorization scheme that will work for your organization.

At the core, categorization is like a set of buckets. Each bucket holds a bunch of incidents, and within the bucket, these incidents would then be logically grouped by a subset of characteristics within the bucket. The first decision that needs to be made is, "What is the highest level of the hierarchy?" Here is the seven-step process to help your organization develop a categorization scheme that works:



7 Steps to Incident Categorization *(continued)*

Step 1: Identify High-Level Categories

Incidents can be categorized by call, by type, by caller, by technology, by incident, or by service. The first decision is which of these is most important to the customer? Typically, organizations that are implementing service management will take the approach of starting with the service. Service-based categorization provides a substantial amount of value to understanding service performance and helps to identify improvements to services.

This upper-level classification will not work with all organizations. External service providers may decide to choose a customer at the highest level. The key is to keep the upper or primary level general but not too broad. Ten to fifteen high-level choices should keep the level of detail at the correct level.

To develop an accurate high-level categorization:

- Pull three months of the most recent incident activity
- Define 10 high-level categories
- In a working group, sort available data into the defined high-level categories
- Any tickets that do not fit? Adjust the high-level categories to incorporate the different tickets
- Use "other" category temporarily to represent other possible choices not yet identified

GOAL: *Develop 10 to 15, high-level working categories.*

Step 2: Verify Categories

How do you get a consensus on the high-level choices? Review the structure after three to six months of use:

- Reassemble project team
- Verify that the identified categories work
- If "other" category used, sort and determine how to categorize the different tickets
- If the structure does not work, modify as needed

GOAL: *Standardize on 10 to 12 categories.*

7 Steps to Incident Categorization *(continued)*

Step 3: Identify Types in Each Category

Next, you must decide the secondary level. To complete this step, look at the incidents in each high-level category and further determine how to divide those tickets up effectively within the categorization. The second level should be specific but should not dive into the minutiae:

- Once you have a category filled with three to six months of data, the next step is to sort and analyze the common types in the category
- In this step, you are creating collections of common types that are in the category
- In a working session, divide the tickets from each category into the identified types for that category
- Repeat the process for each high-level category

GOAL: *Develop 10 to 15 types per category from Step 2.*

Step 4: Identify Items in Each Type

The third level provides much more granularity into the specifics of what is occurring in the incident. The level of detail here has to be driven by organizational need and the type of incidents that are captured:

- Once you have the types identified, the next step is to analyze what items are in each type
- In a working session, divide the tickets into common items
- Create collections of common items that are in each type

GOAL: *Develop 10 to 15 items per type identified in Step 3.*

Step 5: Pilot the Structure

The next step is to establish a structure that will be used and tested in the live environment. At this point, the structure is in draft form to allow for modification based upon actual calls that are received. Each call that does not fit into the structure should be reviewed to determine if a change is needed. To not slow down the flow and handling of incidents, an "other" category is often used. All analysts are encouraged to put incidents into the "other" category when the structure doesn't handle the type of incident reported. Analyze the "other" categories on a weekly or bi-weekly basis to determine additional category/type/item (CTI) structures that must be added. Long-term use of the other structure should be avoided.

- Now that you have 10 high-level categories, 10 types per category, and 10 items per type, it is time to try it in the live environment
- Pilot the draft structure
- Use "other" to capture those new items that either do not fit into the identified category/type/item structure or are new

GOAL: *Gather information on how the draft structure works during the pilot in the live environment.*

7 Steps to Incident Categorization *(continued)*

Step 6: Improve the Structure

After the pilot is complete, it is crucial to now go back and review the "other" categories and determine if the categorization structure works for all incidents identified in the pilot and after. Once you've reviewed the "other" category, you should probably remove it from the structure as an option. It is imperative not to change the categorization structure too often after the pilot as the organization will lose the historical perspective of the data.

GOAL: *Improve as needed to meet the evolving needs of the business.*

Step 7: Put the Categorization Structure Under Change Control

Once the team finalizes the categorization structure, place it under change control. Any new categorizations that are identified should only be added after an RFC is submitted and the risk of changing the structure is adequately assessed. However, some circumstances will commonly require adjustments to the categorization:

- When new services are introduced. The category structure should be updated if the service does not fit into the existing CTI structure.
- When services are retired. The category structure should be updated by archiving the appropriate data and removing the service from the CTI structure.
- When services are changed. Identify if modifications are necessary. Typically modifying services does not require an adjustment of the CTI structure at the higher levels but may require changes at the lower levels of the structure.

GOAL: *Require the organization to agree on changes to minimize risk.*

Pitfalls to Avoid

Too Many or Too Few. There are many ditches to avoid in categorization. If the categorization has CTI structures with too many tickets or too few, this is an indication that the categorization scheme is not effective. The exact number is hard to determine but is more easily expressed in percentages. If you have a CTI structure that holds 25% of your ticket volume, then the structure may not have enough detail. If a CTI structure contains less than 2%, then it probably is too specific.

Avoid Constant Re-Categorization. Every change to the categorization will modify the way existing data is structured and will impact historical analysis. Changes to the categorization must be carefully planned for the risk that it can introduce. It should not, however, discourage change. Organizations are not stagnant, and neither should the categorization scheme be frozen in time.

Do Not Categorize by Symptoms. It is also essential to focus on capturing information that is factual and not symptom-based. A specific IT incident can have many different symptoms. To categorize by symptoms would very quickly permit multiple categorizations for one type of incident and will immediately produce unreliable data. Symptoms are more appropriate for metadata fields or other available fields in the incident record.

Even the best-defined categorization scheme is subject to error.

Critical Success Factors

What Reports Are Needed? Reporting from the incident management system is essential for overall quality improvement of services, processes, technologies, people, and the overall customer experience. All service management processes use this data to support decision-making. It is important to keep this in mind when data is structured, captured, and used in reports that are provided to these processes. All existing processes that are defined and managed will need this data as an input, and their needs must be taken into account. The collected data should drive improvements that are meaningful to the business and IT.

Decide first what data you need out of the incident management system. If you can get agreement on what needs to be in the reports for the incident management process and services, then it will help the organization to further define the requirements in the categorization activity. Additionally, if service level agreements are implemented, review the agreements to help to identify additional required measurements.

Maintain a Customer or Business Focus. The tendency for an IT organization is to focus the CTI structure on the internal view of IT. An internal-only view will serve the purpose of identifying improvements in components but won't serve the need to drive improvements in services. The data collection must be business-driven, not IT-driven. The external view will provide data collection that will support better decision-making and analysis based upon what is important to the business.

Be Sure to Train. Training is essential to the correct categorization of incidents. Even the best-defined categorization scheme is subject to error. Organizations that are trained on how to categorize within the ITSM system and know how to handle exceptions will have higher quality data. Redundancy of categorization must be avoided through both design of the categorization but also in the operational use of the categorization.

Use Closure Categories. Changes to the categorization of an incident throughout the incident management process should be avoided. If a customer calls in and reports an incident and the categorization is selected but later it is determined to be incorrect, the best way to handle this situation is to create a closure categorization. Closure categorization provides the organization with a way to improve the process and improve the training of analysts recording the incidents. Also, some incidents will present symptoms that indicate a particular structure, but it is uncovered through diagnosis that the issue turns out to be something very different. Both categorizations can be helpful to find the solution the next time the issue occurs.

Put Structure Under Change Control. Once the environment has stabilized, the categorization should be under change control to ensure that any changes will keep the underlying data in its highest level of accuracy.

The Benefits of Good Categorization

The benefits of a good categorization scheme are many. The categorization will ease the process of logging incidents, reduce redundancy, and strengthen the organization's ability to manage knowledge and use it to support decision-making. The underlying data will enable the organization to take a proactive view of service management and identify improvement opportunities. The view will be across functional silos not based upon the technology that is managed. A well-designed categorization will provide a better overall view of the services and how they are meeting customer expectations and service level targets.

Someone once said that nothing in life worth doing is easy, and it is especially true with categorization. Creating a useable and sustainable categorization is a tough exercise that will pay off in the end. The data collected in the incident management process represents every touchpoint, every aspect of the customer experience. If we capture that knowledge in a way that it can be reused to support continual improvement, the organization will improve services, improve customer satisfaction, and improve efficiency and effectiveness of operation. That is definitely something worth doing.

HDI

For over 30 years, HDI has partnered with thousands of organizations to improve their customer service and service management performance by educating their people, elevating their processes, and empowering their strategy. From C-level professionals to directors, managers, and frontline staff, HDI is the definitive source of industry information, leadership, and performance planning. Through events, certification and training, consulting, community, and industry resources, HDI aims to transform service and support organizations and reimagine their approach to delivering exceptional service and value. Learn more at ThinkHDI.com.

HDI is part of Informa PLC, a leading B2B services group and the largest B2B events organizer in the world. To learn more and for the latest news and information, visit ThinkHDI.com and www.informa.com.

About the Author

Julie Mohr is a dynamic, engaging change agent who brings authenticity, integrity, and passion to practitioners worldwide. Through her books, articles, speaking, consulting, and teaching, her purpose is to spark change in the world with thought-provoking dialog and interaction on topics of authentic leadership, business strategy, knowledge management, organizational culture, and innovation. Julie has a B.S. in computer science from The Ohio State University and an MaED from the University of Phoenix and is currently pursuing her Ph.D. in Management and Organizational Leadership in Information Systems & Technology from the University of Phoenix. She is an ITIL Expert, Certified Help Desk Director, and Certified Governance IT Professional. She is an HDI Business Associate and teaches training and certification classes for service and support professionals. Visit her website, and follow her on Twitter @JulieMohr, YouTube, and LinkedIn.