SHOULD THE INCIDENT BE REOPENED OR A NEW ONE LOGGED

BY: DENIS MATTE

When we think the incident is resolved we close it. Of course, according to ITIL® the user confirmed its resolution and accepted its closure. However, from time to time we miss the mark. The user calls back because the issue came back or was not resolved. In this situation we can either:

1. Re-open the original incident or,
2. Log a new one.

ITIL's guidance fluctuates in this regard. In ITIL® v2 a tip was provided whereby "If a closed Incident is reopened, it is important to record the reason and adjust the workload values assigned if further work is required - if not, a new Incident should be raised and linked to the original one." (Service Support Section 5.6.5, p.86). The 2007 Edition of Service Operations simply indicates that the rules for reopening must be clear. "For example, to agree that if the request needs to be reopened within one working day then it can be reopened — but that beyond this point a new service request must be raised" (Section 4.2.5.9, p. 53). However, this guidance was moved in the 2011 Edition to the Request Management section (Section 4.3.5.9, p. 94). As a result ITIL® no longer provides guidance for reopening incidents.

Given this void, two common approaches for logging a new incident will be reviewed. Then we conclude with an explanation why, most of the time, the incident should be reopened.

1. Logging a new incident because "Every Call Must Be Logged"

Some organizations log a new incident because the Service Desk's Call Center has a policy that "every call must be logged". Since the user called back, a new incident is logged.

However, scattering work notes across several incident records makes it difficult to quickly review its chronology. Collaboration is harder when escalating since multiple records must be consulted and reconciled. It is true that records can be linked in most ITSM tools. Nonetheless, if the Call Center Agent forgets to link/associate related incidents, or if the IT Specialist does not notice the linked incident(s) troubleshooting is done again and this is inefficient and increases resolution time. Consequently, the IT specialist may inadvertently frustrate the user by asking questions previously answered and to perform procedures already tried. Needless to say that IT's credibility would also be affected.

To address management's need to measure calls received by the Call Centre, reports can be generated from the Automatic Call Distribution (ACD) thus, this policy can then be adjusted to state that "all work must be recorded".

2. Logging a new incident to avoid breaching the SLA

Some organizations log new incidents to avoid breaching their Service Level Agreement (SLA). This approach is used because of the way their ITSM tool calculates SLAs or to have more time.

Certain ITSM Tools calculates the SLA's elapsed time consecutively from the date logged. Let's say for example that the SLA target resolution is four hours and that the incident was logged Monday morning at 8:00 a.m. That incident is then closed two hours later well within its four hours target resolution time. When it is reopened the following day, it automatically breaches the SLA because IT was unable to resolve the issue within four consecutive hours. On the other hand, other tools calculate the SLA by counting down the allocated time. Thus, in our example two hours would be left when the incident is reopened and would not breach until all of the allowed time elapsed (i.e. four hours). As a result organizations with the aforementioned tool would be inclined to log a new incident to avoid breaching their SLA.

Regardless of how the tool calculates the SLA, some organizations log a new incident as it gives IT a new resolution target. This is good for IT but not so good for the user. Moreover, caution is in order since people may prematurely close incidents simply to avoid breaching the SLA given that they get more time by logging a new one. Of course, breaching SLAs is not something to aspire to however, breaching provides an important metrics.

Reopening for Metrics

Calculating the number of reopened incidents is an excellent performance indicator of the Incident Management process. Looking at why incidents were re-opened may indicate a need for additional training, revised procedures, new knowledge base content or better release regression tests. Breaching the SLA because the incident was reopened is an indication that something unusual happened causing IT to miss its commitment. Moreover, systematically analyzing the root cause why incidents have been reopened or that the SLA breached is a good Continuous Service Improvement method.

In conclusion, reopening incidents not only centralizes work notes in one record it also avoids "playing" the breach avoidance game. It also provides an excellent measure of the Incident management process' performance. All these metrics are lost when a new incident is logged. However, even though the user called back for what appears to be an unresolved issue, a new incident may be required when in fact a new issue is reported even though it may be related to the original one.

About the Author:

Denis Matte has over 20 years of IT experience in the private and public sector. As a consultant he helped organizations implement ITSM integrated toolsets and ITIL based processes by designing and managing projects at the operational, tactical and strategic levels. He currently manages the ITSM team in a public organization that administers the ITSM tool and helps internal groups progress in ITIL and IT Service Management. Denis Matte is a certified ITIL Expert, Project Manager and Technical Trainer with formal education in Project Management and Management of Change. In his spare time he publishes www.ITILfromExperience.com and Tweets @ ITILfromExp