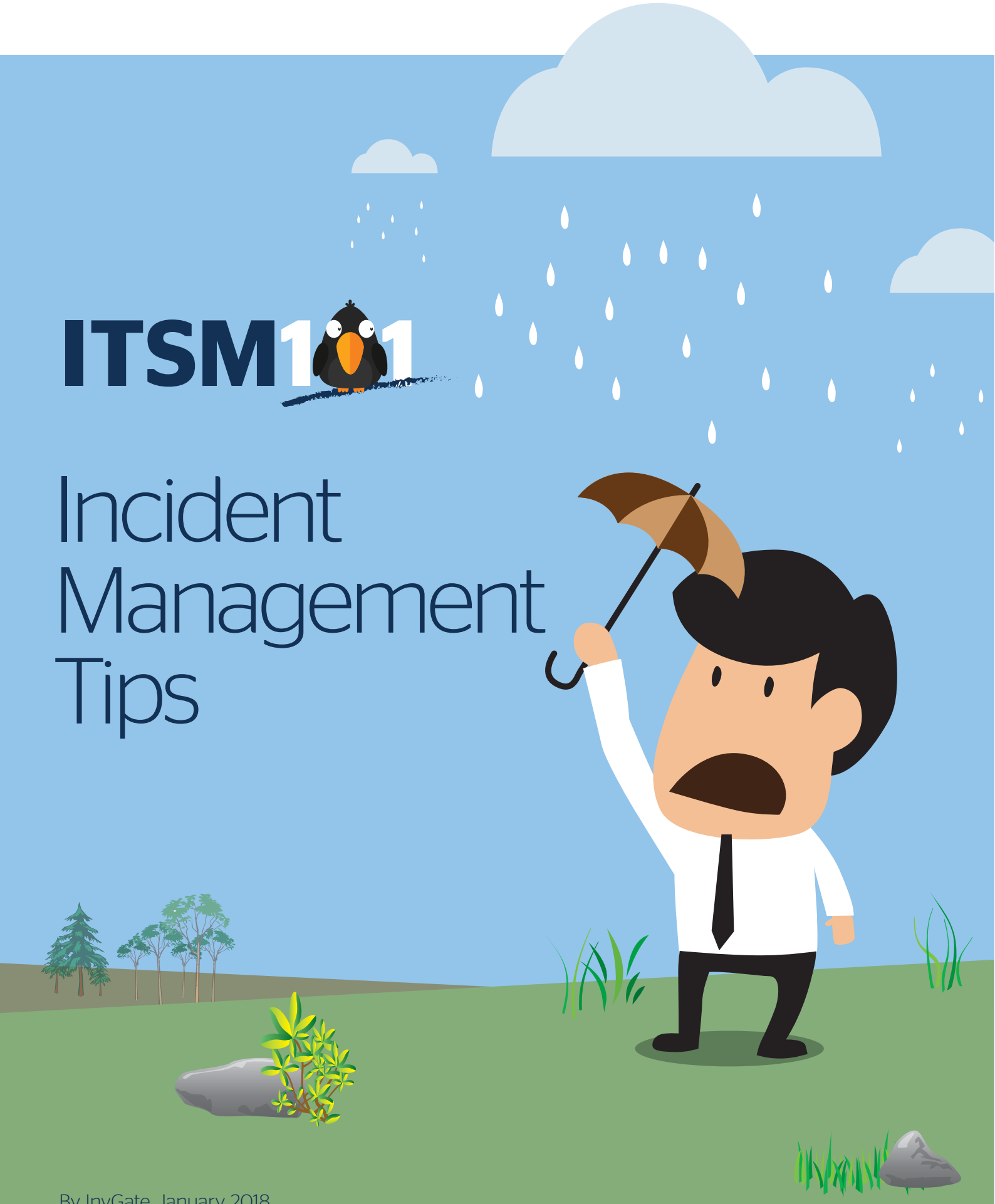
invgate

ITSM101

Incident Management Tips



By InvGate, January 2018

Dealing with IT issues is the most commonly adopted IT service management (ITSM) activity and, if the ITIL ITSM best practice framework is being used, this would be called incident management.

The incident management process is the set of activities that ensures all IT issues (termed "incidents" by ITIL) are logged and progressed effectively and consistently through to resolution. All while ensuring that nothing is lost, ignored, or forgotten about. With ITIL defining incident management as the process responsible for managing the lifecycle of all incidents to ensure that normal service operation is restored as quickly as possible and that business impact is minimized.

This paper looks at how incident management can add value to your organization, along with providing tips on how to make it work effectively in the real world.

Incident Management Overview

In a traditional corporate ITIL adoption – people tend not to call it an "ITIL implementation" due to ITIL being about people as well as process and technology – the incident management process contains the following steps:

- Identification
- Logging
- Categorization
- Prioritization
- Initial diagnosis (incident matching)
- Escalation
- Investigation and diagnosis
- Resolution and recovery
- Closure

With what ITIL terms "ownership, monitoring, tracking, and communications" throughout.

Here we will look at each of these incident management process steps in turn.

Identification

Identification is the part of the incident management process where we figure out that something's wrong or isn't performing as it should be. The ITIL Glossary definition of an incident is:

> *"An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item (CI) that has not yet impacted service."*

There are a number of different ways an incident can be detected. In an ideal world, automated monitoring, carried out as part of an event management process, would identify the incident and correct it via automation before any impact on the end user community. That said, we don't always live in a real world, so the reality is that we need to look at other ways of identifying incidents – be it via support teams or via our end users/customers.

When an incident is identified by IT personnel the onus is on that person to ensure that an incident ticket is raised and to work with service desk colleagues, and other support teams, to manage it through to resolution.

In the case of an end user or customer identifying an incident, the priority is for the service desk agent to get a ticket raised and prioritized, with the incident corrected as quickly as possible. In some instances, service desks will resolve the issue and then log the details later in order to help the end user more quickly.

Key tip: *separate incidents from service requests to allow for both better task prioritization and reporting on operational performance.*

Logging

This is the part of the process where the incident is captured in an incident record or service desk ticket. One of the biggest issues that we see with incident logging is overly-complicated forms within the service desk or ITSM tool. And one of the golden rules of following any best practice methodology is that you should always make it easy for people to do things right. With that in mind, the incident form should be short and to the point, with easy-to-use drop-down menus and free text fields when detailed information needs to be collected.

You can always add in more details as your incident management process matures. But when starting out with incident management, it's recommend that the focus is on asking the most critical questions such that the fix effort can get under way as soon as possible. Some example questions include:

- What's happening?
- What impact is this causing?
- Is anyone else affected?
- When did it start?
- Has anything changed on your device?

***Key tip**: remember that while logging incidents is important for operational management, knowledge management, and service improvement purposes – helping the end user get back to work quickly is the priority.*

Categorization and Prioritization

Categorization and prioritization are the steps needed to ensure that the resolving team has the best chance of resolving the incident at the first point of contact. The first level of categorization should be really simple, so make it as easy as possible for end users to log incidents, especially in a self-service environment. As an example, the first level of categorization could be something like:

- Hardware
- Software
- Network
- Voice

You can always add more complexity to additional levels, but by keeping the initial level simple, it will make it easier for both end users and service desk analysts to log incidents with the correct category and assign them to the right resolution team.

Prioritization is the part of the process that helps the resolving team to manage their workload. When establishing incident priorities best practice suggests that you look at:

- **Impact** – the degree to which the provision of services is disrupted within the organization, and the effect the interruption has on other areas of the infrastructure.
- **Urgency** – the speed with which the incident must be resolved.
- **Expected effort** – the anticipated amount of energy, time, and cost required to be able to begin restoring services after the occurrence of an incident.

Effective incident prioritization is key to making sure that the right incidents get seen to, and resolved, first. If your ITSM tool has an inbuilt priority matrix, use it. If not, have a set of standard questions or build your own matrix such that you can assign a sensible priority to each incident rather that going down the "if in doubt just tick the middle option" route.

Key tip: *avoid using high/medium/low terminology at the point of end-user engagement. Because, to the individual logging their incident, it's highly likely always to be of high urgency and all you will end up with is a queue of high-priority incidents and a support team not knowing what to fix first.*

Initial Diagnosis (Incident Matching)

Initial diagnosis is the part of the call, or other contact method, where you decide whether the incident can either be fixed at the first line or needs to be escalated to other support personnel or teams. Initial diagnosis is like the triage stage in a hospital – if you have ever been unfortunate enough to go to the emergency department. The first person you see after booking in at the front desk is the triage nurse who assesses whether you can be patched up there and then or if additional treatment is needed.

In a service desk environment, the first analyst should assess the call to determine if they can fix it straight away over the phone or if they need to escalate it to second-line support. Scripts, known error databases (KEDs), and knowledge bases can all help to improve first time fix rates.

One easy way of improving fix rates at the service desk stage is to invite other support teams to your weekly service desk meeting to give their top tips for troubleshooting specific issues over the phone – bring the fix closer to the end user. The advantages of this approach are twofold – the service desk analysts are upskilled, empowered, and more engaged; and, if more incidents are fixed on the front line, second- and third-line support teams are free to focus on planned, and less reactive, work.

Key tip: *having a high first contact resolution (FCR) level is considered industry best practice, but be careful – metrics drive behaviors. So, look out for the FCR metric driving the wrong behavior, with the first-time fix seen as more important than wasting the end user's time (as they wait for a suitable fix to be found).*

Escalation

If an incident can't be resolved at the first point of contact, then it needs to be escalated in order to quickly restore service. There are two types of escalation in a typical service desk set up:

1. Functional
2. Hierarchical

Functional escalation is where the next level of technical support and expertise is needed to resolve the incident. So, for example, a functional escalation could be from the service desk to second-line support or from second-line support to application support or network services.

To facilitate this, ensure that you have the priority-based roles and responsibilities for all support teams documented in your operational level agreements (OLAs) so that there's no potential for confusion. Some examples of what to include are:

- Timescales for escalation
- Time scales for responding to an escalation
- Roles and responsibilities – who does what
- How to respond in the event of a major incident.

Hierarchical escalations, on the other hand, are about seniority and are typically invoked in the event of an end user or service owner complaint, or if the priority of the incident needs to be raised. Examples of hierarchical escalations include: from service desk analyst to team leader, from team leader to manager, or from manager to head of department, and so on.

Hierarchical escalations are needed if a manager with more authority needs to be consulted in order to take decisions that are beyond the authority levels assigned to a certain level of staff. For example, to assign more resources to resolve a specific incident quickly, or to raise a purchase order for additional equipment. A predefined escalation hierarchy can save time in the event of a management escalation, for example from:

- Service Desk Analyst to
- Service Desk Team Leader to
- Service Desk Manager to
- Head of IT to
- CTO.



Key tip: *escalations will hopefully be a rarity in your IT organization but it doesn't mean that there's no need to plan for them. Spend time understanding the possible escalation scenarios and who would need to do what when. These can, and should, be tweaked over time as both needs, and personnel, change.*

Investigation and Diagnosis

The reality is, investigation and diagnosis occurs during every stage of the incident lifecycle along with monitoring and communication (including updates). As soon as the incident is logged the service desk analyst begins triaging the call and collecting information. This may result in a first-time fix, or the call may be escalated to second-line support and beyond where investigation and diagnosis will continue until the issue has been fixed and normal service is restored.

Documentation and support in the form of wikis, knowledge bases, or training sites can make a real difference to this stage of the incident lifecycle. By better sharing knowledge, and top tips, you'll be able to improve your service desk's incident resolution rates from good to great.

Key tip: *a key part of effective knowledge management is being able to see how a previous, similar, incident was resolved – the steps undertaken that worked and also those that didn't. So, when resolving an issue for which there's no formal knowledge article, ensure that you capture everything you tried for the benefit of the next person faced with such an issue.*

Resolution and Recovery

The applied resolution has worked and the issue looks to be fixed. But, before moving on from the incident, it's wise to test and test again. Why? Because closing an incident prematurely creates both additional work for the end user and service desk staff, and a poor impression of the service desk and IT department as a whole.

Key tip: *it's great that the incident is fixed from your perspective but you also need to check that things have been resolved for the end user or service owner. It's why best practice suggests a second element of incident closure – customer confirmation.*

Incident Closure

This really two elements: customer confirmation and closing the incident record in your ITSM or service desk tool.

Where possible, contact the end user/customer to confirm that everything is now okay and that they're happy for their incident to be closed. The second stage is to update the incident record with what happened and what you did to fix the issue before closing it off.

Remember what was said about knowledge sharing earlier? This is part of it. Simply writing "fixed" in an incident record isn't going to help other service desk agents if the same issue returns. The captured text doesn't have to be War and Peace, just a quick overview of what the issue was and how you fixed it.

Key tip: *ensure that service desk agents understand the importance of incident records throughout the incident lifecycle – from capturing the right end user and technology details, through being up-to-date with progress, to fully documenting the cause(s), fixes tried, and the ultimate resolution. Not doing so will cost the team dearly as incidents reappear over time.*

Summary

Incident management is one of the most important ITSM processes you will use because it affects everyone within the organization at some point. And nigh on every company needs some form of IT support whether in-house or outsourced.

Incident management and the IT service desk are also a highly-visible part of what the IT department does – you could argue that they are the public face of IT. So, if your incident management process isn't effective, you will adversely affect the business perceptions of IT as a whole.

Don't believe this? Industry analyst have proven this with their research. A large part of how employees feel about the corporate IT service provider is based on their IT support interactions. Why? Not only is it because it's a rare human-to-human interaction with IT, it's also at a time when the end user really needs help and will be far more alert to what the IT department does and doesn't do well.

So, ensure that your incident management process works well, with issues captured consistently, service restored as soon as possible, and nothing lost, ignored, or forgotten about. It makes a big difference to employees and, ultimately, business operations and success.

About InvGate

InvGate is a provider of IT service management (ITSM) and IT Asset Management (ITAM) solutions, designed to simplify and improve the lives of IT professionals.

InvGate Service Desk helps customers to provide better IT support, offering a single point of contact for end users to report IT issues and make requests for new services. With capabilities aligned with the ITIL best practice framework, InvGate Service Desk enables your company to improve IT support efficiency, to reduce costs, and to improve the quality of service and the customer experience for end users.

If you'd like to try InvGate for yourself, then you can start your free 30-day trial today.