



How to Use Automated Notification to Support IT Incident Management

A white paper produced by OnSolve

Author: Ann Pickren, business continuity expert and president of OnSolve



EXECUTIVE SUMMARY

Situation

Today's IT environment is more complex than ever before, and with that complexity comes a whole new range of demands placed upon IT managers—not the least of which is the need to accomplish more with fewer resources. The pressure on resource allocation and budgets demands a holistic approach to the identification of business opportunities for automated notification and how IT can benefit from the notification enablement for key processes.

Need

With the vast number of notification solutions in the industry today, many companies and notification vendors find themselves trying to force fit a solution designed for emergency notification into a tool for IT incident management alerts and escalations. Unfortunately this does not provide a robust solution that allows IT organizations to drive efficiency, quality and customer support.

With the vast number of notification solutions in the industry today, many companies and notification vendors find themselves trying to force fit a solution designed for emergency notification into a tool for IT incident management alerts and escalations.

Challenge

To address the growing demand for quality delivery of services from IT, the operations team must rely on tools to support ITIL processes within the organization. Some of the most prevalent tools are based around ITSM, like incident tickets, helpdesk issues, etc. In many cases, multiple ITSM tools are used to address some of the same issues for IT operations. While manual notification solutions can assist in the process,

IT organizations typically don't have the time to identify an incident, then manually launch and monitor responses from a notification solution. This scenario drives the need for automated integration between service management tools and notification solutions, a need that is not exclusive to ITSM departments.

Solution

Instead of devoting IT resources to monitoring systems and processes, automated notification can do the job for you. When events happen, automated alerts are sent to the appropriate staff, taking into account whether they are on duty, on call or out of office, letting recipients quickly fix problems before they cause downtime or delays. If the tool you choose is robust, flexible and full-featured, the tool can be used at every level of the enterprise to increase efficiency.

Result

Automated notification has proven to be an invaluable tool for incident management, quickly delivering a recognizable return on investment by reducing response time for IT incidents. These benefits are not unique to the IT department, and can provide great value when extended throughout the enterprise, ultimately helping to streamline business operations, increase efficiency and enhance productivity.

With the vast number of notification solutions in the industry today, many companies and notification vendors find themselves trying to force fit a solution designed for emergency notification into a tool for IT incident management alerts and escalations. Unfortunately this does not provide a robust solution that allows IT organizations to drive efficiency, quality and customer support.

It's well established that a reliable notification solution is a critical component of efficient IT operations. However, it makes no sense to apply a generic solution to the complex operations of an IT department as doing so will only hamper operations while handcuffing the team to a poorly chosen investment.

This paper will explore how notification works in general, and then apply those concepts to the unique needs of a typical IT department. Using that information, it will be much easier to determine the right solution for your organization.

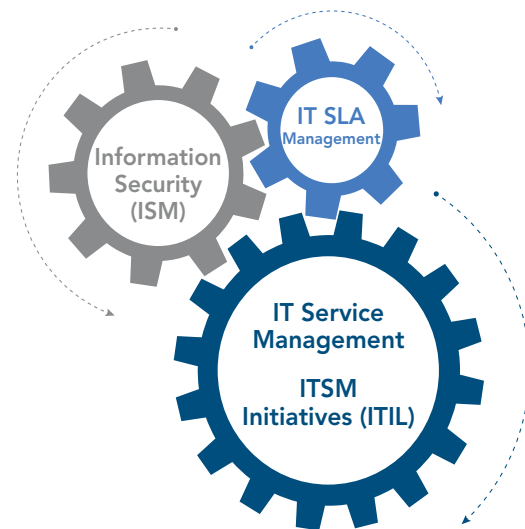
The importance of notification in IT incident management

Today's IT environments are not like they used to be. They've become much more complex, and with that complexity has come a whole new range of demands placed upon IT managers—not the least of which is the need to do more without adding new resources. This pressure on resource allocation and budgets demands a holistic approach to the identification of business opportunities for automated notification and how IT can benefit from the notification enablement for key processes.

While automated notification cannot solve all the challenges associated with IT management, there are many IT issues that can benefit from the integration of notification as a tool throughout ITIL processes.

IT operations and management have the benefit of being a service in high demand, and with that comes

the added importance and expectation from stakeholders for consistent and timely communications in the event of an IT incident or disruption of services. Time is not a luxury, but is of critical importance in the response and resolution of incidents and the communication of information regarding those incidents.



IT departments must manage many moving processes to serve the greater needs of the company.

To address the growing demand for quality delivery of services from IT, the operations team must rely on tools to support ITIL processes within the organization. Some of the most prevalent tools are based around ITSM, like incident tickets, helpdesk issues, etc. In many cases, multiple ITSM tools are used to address some of the same issues for IT operations. While manual notification solutions can assist in the process,

IT organizations typically don't have the time to identify an incident, then manually launch and monitor responses from a notification solution. This is driving the need for automated integration between service management tools and notification solutions, a need that is not exclusive to ITSM departments. Within the IT environment there are many opportunities to build integration with monitoring points that can instigate the launch of notifications when certain thresholds or triggers are met. This leads to the need for tighter integration with all of the tools used within IT to automatically launch notifications based on the criteria of the incident threshold or trigger.

Notification enablement in this type of environment follows the same principles of planning for messages about general business interruptions or crisis communication. Before the integration can be initiated, a process for messaging must be defined that identifies who should get the notification, what the message should say, when should it be delivered and, importantly, when escalation might be required. Don't forget that the IT incident might require the definition of unique groups and different messages. Obviously the IT resources that have responsibility for resolution must be notified, but information must also be provided for IT management and stakeholders (employees, customers, suppliers, etc.) who have a need to know about the incident. And each incident and the criticality or severity of that incident might require a different definition of these groups for notification and the timing for those notifications.

A brief history of automated notification

Arguably, automated notification began with one-way numeric pagers that were primarily used by medical staff for on-call resources. These pagers offered a more reliable way to get in touch with staff, no matter where

they were located. However, since pagers were primarily one-way communication tools, recipients were hampered because pagers lacked a built-in mechanism for response. Pagers were still popular and widely used for a long time, though often cost-restrictive for widespread use inside organizations.

When two-way pagers came along they opened up the opportunity for closed-loop communication, and with that came continued growth in the pager market. Pager technology is still in use in many organizations today, and though pagers serve a basic need for communication, they are still limited in their ability to exchange information.

While that has been successful in the past, the complexity of notification rules and escalation requirements, along with automation of the notification process, is quickly making these options lose viability as an efficient means of communications during IT incidents.

With the introduction of notification solutions in the 1980s, technology and applications offered solutions to expand the contact devices that could be used, extending beyond pagers. Those notification solutions typically consisted of point-to-point, one-way emails and pagers, with email working only within closed corporate networks. Computer-generated text-to-speech was so primitive as to be completely impractical except for the most cryptic alerts, used primarily by corporate IT personnel for network maintenance issues.

The early '90s saw the introduction of email for the masses, but only with subscription services and at dial-up speeds. At this time we also saw advances in Integrated Services Digital Network (ISDN) and T1 technology, dramatically decreasing the cost of telephony ports while increasing the capacity of trunk lines.

By the year 2000, costs and capacities were at a point that sending an urgent message with thousands of simultaneous phone calls became practical and cost-effective. Email had also advanced to become a universal communication medium, making it practical for reaching many people quickly.

The 2000s saw the need for effective mass communication grow, with new technologies making new solutions possible. Chief among them were VXML, improved text-to-speech, SMS, and Web 2.0.

The impact of mobile technology

The advent and subsequent proliferation of mobile phones marked a tremendous milestone for connectivity of the mobile workforce, and notification solutions have grown correspondingly. Today, as people now carry mobile devices with them almost wherever they go, the need for notification solutions that can reach any number of people at any time on a variety of devices has become paramount.

The notification landscape itself has changed with advancements in technology that have allowed many companies to design and bring to market different notification-based solutions. Enterprises of all kinds have found a need to notify and alert groups—from one to thousands—of business interruptions, pending disaster or simply for day-to-day communication.

The landscape has now matured significantly in the use of automated emergency notification solutions to address multiple use cases, including IT alerts, business continuity and disaster recovery, emergency notification, and to enhance overall efficiency and productivity throughout the enterprise.

Why automated notification?

Information technology dependencies have grown dramatically. More and more we are seeing IT systems as the lifeline of a company's ability to deliver products and services. So, when (not if) those systems fail, there is an enormous sense of urgency to find a resolution to the cause of the system breakdown or interruption, and to quickly communicate with all the stakeholders who are impacted by the disruption of services.

As long as there are events that interrupt the status quo, there will be a need to inform those who are affected by the interruption as well as those who can get things back on track. Nowhere is that more evident in the modern IT department.

The use of technology to reach key IT personnel started with the advent of pagers many years ago. The adoption of "rotational pagers" meant there was often a need to have one individual make sure the next on-call staff individual received the pager when responsibilities transitioned from one to another. While one-way and two-way paging for IT staff have been in use many years, their capabilities are much more limited than the technologies available today for automated notifications.

Notification requirements for IT

With the increasing complexity of IT operations, there are many ways in which an automated notification solution can bring value. However, caution should be taken in making the assumption that a notification tool that is used in other areas of an organization (business continuity, crisis communications, employee health and safety, or general business operations) will have the feature set and functionality that is required to meet the demands of an IT department.

Beyond the standard notification feature set that is seen in many of the industry-leading solutions, IT notification solutions must also be able to address IT-specific issues, including:

IT environment	Required notification functionality
IT skill-based resources	Ability to escalate through specific skills for specific employees
Multiple shifts with on-call responsibilities that rotate based on schedules	Robust schedule and shifts with intelligence to automatically send notifications to the correct individuals, depending on the shift and current on-call schedule
IT management oversight and need for situational awareness (possibly with or without call to action)	Escalation through management layers for awareness of developing incidents and the individuals who take ownership of the resolutions
Monitoring and threshold management of critical components and applications	Integrated notification capabilities to recognize triggers or thresholds and automatically launch pre-determined notifications to address the developing incidents
IT service management tools	Automated integration of notifications both to receive information from ITSM tools, and then to launch notifications, with the ability to then return information to the ITSM tool and update information
Complex operating procedures	Need for an automated workflow that can be configured to interpret information and take actions based on defined criteria, including launching multiple notifications and integration into other tools within the IT environment
Integration to enterprise applications	Strong API for notification solutions and a run book automation tool for building custom logic

There are many products in today's market that can help address these and other notification requirements. Each comes with a variety of options, ranging from those that can be installed/licensed in your environment to cloud-based and SAAS-hosted solutions. In some cases a hybrid solution, combining installed and cloud or SAAS services, might be the best answer for your specific needs. The main reason most organizations select a SAAS model is to minimize the risk of dependency on its own IT environment for the delivery of critical systems, when in fact, the IT environment might have been impacted by the incident.

How to justify the cost of a solution

Among the many reasons for justifying the cost of a notification system with the advanced integration discussed in this article should include:

- **Performance** – Pre-defined processes that support initiatives for quality and performance in the IT environment
- **Consistency** – Workflows that define initiation and actions, taking away manual intervention that can result in failure to follow defined processes
- **Efficiency** – Reduced time and streamlined processes for service delivery
- **Reliability** – Repeatable, consistent results that eliminate human errors and follow defined standard operating procedures

How to approach notification services implementation

Once the decision has been made to take the steps to define and implement a notification solution for the IT environment, specific implementation steps will ensure the organization gets the full value of the notification solution.

1. **Begin by analyzing the notification behaviors you want to achieve** – Don't make a decision on a tool based on just a few features. Take the time to analyze what features are most important and prioritize those in your selection of a tool.
2. **Develop standard operating procedures** – The tool can then automate the process. Make sure to define the incidents and the criticalities that will drive the development of your notification processes.
3. **Map your notification process** – Include who should be notified, what the message should be,

what the escalation tiers should include, and what actions must be taken for the responses returned from the notification.

4. **Design your framework** – Understand how notification will integrate throughout the organization. Integration concepts should include which enterprise applications would benefit from notification enablement, and how that will be accomplished.
5. **Integrate notification with ITIL processes** – While notifications are a critical part of incident management, notification technology can be used throughout many ITIL processes, including but not limited to change management, configuration management, availability management, service continuity management, problem management and many others.
6. **Perform technical integration** – Use a variety of tools that work with the notification solution for complex and customized integrations. Whether it's the use of a Web services API or run book automation, integrations can be accomplished in a cost-effective manner.

How consolidation can streamline enterprise-wide operations

Since point solutions are adopted to address a particular need, they often seem like a perfect solution. However, having multiple notification solutions within an organization can actually foster

- More work
- Greater risk
- Additional overhead
- Increased confusion
- Higher costs

Addressing these point solutions and bringing a single, consolidated solution for the full set of requirements, organization-wide, will drive enhanced efficiency in the management and oversight of the notification platform. It will also bring a consistent notification methodology for all critical communications across the organization, ultimately eliminating the silos that can develop around each of the point solutions. Best of all, a consolidated platform, time and again, can be justified by the cost savings and ultimate return on the investment that your organization makes in deploying an enterprise notification platform.

Seen holistically, this concept of consolidation offers a solution that ties all the enterprise needs for notifications into a single solution, while at the same time, meeting the unique needs created by each use case.

However, moving towards this consolidation in a notification platform requires a strong vendor who understands the many use cases for notifications and how those vary in requirements. Not every vendor understands or takes this holistic approach to the development and delivery of a robust notification platform.

Automated notification at every level of the business

- **Information technology**
Instead of devoting IT resources to monitoring systems and processes, automated notification can do the job for you. When events happen, automated alerts are sent to the appropriate staff, taking into account whether they are on duty, on call or out of office, letting recipients quickly fix problems before they cause downtime or delays.
- **Business operations**
When events happen that may impact operations, supply or distribution, use automated notification to notify distributors, vendors and partners. It's great for managing projects, alerting teams of scheduling changes, sharing HR announcements, broadcasting company-wide notifications and streamlining processes while increasing efficiency
- **BC/DR**
When business is interrupted by events like power outages or natural disasters, you need to communicate with your people. When minutes count, automated notification can deliver a message to thousands at once, alerting the people who keep your business running and giving them a way to respond with critical information during a crisis.
- **Emergency notification**
When disaster strikes, response teams must be mobilized. Manual systems are prone to failure, distract staff, tie up phone lines and can delay rescue efforts. Automated notification lets you send alerts to thousands of recipients at once, and by a wide variety of communication modes, reducing response times and saving lives and property.

SUMMARY

There are many cases that illustrate how automated notification has proven to be a valuable tool for incident management, quickly delivering a recognizable return on investment by reducing response time for IT incidents. At first look, these benefits seem unique to the IT department, but on closer inspection one can find great value in extending or expanding the use of notification throughout the enterprise.

The goal then becomes choosing a solution that addresses the specific needs of the IT department, but also has the flexibility to work in other departments as well. The way to do this is by first determining the unique needs of specific departments, then taking a step back for a more holistic of your organization. This way your organization can reap the benefits of more streamlined operations, increased efficiencies and enhanced communication on every level.

About OnSolve

OnSolve is the market leader in real-time, mass notification and collaboration solutions used by the world's largest brands and thousands of government agencies to deliver critical information in any situation. Mass notification and collaboration is an essential element of emergency response and business continuity planning, keeping teams on track and coordinating during critical events. The OnSolve suite of critical communication tools is a key component of the business continuity, emergency response, IT alerting, employee safety and security programs of every organization we serve. Visit us on the Web at onsolve.com.