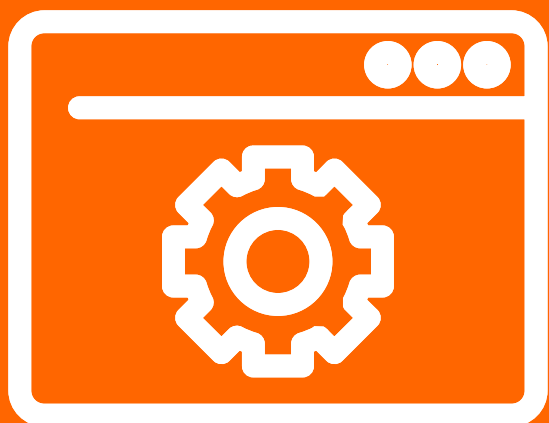







The Limits of IT Service Management (ITSM) for Managing Disruption; Why ITSM software and tools aren't fit for purpose



What is IT Service Management?

In Information Technology, incident management refers to a process used by DevOps and Ops teams to respond to unplanned events or service interruptions. Incident management, along these lines, has meant restoring services to their operational state as quickly as possible.

The steps typically involved in IT incident management and response have included the following:

-  Preparation
-  Detection and reporting
-  Triage and analysis
-  Containment and neutralization
-  Post-incident activity

At least, that's according to IT Service Management, or ITSM.

ITSM is the generic term used to describe a strategic approach to designing, delivering, managing, and improving the way businesses use their information technologyⁱ.

Originally devised to go beyond the traditional model of IT support, ITSM is meant to be more inclusive, describing the end-to-end processes and tools IT teams use to manage services, inclusive of all information technologies within the organization.

What does it involve?

ITSM consists of all the relevant activities and processes that go in to supporting an IT service through its entire lifecycle. Those activities and processes are likely to include service management, change management, problem management, asset management, information and knowledge management, and, of course, incident management (See more below)ⁱⁱ.

Relevant	ITSM processes
Change management	Often, inclusive of release management. When a service is out of step with business expectations, it must be modified, expanded, or otherwise altered. IT must determine how these changes will affect the service deployment, implement them appropriately, then monitor if the changes have the intended effect.
Asset management	Services require software and hardware assets to function. These assets should be tracked, updated appropriately and mapped to show how they interact. Configuration management, capacity management, and asset management deal with these concerns and can be blended or separate processes.
Project management	IT services transition between various stages of the lifecycle at different times and different speeds. Project management skills enable IT organizations to maintain orderly services and avoid problems such as outdated systems or shadow IT.
Knowledge management	Knowledge management crosses into the other ITSM processes, a way to avoid duplicated work and discovery by organizing and making available information about IT services.
Incident management	When an IT service is disrupted by performance issues or an outage, the IT service desk must address the issue, restore service availability, make improvements, and codify procedures to prevent reoccurrence.
Problem management	A problem is the root cause of an incident. An IT organization might remediate an incident but not fix the problem, leading to future incidents. Therefore, problem management is a way to permanently fix issues to improve service delivery and performance.

Where does ITIL fit in?

Indeed, the goal of IT service management frameworks (generally) is to ensure that the right service management processes, people, and technologies are in place. One of the better recognized frameworks, and most widely used structure for ITSM, is ITIL (Information Technology Infrastructure Library).

ITIL, as the name suggests, is a globally recognized collection of best practices for managing information technology. It's been around since the 1980s, when established to help government IT departments in the U.K. deploy a consistent set of best practices.

Today, ITIL processes cover how to set a strategy, create a design, manage change, handle service operation and management, and make continual service improvements (See more, below)ⁱⁱⁱ.

ITSM processes	
Strategy	Specifies that each stage of the service lifecycle must stay focused upon the business case, with defined business goals, requirements, and service management principles.
Design	Provides guidance for the production and maintenance of IT policies, architectures, and documents.
Transition	Focuses on change management role and release practices, providing guidance, and process activities for transitioning services into the business environment.
Operations	Focuses on delivery and control process activities based on a selection of service support and service delivery control points.
Continual service improvement	Focuses on the process elements involved in identifying and introducing service management improvements, as well as issues surrounding service retirement.

When ITSM breaks down

It's obvious why ITSM is an attractive model for IT teams. Within the limited confines of IT-centric incidents and disruptions, such as helpdesk support and troubleshooting procedures, ITSM lays out clear processes and actions, through well-articulated workflows.

Those processes and actions, in turn, offer clear efficiencies in IT resource management, helping organizations save time and money, reduce incident downtime, and increase visibility and response.

If only it were that easy, though.

As has become clear, not all incidents are IT-centric. Risks and hazards come in all shapes and sizes. And even those that don't emerge from IT are likely to have major ramifications for IT services.

What, then, does ITSM have to offer?

Unfortunately, nothing.

Indeed, ITSM has nothing to say about the management of incidents that emerge outside of IT, e.g., natural hazards, reputational threats, and physical security threats – even those that eventually impinge on IT services.

The framework offers no actions to take to analyze, identify, and correct those problems; nor does it provide actions to take to prevent future incidents. What's worse, it's non-IT-specific incidents that are increasing in kind, cost, and intensity.

When those incidents hit IT infrastructure, as they inevitably will, IT teams solely armed with ITSM software and tools won't be prepared to respond and recover.

How could they? IT teams solely reliant on ITSM software and tools don't have the requisite all-hazard processes and operational tools to help manage most incidents. Even a process as simple as coordinating with operational business managers on non-IT incidents is beyond the remit of ITSM, as ITSM doesn't give IT teams the language or processes to coordinate with operational business managers in response to incidents that are not-IT-centric.

What's more, ITSM roles and responsibilities wouldn't be fit for purpose; ITSM functions established to align with an organization's business outcomes would also be rendered unfit for purpose.

Why's that?

Narrowly focused on the fulfilment of changes, ITSM doesn't provide the requisite situational awareness to respond to incidents that aren't wholly IT-specific; ITSM fails to provide both decision-support tools and crisis communications.

And those aren't the only critical event management challenges ITSM software and tools fail to solve. The extensive list includes:

-  Getting timely information to all stakeholders during a critical event
-  Coordinating between different business units and management levels
-  Providing a centralized location for critical information, such as impacts, responses, and key messages
-  Gaining situational awareness to manage natural hazards and other common threats
-  Going beyond routine IT systems-support to help the rest of the organization
-  Enabling crisis and executive team collaboration
-  Following the flow of relevant information that's scattered across emails, meetings, documents, calls, and chat
-  Enabling the identification of affected workers and providing communications to reach them
-  Providing consistency in key-communications methods and content
-  Providing consistent messaging to customers, investors, workers, and the wider community

All-hazards software and tools to manage all incidents

What does? That's where critical event management and crisis management software platforms come in.

In contrast to narrowly-tailored ITSM software tools, critical event management platforms provide enterprise-wide situational awareness and coordination for any critical event – inclusive of, but not limited to, IT disruptions.

That's not all.

Not developed specifically for IT operations, critical event management platforms can be owned by any team in the organization – not just IT. That makes it easier to get everyone on the same page, with the same business-objective perspective that improves visibility and cuts down on costs.

As a result, these platforms allow for better coordination with operational business managers. And as the platforms themselves don't require lengthy change management cycles, like ITSM software tools, there's no need for extra IT resources.


All-hazards management for critical events as a strategic investment

What's not to love? Indeed, the advantages of all-hazards management systems for critical events, over ITSM software tools, are exceptional. Which makes all-hazards management a strategic investment to consider.

All-hazards management for critical events:


- 

Enables teams across all areas of the business to collaborate, consistently respond to customers, and share information during a crisis



Reduces the need for people to dial into meetings to find out what's going on
- 

Automates and leads people through procedures with fully-configurable workflows



Monitors and generates incident response tasks; logs and shares updates, decisions, facts, and assumptions; produces situation reports
- 

Reduces reliance on IT to provide situation reports, enabling IT to focus on resolution



Automates communications based on business rules in workflows
- 

Provides stakeholders outside IT with easy, self-serving dashboards and workspaces tailored to their view of the incident



Creates crisis strategies and action plans from a library of 80-plus best-practice templates; or enables easy tailoring to your organization

 - That way, when events occur, the plan comes to life, the team knows what to do, and progress gets tracked in real time
- 

Ensures employee safety with location-based notifications, welfare checks, and panic button
- 

Manages critical events consistently, whether originating from IT or externally



Conducts exercises and post-incident reviews; captures lessons learned and improvement actions
- 

Ensures all stakeholders have consistent situational awareness and messaging, across the enterprise

A complete solution for any risk or hazard, Noggin stands out from the bunch as a strategic investment. For one, the next-generation disruption management solution offers best-practices out of the box.

That's not all. Benefits run the gamut.

No-code customization enables customers to tailor Noggin solutions to their risk profile or (easily) build their own. And a full range of integration options also make it easy to connect and synchronize data and plug in existing customer systems, e.g., single-sign on, messaging, and mapping.

What's more, subscribing to critical event management (CEM)-as-a-Service gives you the ability to deploy best-practice modules quickly – with nothing to install and scalability to meet all demand.

In close, change is hard. But not having the right tools to respond to the likeliest disruptions is even harder (and costlier).

Unfortunately, too many organizations run the risk. Overly reliant on ITSM software and tools when critical event management software provides for better quality decision-making, faster response time, and reduced impact from critical events. And with critical event management software, IT wins, too, with more time to coordinate work.

The moral of the story: don't miss out. Invest in critical event management software, like Noggin, to give your executives, crisis teams, and other enterprise stakeholders (IT and beyond) the tools they need to collaborate, consistently respond to customers, and share information during any crisis – not just an IT incident.

Sources

- i. Stephen J. Bigelow, *Tech Target: ITSM (IT Service Management)*. Available at <https://www.techtarget.com/searchitoperations/definition/ITSM>.
- ii. *Ibid.*
- iii. Stephen J. Bigelow and James Montgomery, *Tech Target: ITIL (Information Technology Infrastructure Library)*. Available at <https://www.techtarget.com/searchdatacenter/definition/ITIL>



Like what you read? Follow Noggin on social media



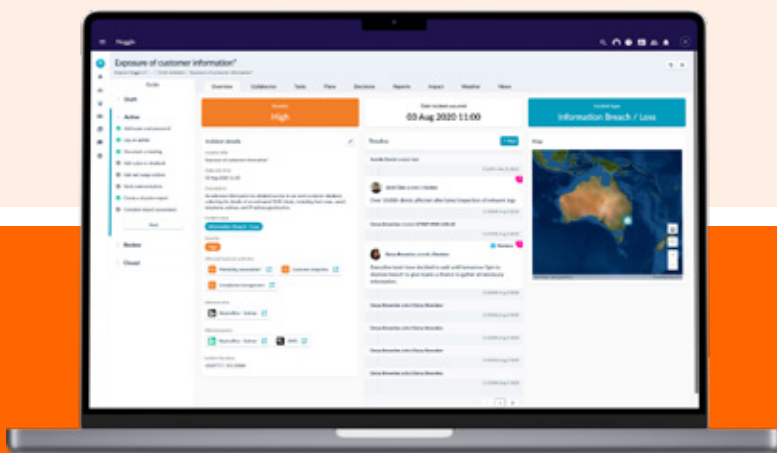
@teamnoggin



facebook.com/teamnoggin



linkedin.com/company/noggin-it



noggin for Crisis

Meet the next-generation tool for corporate crisis and business continuity management teams to collaborate, plan, track their response, and share information. Built on the Noggin Core platform, Noggin Crisis gives response teams and decision makers the tools to know what's happening, collaborate quickly and effectively, make better decisions, and enact the right plans to take action when it counts the most.

The Noggin Crisis solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.

To learn more,
visit: www.noggin.io
or contact: sales@noggin.io