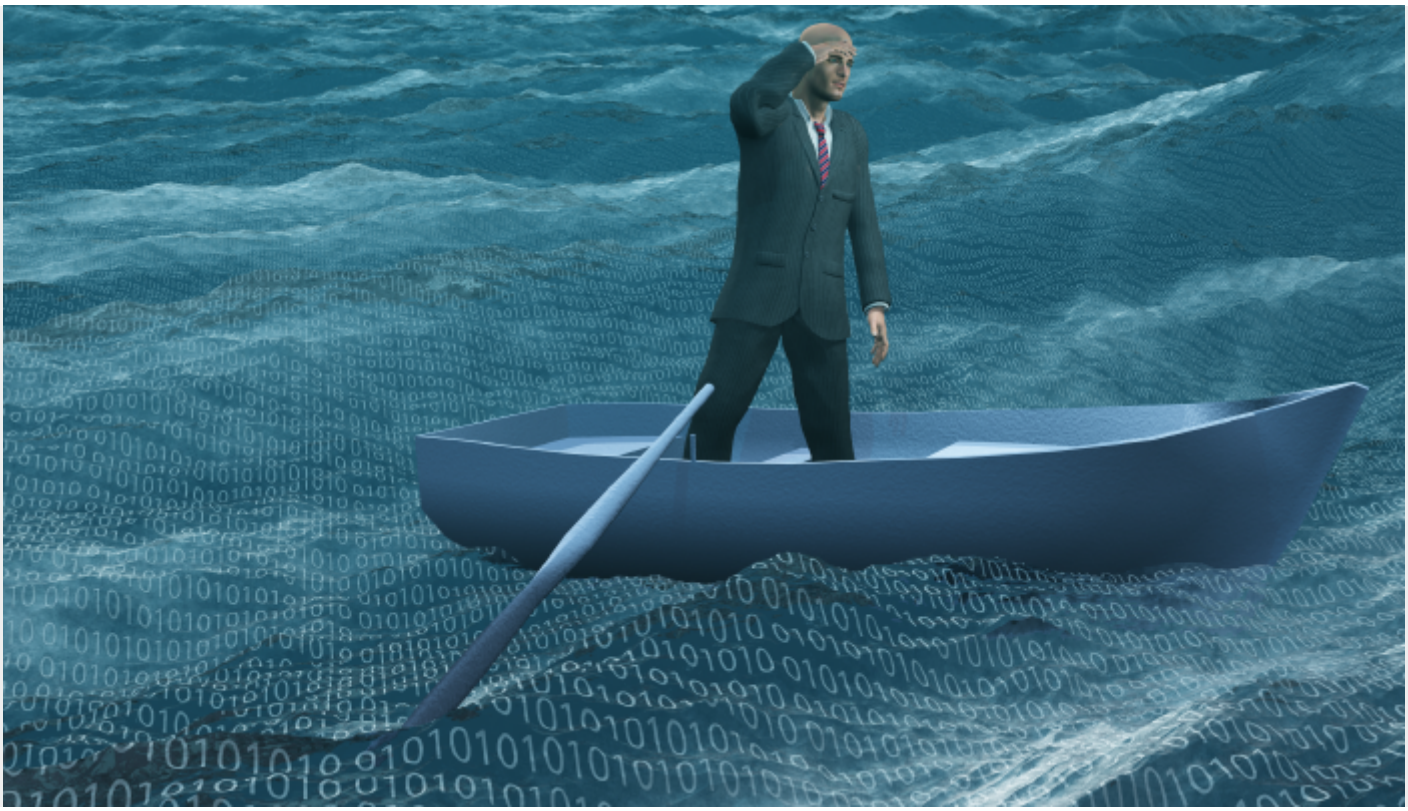
THE INCIDENT COMMANDER (IC) ROLE EXPLAINED



When users can't log in, access data, or process transactions, they aren't happy. No one is happy when technology isn't working as it should.

And it doesn't matter the size or platform, on premise or cloud-hosted—no one is immune to potential outages and degraded services. CRN chronicles 10 of the biggest cloud outages so far this year. The causes are varied, ranging from changes gone wrong to overloads from demand surges.

Regardless of the cause, any major incident requires handling with greater urgency and shorter timescales. That means a firm hand is needed to coordinate the efforts to restore services to normal working conditions. And that brings us to the role of incident commander (IC).

Incident Commander in the war room (Source)

What is an incident commander?

For the most part, you won't hear the title "Incident Commander" in someone's job title at the IT department. The reference is mainly found in health and safety domains, where the IC is responsible for managing teams involved in emergency situations that by nature involve danger and rescue such as fire services. FEMA has an apt description for that kind of role in an organization:

> *The IC has overall management responsibility for the incident.*

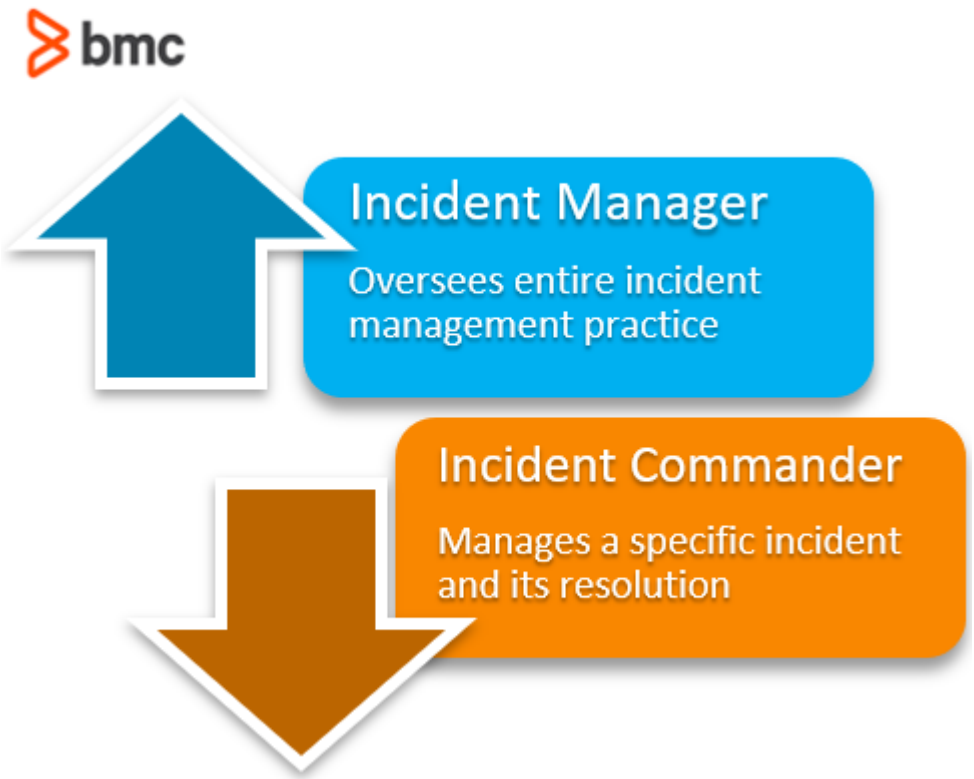
In service management, whenever there is a major incident, the organization must designate one person who's responsible for leading a temporary cross-functional team to focus all energies and attention towards a swift resolution.

ICs are needed for major incidents—not every single incident. Remember how ITIL 4 describes an incident:

> *An incident with significant business impact requiring an immediate coordinated solution.*

Isn't the incident manager the IC?

Some texts use the term 'incident manager' as a synonym for the IC. A closer look reveals that the incident manager is responsible for the operational activities of the incident management practice and may not necessarily be the designated person for certain major incidents.



At one of my previous employers, the IC was one of the heads of department. This role was separate from the incident manager who sat in operations.

What does an IC do?

The IC's work is to maintain oversight of the major incident procedure. The IC is accountable for the activities involved in managing the major incident to complete resolution. These tasks include:

- **Occupying the war room** (or establishing the conference call) to manage interactions and escalations with relevant stakeholders involved in the incident.
- **Identifying and onboarding key technical specialists** required to swarm over the incident and quickly analyze symptoms and suggest possible solutions.
- **Accessing resources (including financial) designated for addressing major incidents**, such as purchasing additional processing or storage capabilities or temporarily contracting expertise from vendors or third-party specialists.
- **Providing status updates** using the agreed communication channels and clarifying the message to be sent out to external parties, e.g. media, regulators, customers, etc.
- **Performing post-resolution follow-up** on agreed actions, e.g. incident reporting, root cause analysis, error control, and lessons learnt.

Qualities and competencies of an IC

One wouldn't expect an IC to be a rookie in the organization. Given the psychological strain that accompanies the pressures of dealing with a major disruption, the kind of person who would command such as situation should have a level of experience that mirrors that of an army general!

When designating an incident commander (or perhaps you've just been appointed one!), here are some qualities to consider:

Key business relationships

The IC will have built up relationships with key stakeholders over time. The reason for this is two-fold:

1. The IC must communicate with a wide range of technical and non-technical personnel to accomplish fast and accurate incident resolution.
2. These same people must also respect and trust the IC's plan of action and management.

Some technical knowledge

The IC should have a good understanding of the lay of the land in terms of configuration of various service components. It's not a must that the IC be a technical specialist in all domains (comb shaped), as it isn't expected that the IC be the hands-on person rebuilding the database from scratch or spinning up new virtual machines.

Good at managing (not necessarily solving the problem)

Good practice in major incident management is to separate the actual restoration activities from the management of the incident itself. (It can be quite disconcerting for the sysadmin to have the CEO behind them questioning the meaning of bash command.)

Creative problem solving

Creative thinking and problem solving are also key competencies required by the IC. Most major incidents are not alike, so new ways of dealing with issues will need to be discovered.

Good at communication

Positive communication is also an important attribute as the way the message of the incident handling is passed can play a big role in shaping the perception of stakeholders as to whether the IC is actually managing the situation in the best possible way.

(Learn more about ways to communicate about incidents.)

Emotional intelligence

There is also a need for significant emotional intelligence (EI), as handling people and emotions is usually the biggest hurdle for the IC—beyond the technical aspects. Daniel Goleman outlines the four domains of emotional intelligence, with a statement that leaders with EI handle crisis better than those without.

Looking at the four domains, we see the following qualities:

- **Self-Awareness.** Being conscious of your feelings about the incident, and how other people feel about it, can help the IC be better in understanding what is going on in their environment, and not be clouded by judgement that may come from previous experiences.
- **Self-Control.** Once aware of your feelings, you can make better decisions on how to react to them. For instance, the IC will recognize flight vs flight emotions, and choose to make the right choices about how to react to people during the incident, even in the face of pressure and loss.

- **Social Awareness.** Being empathetic of people's feelings will be a key asset for the IC especially in understanding impact of the incident on business services and processes. That means the IC will not play down the urgency that the business expects from technology and suppliers to restore services as quickly as possible. Similarly, the IC must be aware of the feelings of the technical teams including vendors who face the challenge of needing to quickly resolve the incident without buckling under pressure.
- **Relationship Management.** The IC has to be inspiring enough to rally all the stakeholders in one direction. The IC must foster the right mindset in everyone involved to work together, manage any conflicts that come, and remember the big picture.

The IC perspective

The IC role is not one that should be taken lightly. It is important that anyone chosen to handle this responsibility must have a perspective that is not limited to technical aspects: the IC must be conscious about shepherding people in the right direction towards the common goal—quick resolution of the incident.

Additional resources

For more on incident management, explore the BMC Service Management Blog and these related articles:

- Incident Management vs Problem Management
- Why Incident Response Plans are Critical for IT
- How To Map the Incident Management Process
- How and Why to Run Incident Drills
- Introduction to Critical Incident Response Time (CIRT): A Better Way to Measure Performance
- Guide to IT Leadership & Best Practices