This playbook is intended to provide an overview of IMS and how the system works and is designed to be read prior to training that the Blackrock 3 Partners would be providing. For questions regarding this document or any questions regarding IMS or the services of Blackrock 3, please e-mail: info@blackrock3.com
Overview of the Incident Management System (IMS)

The Federal Emergency Management Agency (FEMA) defines an incident as “an occurrence or event, natural or human-caused, which requires a response to protect life and property.” IT incidents, while not typically life threatening, may certainly threaten the livelihood of a business, cause financial loss, impact the company’s reputation and erode trust with its customers. To that end, an IT incident that requires an incident response will benefit from being managed by a clear system that every incident responder understands. Without defined rules of engagement, identified roles and responsibilities and clear leadership, the team managing the incident may lose track of time or struggle as a leaderless group with no sense of direction because there is no consolidated plan of action. In short, any type of incident will benefit from being managed by a well-defined system.

Fire Departments have long recognized the benefits of a flexible, scalable, command structure for managing a wide variety of incidents. The concept of the Incident Management System (IMS) was developed more than 40 years ago, in the aftermath of a devastating firestorm in Southern California. The overall cost and loss associated with these fires totaled $18,000,000 per day ($110,000,000 per day in 2016 dollars) or $1.400,000,000 for the entire incident! Although all of the responding agencies cooperated to the best of their ability, numerous problems with command, control, communication and coordination hampered their effectiveness.

As a result, Congress mandated that the U.S. Forest Service design a system that would “make a quantum jump in the capabilities of Southern California wildland fire protection agencies” to effectively coordinate interagency action and to allocate fire suppression resources in dynamic, multiple-fire situations. This resulting management framework, IMS, is in use in various forms around the world by federal, state, and local governments, public safety agencies, and some private sector hospitals and corporations. And while there may be subtle differences among them, they share a set of common operating principles. This is why IMS from the fire service translates to the IT environment; because all emergencies share the need to

Key Point:
The IMS does not solve problems. People using IMS as a tool and making good decisions solve problems.
bring a team together quickly under focused and directed leadership to solve a problem in the shortest amount of time.

This *Incident Management System Playbook* is designed to give the internal team members a working foundation to understand the basics of the IMS. In order to set the stage for implementing IMS, operating as an *Incident Commander (IC)*, or participating as a *Subject Matter Expert (SME)*, it is important to understand this fundamental concept:

**When an incident occurs, all individuals responsible for resolving the problem must shift their thinking, decision-making, and operational posture from *Peacetime* to *Wartime.***

*Peacetime* is the *Uptime* steady state, system normal environment of Continuing Operations (ConOps). In short, it is business as usual.

*Wartime* is the *Downtime* incident mode of operation that occurs when any application or infrastructure element experiences a problem beyond the steady state, system normal usual course of business. In *Wartime*, responders must shift their sense of urgency and focus to the problem. Their language and method of communications must be crisp and clear. All resources of the company should be at the disposal of the problem solvers so they can protect reputation, customer trust and minimize financial impact.

In *Wartime*, the response team has to think and act as fast as the incident is unfolding. To do that, communications must be directed at a specific person or the function they represent, with a time deadline for action and those actions must be completed and confirmed. Think about talking like you would post on Twitter – short, crisp and to the point.

Solving *Wartime* problems that threaten the livelihood of a company, no matter how large or small, requires a *Wartime* mentality, behaviors, and organizational structure. IMS is the framework, which brings together a pool of experts in order to form a high speed collaborative and cohesive incident response effort.

Boiled down to the most basic concepts, IMS provides a basic framework to bring an incident response together in order to:

- Size-up, triage and understand the problem.
- Obtain the right talent at the right time to resolve the problem.
- Organize that talent under an Incident Commander.
- Provide a directed forum for that talent to digest data from tools and monitoring and engage in collaborative discussion, in order to develop a plan to resolve the problem.
- Being mindful of time, collectively drive the incident toward resolution.
• Investigate the technology failure and the incident response of the people in order to conduct a useful After Action Review (AAR).

• Use the AAR as a learning tool to reduce technology failures and improve the people part of the incident response.

IMS is not a recipe. It’s an approach and a methodology for setting the rules of engagement for managing the people response to an incident. IMS is about how the people relate to each other when the stakes are high, the decision-making environment is poor and the outcome of the incident is uncertain. IMS is what the IC uses once the incident responders are assembled and can begin the problem solving effort.

Role of the Incident Commander

The anchor point for IMS is the position of IC. Without leadership and a process to organize and direct personnel and resources, the effort to solve any problem may end up being as chaotic as the problem itself.

For any incident to be successfully managed, there must be one person in charge – the IC.

The IC should:

• Have an accurate understanding of the problem, or focus the group discussion on gaining an accurate understanding. The goal is not to get everyone thinking alike; the goal is to get everyone thinking in the same direction.

• Develop an action plan with input from the right experts when needed.

• Have access to whatever pool of resources is required to resolve the problem.

• Establish reliable methods to communicate across the various disciplines handling the incident.

• Provide information to key stakeholders (executives, customers, vendors, etc.) in a timely manner.

Figure 1: If you are the IC, your primary goal is to keep the response focused, on track, and moving toward resolution.
The IC must stay focused on moving the incident toward an established end point. This is no easy task, as many public safety ICs will quickly admit.

Additionally, ICs have the burden of wearing multiple hats during the course of an incident. Aside from organizing the incident responders, an IC may be fielding questions from executives regarding estimated downtime, updating internal communications, surveying customer experience, and releasing personnel from the incident who may be needed elsewhere in the company. These are very real demands made by others who may or may not appreciate the complexity of managing an incident. It becomes your task as an IC to accomplish many things at once.

A good incident response team is able to quickly transition from Peacetime to Wartime – perhaps several times a day – in order to bring a known incident response to an unknown Downtime problem and return the systems back to Peacetime. The only variable should be the nature of the incident, not your response to it!

It is also the IC’s job to:

- Prioritize the incoming flow of information.
- Focus the discussion and invite healthy conversation.
- Determine which items warrant direct attention and which ones can be delegated.

The IC is Responsible for Developing the Wartime Battle Plan for the Incident

There are certain objectives that must be met during the lifecycle of any incident. They are the milestones of an incident response achieved by good decision-making and action by the IC. There are four key actions areas an IC should address when directing the response and can be remembered by using the mnemonic STAR:

- Size-up the problem
- perform Triage to determine the severity
- develop an Action plan
- define Recovery and estimate the odds of the plan’s success

Key Point:
A good IC isn’t concerned about making quick decisions, but should focus on making the best decision in the shortest amount of time.
Regardless of the nature of the incident, it is critical to take time to understand the problem or at least the presence of a problem, over and above normal operations, as early as possible.

**Size-up**

Without truly identifying the problem, IT incident responders are basing decisions on anecdotal information, speculation and luck. The suggested process below is a way to think about Size-Up for any incident.

**Initial Actions**

1. Discovery of issue.
2. Evaluation of data from monitoring tools
3. Dispatch responders and/or escalation. Initial notifications per company policy
4. Define severity (SEV/Priority) level
5. Establish communications.
6. Establish command.
8. Define initial Incident Objectives (use the CAN format – see below).
9. Assign tasks by person of function within a timeframe.
10. Notify others as appropriate for the SEV level.
11. Reassess situation

An easy way to remember the elements of Size-up can be found in the format of a **CAN** report:

- **C**onditions – What is happening?
- **A**ctions – What is being done or needs to be done to solve the problem?
- **N**eeds – What resources are needed?

**CAN** reports are excellent briefing tools and can be used in a variety of situations.
Triage

The answers to the questions listed above will help you more accurately assign an appropriate severity (SEV) level, which will bring a pre-planned, defined incident response. In some cases, a situation may be deemed an event (non critical incident), not requiring the use of IMS. As the IC it is important to announce the SEV level clearly to everyone involved. This puts the problem in context so that all incident responders understand the urgency. If the severity of the problem changes, so must the SEV level, which should again be verbalized by the IC.

Figure 3 can be used as a quick guide to determine and communicate the severity of the situation to anyone working on the incident. An IC may say, “We are working a red box problem, let’s get another DBA on the line.” It’s certainly a shorthand guide to complex problems, but may be effective in helping anyone on the bridge quickly understand the severity of the situation.

![Figure 3: Potential impact of a given problem based on the frequency of occurrence and its severity.](image)

Events occurring in the green and yellow boxes are really not categorized as incidents and are typically handled by an individual or a small group of incident responders. They may happen with a certain frequency and have minimal impact to the system or customers. In many cases green and yellow box issues are tickets or cases rather than incidents. Solutions are oftentimes evident and mostly require the incident responders to implement a known solution rather than figure out a plan based on conditions. Green and yellow box problems are typically defined by SEV 4 and SEV 3 events, or other non-emergencies.

Events occurring in the red and black boxes are true incidents that benefit most from the use of the IMS. These types of incidents may be multi-faceted and/or have no clear-cut solution or may significantly impact services to customers. In short, these are situations that may likely require numerous different technology SMEs in the roles of incident responders and may go on for
several hours or longer. There may be lot of trial and error and trailblazing to figure out an appropriate solution. The problem may be unique – no clear cause for which there is no clear solution. An IC might look at a problem and quickly assign it a color designator from Figure 3, which will then correspond to a specific SEV level. Red box problems typically represent SEV 1 & 2 and black box problems can be viewed as SEV 0.

**Act**

The IC must develop – or facilitate the development of – a sound incident response plan based on facts and probabilities.

A good plan includes the following components:

- A clear size-up, triage and understanding of the problem.
- A straightforward objective or set of objectives.
- Identification of the best and worst-case scenarios.
- Input and support of trustworthy and cooperative experts.
- A timeline.
- Continuous evaluation for progress and success.
- A back-up plan.

**Recover**

The final stages of many incidents are oftentimes ambiguous or poorly defined. It may not be clear that the solution is definitive and that a return to a normal state of operations (*Peacetime*) is uncertain. Many times, a piece of code may be written to provide a temporary fix – a way to place a bandage on the situation and get the system up and running but not really address the underlying problem. The long-term ramifications may not be understood and, in some cases, a fix now could result in planting a time bomb that will likely show up later. Chances are, the bandage fix is not memorialized and problems downstream could eventually become more complicated. The IC must determine if the end state of the incident results in a return to pre-incident conditions or some adaptive state. Either case might be acceptable, it is vital to the team to perform a comprehensive After Action Report (AAR) to determine the root cause(s) and reason(s) for the incident. It is also critical that the *Peacetime* organization know the terms of any adaptive changes that were made in *Wartime*. All environments, when faced with an incident – some disturbance in the operating universe – will respond with accepting the change, rejecting the change, or adapting in some way to the change. The IC will be responsible for the change,
and must ensure it is appropriate and healthy for the environment, not just looked at as a lucky near miss!

**Span of Control**

If the incident requires more than a few incident responders, the command structure will need to grow accordingly. This is one of the key characteristics of IMS: it is modular and can scale up or down according to the size and severity of the incident.

Smaller incidents may require a bare bones command structure as you see in Figure 5. This example shows the org chart for a small group assembled to solve a low severity (green or yellow box) incident, perhaps a database problem with no customer impact. There is still an IC, even though there are not a lot of people working the issue. Again, it’s an incident, even though it’s believed to be small, the system is in place in case the incident grows in size or severity. In that case, the basic structure could ultimately look like what is seen in Figure 6, in observance of another concept of the IMS called *span of control.*

Span of control, is the maximum number of people that one person can effectively supervise at a given time. This concept has been widely studied in many high-consequence situations. That is not to say that the recommended span of control must never be violated, but remember incidents are dynamic and can change. The IC role is initially filled by the first person on the bridge, but command can be transferred to any other person at any time. Incident command, just like any other function is fungible, meaning it can be moved from person to person to meet the needs of the incident. If a person more qualified comes on the bridge, command can be transferred to that person (more on this later). Figure 6 represents an example of what the IMS chart may look like for SEV 2 incident. The positions may differ from company to company but the concepts are the same.
You can see that there are number of incident responders working the problem. Imagine they are all on a conference bridge at the same time. Rather than the IC speaking directly with everyone, or everyone trying to compete for airtime, he or she might choose to organize the group into functions and appoint a leader. You can see that out of the 10 functions represented, the IC only directly interacts with the App Manager, DB Manager and Infrastructure. The scribe is a person charged with documenting the incident, and doesn’t technically report to the IC like the other functions. The IC might even consider moving the App Manager or DB Manager or Infrastructure to another conference bridge or some other form of communication method so as not to clutter up the main communications channel with deep technical talk by the Subject Matter Experts (SME).

If the incident continues to escalate, the chart can expand and add more functional groups (Figure 7), in this case Security and Disaster Recovery. As you can see, there would be a large number of responders on the bridge, but they are all organized in such a way that the IC maintains a reasonable span of control.

Figure 6: Small incident, handled by only a few responders. In incident response a reasonable span of control is 1 supervisor for every 5-7 responders.
Remember, smaller incidents require smaller management. Bigger incidents require more incident responders, thereby creating a greater need for larger management structures.

**Delegate when necessary, but an IC should not give away the ultimate decision-making authority.**

It should be said that the IC for the incident should remain the IC until relieved by a higher authority, or relinquish command to another IC for the next operational period. There is a process for this action, which is known as the transfer of command. When command is transferred to the next IC, the following actions will occur.

**Verbalized on the incident conference bridge:**

- A formal announcement on the bridge that command is being transferred.

- Provide Situational Status (SitStat). In this case, the same CAN report format is used as a briefing tool in this situation (different than the size-up phase), showing its usefulness as a template for constructing an information exchange.

**Offline, between current and incoming IC:**

- Identify command structure and assigned groups.
• Refine objectives and needed notifications.

• Refine timeline for mitigation.

**IMS Terms and Definitions**

**Alerting** – the process of sending the required communication to an available technical expert or other person tasked to respond to an incident. Alerting is the physical process of dispatching a person.

**Communications Officer (Comms)** – is the person responsible for all incident responder notifications and may also assist the IC with issuing executive briefings or stakeholder notifications. When the IC needs to reach an SME or executive, the Comms Officer should be tasked with making the notifications.

**Continuous Operations (ConOps)** – is the person monitoring the system and watching for issues outside the current incident. ConOps can assist with other command tasks as needed and as available.

**Dispatch** – the process of alerting available resources to respond to the designated communications channel. Being dispatched is not an informal request, it is a directive that should be considered an ‘order’. When an available technical expert is dispatched by whatever method the company uses, it is incumbent for that expert to respond to the incident ASAP.

**Escalation** – the act of dispatching additional or new technical problem solvers to an incident. Escalation is not about contacting another on call resource because the primary is not responding.

**Event** – a non-incident that does not meet the company’s criteria for an incident response. Events are non-critical and do not require the use of IMS. Events may become incidents.

**Incident** – a situation that meets the company’s criteria for an incident response and the use of IMS including the position of incident commander and all other experts identified in the incident response plan.

**Incident Commander (IC)** – is the leader of the incident responsible for focusing the group, developing incident objectives, providing direction and time management. The IC may or may not be the person that initially establishes the incident bridge, and may not be the most senior person in the *Pacetime* org chart. It is not necessary for the IC to be the deepest technical expert in the problem area. The IC must be an expert in the process and function of incident command. All significant actions are to go through the IC. This person shall remain the IC for the duration of the event or until command is transferred to another person or IC. Formal transfer of command information should be exchanged prior to the new IC taking charge.
**Liaison Officer (LNO)** – the LNO position is activated by the incident commander in order to facilitate communications between the IC or the command communications channel and other communications channels or groups that may be operating on the incident. An example may include a LNO moving between a command channel and executive channel (typically a conference bridge), in order to provide and receive updates or any other information important to the problem solving effort.

**Notification** – the act of making identified persons within an organization aware of incident. Being notified is not being dispatched, and the information provided is intended to keep persons, business units, etc. up to speed on the status of an incident.

**Operations (OPS)** – When the span of control greatly exceeds 5-7 direct reports to the IC an operations lead may be appointed. The Operations lead handles the tactical objectives, which are driven by the Incident Commander’s strategic goals. When OPS is established many of the direct reports that were going to the IC would now report to OPS. The OPS officer directs most of the operations involved in the incident. When the span of control exceeds 5-7 direct reports for OPS then groups should be established which then report to OPS.

**Operational Period** – any period of time established by the incident commander or unified command whereby active incident operations are in progress.

**Plans Group (Plans)** – is a group that is established by the IC on large scale or complex incidents and does not need to reside within the Technical Operations Team. The Plans group is comprised of SMEs who are trying to think several steps ahead of the incident planning. While the IC and the personnel are involved in actively trying to resolve the problem, Plans listens to the activity and war-games alternative plans and contingencies. Plans does not actively participate in the Plan A problem solving effort. Their function is to war-game potential outcomes of the tactics employed (i.e., what could go wrong if they take action A? What should Plans B, C, and D be? What are the advantages/disadvantages to these plans?)

**Scribe** – the primary person assigned documentation responsibilities for the incident. The Scribe records key events, decisions, assigned tasks and other important information/events in real time as it occurs. The scribe keeps an incident timeline.

**Situational Status (SitStat)** – also known as the scribe and is the person who is recording all of the information related to the event. Has responsibility for keeping track of the Situational Status (SitStat), updating IRC or other forms of incident documentation.

**Subject Matter Experts (SME)** – are human resources supporting and working with the IC, even if during *Peacetime* operations the SME may be the supervisor of the IC. When operating in incident mode (*Wartime*) using IMS, the IC is in charge. The number of SMEs required will be based upon the conditions identified. The IC should attempt to identify the nature and assign
SMEs based on this assessment. The SME group will vary from company to company and may be a globally distributed workforce. In larger companies with complex environments, SME’s called to an incident bridge may be many time zones away and not personally acquainted with the IC or anyone else on the bridge.