Incident Command

Wall chart. The full guide, forms and job aids are at im.htora.dev. CC BY 4.0.

The Incident Commander's first 30 minutes

#	Item	Done when
1	Take command out loud: your name, the time, the incident name and where the command bridge is. Open your activity log (ICS 214).	The announcement is in the channel and the first log entry has a time.
2	If someone was in command before you, take a briefing from them, using the ICS 201 if one exists.	You can say what is affected and what has been done so far.
3	Open a command bridge and an out-of-band channel, and record both in the ICS 205. Treat email, chat and identity as visible to the attacker until scoping shows otherwise.	Every responder has joined the out-of-band channel.
4	Size up: what happened, what is affected, what is still happening and what is unknown.	Each of the four has a written answer, even if the answer is unknown.
5	Set up to three objectives, each with an outcome, a measure and a time. Examples are in Writing objectives.	The objectives are written where every responder can read them.
6	Name an Operations Lead, or an Operations Section Chief from Type 3, and hand over the technical work. Stay off the keyboard.	The Operations Lead has accepted and briefed the technical responders.
7	Decide the incident type, 5 to 1, with the type chooser, and fill the positions it calls for.	The type is logged and each seat it calls for has a name against it.
8	Confirm your authority limits, and who approves anything above them.	You have the name and number of the executive above you.
9	Tell counsel if personal data, regulators, law enforcement, extortion or insurance may be involved. The clocks are in notification deadlines.	Counsel has acknowledged, or the log says why they were not called.
10	Set the times of the first briefing and the first executive update, using the update schedule for the severity.	Both times are announced and in the log.
11	Write the incident briefing (ICS 201) before the first briefing.	The ICS 201 is filed where the next Incident Commander will find it.
12	Check hours: who has been awake since when, and who relieves them. Record hazards and rest rules in the ICS 208.	Every responder has a relief time.

Severity and type

PIVTR-D risk level	Severity	First report	Full report	Usual starting type
Low	SEV 4	Within 2 days	Within 5 business days	5
Medium	SEV 3	Within 4 hours	Within 72 hours	5 or 4
High	SEV 2	Within 2 hours	Within 48 hours	4 or 3
Critical	SEV 1	Within 1 hour	Within 24 hours	3, 2 or 1

Which seats to fill

Seat	Fill it	Earliest type
Incident Commander	Every incident. At Type 5 it is often the analyst who found it. From Type 2, add a Deputy Incident Commander, or a second Incident Commander for alternate periods.	5
Deputy Incident Commander	When the Incident Commander needs relief across operational periods or has command work to hand off. Must be able to take over command at any time.	2
Operations Section Chief	Every incident above Type 5. At Type 4 the seat is the Operations Lead, who becomes the Operations Section Chief at Type 3.	4
Division/Group Supervisor	Every group or division Operations sets up. Each leads three to seven people.	4
Public Information Officer	As soon as anyone outside the response team has to be told.	4, as Communications Lead
Planning Section Chief	When the incident runs past one shift.	3
Situation, Resources and Documentation Unit Leaders	When the Planning Section Chief can no longer do the unit's work alone. Documentation from the start when litigation, a regulator or an insurance claim is likely.	3
Liaison Officer	When outside parties are engaged.	3
Legal advisor	When personal data, regulators, law enforcement, extortion or insurance may be involved.	Any, when a trigger applies
Safety Officer	When the incident runs past one operational period, or when containment could touch a physical process.	3
Logistics Section Chief	When responders need access, tools or facilities the response team cannot arrange for itself.	2
Finance/Admin Section Chief	When outside costs, contracts or insurance claims begin.	2
Intelligence/Investigations	When the investigation is the main effort, law enforcement works alongside, or counsel directs the investigation for privilege.	2
Technical Specialist	When the response needs a skill nobody on the roster has, such as a forensic analyst, a negotiator or an OT engineer.	Any

The Planning P



The stem of the Planning P runs once, and its loop repeats every operational period.

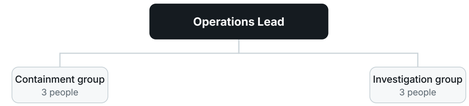
Meeting agendas

Meeting	Facilitator	Length	Agenda
Objectives meeting	Incident Commander	20 minutes	Review progress against the current objectives. Set up to three objectives for the next period, each with an outcome, a measure and a time. Set command emphasis and the period length. Decide what goes to executives.
Command and General Staff meeting	Planning Section Chief	30 minutes	Incident Commander presents the objectives and emphasis. Each section and Command Staff member raises constraints, needs and decisions. Incident Commander decides or takes items to the executive group.
Tactics meeting	Planning Section Chief	45 minutes	Operations proposes groups and tasks for each objective. Planning checks them against scope. Logistics confirms people, tools and access. Safety reviews risk to people and physical processes. The result is an ICS 215 worksheet, the Safety Officer's ICS 215A and the resource orders.
Planning meeting	Planning Section Chief	30 minutes	Situation briefing. Operations presents the plan. Each section confirms it can support it. Incident Commander approves the plan in principle and sets the IAP deadline.
Operations briefing	Planning Section Chief	20 to 30 minutes	Roll call and the period. Incident Commander gives command emphasis. Situation and objectives. Operations delivers each group's assignment. Logistics gives the communications plan. Safety message. Public Information and Liaison notes. Incident Commander closes and the period starts.

How the organization grows

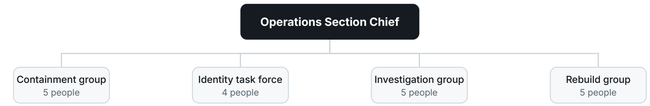
One incident, three sizes. Each chart shows the Operations Section only. Split any unit before it passes seven people, and add a layer before a supervisor has more than seven reporting.

About 8 responders, Type 4



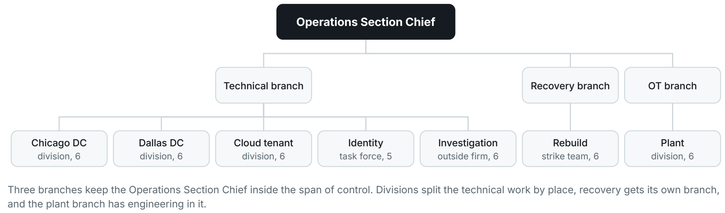
The Operations Lead supervises two groups directly. Command is the Incident Commander and a Communications Lead, who becomes the Public Information Officer as the incident grows.

About 25 responders, Type 3



Three groups and a task force report to the Operations Section Chief, inside the span of control.

About 60 responders, Type 2



Three branches keep the Operations Section Chief inside the span of control. Divisions split the technical work by place, recovery gets its own branch, and the plant branch has engineering in it.