Incident Command for IT Operations

GLOSSARY

The following terms and definitions are commonly used in public safety incident response and with our IT incident response teams. Not all companies adopt all terms, so some may not be familiar to you or your organization.

Communications Officer — This job function is 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. *See also: Liaison Officer*

Conditions - Actions - Needs Report (CAN Report) — Tactical report format, ideally less than 60 seconds or 80 words. Used to provide clarity and status updates quickly. Delivered in verbal or written format. Communications template for brief and concise sharing of information with those inside or external to the incident. Used by the IC to improve situational awareness of responders on a periodic basis. May be used by the LNO for outbound communications to key stakeholders. May be used by SMEs to provide task assignment updates to the IC and team.

Dispatch — The action of reaching out to a particular person representing a job function (database, network, storage, security, etc.), team, or group for the purpose of summoning a needed function to the incident. Dispatch is different from notification in that it is an order rather than a request.

Emergency — a term often used by impacted customers or stakeholders, implying a state of stress or emotional involvement. In contrast, a significant adverse event or situation that requires the focused response of trained individuals with resources to resolve should be considered an incident, not an emergency.

Event — A point-in-time fact relevant to the operations of your infrastructure or application, but which is not considered to be an incident. Events don't require implementation of the Incident Management System or an Incident Commander. Events may turn into incidents.

Incident — An occurrence, either human-caused or a natural phenomenon, that requires action or support by emergency services personnel to resolve, including prevention of injury or loss of life, or prevention of damage to property and/or natural resources. An unplanned interruption to an IT service or reduction in the quality of an IT service (ITIL).

Incident Action Plan (IAP) — A course of action or specific objectives, as determined by the IC, to resolve the incident.

Incident Command System (ICS) — Developed in the 1970s by the California Fire Service to improve management of wildfires. Later adopted for use in structure fire response. ICS is a scalable management structure for any type of incident.

Incident Commander (IC) — The person responsible for commanding an incident.

Incident Life Cycle — Issue → Monitoring → Notification/Dispatch → Response → Resolution → After Action Review

Incident Management System (IMS) — A framework to organize and lead the talent and resources required to respond to emergencies of all kinds. IMS establishes the framework of incident response and the norms of behavior for the incident responders. High severity/priority events place the incident responders under critical time pressure to resolve IT incidents when customer trust, adverse financial impacts, and the company's reputation are at stake. Using IMS increases your chances at having a good outcome and protecting the company's business.

Incident Response Team (IRT) — A general term for the group tasked with mitigating incidents within an organization. This will include SMEs, Communications Officers/LNOs, Scribes, and Incident Commanders.

Incident Bridge — The technology platform used by incident response teams to assemble and resolve an incident (typically an audio call, Teams, Zoom, Slack, etc.)

Introduction - Main Points - Summary Briefing (IMS Briefing) — Situation briefing format useful for outbound communications to key stakeholders. Delivered in verbal or written format. Ideally 1-2 minutes, or approximately 200 words. Primary characteristics: non-technical in nature, somewhat narrative, useful for business impact. The IMS briefing format allows for more detailed and robust incident communications than the CAN report.

Joint Information Center (JIC) — A group assembled by the IC or Unified Command to provide large scale externally facing information to a group of people.

(continued on back)

Liaison Officer (LNO) — Key command staff position tasked with communicating to individuals, teams or groups as determined by policy and procedure, or as directed by the IC. *See also: Communications Officer*

Mean Time To Assemble (MTTA) — Key business metric identifying the time it takes to dispatch and assemble a group of key responders.

Mean Time To Respond (MTTR) — Key business metric identifying the time gap between incident discovery and dispatching key responders.

Mean Time To Restore (MTTRe) — Key business metric identifying the period of time from MTTA to the formal declaration of the end of an incident.

Notification — A message (urgent or otherwise) sent to a person, usually related to an alert or incident. Notifications are intended to be informational, rather than a dispatch or command. Notifications are not a call to respond, although they may be used to inform people of events.

Operational Maturity (OM) — A numerical designation (from 1-5) that identifies the overall efficiency of the total incident response program for a company. This is based on the Blackrock 3 Operational Maturity Model.

Predictable - Repeatable - Optimized - Clear - Evaluated - Scalable - Sustainable (PROCESS) — An acronym that represents the seven key attributes of an effective incident response program. Each letter of PROCESS is an interdependent link in the incident response chain.

Root Cause Analysis (RCA) — The process, after an incident resolves, of determining the causes/reasons why the technology failed and the incident occurred. This analysis is crucial to improving future operations, and is performed alongside the After Action Review (AAR).

Scribe — The person who records all of the information and key events related to the incident. They are responsible for keeping track of the Situational Status (Sit Stat), and updating technical briefs or other forms of incident documentation.

Senior Corporate Leadership (C-Suite) — Senior leadership group. This group may be called upon during an incident for high level business and policy level decisions regarding resolution and business impact.

Service Level Agreement (SLA) — A contract or agreement between parties that directly spells out specific terms of performance and in some cases, penalties that may arise from failing to perform as agreed.

Severity Assessment (SEV) — A triage, performed at the beginning of any bridge call by the IC, that determines the level of severity of an incident. SEV assessments determine what kind of technical help (SMEs) are needed to resolve the incident. SEV levels can vary or be changed during an incident based on conditions and progress.

Situational Awareness (SA) — The action, at the beginning of any bridge call by the IC, of gaining all information available to truly understand the nature of the incident. SA involves focus and observation, and provides the basis for the conditions part of the CAN report.

Span of Control — A description of the supervisor to responder ratio during a response. Per ICS standards, any person in a supervisory role should only directly manage 5-7 direct reports to avoid being overwhelmed.

Subject Matter Expert (SME) — A person or group with specific knowledge and expertise on an aspect of the technology environment of any part of the business.

Tactical Documentation — The act of capturing key events during an incident. Typically done by the Scribe but also applies to individual responders who need to keep track of key events and incident progress.

Tone - Interaction - Management - Engagement (TIME) — The four critical elements that an Incident Commander must attend to during an incident. Setting the right professional tone of the response; ensuring that the team is interacting in a positive way; managing the administrative aspects of the incident such as span of control and tasks assigned to responders; and ensuring that the correct type and number of responders are fully engaged in the resolution effort.

Training - Accountability - Leadership - Empowerment - Notification (TALENT) — An acronym that describes a non-technical evaluation of incident response soft skills. Can be helpful for evaluating performance after an incident, as well as providing solutions and areas of improvement for those individuals being evaluated.

Triage — A mode of sorting and assigning priority in an incident. Similar to medical professionals, during an incident IT professionals become first responders.

Unified Command (UC) — A group of individuals assembled to aid an IC with business and policy decisions that could be required during a high severity incident. Typically comprised of the company's senior leadership.

Universal Coordinated Time (UTC) — A globally used standard for time.