(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 February 2016 (04.02.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/018637 A1

(51) International Patent Classification:
G06Q 10/00 (2012.01)

(21) International Application Number:
PCT/US2015/040704

(22) International Filing Date:
16 July 2015 (16.07.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/029,714 28 July 2014 (28.07.2014) US

(71) Applicant: **JPMORGAN CHASE BANK, N.A.** [US/US]; 270 Park Avenue, New York, NY 10017 (US).

(72) Inventors: **HAUTALA, Eric, John**; 2 Satucket Rd., Rockland, MA 02370 (US). **TOHLEN, Mary, Jane**; 10066 W Hwy 32, Salem, MO 65560 (US). **FUCITO, Robert, Anthony**; 15 Highland Drive, Jackson, NJ 08527 (US).

(74) Agent: **LI, Ce**; Goodwin Procter, LLP, 901 New York Avenue, NW, Washington, DC 20001 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: SYSTEM AND METHOD FOR CRISIS AND BUSINESS RESILIENCY MANAGEMENT

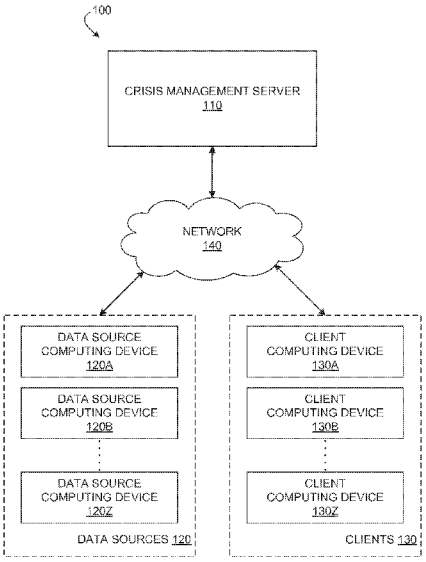


FIG. 1

(57) Abstract: Methods and systems for providing a crisis management platform are described. A method includes receiving a first notification of an event, such as a crisis event. A second notification of the event is transmitted to user equipment devices of a plurality of individuals. A user selection of a crisis-related option from a plurality of crisis-related options is received after transmitting the second notification is transmitted, and an action is taken in response to receiving the user selection of the crisis-related option. An electronic document is designed and distributed as a portable tool with easily accessible information for a crisis team to use as a straightforward reference to manage the decisioning and workflow coordination related to crisis management. Interactive user interfaces with hyperlinks to various electronic resources and tools may be provided to automatically and methodologically inform various users of their roles and guide them through a crisis response procedure.

WO 2016/018637 A1

SYSTEM AND METHOD FOR CRISIS AND BUSINESS RESILIENCY MANAGEMENT

CROSS-REFERENCE TO RELATED APPLICATION(S)

[0001] The present application claims priority to, and the benefits of, U.S. Provisional Application No. 62/029,714 of the same title, filed on July 28, 2014, which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] Embodiments of the invention relate generally to workflow management and, more specifically, to providing an interactive system and method for crisis and business resilience management.

BACKGROUND

[0003] Crisis management is a process in which an organization (such as a corporation, a government entity, etc.) attempts to mitigate the effects of a threatening event before, during, or after the event has occurred. Crisis management differs from risk management in the sense that, while risk management is focused on finding ways to avoid the event, crisis management is focused on the effects of the event and managing the potential or actual chaos and disorder that have resulted or are likely to result from the event.

[0004] Crisis management in a corporate setting may involve events that threaten to harm the corporate infrastructure as well as stakeholders and clients. Examples of crises faced by corporations can be diverse, including, for example, financial events (e.g., economic downturns), legal issues (e.g., lawsuits, criminal allegations, etc.), as well as natural phenomena (e.g., infrastructure disabling storms or earthquakes). Accordingly,

corporations have developed written policies for identifying, assessing, understanding, and coping with crises from the moment a crisis first occurs to the point that the recovery procedures start. In general, however, these approaches are often not streamlined, not universally applicable to all types of crises, and are often employed inconsistently from crisis to crisis as well as internally from corporate site to corporate site.

[0005] Emergency alert or mass notification systems were also implemented to broadcast warnings or notifications about crisis situations. However, such systems are limited to one-way communications and typically rely on human operators to prepare the content of the warnings or notifications.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] The present invention is illustrated by way of example, and not by way of limitation, and will become apparent upon consideration of the following detailed description, taken in conjunction with the accompanying drawings, in which like reference characters refer to like parts throughout, and in which:

[0007] **FIG. 1** is a block diagram illustrating an exemplary computer network in which embodiments of the present invention may operate;

[0008] **FIG. 2** is a block diagram illustrating an exemplary crisis management system in accordance with an embodiment of the invention;

[0009] **FIG. 3** is a flow diagram illustrating a method for providing crisis management services in accordance with an embodiment of the invention;

[0010] **FIG. 4** is a flow diagram illustrating a method for providing a crisis management interface in accordance with an embodiment of the invention;

[0011] **FIG. 5** illustrates a diagrammatic representation of a machine in the exemplary form of a computer system configured to perform one or more of the operations described herein; and

[0012] **FIGs. 6-18** show exemplary user interface screens displaying features of an electronic tool for crisis management in accordance with embodiments of the invention.

SUMMARY OF THE INVENTION

[0013] Disclosed herein are systems and methods for providing a crisis management platform that allow for efficient and effective crisis management using live tools, templates, and guides for a consistent, globally-unified approach to crisis responses within an organization. According to embodiments of the present invention, an electronic document may be designed and distributed as an essential portable tool with easily accessible information for the a crisis team to use as a straightforward reference to manage the decisioning and workflow coordination related to crisis management. For example, interactive user interfaces with hyperlinks to various electronic resources and tools may be provided to automatically and methodologically inform various users of their roles and guide them through a crisis response procedure.

[0014] According to one particular embodiment of the present invention, a number of interactive user interfaces may be provided to instruct and coordinate participants in a crisis management procedure, such as displaying a predefined framework or timeline for crisis responses, predefined roles and responsibilities of participants in the crisis management procedure, and step-by-step instructions for the participants to carry out the crisis management procedure according to their respective roles and responsibilities.

[0015] According to another particular embodiment of the present invention, a user interface may be provided to display an interactive event timeline comprising prompts and options for user actions at a predefined pace. The event timeline or related crisis response protocols and instructions may be modified or updated during or after a crisis event.

[0016] According to yet another embodiment, communications may be automatically initiated to provide alerts, notifications, and/or instructions to some or all of the participants in the crisis management procedure upon occurrence of a crisis event. For example, a method may include receiving a first notification of an event, such as a crisis event. A second notification of the event is transmitted to user equipment devices of a plurality of individuals (e.g., personnel who may have been designated as "first-responders" to the crisis). A user selection of a crisis-related option from a plurality of crisis-related options is received after transmitting the second notification. For example, the crisis-related options may include, but are not limited to, an "activate" option which may serve as an activation command for triggering a cascade of relevant protocols to handle the event, a "hold and monitor" option to allow time to assess the situation, and a "stand down" option when no further action is to be taken.

[0017] The systems and methods described herein may serve as a central point of control for the organization and provide facilitation and coordination during crisis situations. Moreover, the disclosed embodiments can be leveraged across all lines of business for their adaptation, saving time, reducing risk, and streamlining communication.

[0018] In the following description, numerous details are set forth. It will be apparent, however, to one skilled in the art, that the present invention may be practiced without these specific details. In some instances, well-known structures and devices are

shown in block diagram form, rather than in detail, in order to avoid obscuring the present invention.

DETAILED DESCRIPTION

[0019] Some portions of the detailed descriptions may be presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations correspond to the terminology used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

[0020] It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise, as apparent from the description that follows, it is appreciated that throughout the description, discussions utilizing terms such as "receiving", "detecting", "monitoring", "generating", "calculating", "transmitting", “enrolling”, “identifying”, "measuring", "recommending", "designating", "increasing", "issuing", "processing", or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers

and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

[0021] The present invention also relate to an apparatus for performing the operations herein. This apparatus may be specially constructed for the required purposes or it may include a general purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer readable storage medium, such as, but not limited to, any type of disk including floppy disks, optical disks, CD-ROMs and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, flash memory devices including universal serial bus (USB) storage devices (e.g., USB key devices) or any type of media suitable for storing electronic instructions, each of which may be coupled to a computer system bus.

[0022] The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general purpose systems may be used with programs in accordance with the teachings herein or it may prove convenient to construct more specialized apparatus to perform the relevant method steps. The structure for a variety of these systems will be apparent from the description that follows. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein.

[0023] The present invention may be provided as a computer program product, or software, that may include a machine-readable medium having stored thereon instructions,

which may be used to program a computer system (or other electronic devices) to perform a process according to the present invention. A machine-readable medium includes any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer). For example, a machine-readable (e.g., computer-readable) medium includes a machine (e.g., a computer) readable storage medium (e.g., read only memory ("ROM"), random access memory ("RAM"), magnetic disk storage media, optical storage media, flash memory devices, etc.), a machine (e.g., computer) readable transmission medium (non-propagating electrical, optical, or acoustical signals), etc.

[0024] **FIG. 1** is a block diagram illustrating an exemplary computer network **100** in which embodiments of the present invention may operate. Referring to **FIG. 1**, computer network **100** may include a crisis management server **110**, a plurality of data source computing devices **120A-120Z**, which are associated with and collectively referred to herein as data sources **120**. Computer network **100** may also include a plurality of client computing devices **130A-130Z**, which are associated with and may be collectively referred to herein as clients **130**. Crisis management server **110** may be communicatively coupled directly or via a communications network **140**. Although crisis management server **110** is depicted as a single server, crisis management server **110** may be one or more computing devices (such as a rackmount server, a router computer, a server computer, a personal computer, a mainframe computer, a laptop computer, a tablet computer, a desktop computer, etc.), and include one or more data stores (e.g., hard disks, memories, databases), networks, software components, and/or hardware components. Data source computing devices **120A-120Z** associated with data sources **120** may be communicatively coupled to communications network **140** via any one of a plurality of communication

channels (e.g., e-mail, SMS service, automated voice message, etc.). Similarly, client computing devices **130A-130Z** associated with clients **130** may also be communicatively coupled to communications network **140** via any one of the plurality of communication channels. Communications network **140** may be a private network (e.g., a local area network (LAN), wide area network (WAN), intranet, etc.), a public network (e.g., the Internet), a cellular network or any combination thereof.

[0025] **FIG. 2** is a block diagram illustrating an exemplary crisis management system **200** in accordance with an embodiment of the invention. Crisis management system **200** may be the same or similar to, and have the same functionality and connectivity as, computer network **100** described with respect to **FIG. 1**. Crisis management system **200** may include a computer-implemented crisis management platform **210**, which may be implemented by a server (e.g., crisis management server **110**), one or more client computing devices **260** (which may correspond to one or more of client computing devices **130A-130Z**), and one or more data source computing devices **270** (which may correspond to one or more of data source computing devices **120A-120Z**). In some implementations, some or all of the functionality of crisis management platform **210** is implemented on one or more of client computing device **260**, data source computing device **270**, or another device. Each of client computing device **260** and data source computing device **270** may be communicatively coupled to each other and to crisis management platform **210** via a communications network (e.g., communications network **140**).

[0026] Crisis management platform **210** may include one or more modules configured to provide crisis management services. Crisis management platform **210**

includes crisis management interface **215**, crisis management module **220**, and data store **250**. The crisis management module **220** includes a task assignment component **225**, a messaging component **230**, a resource management component **235**, and a conferencing component **240**. More or less modules and components may be included in crisis management platform **210** without loss of generality. For example, two or more of the modules may be combined into a single module, or one of the modules may be divided into two or more modules. In one implementation, one or more of the modules may reside on different computing devices (e.g., different server computers, on a single client device, distributed among multiple client devices, etc.).

[0027] In one embodiment, crisis management interface **215** may be communicatively coupled to client computing device **260**. Client computing device **260** may be referred to as a "user device". An individual user may be associated with (e.g., own and/or operate) client computing device **260**, and may also be associated with additional client computing devices (e.g., one or more of client computing devices **130A-130Z**). Client computing device **260** may be owned and utilized by different users at different locations. Client computing device **260** includes a user interface (UI) **265**, which allows the user to send and receive information to crisis management platform **210** via crisis management interface **215**. For example, UI **265** may be a web browser interface that can access, retrieve, present, and/or navigate content (e.g., web pages such as Hyper Text Markup Language (HTML) pages) provided by crisis management platform **210**. In one embodiment, UI **265** may be a standalone application (e.g., a mobile app), which may have been provided to the user by crisis management interface **215**, and allows the user to send and receive information to crisis management interface **215**. In one embodiment, UI

265 may be implemented as an interactive slide show presentation document, as illustrated in FIGs. 6-18.

[0028] In one embodiment, crisis management platform **210** may include crisis-related resources, which may be stored and maintained in data store **250**. In one embodiment, the data store **250** may be a memory (e.g., random access memory), a cache, a drive (e.g., a hard drive), a flash drive, a database system, or another type of component or device capable of storing data. The data store **250** may also include multiple storage components (e.g., multiple drives or multiple databases) that may also span multiple computing devices (e.g., multiple server computers), and may be cloud-based. In some embodiments, the data store **250** may be separate from crisis management platform **210**, and may be, for example, distributed among and accessible to client computing device **260**, data source computing device **270**, and other devices.

[0029] The crisis-related resources may include, for example, an identity database (for keeping track relevant personnel), resource data (such as external resources to aid in crisis management), a document database (for keeping track of crisis-related documents such as reports, meeting minutes, etc.), messaging templates (for transmitting messages and indications to relevant personnel), and protocol data (which may summarize actions to be taken in response to notifications).

[0030] In one embodiment, task assignment component **225** may assign crisis-specific tasks to relevant personnel (e.g., personnel corresponding to identities stored in the identity database). The personnel may be assigned specific tasks automatically by the crisis management module **220**, by a user of the client computing device **260**, or both. In

one embodiment, messages and event indications are transmitted to personnel based on an assigned task.

[0031] In one embodiment, messaging component **230** allows for the user to generate messages (e.g., from pre-defined message templates) and have these message transmitted to relevant personnel.

[0032] In one embodiment, resource management component **235** may provide the user with several crisis-related resources. Illustrative crisis-related resources are shown in FIGs. 6-18.

[0033] In one embodiment, conferencing component **240** allows for the audio/video conferencing between client computing devices (e.g., one or more of client computing devices **130A-130Z**). The user of client computing device **260** may, for example, initiate a conference with other users/personnel at any time by transmitting a conference request to the crisis management interface **215**, in which the request includes a list of identities of personnel. In some embodiments, the messaging component **230** automatically determines identities of personnel with whom the user is to have a conference with. For example, the messaging component **230**, in response to the user selecting a crisis-related option, may identify within stored protocol data that, at a particular time, particular personnel are to be contacted. The conference is then automatically initiated and the relevant personnel are identified from the identity database and invited to or scheduled to participate in the conference.

[0034] As illustrated in **FIGS. 3** and **4**, each of methods **300** and **400**, respectively, may be performed by processing logic that may include hardware (e.g., circuitry, dedicated

logic, programmable logic, microcode, etc.), software (such as instructions run on a processing device), or a combination thereof. In one embodiment, methods **300** and 4**00** may be performed by one or more processing components associated, respectively, with crisis management interface **215** and crisis management module **220** (which includes task assignment component **225**, messaging component **230**, resource management component **235**, and conferencing component **240**) of crisis management platform **210**.

[0035] **FIG. 3** is a flow diagram illustrating a method **300** for providing crisis management services in accordance with an embodiment of the invention. Method **300** begins at block **310**, in which a notification of an event is received. The event may correspond to a crisis event. In one embodiment, the notification of the event may be received by a crisis management server (e.g., crisis management server **110** implementing crisis management platform **210**). In one embodiment, the notification of the event may have been received from one a client computing device (e.g., client computing device **260**), a data source computing device (e.g., data source computing device **270**), or from another source.

[0036] At block **320**, a first subset of identities is identified from a plurality of identities. For example, the plurality of identities may be stored in an identity database (e.g., in data store **250**). Each of the plurality of identities may correspond to an individual. The subset of identities may identify particular individuals that have crisis management roles assigned. In one embodiment, the first subset of identities may be identified based on receiving a designation of the identities from a user of the client computing device (e.g., client computing device **260**). For example, the user of the client computing device may designate roles for one or more individuals to define the subset of

identities. In one embodiment, the subset of identities may have been previously identified. For example, specific individuals may have previously had their roles assigned (e.g., assigned roles stored in data store **250**), in which the assigned roles associated with identifies of the individuals defines the subset of identities.

[0037] At block **330**, a second notification of the event is transmitted to user equipment devices of each of a first plurality of individuals corresponding to the first subset of identities (e.g., using messaging component **230**). In one embodiment, the user may specify a messaging template. The second notification may be automatically generated from the messaging template (e.g., using messaging component **230**).

[0038] At block **340**, a user selection of a crisis-related option from a plurality of crisis-related options is received after transmitting the second notification. In one embodiment, the user may use conferencing services to discuss the event with one or more individuals (e.g., using conferencing component **240**) prior to the selection of the crisis-related option.

[0039] At block **350**, an action is performed in response to the user selection of the crisis-related option. The action is described in detail with respect to **FIG. 4**.

[0040] **FIG. 4** is a flow diagram illustrating a method **400** for providing a crisis management interface in accordance with an embodiment of the invention. Method **400** begins at block **410**, in which a user interface is provided, which includes a plurality of crisis-related options. In one implementation, notification of a crisis may have already been received (e.g., in a similar manner as described with respect to block **310** of **FIG. 3**).

[0041] At block **420**, a user selection of one of the plurality of crisis-related options is received. Block **420** may be performed in a manner similar to that described with respect to block **340** of **FIG. 3**.

[0042] At block **430**, a determination is made as to which option was selected (e.g., using crisis management interface **215**).

[0043] If it is determined, at block **430**, that an "activate" option (which indicates that a crisis protocol is to take effect) was selected, method **400** proceeds to block **440**, in which a notification of the crisis is transmitted to one or more designated individuals (e.g., which may correspond to a subset of identifiers from a plurality of identifiers). Method **400** is then ended, and may be repeated continuously.

[0044] If it is determined, at block **430**, that a "stand down" option was selected, method **400** proceeds to block **450**, in which a notification is transmitted to one or more designated individuals indicating that no action is to be taken. Method **400** is then ended, and may be repeated continuously.

[0045] If it is determined, at block **430**, that a "hold" option was selected, method **400** proceeds to block **460**, in which user input is awaited (e.g., until a new crisis-related option is selected). Method **400** then proceeds to block **420** in which a user selection of one of the crisis-related options is received.

[0046] It should be noted that the sequence of operations described in conjunction with methods **300** and **400** may be different from that illustrated, respectively, in corresponding **FIGS. 3** and **4**, while some operations may be omitted without departing from the nature of the embodiments described herein. It should be appreciated by one of ordinary skill in the art that the blocks illustrated in methods **300** and **400** are provided for

purposes of illustrating embodiments of the invention and are in no way intended to be limiting in scope.

[0047] In some embodiments, user input may be received by a client computing device (e.g., client computing device **260** implementing UI **265**), which may be transmitted to a crisis management server (e.g., crisis management platform **210** implemented on crisis management server **110**). In some embodiments, the client computing device implements the functionality of the crisis management server (e.g., some or all of crisis management platform **210** is implemented on client computing device **260**). A user interface (e.g, UI **265**) may be implemented on the client computing device, which receives the user inputs.

[0048] Exemplary user interfaces are shown in FIGs. 6-18 which illustrate some of the functionality described herein from the perspective of the user interface of the client computing device.

[0049] **FIG. 6** shows an exemplary "Crisis Command Structure (CCS)" screen which outlines a predefined framework for a crisis management procedure according to one embodiment of the present invention.

[0050] In this interactive display, a number of potential participants (e.g., individuals, teams, or entities) are shown in rectangular boxes, such as a Global Resiliency and Crisis Management (GRCM) team, a Global Security (GS) team, a Corporate Communications ("Corp Comms") team, Organization Senior Management ("Org Sr. Mgmt"), Regional Crisis Management Team (RCMT), Site Incident Management Team (SIMT), Business Unit Crisis Teams, Production Assurance Center (PAC) teams, and a Crisis Team. The Crisis Team may further include various members such as Oversight Lead, Information Manager, Crisis Manager, Resource Manager, and so on. The business

representatives may include Business Resiliency Coordinators (BRCs), alternative BRCs, and a Business Manager. The Support Representatives, which are determined for each incident, may include personnel from Human Resources, Communications, Real Estate, Technology, Risk Management / OCM (Operations Control Management), and Legal / Compliance teams. Each of these teams and team members may have predefined roles and responsibilities in the crisis management procedure.

[0051] By clicking, or hovering a pointer over, a rectangular box displayed in **FIG. 6**, the role and responsibilities of a corresponding participant in the crisis management procedure may be displayed. **FIG. 14** shows an exemplary screen displaying a set of predefined roles and responsibilities of the Crisis Management Team (shown as "Crisis Team" in **FIG. 6**) according to one embodiment of the present invention. This "Roles and Responsibilities Definitions" screen in **FIG. 14** may be reached via hyperlinking from the **FIG. 6** screen upon clicking the "Crisis Team" name or box.

[0052] **FIG. 6** also shows bi-directional arrows connecting the Crisis Team with the various potential participants in the crisis management procedure. Each of these arrows may be clickable to reveal a corresponding set of engagement and communication protocols and/or communication models and templates for interactions between the connected teams or entities during a crisis response.

[0053] According to some embodiments of the present invention, the exemplary user interface shown in **FIG. 6** may be automatically activated or initiated upon receipt of a notification about a crisis event. For example, triggered by an event alert (e.g., a sudden crash of a relevant stock or other financial instrument, or filing of a legal action), a

computer-based crisis management tool may automatically launch this interactive screen as the starting point of the predefined crisis management procedure.

[0054] According to one embodiment, a click in the **FIG. 6** screen on the "Timeline" arrow may cause an interactive event timeline to be displayed. **FIG. 7** shows one such predefined event timeline which sets forth a number of prompts and options for user actions at a predefined pace. Starting from occurrence of a crisis event, an immediate first step is "Initial Assessment" of the crisis event where a core team is made aware of potential crisis and the oversight team member(s) may be notified. A "Click Here" button (next to "Initial Assessment") may take the user to another user interface (e.g., **FIG. 8**) which shows more detailed instructions for the initial assessment stage as well as buttons (in the lower left corner) for navigation back to the CCS framework screen of **FIG. 6** or the event timeline screen of **FIG. 7**.

[0055] As shown in **FIG. 7**, about fifteen minutes after occurrence of the crisis event, a triage determination on next steps is made. Similarly, a second "Click Here" button (next to "Triage") may take the user to another user interface (e.g., **FIGs. 9-10**) which shows more detailed instructions for the triage stage and related decision criteria ("Activation Triggers"). Within an hour of the crisis event, the triage decision may cause the crisis management team to either activate a Crisis Command Center to actively deal with the crisis event or hold and monitor the crisis situation (or simply stand down with respect to the crisis event). Detailed instructions or guidance for each of these subsequent steps may be shown on the "Event Timeline" screen in **FIG. 7** or other hyperlinked pages such as those illustrated in **FIGs. 11-13**.

[0056] **FIG. 6** further shows a "Tool Box" icon which could be clicked by a user to access electronic resources such as a suite of crisis response tools shown in **FIG. 15**. These tools may be categorized according to their functions or purposes, such as Assessment, Initiation, Meetings, Communication, and References, which represent electronic resources internal to the computer system or electronic document displaying the Tool Box screen of **FIG. 15**. According to a preferred embodiment, not all the crisis response tools are available to all participants; instead, the tools are made accessible selectively to the various teams and team members based on their predefined or assigned roles and responsibilities in the crisis management procedure. It should be noted the small rectangular buttons in **FIGs. 9** and **11-13** which are marked "C-1," "C-2" and so on represent hyperlinks to crisis response tools such as meeting and communication model templates.

[0057] **FIG. 16** shows the exemplary user interface for one of those crisis response tools — External Communication Protocol — according to an embodiment of the present invention. A step-by-step process flow is specified for the drafting, review, approval, and distribution of a communication in connection with a crisis event. By requiring the Crisis Management Team as well as various other teams to follow this procedure, the organization may issue consistent messages to the target audience in a coordinated fashion.

[0058] **FIG. 17** shows the exemplary user interface for another of those crisis response tools — Communication Model — according to an embodiment of the present invention. Apart from hyperlinks to the External Communication Protocol towards the top of the screen, a number of communication models, including their respective purpose, tool or mailbox, template, distribution lists (i.e., target audience), and required approval, are

listed for the Triage and Activate stages of the exemplary crisis management procedure. The various communication model templates may be hyperlinked via rectangular clickable buttons.

[0059] **FIG. 18** shows yet another exemplary crisis response tool — Crisis Escalation Protocol — according to an embodiment of the present invention. Based on the scale of impact by a crisis event, the Crisis Escalation Protocol specifies different levels of event classification and escalation criteria and corresponding communication processes.

[0060] According to one embodiment of the present invention, some or all of the above-described user interfaces or interactive displays are preferably configured for rendering on each of a number of user computing devices including desktop computers, laptop computers, tablet computers, and mobile computing devices including smart phones. The electronic document or tool for crisis management may be configured as a mobile and/or desktop application compatible with a variety of computing platforms.

[0061] **FIG. 5** illustrates a diagrammatic representation of a machine in the exemplary form of a computer system **600** within which a set of instructions, for causing the machine to perform any one or more of the methodologies discussed herein, may be executed. In alternative embodiments, the machine may be connected (e.g., networked) to other machines in a local area network (LAN), an intranet, an extranet, or the Internet. The machine may operate in the capacity of a server or a client machine in a client-server network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The machine may be a personal computer (PC), a tablet PC, a set-top box (STB), a personal digital assistant (PDA), a cellular telephone, a web appliance, a server, a network router, switch or bridge, or any machine capable of executing a set of instructions

(sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

[0062] The exemplary computer system **600** may include a processor **602**, a main memory **604** (e.g., read-only memory (ROM), flash memory, dynamic random access memory (DRAM) (such as synchronous DRAM (SDRAM) or Rambus DRAM (RDRAM), etc.), a static memory **606** (e.g., flash memory, static random access memory (SRAM), etc.), and a data storage device **618**, which communicate with each other via a bus **630**.

[0063] Processor **602** represents one or more general-purpose processing devices such as a microprocessor, central processing unit, or the like. More particularly, the processing device may be complex instruction set computing (CISC) microprocessor, reduced instruction set computer (RISC) microprocessor, very long instruction word (VLIW) microprocessor, or processor implementing other instruction sets, or processors implementing a combination of instruction sets. Processor **602** may also be one or more special-purpose processing devices such as an application specific integrated circuit (ASIC), a field programmable gate array (FPGA), a digital signal processor (DSP), network processor, or the like. Processor **602** is configured to execute processing logic **426** for performing the operations and steps discussed herein.

[0064] Computer system **600** may further include a network interface device **608**. Computer system **600** also may include a video display unit **610** (e.g., a liquid crystal display (LCD) or a cathode ray tube (CRT)), an alphanumeric input device **612** (e.g., a

keyboard), a cursor control device **614** (e.g., a mouse), and a signal generation device **616** (e.g., a speaker).

[0065] Data storage device **618** may include a machine-readable storage medium **628** (or more specifically a computer-readable storage medium) having one or more sets of instructions (e.g., software **622**) embodying any one or more of the methodologies of functions described herein. For example, software **622** may store instructions to implement a crisis management platform. Software **622** may also reside, completely or at least partially, within main memory **604** and/or within processor **602** during execution thereof by computer system **600**; main memory **604** and processor **602** also constituting machine-readable storage media. Software **622** may further be transmitted or received over a network **620** via network interface device **608**.

[0066] Machine-readable storage medium **628** may also be used to store instructions to implement a crisis management platform. While machine-readable storage medium **628** is shown in an exemplary embodiment to be a single medium, the term "machine-readable storage medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The term "machine-readable storage medium" shall also be taken to include any medium that is capable of storing or encoding a set of instruction for execution by the machine and that causes the machine to perform any one or more of the methodologies of the present invention. The term "machine-readable storage medium" shall also be taken to include, but not be limited to, transitory computer-readable storage media, including, but not limited to, propagating electrical or electromagnetic signals. The term "machine-readable storage medium" shall

also be taken to include non-transitory computer-readable storage media including, but not limited to, volatile and non-volatile computer memory or storage devices such as a hard disk, solid-state memory, optical media, magnetic media, floppy disk, USB drive, DVD, CD, media cards, register memory, processor caches, random access memory (RAM), etc.

[0067] Whereas many alterations and modifications of the present invention will no doubt become apparent to a person of ordinary skill in the art after having read the foregoing description, it is to be understood that any particular embodiment described and shown by way of illustration is in no way intended to be considered limiting. Therefore, references to details of various embodiments are not intended to limit the scope of the claims, which in themselves recite those features regarded as the invention.

What is claimed is:

1. A computer-implemented method for crisis management, the method comprising:

creating, by at least one computer processor, an electronic document containing:

(a) at least one first interactive display of a predefined framework or timeline for a crisis management procedure,

(b) at least one second interactive display of predefined roles and responsibilities of participants in said crisis management procedure, and

(c) at least one third interactive display of step-by-step instructions for said participants to carry out said crisis management procedure according to their respective roles and responsibilities;

incorporating, in said at least one first, second, and third interactive displays, one or more hyperlinks to at least one other interactive display or electronic resource internal or external to said electronic document, said at least one electronic resource comprising one or more communication protocols and model templates for emergency responses as part of said crisis management procedure;

configuring said electronic document to be displayable on each of a plurality of computing devices including desktop computers, laptop computers, tablet computers, and mobile computing devices; and

distributing said electronic document to a plurality of potential participants in said crisis management procedure.

2. The computer-implemented method according to claim 1, wherein said at least one electronic resource further comprises a suite of crisis response tools accessible via said

electronic document by said participants according to their respective roles and responsibilities.

3. The computer-implemented method according to claim 1, wherein said electronic document further comprises interactive instructions for at least one of:

(i) an initial assessment of a crisis event;

(ii) a triage determination on next steps in response to said crisis event;

(iii) activation of a crisis command center to deal with said crisis event;

(iv) holding and monitoring situations related to said crisis event; and

(v) standing down with respect to said crisis event.

4. The computer-implemented method according to claim 1, wherein said electronic document further comprises engagement protocols for communications among said participants in said crisis management procedure.

5. The computer-implemented method according to claim 1, further comprising:

providing a user interface displaying an interactive event timeline comprising prompts and options for user actions at a predefined pace.

6. The computer-implemented method according to claim 1, wherein said participants in said crisis management procedure comprise one or more of: a crisis management team, an oversight lead, a crisis manager, an information manager, a resource manager, and a support team.

7. The computer-implemented method according to claim 1, further comprising:

modifying or updating said electronic document during or after a crisis event.

8. The computer-implemented method according to claim 1, further comprising:

automatically initiating communications to some or all of said participants in said crisis management procedure based on said electronic document upon occurrence of a crisis event.

9. The computer-implemented method according to claim 1, further comprising:

receiving, by at least one computer processor, a first notification of an event;

identifying, by at least one computer processor, a first subset of identities from the plurality of potential participants; and

transmitting a second notification of the event to user equipment devices of each of a first plurality of individuals corresponding to the first subset of identities.

10. The computer-implemented method according to claim 9, further comprising:

receiving a user selection of one of a plurality of crisis-related options after transmitting the second notification; and

in response to determining that the user selection corresponds to an activation command:

identifying a second subset of identities from the plurality of potential participants; and

transmitting a third notification of the event to user equipment devices of each of a second plurality of individuals corresponding to the second subset of identities.

11. A computer-implemented system for crisis management comprising a computer platform, the computer platform comprising:

at least one computer processor coupled to one or more data stores and configured to:

create an electronic document containing:

(a) at least one first interactive display of a predefined framework or timeline for a crisis management procedure,

(b) at least one second interactive display of predefined roles and responsibilities of participants in said crisis management procedure, and

(c) at least one third interactive display of step-by-step instructions for said participants to carry out said crisis management procedure according to their respective roles and responsibilities;

incorporate, in said at least one first, second, and third interactive displays, one or more hyperlinks to at least one other interactive display or electronic resource internal or external to said electronic document, said at least one electronic resource comprising one or more communication protocols and model templates for emergency responses as part of said crisis management procedure;

configure said electronic document to be displayable on each of a plurality of computing devices including desktop computers, laptop computers, tablet computers, and mobile computing devices; and

distribute said electronic document to a plurality of potential participants in said crisis management procedure.

12. The computer-implemented system according to claim 11, wherein said at least one electronic resource further comprises a suite of crisis response tools accessible via said electronic document by said participants according to their respective roles and responsibilities.

13. The computer-implemented system according to claim 11, wherein said electronic document further comprises interactive instructions for at least one of:

(i) an initial assessment of a crisis event;

(ii) a triage determination on next steps in response to said crisis event;

(iii) activation of a crisis command center to deal with said crisis event;

(iv) holding and monitoring situations related to said crisis event; and

(v) standing down with respect to said crisis event.

14. The computer-implemented system according to claim 11, wherein said electronic document further comprises engagement protocols for communications among said participants in said crisis management procedure.

15. The computer-implemented system according to claim 11, further configured to:

provide a user interface displaying an interactive event timeline comprising prompts and options for user actions at a predefined pace.

16. The computer-implemented system according to claim 11, wherein said participants in said crisis management procedure comprise one or more of: a crisis management team, an oversight lead, a crisis manager, an information manager, a resource manager, and a support team.

17. The computer-implemented system according to claim 11, further configured to:

modify or update said electronic document during or after a crisis event.

18. The computer-implemented system according to claim 11, further configured to:

automatically initiate communications to some or all of said participants in said crisis management procedure based on said electronic document upon occurrence of a crisis event.

19. The computer-implemented system according to claim 11, further configured to:

receive a first notification of an event;

identify a first subset of identities from the plurality of potential participants; and

transmit a second notification of the event to user equipment devices of each of a first plurality of individuals corresponding to the first subset of identities.

20. The computer-implemented system according to claim 19, further configured to:

receive a user selection of one of a plurality of crisis-related options after transmitting the second notification; and

in response to determining that the user selection corresponds to an activation command:

identify a second subset of identities from the plurality of potential participants; and

transmit a third notification of the event to user equipment devices of each of a second plurality of individuals corresponding to the second subset of identities.

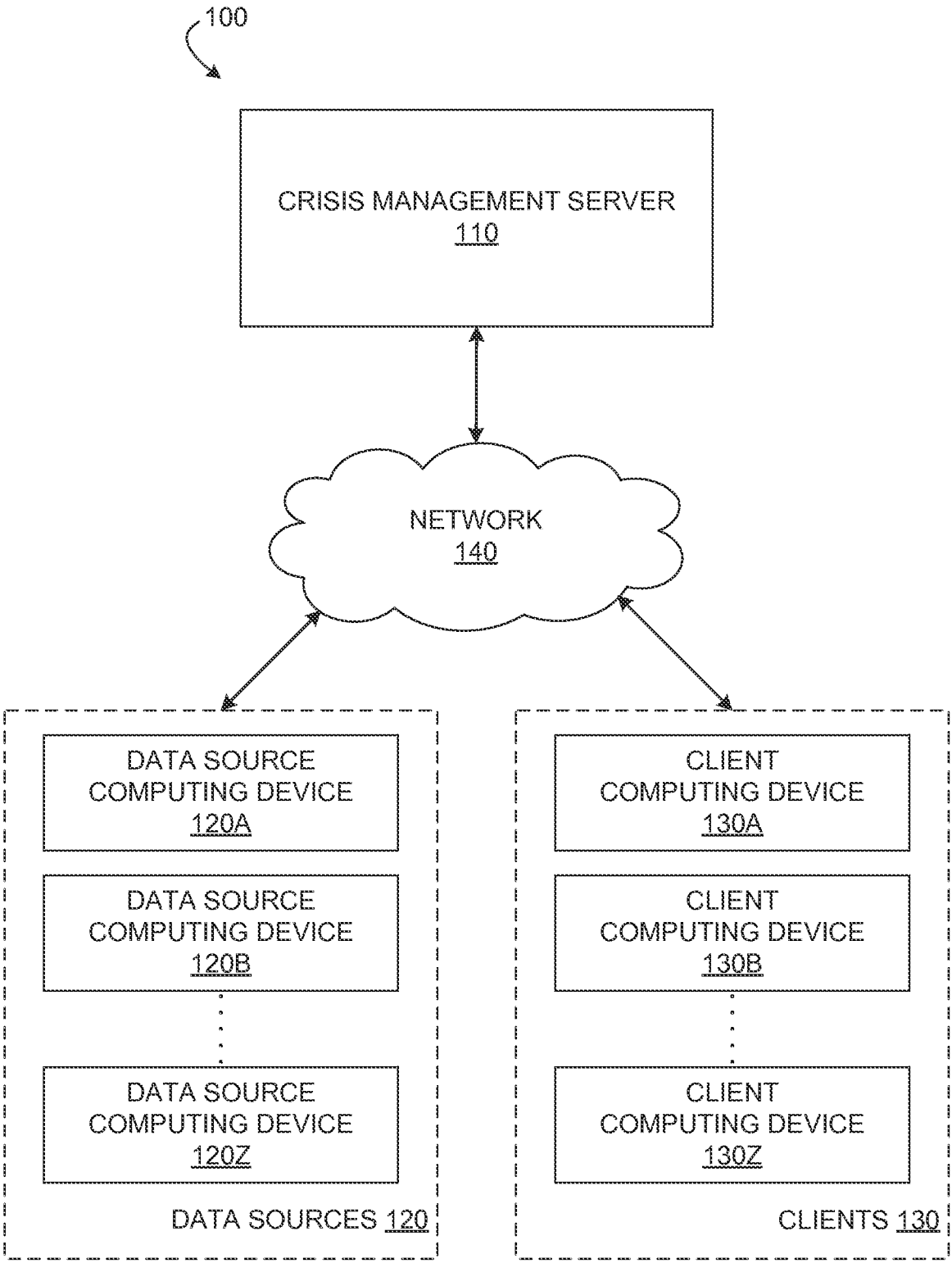

100
CRISIS MANAGEMENT SERVER
110
NETWORK
140
DATA SOURCE
COMPUTING DEVICE
120A
DATA SOURCE
COMPUTING DEVICE
120B
DATA SOURCE
COMPUTING DEVICE
120Z
DATA SOURCES 120
CLIENT
COMPUTING DEVICE
130A
CLIENT
COMPUTING DEVICE
130B
CLIENT
COMPUTING DEVICE
130Z
CLIENTS 130

FIG. 1

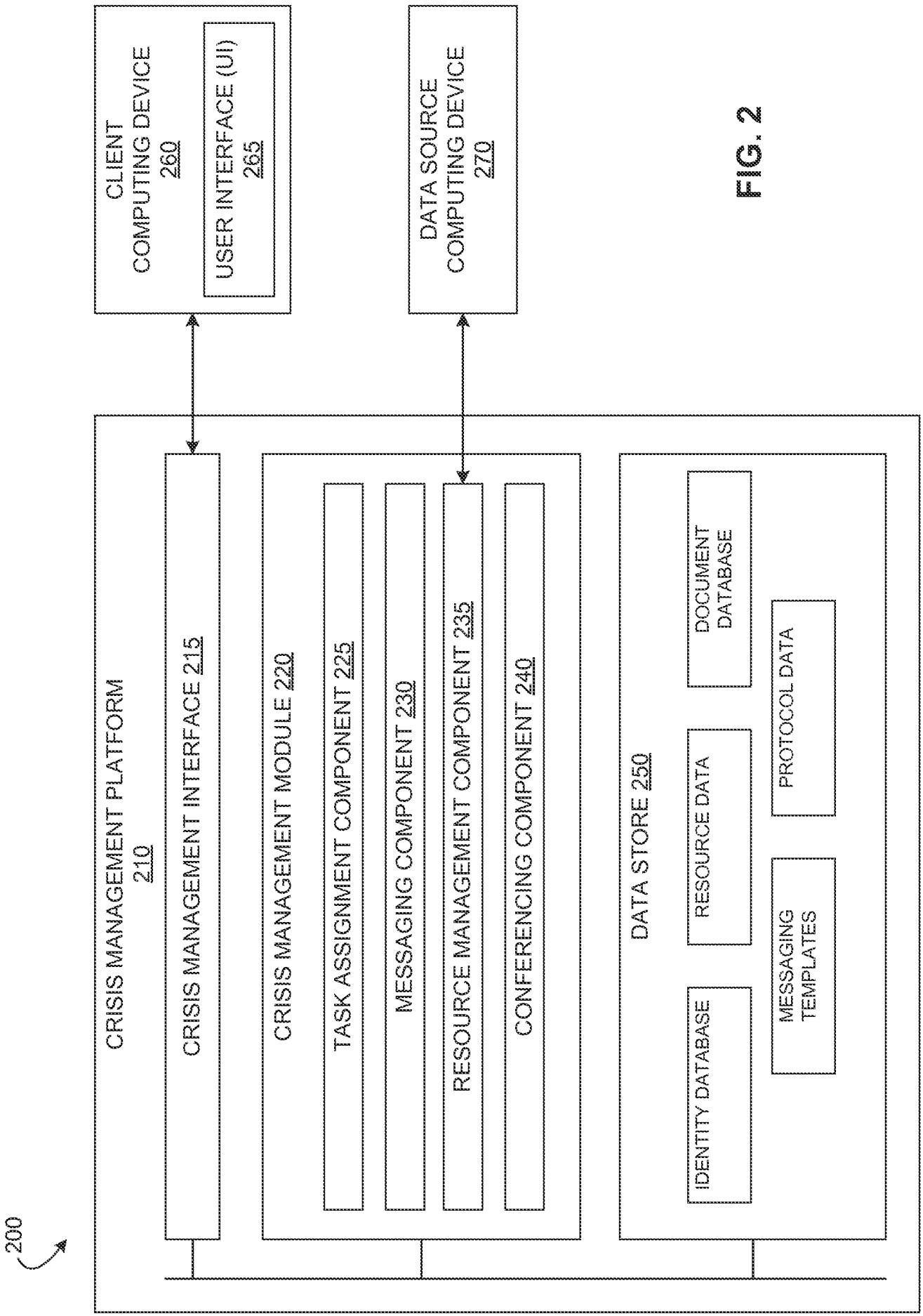

200
CLIENT COMPUTING DEVICE 260
USER INTERFACE (UI) 265
DATA SOURCE COMPUTING DEVICE 270
CRISIS MANAGEMENT PLATFORM 210
CRISIS MANAGEMENT INTERFACE 215
CRISIS MANAGEMENT MODULE 220
TASK ASSIGNMENT COMPONENT 225
MESSAGING COMPONENT 230
RESOURCE MANAGEMENT COMPONENT 235
CONFERENCING COMPONENT 240
DATA STORE 250
IDENTITY DATABASE
RESOURCE DATA
DOCUMENT DATABASE
MESSAGING TEMPLATES
PROTOCOL DATA

FIG. 2

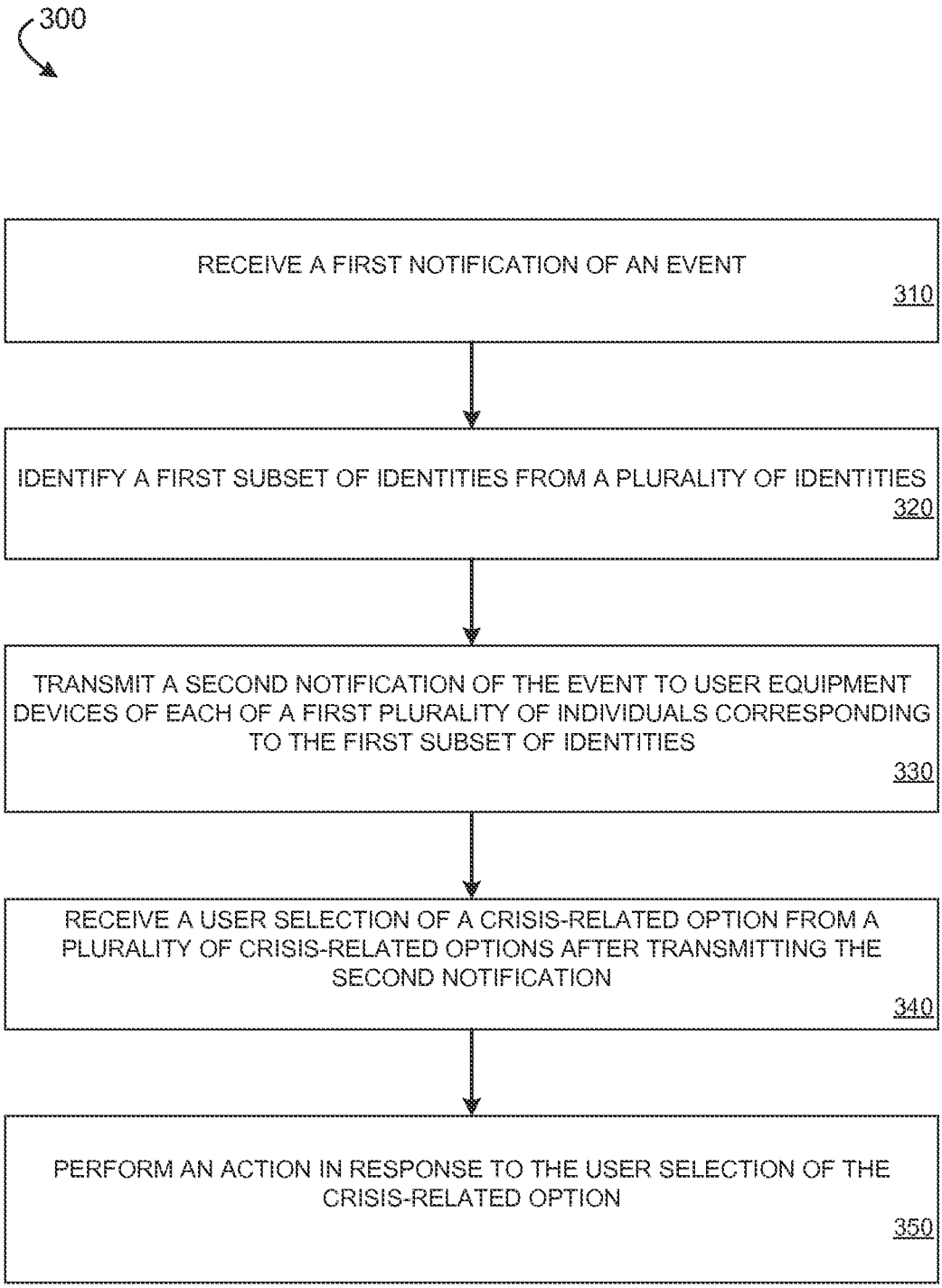

300
RECEIVE A FIRST NOTIFICATION OF AN EVENT
310
IDENTIFY A FIRST SUBSET OF IDENTITIES FROM A PLURALITY OF IDENTITIES
320
TRANSMIT A SECOND NOTIFICATION OF THE EVENT TO USER EQUIPMENT DEVICES OF EACH OF A FIRST PLURALITY OF INDIVIDUALS CORRESPONDING TO THE FIRST SUBSET OF IDENTITIES
330
RECEIVE A USER SELECTION OF A CRISIS-RELATED OPTION FROM A PLURALITY OF CRISIS-RELATED OPTIONS AFTER TRANSMITTING THE SECOND NOTIFICATION
340
PERFORM AN ACTION IN RESPONSE TO THE USER SELECTION OF THE CRISIS-RELATED OPTION
350

FIG. 3

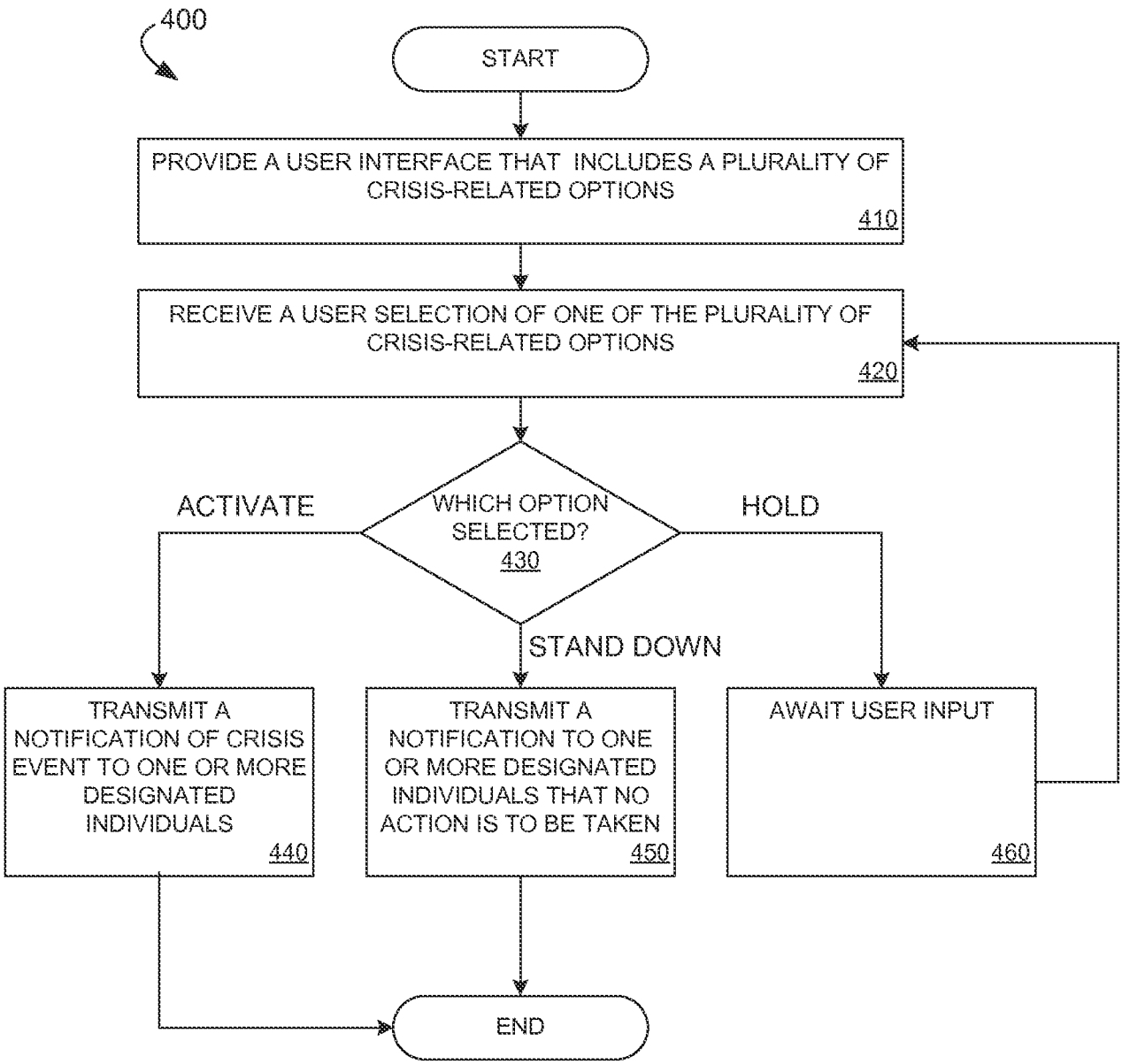

400
START
PROVIDE A USER INTERFACE THAT INCLUDES A PLURALITY OF CRISIS-RELATED OPTIONS
410
RECEIVE A USER SELECTION OF ONE OF THE PLURALITY OF CRISIS-RELATED OPTIONS
420
WHICH OPTION SELECTED?
430
ACTIVATE
STAND DOWN
HOLD
TRANSMIT A NOTIFICATION OF CRISIS EVENT TO ONE OR MORE DESIGNATED INDIVIDUALS
440
TRANSMIT A NOTIFICATION TO ONE OR MORE DESIGNATED INDIVIDUALS THAT NO ACTION IS TO BE TAKEN
450
AWAIT USER INPUT
460
END

FIG. 4

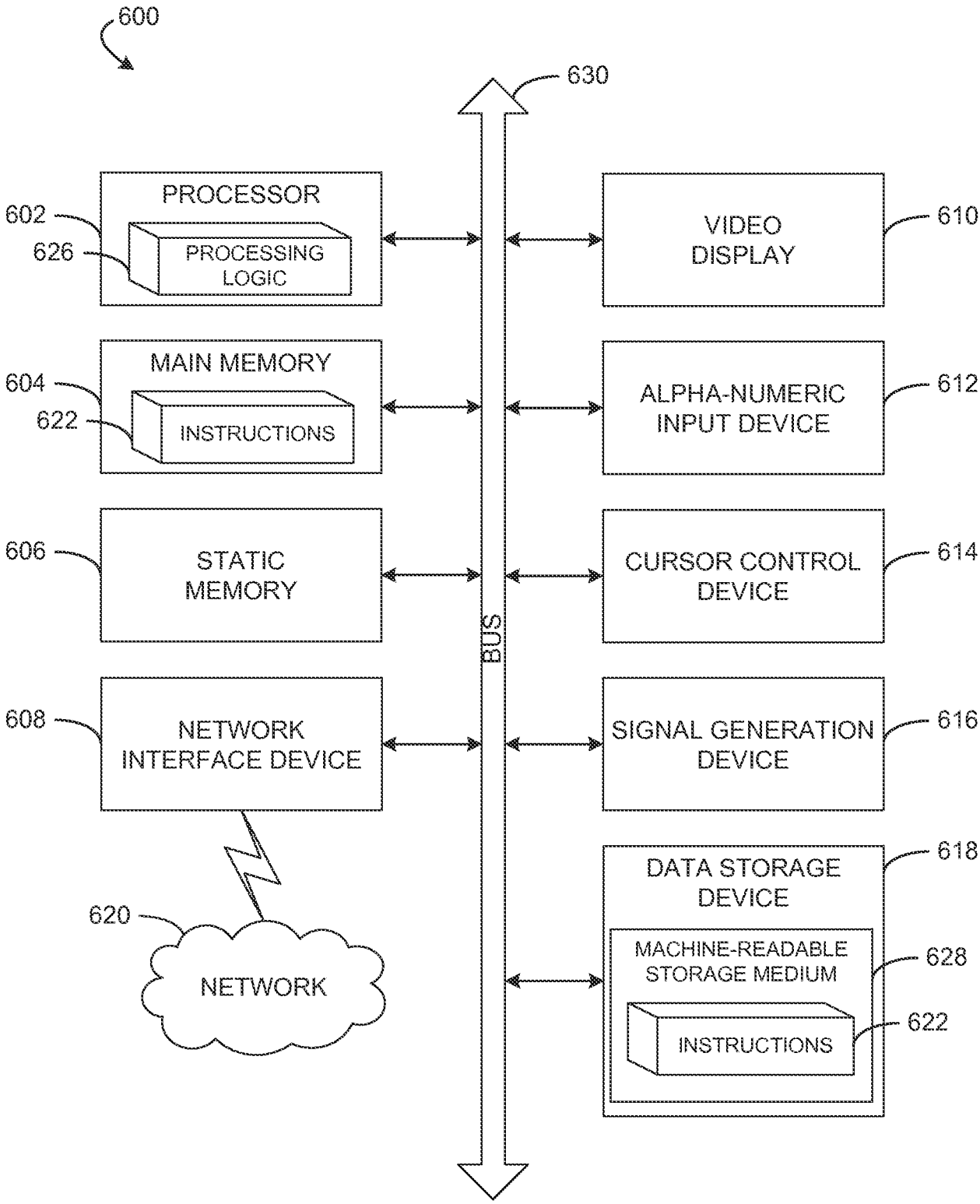

600
630
PROCESSOR
602
626
PROCESSING LOGIC
MAIN MEMORY
604
622
INSTRUCTIONS
606
STATIC MEMORY
608
NETWORK INTERFACE DEVICE
620
NETWORK
BUS
VIDEO DISPLAY
610
ALPHA-NUMERIC INPUT DEVICE
612
CURSOR CONTROL DEVICE
614
SIGNAL GENERATION DEVICE
616
DATA STORAGE DEVICE
618
MACHINE-READABLE STORAGE MEDIUM
628
INSTRUCTIONS
622

FIG. 5

FIG. 6

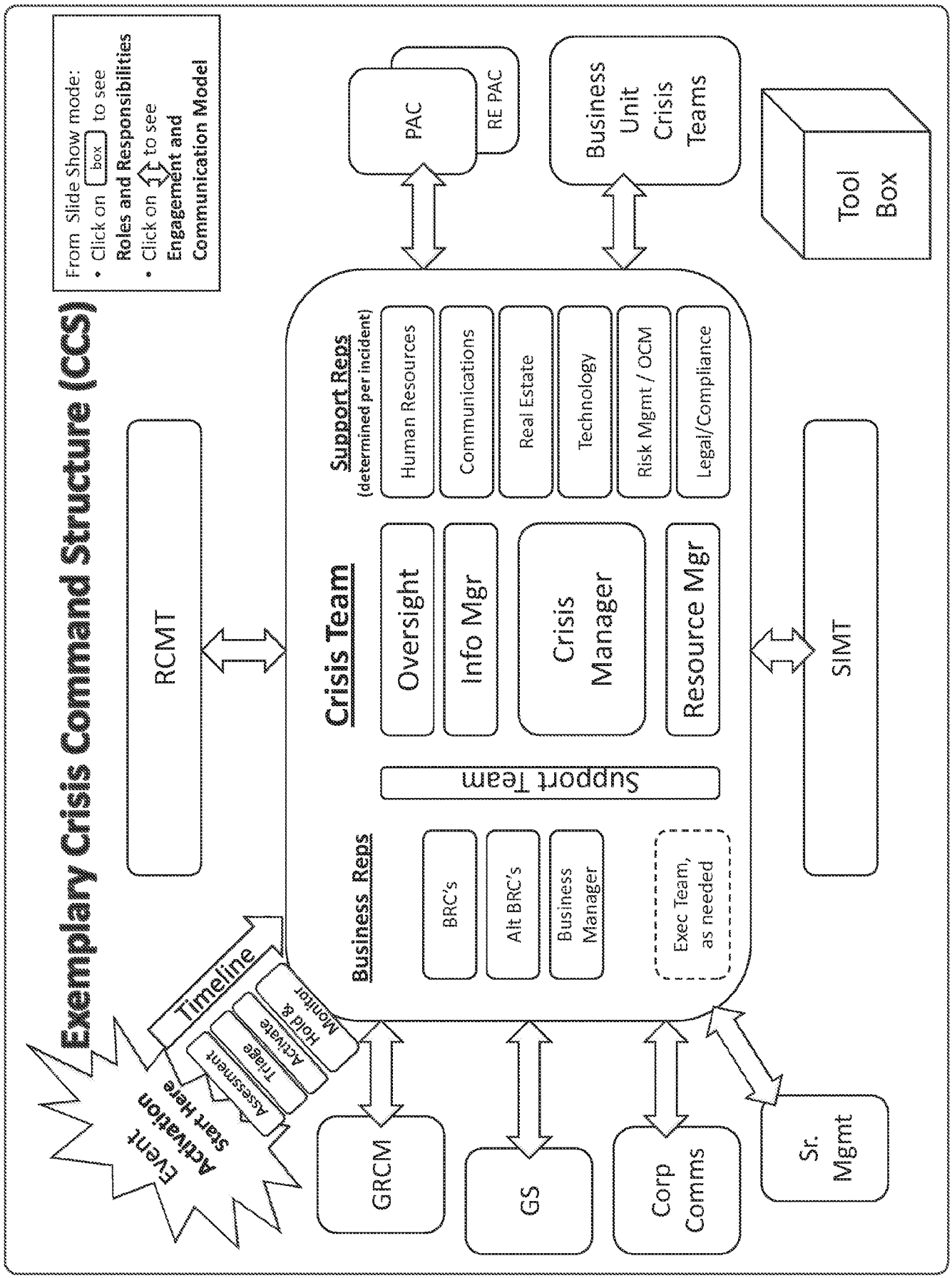

Exemplary Crisis Command Structure (CCS)
From Slide Show mode:
• Click on box to see Roles and Responsibilities
• Click on ↕ to see Engagement and Communication Model
RCMT
PAC
RE PAC
Business Unit Crisis Teams
Tool Box
Support Reps
(determined per incident)
Human Resources
Communications
Real Estate
Technology
Risk Mgmt / OCM
Legal/Compliance
Crisis Team
Oversight
Info Mgr
Crisis Manager
Resource Mgr
Support Team
Business Reps
BRC's
Alt BRC's
Business Manager
Exec Team, as needed
SIMT
Timeline
Event Activation start Here
Assessment
Triage
Activate
Hold &
Monitor
GRCM
GS
Corp Comms
Sr. Mgmt

FIG. 7

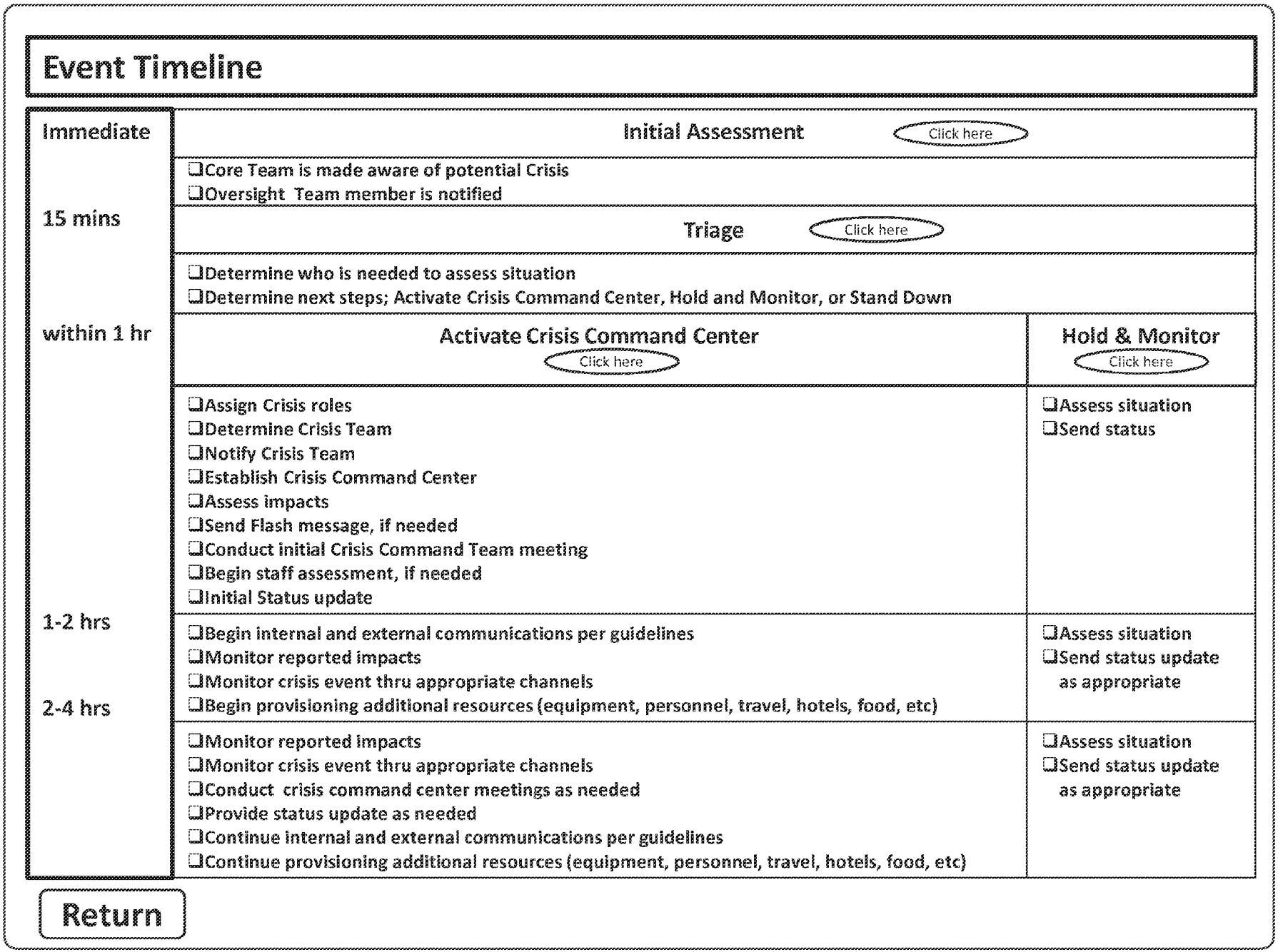

Event Timeline
Immediate
Initial Assessment
Click here
❑Core Team is made aware of potential Crisis
❑Oversight Team member is notified
15 mins
Triage
Click here
❑Determine who is needed to assess situation
❑Determine next steps; Activate Crisis Command Center, Hold and Monitor, or Stand Down
within 1 hr
Activate Crisis Command Center
Click here
Hold & Monitor
Click here
❑Assign Crisis roles
❑Determine Crisis Team
❑Notify Crisis Team
❑Establish Crisis Command Center
❑Assess impacts
❑Send Flash message, if needed
❑Conduct initial Crisis Command Team meeting
❑Begin staff assessment, if needed
❑Initial Status update
❑Assess situation
❑Send status
1-2 hrs
2-4 hrs
❑Begin internal and external communications per guidelines
❑Monitor reported impacts
❑Monitor crisis event thru appropriate channels
❑Begin provisioning additional resources (equipment, personnel, travel, hotels, food, etc)
❑Assess situation
❑Send status update as appropriate
❑Monitor reported impacts
❑Monitor crisis event thru appropriate channels
❑Conduct crisis command center meetings as needed
❑Provide status update as needed
❑Continue internal and external communications per guidelines
❑Continue provisioning additional resources (equipment, personnel, travel, hotels, food, etc)
❑Assess situation
❑Send status update as appropriate
Return

FIG. 8

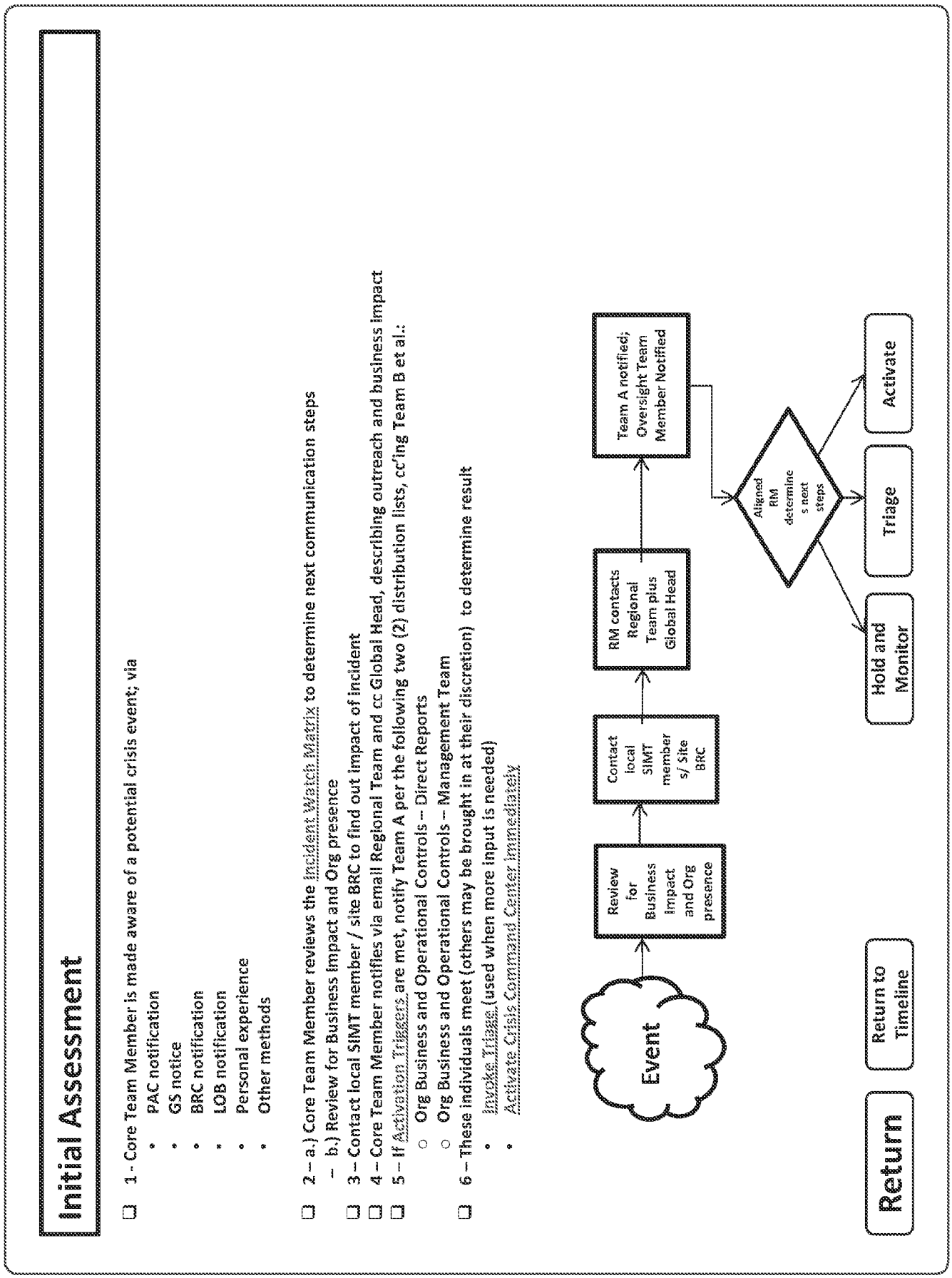

Initial Assessment
1 - Core Team Member is made aware of a potential crisis event; via
PAC notification
GS notice
BRC notification
LOB notification
Personal experience
Other methods
2 – a.) Core Team Member reviews the Incident Watch Matrix to determine next communication steps
– b.) Review for Business Impact and Org presence
3 – Contact local SIMT member / site BRC to find out impact of incident
4 – Core Team Member notifies via email Regional Team and cc Global Head, describing outreach and business impact
5 – If Activation Triggers are met, notify Team A per the following two (2) distribution lists, cc'ing Team B et al.:
Org Business and Operational Controls – Direct Reports
Org Business and Operational Controls – Management Team
6 – These individuals meet (others may be brought in at their discretion) to determine result
Invoke Triage (used when more input is needed)
Activate Crisis Command Center immediately
Return
Return to Timeline
Event
Review for Business Impact and Org presence
Contact local SIMT member s/ Site BRC
RM contacts Regional Team plus Global Head
Team A notified; Oversight Team Member Notified
Aligned RM determine s next steps
Hold and Monitor
Triage
Activate

FIG. 9

Triage

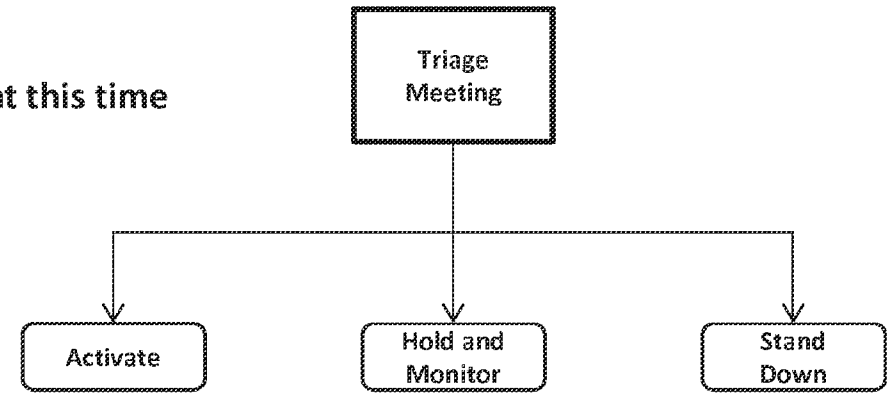
- ❑ 1 - Assign one individual responsible to for running the triage; generally Crisis Manager

- ❑ 2 - Crisis Manager and Oversight Lead determines who to bring into triage meeting; generally
  - Core Team Member(s)
  - Oversight Team Member(s)
  - Individual who reported the event
  - Individual(s) who know about the event (GS, Real Estate, LOB, etc.)
  - Key impacted (or potentially impacted) parties

  This should be no more than 4-10 individuals

- ❑ 3 – Crisis Manager and Oversight Lead set time and logistics of meeting; → C-1
  generally within 15 minutes of notification

- ❑ 4 – Crisis Manager conducts meeting
  a) Discuss situation and known information at this time
  b) Discuss impacts or potential impacts
  c) Discuss if Activation Triggers are met
  d) Determine outcome
    - Activate Crisis Command Center
    - Hold and Monitor
    - Stand Down



- ❑ 5 – Crisis Manager communicate results if "hold and monitor" or "stand down"

C-2 C-3

Return | Return to Timeline

FIG. 10

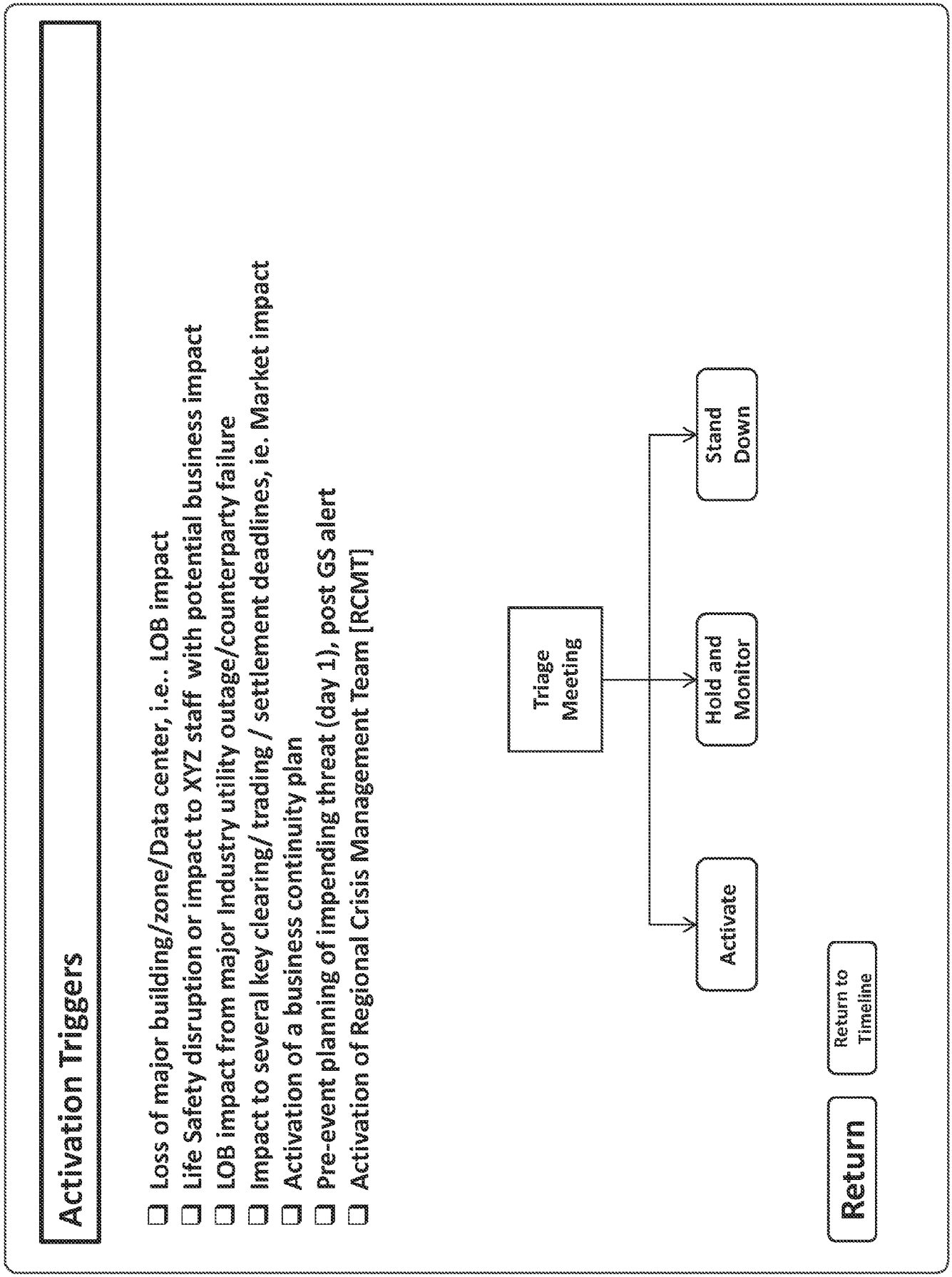
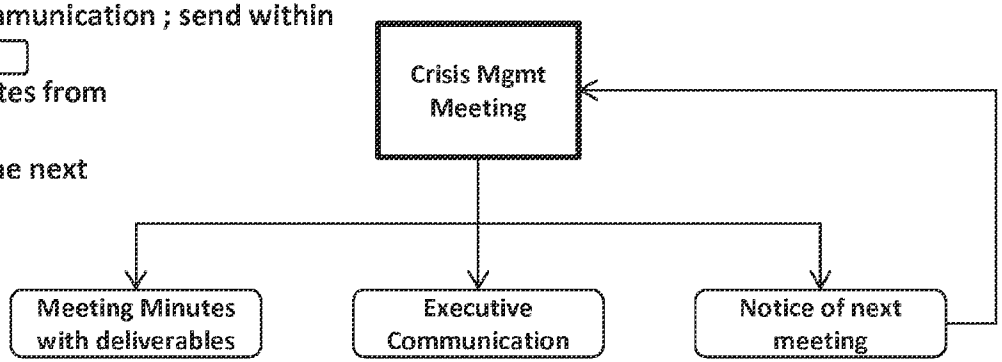

Activation Triggers
❑ Loss of major building/zone/Data center, i.e.. LOB impact
❑ Life Safety disruption or impact to XYZ staff with potential business impact
❑ LOB impact from major industry utility outage/counterparty failure
❑ Impact to several key clearing/ trading / settlement deadlines, ie. Market impact
❑ Activation of a business continuity plan
❑ Pre-event planning of impending threat (day 1), post GS alert
❑ Activation of Regional Crisis Management Team [RCMT]
Triage Meeting
Activate
Hold and Monitor
Stand Down
Return
Return to Timeline

FIG. 11

Activate Crisis Command Center

- ❑ 1 - Assign Crisis Command Center roles
  - a) Oversight Lead – RCMT Team member
  - b) Crisis Manager – Core Team member responsible for site, if available
- ❑ 2 - Crisis Manager and Oversight Lead determines the scope of the Crisis Command Center and whom to invite
  - a) If in doubt invite all Crisis Team Members (full activation)
- ❑ 3 - Crisis Manager and Oversight Lead determines time and logistics of the Crisis Command Center meeting; generally within 15 minutes of notification
- ❑ 4 - Crisis Manager assigns
  - a) Info Manager
  - b) Resource Manager
- ❑ 5 - If high visibility crisis, Oversight Lead considers sending immediate note to Sr. Management notifying that a crisis call is being convened and a status update will be sent as soon as possible ➔ C-4
- ❑ 6 - Resource Manager pulls list of impacted (or potentially impacted) Staff
- ❑ 7 - Resource Manager pulls list of impacted (or potentially impacted) Serket plans
- ❑ 8 - Resource Manager sends notification to those who should attend Command Center Meeting ➔ C-5
- ❑ 9 - Resource Manager opens the conference bridge line and CCS Command & Control Adobe Chat for the Core team
- ❑ 10 - Crisis Manager conducts meeting using Crisis Command Center Agenda
- ❑ 11 - Crisis Manager determines next Crisis Command Center meeting; should be 1 -2 hours prior to RCMT Meetings
- ❑ 12 - Oversight Manager takes notes to deliver at RCMT Meeting
- ❑ 13 - Info Manager creates Executive Communication ; send within 1 hour after closure of meeting ➔ C-6
- ❑ 14 - Info Manager creates meeting minutes from Org Crisis Command Center Meetings
- ❑ 15 - Resource Manager sends invite to the next meeting; via Outlook ➔ C-7
- ❑ 16 – Resource Manager assigns role for Crisis Command Open Bridge, if needed



Return

Return to Timeline

FIG. 12

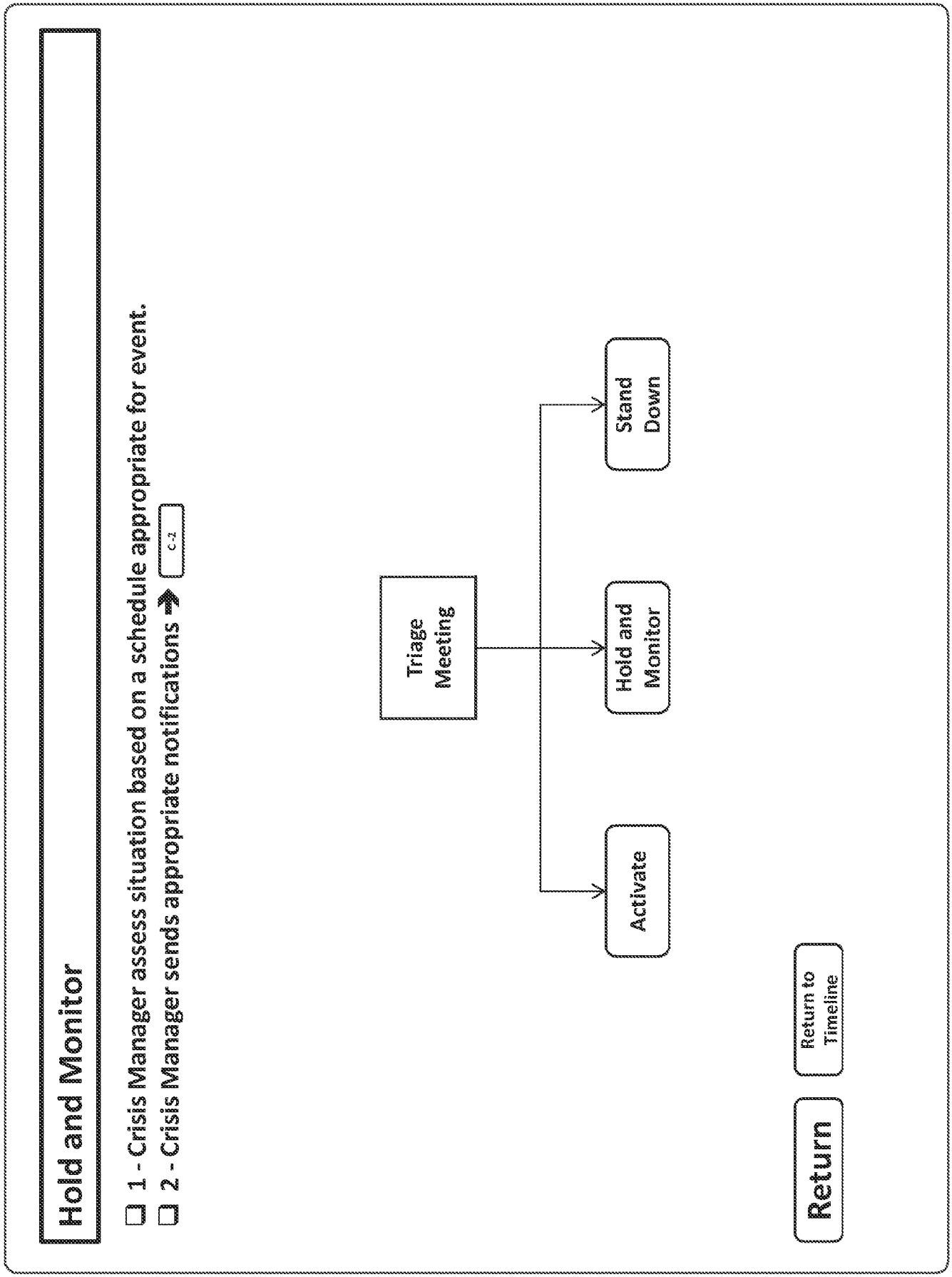

Hold and Monitor
1 - Crisis Manager assess situation based on a schedule appropriate for event.
2 - Crisis Manager sends appropriate notifications
C-2
Triage Meeting
Stand Down
Hold and Monitor
Activate
Return
Return to Timeline

FIG. 13

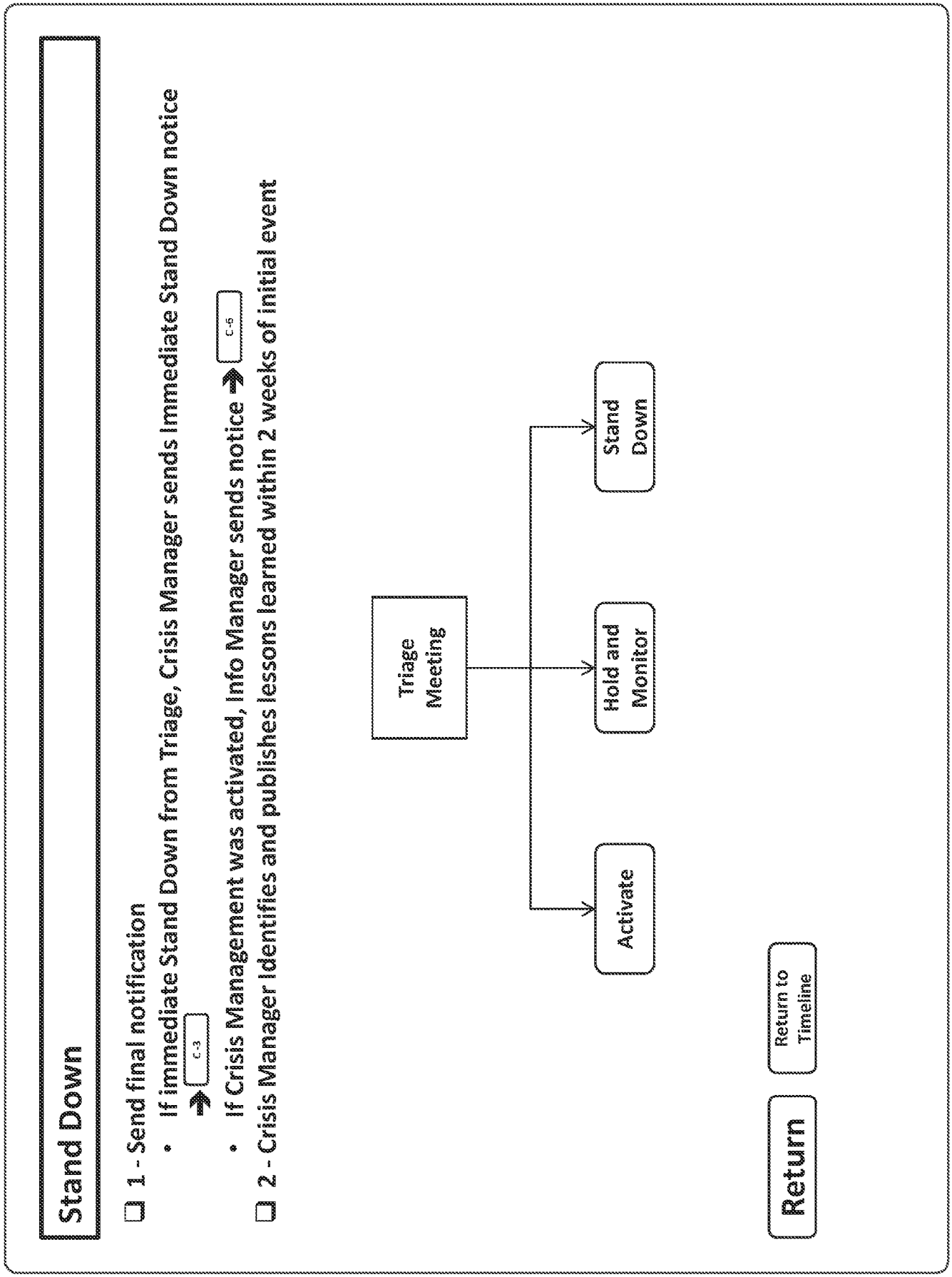

Stand Down
1 - Send final notification
If immediate Stand Down from Triage, Crisis Manager sends Immediate Stand Down notice
C-3
If Crisis Management was activated, Info Manager sends notice
C-5
2 - Crisis Manager Identifies and publishes lessons learned within 2 weeks of initial event
Triage Meeting
Activate
Hold and Monitor
Stand Down
Return
Return to Timeline

FIG. 14

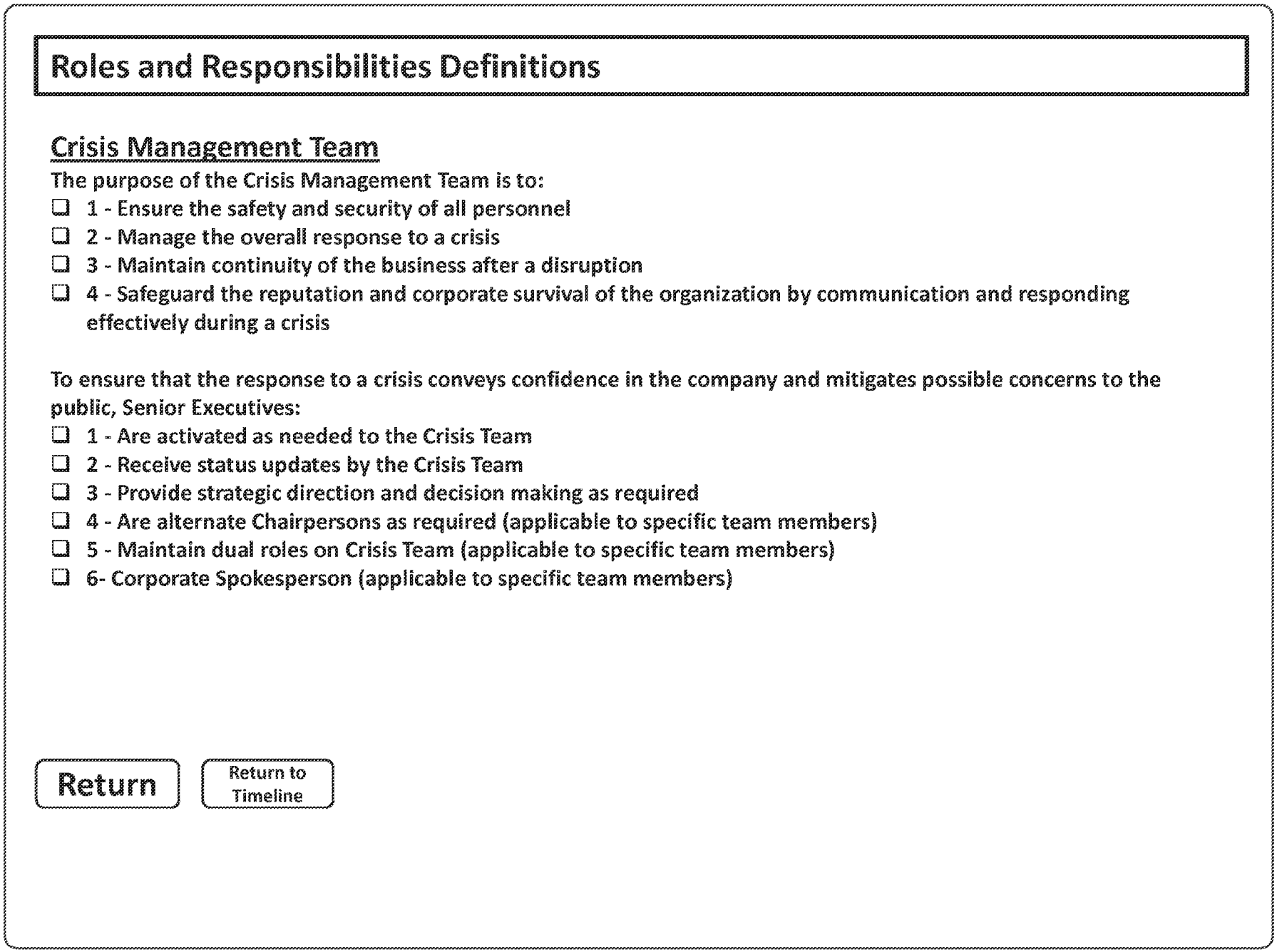

Roles and Responsibilities Definitions
Crisis Management Team
The purpose of the Crisis Management Team is to:
1 - Ensure the safety and security of all personnel
2 - Manage the overall response to a crisis
3 - Maintain continuity of the business after a disruption
4 - Safeguard the reputation and corporate survival of the organization by communication and responding effectively during a crisis
To ensure that the response to a crisis conveys confidence in the company and mitigates possible concerns to the public, Senior Executives:
1 - Are activated as needed to the Crisis Team
2 - Receive status updates by the Crisis Team
3 - Provide strategic direction and decision making as required
4 - Are alternate Chairpersons as required (applicable to specific team members)
5 - Maintain dual roles on Crisis Team (applicable to specific team members)
6- Corporate Spokesperson (applicable to specific team members)
Return
Return to Timeline

FIG. 15

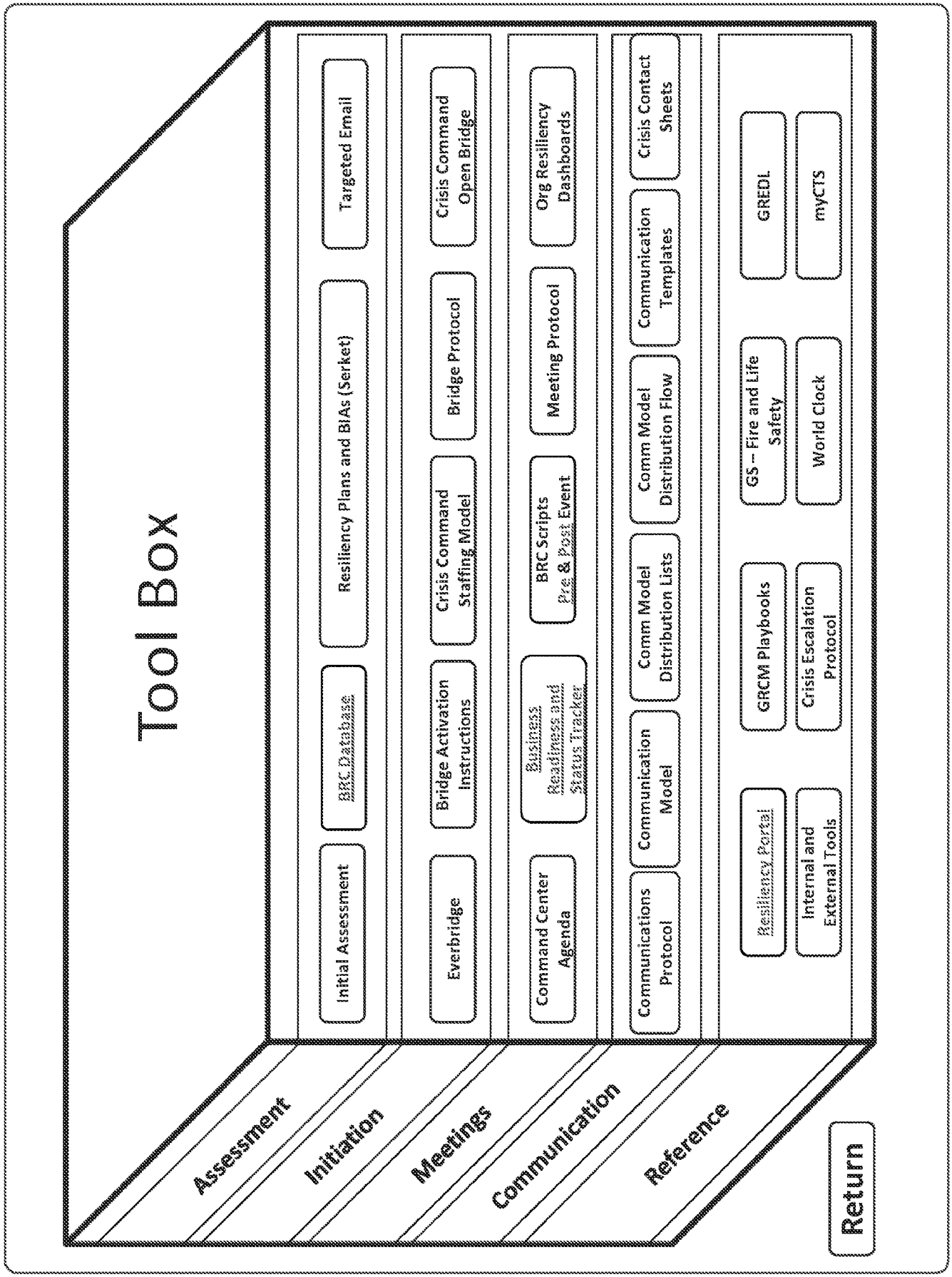

Tool Box
Assessment
Initiation
Meetings
Communication
Reference
Return
Initial Assessment
BRC Database
Resiliency Plans and BIAs (Serket)
Targeted Email
Everbridge
Bridge Activation Instructions
Crisis Command Staffing Model
Bridge Protocol
Crisis Command Open Bridge
Command Center Agenda
Business Readiness and Status Tracker
BRC Scripts Pre & Post Event
Meeting Protocol
Org Resiliency Dashboards
Communications Protocol
Communication Model
Comm Model Distribution Lists
Comm Model Distribution Flow
Communication Templates
Crisis Contact Sheets
Resiliency Portal
Internal and External Tools
GRCM Playbooks
Crisis Escalation Protocol
GS – Fire and Life Safety
World Clock
GREDL
myCTS

FIG. 16

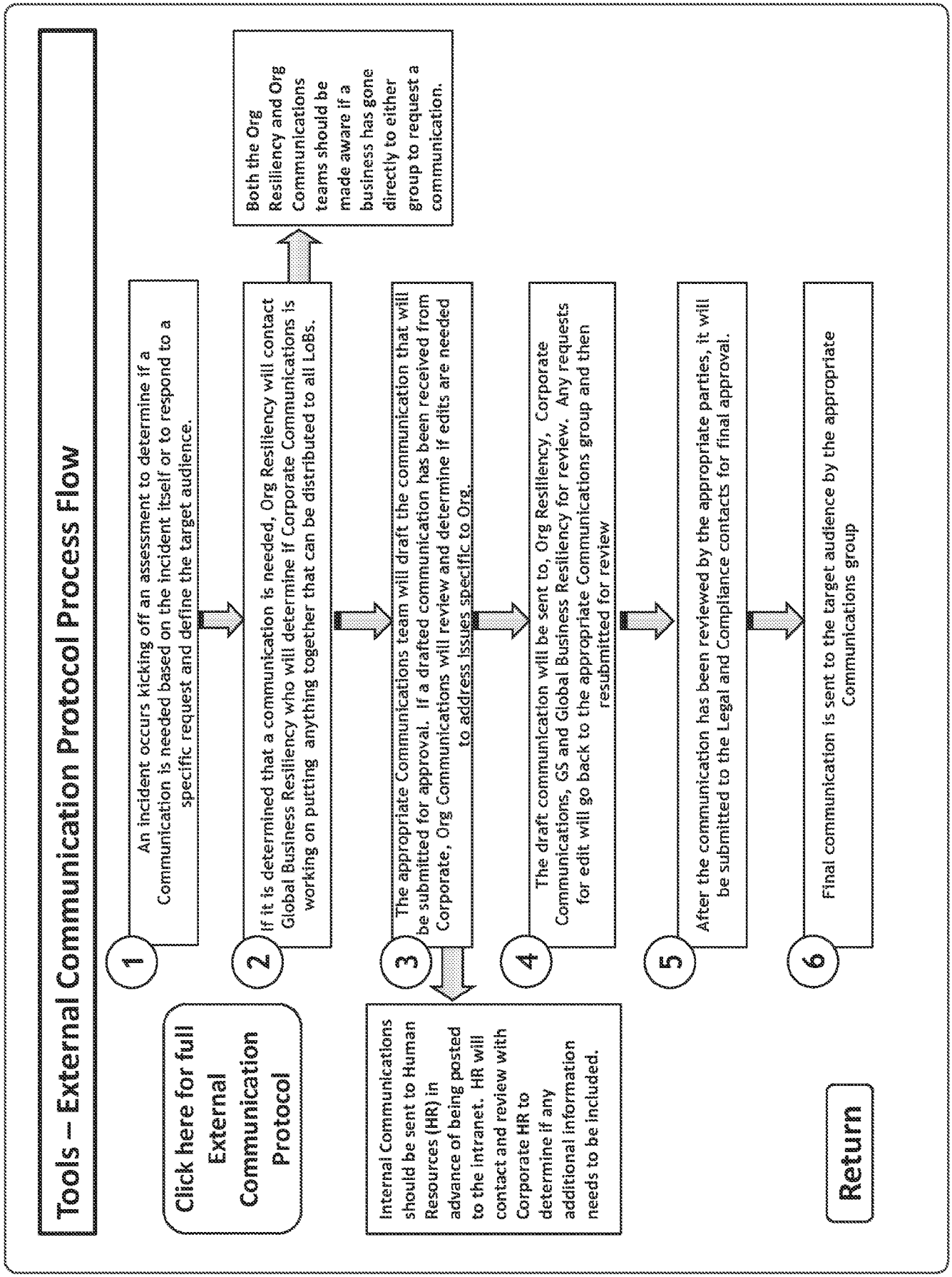
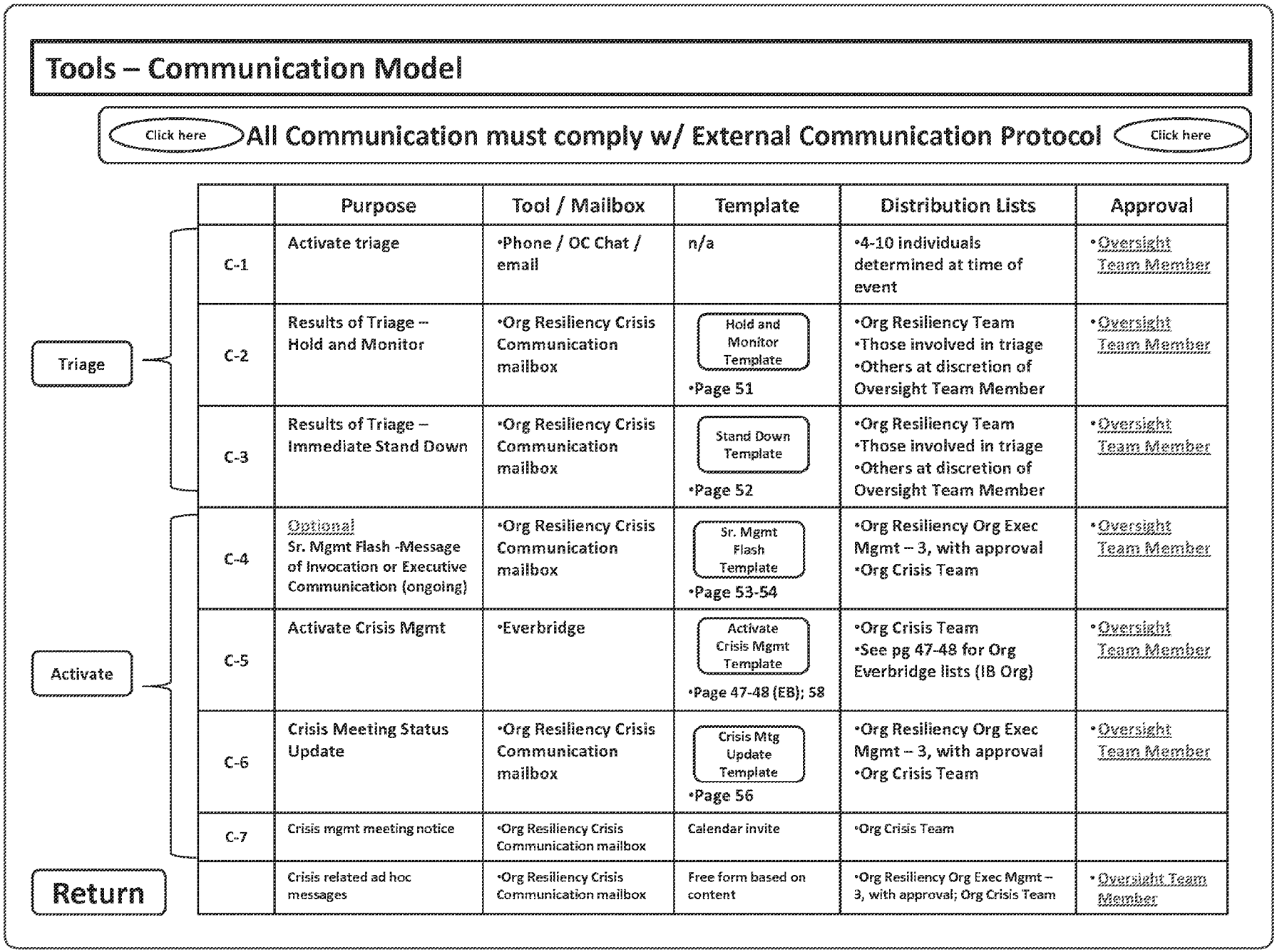
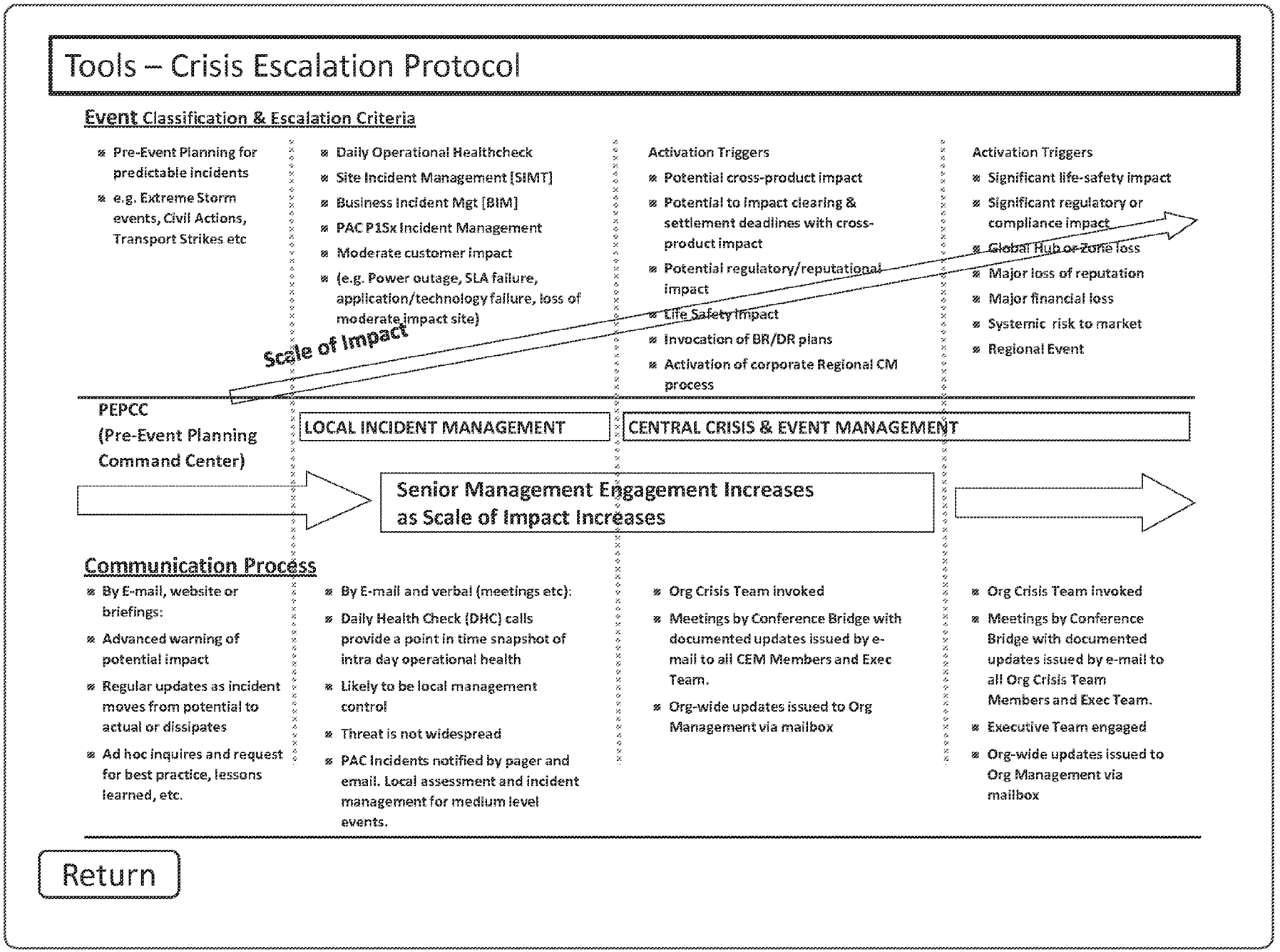

Tools – External Communication Protocol Process Flow
Click here for full External Communication Protocol
1
An incident occurs kicking off an assessment to determine if a Communication is needed based on the incident itself or to respond to a specific request and define the target audience.
2
If it is determined that a communication is needed, Org Resiliency will contact Global Business Resiliency who will determine if Corporate Communications is working on putting anything together that can be distributed to all LoBs.
Both the Org Resiliency and Org Communications teams should be made aware if a business has gone directly to either group to request a communication.
3
The appropriate Communications team will draft the communication that will be submitted for approval. If a drafted communication has been received from Corporate, Org Communications will review and determine if edits are needed to address issues specific to Org.
Internal Communications should be sent to Human Resources (HR) in advance of being posted to the intranet. HR will contact and review with Corporate HR to determine if any additional information needs to be included.
4
The draft communication will be sent to, Org Resiliency, Corporate Communications, GS and Global Business Resiliency for review. Any requests for edit will go back to the appropriate Communications group and then resubmitted for review
5
After the communication has been reviewed by the appropriate parties, it will be submitted to the Legal and Compliance contacts for final approval.
6
Final communication is sent to the target audience by the appropriate Communications group
Return

FIG. 17



	Purpose	Tool / Mailbox	Template	Distribution Lists	Approval
C-1	Activate triage	•Phone / OC Chat / email	n/a	•4-10 individuals determined at time of event	•Oversight Team Member
C-2	Results of Triage – Hold and Monitor	•Org Resiliency Crisis Communication mailbox	Hold and Monitor Template •Page 51	•Org Resiliency Team •Those involved in triage •Others at discretion of Oversight Team Member	•Oversight Team Member
C-3	Results of Triage – Immediate Stand Down	•Org Resiliency Crisis Communication mailbox	Stand Down Template •Page 52	•Org Resiliency Team •Those involved in triage •Others at discretion of Oversight Team Member	•Oversight Team Member
C-4	Optional Sr. Mgmt Flash -Message of Invocation or Executive Communication (ongoing)	•Org Resiliency Crisis Communication mailbox	Sr. Mgmt Flash Template •Page 53-54	•Org Resiliency Org Exec Mgmt – 3, with approval •Org Crisis Team	•Oversight Team Member
C-5	Activate Crisis Mgmt	•Everbridge	Activate Crisis Mgmt Template •Page 47-48 (EB); 58	•Org Crisis Team •See pg 47-48 for Org Everbridge lists (IB Org)	•Oversight Team Member
C-6	Crisis Meeting Status Update	•Org Resiliency Crisis Communication mailbox	Crisis Mtg Update Template •Page 56	•Org Resiliency Org Exec Mgmt – 3, with approval •Org Crisis Team	•Oversight Team Member
C-7	Crisis mgmt meeting notice	•Org Resiliency Crisis Communication mailbox	Calendar invite	•Org Crisis Team	
	Crisis related ad hoc messages	•Org Resiliency Crisis Communication mailbox	Free form based on content	•Org Resiliency Org Exec Mgmt – 3, with approval; Org Crisis Team	•Oversight Team Member

FIG. 18


Tools – Crisis Escalation Protocol
Event Classification & Escalation Criteria
Pre-Event Planning for predictable incidents
e.g. Extreme Storm events, Civil Actions, Transport Strikes etc
Daily Operational Healthcheck
Site Incident Management [SIMT]
Business Incident Mgt [BIM]
PAC P1Sx Incident Management
Moderate customer impact
(e.g. Power outage, SLA failure, application/technology failure, loss of moderate impact site)
Activation Triggers
Potential cross-product impact
Potential to impact clearing & settlement deadlines with cross-product impact
Potential regulatory/reputational impact
Life Safety Impact
Invocation of BR/DR plans
Activation of corporate Regional CM process
Activation Triggers
Significant life-safety impact
Significant regulatory or compliance impact
Global Hub or Zone loss
Major loss of reputation
Major financial loss
Systemic risk to market
Regional Event
Scale of Impact
PEPCC (Pre-Event Planning Command Center)
LOCAL INCIDENT MANAGEMENT
CENTRAL CRISIS & EVENT MANAGEMENT
Senior Management Engagement Increases as Scale of Impact Increases
Communication Process
By E-mail, website or briefings:
Advanced warning of potential impact
Regular updates as incident moves from potential to actual or dissipates
Ad hoc inquires and request for best practice, lessons learned, etc.
By E-mail and verbal (meetings etc):
Daily Health Check (DHC) calls provide a point in time snapshot of intra day operational health
Likely to be local management control
Threat is not widespread
PAC Incidents notified by pager and email. Local assessment and incident management for medium level events.
Org Crisis Team invoked
Meetings by Conference Bridge with documented updates issued by e-mail to all CEM Members and Exec Team.
Org-wide updates issued to Org Management via mailbox
Org Crisis Team invoked
Meetings by Conference Bridge with documented updates issued by e-mail to all Org Crisis Team Members and Exec Team.
Executive Team engaged
Org-wide updates issued to Org Management via mailbox
Return

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 15/40704

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 10/00 (2015.01)
CPC - G06Q 10/06315; G06Q 10/06; G06Q 10/087
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
CPC: G06Q 10/06315; G06Q 10/06; G06Q 10/087; IPC(8): G06Q 10/00 (2015.01); USPC: 705/7.25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 705/7.28; 705/7.12
CPC: G 06Q 30/0202, G 06Q 10/06375 (keyword limited, see below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, Google Web, Google Patents
Search terms: emergency, crisis, earthquake, terrorist attack, contingency planning

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/0063234 A1 (Refsland et al.) 05 March 2009 (05.03.2009), entire document, especially abstract, para [0115], [0105], [0069], [0007], [0117], [0078], [0179], [0141]-[0143], [0015], [0092], [0135], [0118].	1-20

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 September 2015 (15.09.2015)	09 OCT 2015

Name and mailing address of the ISA/US	Authorized officer:
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)