Crisis Management Team Training 2022

v21 Updated 12/01/2022

Introduction

Please put on your headphones to listen to the audio content. Upon completion, please scroll down to advance.

Click to expand text accessibility —

I am Mike Roffler, CEO and President of First Republic. At First Republic, we are dedicated to safeguarding the well-being of our colleagues, our company, and our clients through proper emergency planning and preparedness. Planning for emergencies is not a luxury, it is a necessity. Sudden, unplanned events affect all companies and the difference between success or failure, is planning.

Although it's impossible to prepare for every crisis, it is essential that we have a team in place, and a plan prepared, to handle a variety of interruptions. The Crisis Management Team (CMT) and the associated plan and procedures serve that purpose. They provide an overall direction using a structured, yet flexible, approach.

As a CMT member, it is critical that you are trained and comfortable with the procedures and protocols to follow during a crisis situation. Through this training, you will learn the ins and outs of the CMT process. As a team member, it is vital that you not only understand the priorities of the bank and the CMT, but also that you understand and know how to use the tools and resources noted in the CMT plan and procedures.

You will find this information invaluable in protecting our colleagues, our clients, and our bank.

We are grateful for your commitment to First Republic and its continued success.

Thank you.

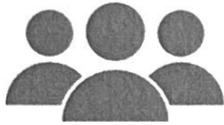# Crisis Management Team Training

🔒 Complete the content above before advancing.

Take a moment to consider what types of threats face First Republic and its colleagues. Whether it's a data breach, category 5 hurricane, mass electrical

outage, or a global pandemic, having a plan to handle and manage crises is critical to the success and longevity of any organization.

CONTINUE

Crisis Management Team

First Republic's Crisis Management Team has been established as the decision-making group to rapidly respond to a "Covered Incident". A Covered Incident is an incident that exceeds the response capabilities of usual business processes that would likely cause material harm to First Republic, its colleagues, clients, and/or other stakeholders.

To effectively manage a crisis, an organization needs a comprehensive process and a team of individuals to provide direction and oversight. First Republic has two related groups that manage the response during a crisis.

Crisis Management Team (CMT) —

- Comprised of Senior Leaders and Executives from across the organization.

- Invoked when the event affects the entire enterprise or has a significant impact on First Republic.

Crisis Management Team Task Force —

- Subset of the Crisis Management Team.

- Invoked for events that have a significant impact on a specific area of First Republic's business.

- Designed to expand and contract, as needed, for areas that are directly affected by the incident.

- May not include representation from every department.

🔒 Complete the content above before advancing.

Crisis Management Team Responsibilities

The main responsibilities of the Crisis Management Team and Task Force are to first ensure the safety of colleagues and then focus on maintaining the top three priorities of First Republic: our reputation, the availability of cash to run the Bank, and the condition of the loan portfolio.

To ensure these responsibilities are met, each Crisis Management Team member provides the status of and impact to their respective areas, along with their expertise on how to resolve any identified problems that threaten the continuation of critical processes.

CONTINUE

Key Roles

The following are the key roles which are activated during a Crisis Management Team or Task Force event:

Crisis Management Team Lead

The CMT Lead makes the decision or can recommend assembling the full Crisis Management Team or Task Force. Throughout the incident response, this individual ensures First Republic's top three priorities are met and acts as the key recipient of information.

Additionally (and as expected), the CMT Lead provides leadership and coordination of Crisis Management Team activities such as:

- Scheduling Crisis Management Team calls and meetings.

- Communicating with impacted stakeholders via the Enterprise Communication System.

- Delegating tasks to other Crisis Management Team members.

- Engaging the Board of Directors, when necessary.

- Monitoring updates, consolidating information, and tracking and deploying resources (such as people, facilities, and technology).

- Deactivating the Crisis Management Team and beginning the transition back to normal operations.

CONTINUE

Crisis Management Team Facilitator

Another key member of the CMT is the Crisis Management Team Facilitator. The CMT Facilitator position is usually filled by a representative from the Information Security Team to provide guidance and support to both the CMT Lead and other CMT Members. Responsibilities of the Facilitator also include:

- Assisting with administrative tasks.

- Maintaining a detailed log of the incident activities.

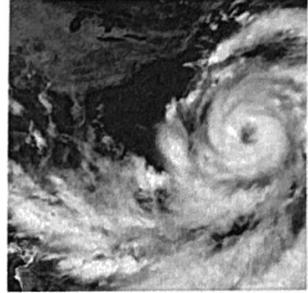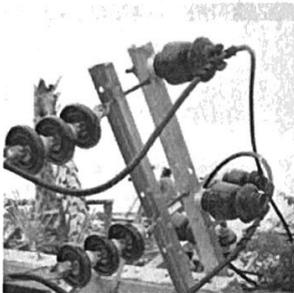- Ensuring follow-ups occur and lessons learned are documented.

Crisis Management Team Support Staff

Lastly, the Crisis Management Team Support Staff helps capture information and is assigned responsibilities, as needed.

CONTINUE

Crisis Management Team Invocation

Identification and Determination

Before an incident can be addressed by the CMT, it must be identified and determined to be a Covered Incident.

Any colleague can bring a concern to a Crisis Management Team member. The CMT member that was first contacted shall promptly notify other members of the team that a potential Covered Incident has occurred and share necessary details. No action will be taken until a determination has been made by the CMT as to whether it is a Covered Incident.

Once the determination has been made, CMT members may be instructed by the CMT Lead to meet in-person at the primary Emergency Operation Center (or EOC) located at Room 3D in 111 Pine Street or meet
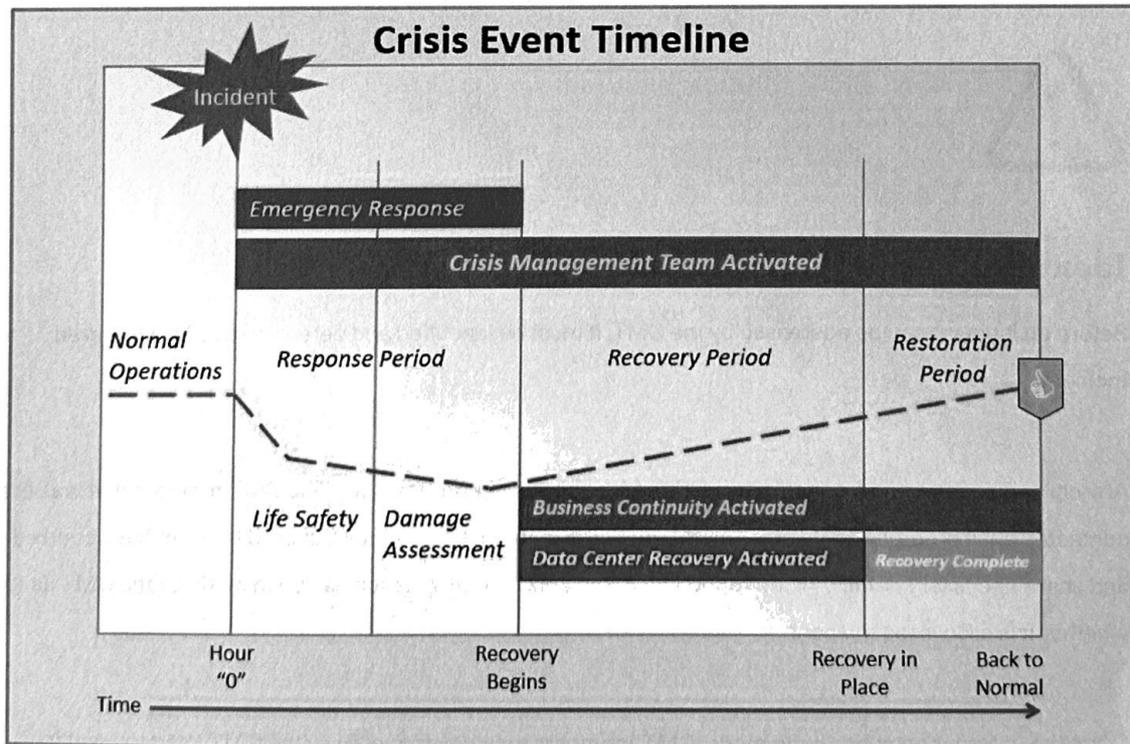
virtually using a video conferencing tool.

If the primary EOC is not available to accommodate an in-person meeting, a nearby accessible location will be selected and the Crisis Management Team will be informed of the alternate location.

CONTINUE

Crisis Event Timeline

We've covered the CMT, the roles and responsibilities of the team members, but what exactly happens if an incident occurs?

Crisis Event Timeline

- Incident
- Emergency Response
- Crisis Management Team Activated
- Normal Operations
- Response Period
- Recovery Period
- Restoration Period
- Life Safety
- Damage Assessment
- Business Continuity Activated
- Data Center Recovery Activated
- Recovery Complete
- Hour "0"
- Recovery Begins
- Recovery in Place
- Back to Normal
- Time

What you see above is the Crisis Event Timeline depicting the various phases of incident response and management.

Emergency response is our initial action and key priority. Emergency Response includes Life Safety and a Damage Assessment in order to prepare for the upcoming Recovery Period.

Once an incident occurs, the Crisis Management Team or Task Force is engaged immediately and remains active throughout the life of the event. During the Recovery Period, technical and business unit teams will work to re-establish our critical business activities.

CONTINUE

Incident Severity Level Chart

The Incident Severity Level Chart below defines the different types of incidents and the severity determination process.

| Category	Description	Notification
Severity 1 (Catastrophe)	Events that significantly impact FRB, e.g., major natural disaster, large scale Information Technology (IT) outages, major IT security breach, pandemic.	Full CMT notified and activated. Continue participation in recovery efforts.
Severity 2 (Crisis)	Events that have a significant impact on a specific area of FRB's business for a limited period of time, e.g., smaller scale IT outages, smaller scale IT security breach.	CMT Task Force notified and activated. Escalate as appropriate. Continue recovery efforts.
Severity 3 (Elevated)	Events that may be resolved through efforts of a few individuals and temporary workarounds, e.g., local transit/weather issues requiring office closure, medical emergency on premises, no impact to business operations.	Marketing and Communications, HR, Information Services, and Corporate Security & Investigations will determine what action will be taken. If outage exceeds critical function Recovery Time Objectives, consider activation of Business Continuity or Disaster Recovery plans.
Severity 4 (Disruption)	Events where observation is necessary, but may not necessarily result into an actual issue. Low probability of occurring.	Only the CMT lead, CMT coordinator and Corporate Security & Investigations should monitor.

There are four levels of incidents from a Severity Level 4 Disruption to a Severity Level 1 Catastrophe. The incident severity will be determined by the Crisis Management Team or Task Force member and the corresponding notifications will be made to either the entire CMT or the CMT Task Force.

Historically, most events have been managed by the CMT Task Force and, thankfully, full Crisis Management Team activations have been rare.

CONTINUE

Crisis Management Team Resources
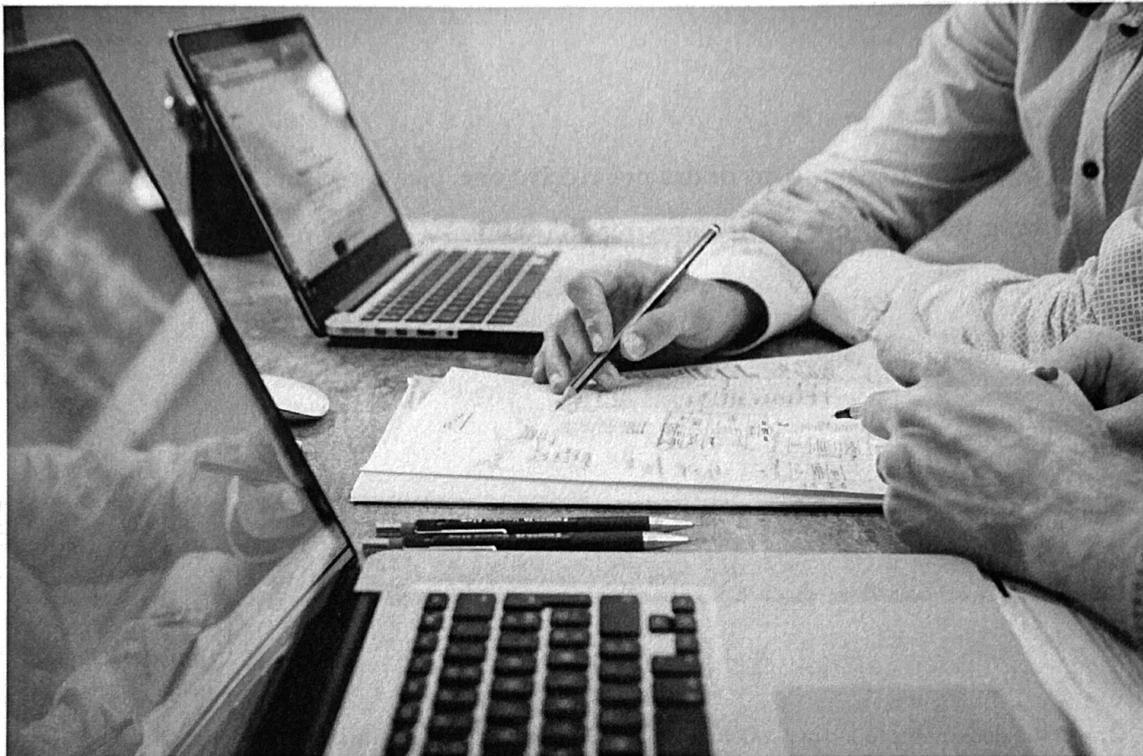
Crisis Management Team Plan and Procedures

In order to better manage each phase of the event timeline, the CMT has

developed predetermined checklists which can be found in the confidential

CMT Plan and Procedures document. These checklists include communication instructions, contact information, and additional instructions for various scenarios. Members of the CMT, Task Force, and Support Staff, receive a copy of the CMT Plan and Procedures quarterly via email. This document should be printed and stored in a secure location that can be easily accessed.

If you cannot locate your copy or did not receive one, please **contact Information Security** at InformationSecurity@firstrepublic.com.

EMAIL INFOSEC

CONTINUE

One of the documents found in the CMT Plan and Procedures is called the Initial Response Checklist. Immediately following the declaration of a Covered Incident, this checklist is used to determine the impact of the incident and to begin collecting information. Topics covered in the Initial Response checklist include:

- Colleague safety.

- Communication Plans.

- The impacts to First Republic by:

  ○ Focusing on our top three priorities (reputation, availability of cash, and the condition of the loan portfolio).

  ○ Establishing an action plan.

- And, if necessary, invoking the Hot Seat Program, which is the internal work area recovery program within First Republic.

Initial Response Checklist

Line	Dial In	Passcode	Host Code
CMT Bridge	(888)-330-1716 (713) 353-7024	2028697	6943
Information Security		7371	
Engineering Bridge Lines	855-208-7957	2711, 4694, 8583	
Tester Bridge Line:		60619	

		Completed	By:
1.	**SAFETY FIRST!** Evacuate *IF* instructed by proper authorities or building management. **If evacuated,** congregate at predetermined assembly points & take a head count. Liaise with floor wardens to ensure all employees were evacuated safely. If evacuation is not required, begin at step 2.	☐	
2.	Identify event & gather preliminary info: Is there an employee safety issue? What sites are impacted? Deploy runners with walkie-talkies to assess incident impact. Which business critical processes are affected? (for a list, *see next section*) What technology is affected? -> is there a DC failover? If yes, 1. Contact a technical point person 2. Designate a Business Unit Test Coordinator, testers, & identify impacted apps. 3. Establish the "testers" bridge line to monitor results. (The start & end times as well as results should be recorded).	☐	
3.	Determine the severity level: MINOR INCIDENT –> **NOTIFY** Task Force. **BANK WIDE**-> **INVOKE** full CMT. **DISRUPTION** -> **MONITOR** & upgrade **LOCALIZED**-> **INVOKE** Task Force. severity level if incident escalates.	☐	
4.	Invoke/Notify* Full CMT or Task Force as prescribed by severity level. Invoke or notify either team using the Enterprise Communication System (https://manager.everbridge.net/dashboard) **Immediately stand up the CMT Bridge Line.**	☐	
5.	Debrief CMT with known information as determined in Step 2. CMT should determine business priorities and establish an action plan. Continue to update team as information becomes available.	☐	

6.	Designate a member of the InfoSec team for the following roles:
	   • Lead scribe, who will assign additional scribes. **Name:** _____
	   • Lead InfoSec & Engineering Contact to establish bridge line. **Name:** _____
	   • Lead InfoSec Coordinator to liaise with Marketing and Comm. **Name:** _____
	   • Lead InfoSec Monitor to monitor InfoSec mailbox during entire incident. **Name:** _____
	   • Evacuation monitors with walkie-talkies (if required) **Name(s):** _____
		☐	

7.	If evacuation occurred in step 1, and reoccupation of the office is not imminent, relocate staff as necessary. (If not continue to step 8). Contact the hot seat coordinator to liaise with CMT to assign seats according to business criticality. Assign staff to monitor evacuated floors / building to prevent unauthorized entry.	☐	
8.	**COMMUNICATIONS:** Communicate to stakeholders (via Enterprise Communication System)* as per Marketing and Communications, using approved channels. Examples of stakeholders: impacted staff, regional/national offices, clients, vendors, etc.	☐	
9.	Delegate tasks and action items to appropriate employees or teams as directed by CMT.	☐	

CONTINUE

Crisis Management Team Event Management Quadrant

In the event of a significant crisis, information can also be captured using the Crisis Management Team Event Management Quadrant. The quadrant is used to keep track of the status of the event and the various action items assigned to personnel. It should be maintained by a Crisis Management Team Support Staff member. This process provides an easy-to-manage method for identifying, assigning, updating, and documenting information or issues associated with the event.

CONTINUE

Event Summary and
Status as of Time

Issues with Status

Timeline of Events

Action Items
with Assignments

CONTINUE

Crisis Communication
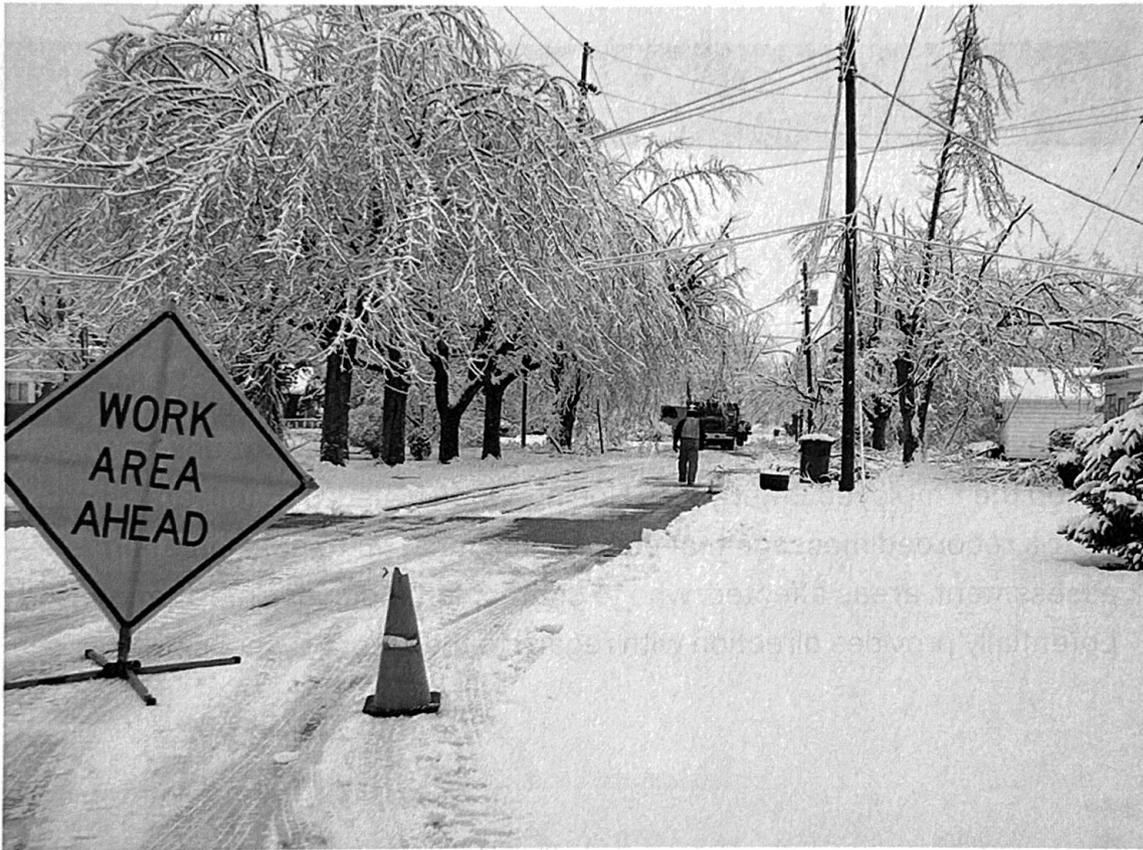
Crisis Communication

Communication is another important factor to consider when responding to a crisis situation. Improper or a lack of communication can not only lead to the spread of misinformation but also cause long-lasting damage to our reputation and brand.

In order to ensure the right message is being conveyed, First Republic's Marketing and Communications department is responsible for crafting all client and enterprise-wide communications.

CONTINUE

Employee Emergency Hotline —

We have established an outbound, one-way method of communication called the Employee Emergency Hotline. Once dialed, our colleagues can hear a recorded message that conveys the most up-to-date situation assessment, areas affected, who to contact for additional information, and potentially provides direction with regard to their work responsibilities.

Emergency Communication System —

For more serious incidents, First Republic utilizes a robust Emergency Communication System that provides communications to colleagues, CMT members, and clients via personal and corporate email, text, and mobile and home phones. In order to account for the safety and well-being of our colleagues during an incident, the Emergency Communication System has

a feature that provides recipients the ability to respond with their acknowledgment and current status.

Contact information is derived from UKG Pro, our HR system of record, so we urge you to ensure your, and your team's, contact information is accurately captured within the system.

Instructions for updating the Employee Emergency Hotline and the Emergency Communication System are located in the Crisis Management Team Plan and Procedures. Due to their importance, each of these systems is tested regularly.

All-Company Email —

Depending upon the incident, the Marketing and Communications department may also send out an all-company email that provides pertinent event information and, if needed, applicable next steps.

Backup Communications —

Additional resources such as two-way radios and satellite phones are available during an incident when a cell signal cannot be found, or the mobile network is down. The location of these communication resources is documented within the CMT Plan and Procedures.

Government Emergency Telecommunications Service

Lastly, the Crisis Management Team also has two other priority-type methods of communication.

The first is called the Government Emergency Telecommunications Service (GETS). When a caller dials a GETS access number from a landline phone, the local carrier recognizes it as a priority call and processes it using special GETS handling instructions.

For the second method of communication, First Republic has subscribed to the Wireless Priority Service (WPS). As the name implies, the Wireless Priority Service will give the caller priority over other calls in a congested cellular network when the probability of completing a normal cellular call is reduced.

Government Emergency Telecommunications Service		**GETS**		**24 Hour Assistance**
Office of Emergency Communications		If your 1-710-627-4387 call fails, try an alternate access number		Help/trouble reporting
		1-888-288-4387	AT&T	1-800-818-4387
John Smith		1-877-646-4387	AT&T	or 703-818-4387
Department of Defense		1-855-333-4387▲	Sprint	**Familiarization Calls**
		1-800-900-4387	Verizon	Make periodic GETS
Dial Access Number:	**1-710-627-4387**	1-855-400-4387▲	Verizon	and WPS test calls to
		▲ Use for GETS calls to toll-free destination numbers		703-818-3924
After Tone, Enter PIN:	**1234-5678-9012**	**WIRELESS PRIORITY SERVICE**		**U.S. Government Property**
		*272 + Area Code + Number + SEND		If found, return to:
When Prompted, Dial:	**Area Code + Number**	From a WPS-Enabled Phone		OEC
		www.dhs.gov/gets	www.dhs.gov/wps		245 Murray Lane SW Mail Stop 0615
		Warning: For Official Use Only by Authorized Personnel		Washington, DC 20528

CONTINUE

Crisis Management Team Exercises

Crisis Management Team Test

In order to ensure our CMT Plan and Procedures, and Communication plans are actually viable and dependable crisis response strategies, First Republic performs an annual tabletop exercise (or test) of the Crisis Management Team.

Testing is designed to exercise our ability to prioritize and address multiple Covered Incidents of unpredictable and escalating nature, while also first ensuring colleague safety and that our top priorities are being met.

Following the test, exercise participants meet to discuss the outcomes of the test and identify opportunities for future improvements. The culmination of these lessons learned discussions are included in a report that is circulated to the Board.

CONTINUE

Wrap-Up
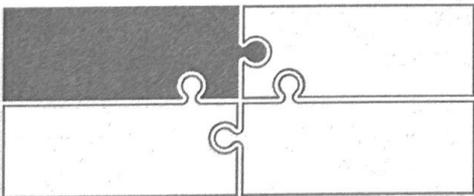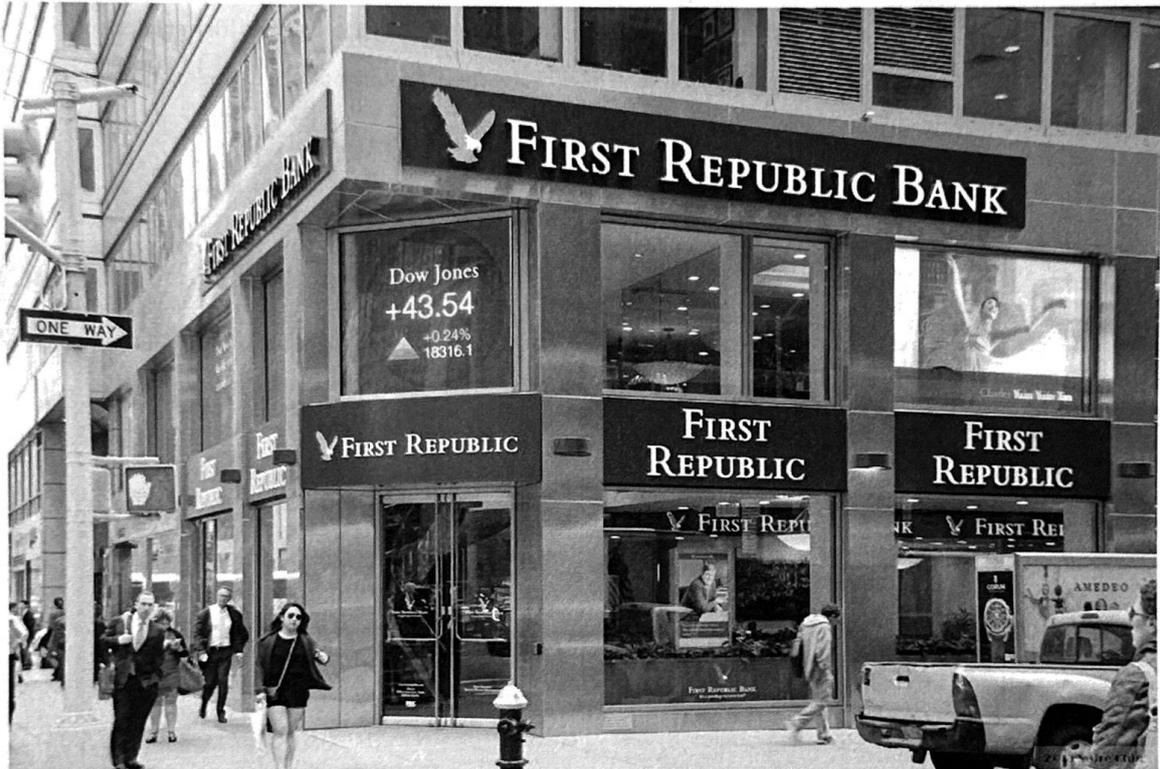
Key Takeaways

We hope this training has helped to familiarize you with the responsibilities, procedures, and resources of the Crisis Management Team.

We would like to reiterate the key takeaways from this training:

- Address life safety first and foremost.

- Understand the Crisis Event Timeline and how to invoke the Crisis Management Team or Crisis Management Team Task Force.

- Understand your role and responsibilities in the event of a Crisis Management Team or Crisis Management Team Task Force invocation.

- Maintain the priorities of First Republic.

- Know the Crisis Communication channels.

- Print and save a copy of the Crisis Management Team Plan and Procedures, and other key confidential resources as needed, for easy reference.

- Manage events through the use of predetermined checklists.

- Participate in Crisis Management Team testing.

CONTINUE

ⓘ   Please reach out to the Business Continuity Management team
with any questions or comments at
InformationSecurity@firstrepublic.com

Quiz

This document includes predetermined checklists and is used by the Crisis Management Team to help manage a crisis.

○ Business Continuity Plans

○ Business Impact Analysis

○ Crisis Management Team Plan and Procedures

Where can I find the Crisis Management Team Plan and Procedures?

◯   On Collaborate

◯   The Floor Warden has a copy

◯   I receive a copy each quarter and if I didn't, I should reach out to Information Security to request it

The full Crisis Management Team should be invoked to handle all crises.

○   True

○   False

If you have any questions about the Crisis Management Team Plan and Procedures or about the Business Continuity Management program, please email:

- ◯ TechnicalSupport@firstrepublic.com

- ◯ InformationSecurity@firstrepublic.com

- ◯ Marketing@firstrepublic.com

Thank You!

Congratulations!

**You have now completed the course:
Crisis Management Team Training 2022 ✔**