



DIGITAL CAPABILITIES RESILIENCE GUIDE

A PRACTICAL FRAMEWORK FOR
CAPABILITY CONTINUITY DURING
DIGITAL DISRUPTION

2026 UPDATE

TERRORISM AND HOMELAND SECURITY COMMITTEE

CONTENTS

The objective is not to protect computers. The objective is to protect mission-essential capabilities.

2026 UPDATE

Developed by **Cedric Patterson**, Chief Fire Administrator, Brazoria County ESD No. 3, and **Sam Greif**, Fire Chief, City of Plano, Texas, Ret., later Deputy City Manager, City of Plano, Texas, Ret., on behalf of the IAFC Terrorism and Homeland Security Committee.

INTRODUCTION	3
PHASE I	
OPERATIONAL SIZE-UP	5
PHASE II	
PREPARE	7
Governance	7
Training	7
Vendors	8
Exercises	8
Artificial Intelligence	8
Declaring Digital Disruption	8
PHASE III	
SUSTAIN OPERATIONS	9
Response Delivery	10
Records & Documentation	11
Business Continuity	11
Community & Coordination	11
PHASE IV	
RESTORE	12
PHASE V	
IMPROVE	14
CONCLUSION	15
DIGITAL CAPABILITIES RESILIENCE TOOLKIT	17
TOOL A	
MISSION CAPABILITY MAP (SAMPLE)	18
TOOL B	
MISSION CAPABILITY VALIDATION EXERCISE	20
TOOL C	
MISSION CAPABILITY VALIDATION RECORD	21
TOOL D	
FIRST 60 MINUTES CHECKLIST	23
TOOL E	
CAPABILITY CONTINUITY DECISION MATRIX	24
TOOL F	
DIGITAL DISRUPTION TABLETOP EXERCISE	25



INTRODUCTION

It is 8:15 on a Tuesday morning. You just sat down with your coffee to open your email. It won't connect. You get up and walk down the hall to your Assistant Chief's office to ask if hers is down too. She says it is. She mentions the staffing software is out too, and she is already working around it by scribbling daily crew assignments on a legal pad. Your cell phone vibrates in your pocket. It's a text from the dispatch supervisor. CAD is dead, 911 isn't routing right, and IT said it might not be isolated. You walk to your vehicle to head over to the dispatch center. The oncoming shift is on the

apron, running through daily equipment checks. Then the station intercom sounds — dispatch has been trying to send E17 and L17 to a reported residential structure fire. No tones have dropped.

You wonder. What else on this network is exposed right now, and how would you know if it's already failing too? Who outside this building needs to hear from you before they hear about it some other way? At what point does this stop being an IT problem, and become something you have to declare?

There wasn't anything one would call different about that morning at the fire station. You didn't have a ransom note on a screen or a hooded

figure at a keyboard. You just had email that wouldn't connect, a legal pad instead of staffing software, a text message, and a station PA broadcast.

That was the whole point. Cyber disruption won't usually announce itself. It will come as a series of small, ordinary failures, and only when they are added together does the picture become clear.

Departments across the country have already experienced exactly these kinds of disruptions — from ransomware attacks that pushed dispatchers onto paper to outages that interrupted CAD, email, payroll, and other mission-essential systems. The details might differ by case, but the leadership challenge does not. These disruptions can cost the department real money and real trust. Consequences include ransom payments, long service gaps, citizen and patient data exposed to people who shouldn't have had access to it. Preparation can't always prevent some of that, but it can determine whether your mission survives it.

This update to the manual is not about computers. It is not about servers, and it is not about firewalls. It is about capability — the ability of your department to dispatch resources, communicate, document care, pay your people, and keep every other commitment you have made to your community. Technology enables that capability. It does not replace it, and it should never be mistaken for it.

The original edition of this publication asked fire chiefs a good question for its time. What should I be asking my IT department? That question still matters, and it is still answered in the pages that

follow. But it is no longer the point. Fire departments once used technology to support the mission. Today, the mission runs on it. CAD, RMS, station alerting, scheduling, payroll, preplans, hydrant data, and patient care reporting. If you take away any one of these, something stops. This guide asks a different, larger question. What do you do when the system you depend on stops working, and no one can tell you when it will start again?

That is not a new kind of problem. It is an old one, wearing a new uniform. When a pump fails, and the crew still needs water on the fire. If a primary channel goes down, and the incident still has to be coordinated. A road closure cannot stop the engine from getting to the fire. There are no time outs. Time won't stand still while we figure it out.

One fire department learned this the summer the military base lost power. The building housing the base's central servers did not support just one agency. It supported nearly every digital capability on the base. The servers themselves sat on generator power, exactly as planned. The air conditioning did not. As the outside temperature climbed into the 90s through the afternoon, so did the temperature inside the server room. The fix wasn't a phone call to the vendor. It was the fire department, running positive-pressure ventilation fans straight into the room, holding the temperature down until public works could get the power back on. The equipment survived. No one had ever validated whether that air conditioning was tied to the generator — not in a preplan, not in an exercise. Exercises validate assumptions. Real incidents expose them. That afternoon, the incident did the exposing.

Exercises validate assumptions. Real incidents expose them.

Five phases follow.

1. **Operational Size-Up** identifies what your department cannot afford to lose.
2. **Prepare** builds the governance, training, and exercises that precede a disruption.
3. **Sustain Operations** — the heart of this guide — addresses how you keep the mission moving while systems are down.
4. **Restore** brings capability back deliberately, not simply quickly.
5. **Improve** ensures the organization is stronger for having gone through it.

Read this the way you would read a preplan. Not cover to cover, and not once. Pull the chapter you need, when you need it. But before you do, go back to that Tuesday morning. Sit with the three questions at the end of it. If you hesitate on even one, that is where to begin.

Not every example in this guide is a documented incident. Some are illustrative scenarios built to teach a decision, not accounts of a specific event. Where a real, named incident is cited, such as Bucks County, Pennsylvania, it is verifiable. Where it isn't named, treat it as a teaching scenario.



PHASE I OPERATIONAL SIZE-UP

What capabilities must never stop?

During a routine drill, a battalion chief was asked whether her crews could still complete patient care documentation if the tablets went dark. She assumed they could. She had never verified it. The answer that day was no — most of her younger paramedics had never completed a paper patient care report in their careers. They knew how to

complete documentation. They knew which buttons to press and which screens to open. What they had never learned was why the paper process still existed.

Every fire chief believes there is a plan. Fewer chiefs have confirmed the plan is actually true. That gap

often starts long before anyone thinks to test it.

A plant operator flipped a switch every day at 1400 because someone had told him to flip the switch every day at 1400. He didn't know what it did. He didn't know who flipped it back off every day, or why, or what would happen if the switch itself failed instead of simply waiting for him. He knew the procedure. He didn't understand the capability it supported.

The battalion chief's crews weren't any different. They understood the software. They had never been asked to understand the capability the software provided. When the software disappeared, so did their confidence.

Knowing what to do is not the same as understanding the capability it enables. Operational Size-Up does not ask you to define your department's mission. You have already done that work. It lives in your Standards of Cover, your community risk assessment, your strategic plan, or your accreditation documentation — whichever of these your department maintains. This phase asks a narrower question: what capabilities make those existing commitments possible, and what happens to each of them if the systems behind it fail?

If your department has none of the above — no formal Standards of Cover, no accreditation, no strategic plan — the same result starts with three questions.

1. *What services does your department provide?*

2. *Which of those services cannot stop, regardless of circumstance?*

3. *What capabilities make those services possible?*

Answer those honestly, and you have already completed the hardest part of this chapter.

The tool for the rest of the work is the Mission Capability Map.

FROM TOOL A – MISSION CAPABILITY MAP (SAMPLE)

MISSION-ESSENTIAL CAPABILITY	MANUAL ALTERNATIVE	VALIDATED?
911 Call Processing Dispatch Resources Incident Command and Accountability Incident Documentation Staffing and Scheduling	Direct line to backup PSAP	☐ Never Tested
	Paper dispatch cards	☒ Validation Exercise
	Tactical worksheet, grease pencil	☒ Tabletop
	Paper incident reports	☒ Tabletop
	Whiteboard, phone tree	☒ Validation Exercise

Notice the last column. It is labeled Validated?, not Assumptions. That distinction matters. A chief cannot manage an assumption — an assumption is invisible until something exposes it, the way one department discovered its server room cooling was never tied to generator power the day its base lost power in the middle of summer. A chief can manage a confidence level: Never Tested; Tabletop; Exercise; Real-World Event. Every entry on your Mission Capability Map deserves an honest answer, even when the honest answer is uncomfortable.

Before moving on, complete a first pass through your Mission Capability Map. It won't be perfect. It doesn't need to be. An incomplete map is still worth far more than none at all.



PHASE II

PREPARE

How does the department prepare before capabilities are threatened?

The network had been compromised for nearly an hour before anyone realized no one had the authority to disconnect the affected systems. IT wanted approval from leadership. Leadership assumed IT had already acted. Legal wanted to understand the impact before anyone moved. Operations just wanted CAD back. Everyone was waiting on someone else.

The decisions that matter most during an incident are usually made long before the incident begins.

GOVERNANCE

Who owns this decision before the incident happens? Not after. Not during, when the phone is already ringing and three people are waiting on each other to act. Before. If your department cannot answer who has the authority to disconnect a compromised system, declare degraded operations, or speak publicly, governance is not a policy gap. It is an operational one, and it will surface at the worst possible time. When authority is unclear before an incident, time becomes the first casualty during one.

TRAINING

Don't worry about memorizing technical terms. Understand what they mean operationally. If someone steals your password, what stops them from logging into your network? That's the

question that matters. Chiefs don't need to become cybersecurity experts. They need to understand enough to make good operational decisions and ask better questions.

VENDORS

Every vendor says reliable. Every vendor says secure. Every vendor says redundant. Ask every vendor:

1. Can we continue operating without your product?
2. How do we access our own data if your service goes down?
3. How long can we realistically operate if your cloud platform is unavailable?
4. When was your disaster recovery plan last exercised?
5. How often have you successfully restored a customer from backup?

The answers to the first two will tell you more than the rest of the presentation combined.

EXERCISES

Schedule real practice on the manual alternative, the same way any other proficiency requirement gets scheduled, not narrated and not pretended. On a set date, the department actually operates without the system for a defined period, and everyone on shift knows it going in. Watch who adapts and who struggles, and pay attention to what the manual alternative was missing that nobody noticed until someone actually tried to use it. Those are the things worth exercising. A department that has never actually dispatched from paper cards will not handle it well the first time it is real, and the first time should never be the real one.

ARTIFICIAL INTELLIGENCE

AI is a force multiplier for organizations that already have good judgment. It is a force multiplier for bad decisions too. Used well, it drafts policy language, summarizes after-action reports, writes job announcements. It builds tabletop exercise injects. Work that used to take hours now takes minutes, and chiefs get that time back for the decisions only a chief can make. Used carelessly, it hallucinates facts with total confidence. It exposes protected information typed into a public tool without a second thought. It produces policy that gets adopted without anyone reviewing it first. The old rule was think before you click. The rule now is think before you prompt — because what you type into an AI system can leave your organization as easily as what you click on.

DECLARING DIGITAL DISRUPTION

Ask yourself. Have you lost:

CAD? RMS? Station alerting? 911 routing?
Network authentication? Cloud access?
Scheduling? Payroll? Email? Public website?
Identity systems? Vendor support? Power to your data center? Communications between IT and Operations?

Or — has confidence in your systems been lost, even if you don't yet know why?

Sometimes uncertainty is the incident. That last one matters most. You do not need a confirmed cause to declare. You need a reason to stop trusting what you cannot currently verify.

Run this exercise against a real capability, not a hypothetical one. You'll learn more about how your department actually operates than you will from another policy review. The purpose isn't to test technology. It's to test people.



THE HEART OF THIS GUIDE

PHASE III

SUSTAIN OPERATIONS

How does the department keep the mission moving when the technology fails?

RESPONSE DELIVERY

Dispatch
Communications
Station alerting
Command

RECORDS & DOCUMENTATION

Incident documentation
EMS documentation

BUSINESS CONTINUITY

Staffing
Payroll
Logistics
Fleet

COMMUNITY & COORDINATION

Mutual aid
Public information
Inspections and prevention
Investigations

The dispatch supervisor waited. CAD had gone down eleven minutes earlier, and everyone in the room believed IT was close to a fix. Nobody had made the call to switch to paper. Nobody wanted to be the one to admit CAD wasn't coming back soon. By the time someone finally pulled the run cards, four calls were already backed up in the queue.

IT was doing its job. Nobody else was doing theirs.

A cyber incident is two incidents happening at once, not one incident with two phases. IT restores the system. Command sustains the mission. When agencies share jurisdictional or functional responsibility for the incident, determine whether Unified Command applies, with IT standing up a Cyber Branch under Operations rather than a second, parallel command. This phase is organized around what your department has to keep doing, not around who owns which piece of technology.

III

IT restores the system. Command sustains the mission.

RESPONSE DELIVERY

Dispatch: CAD can go down from ransomware, a power outage, or a vendor's cloud outage — the cause doesn't change what has to happen next. During the January 2024 ransomware incident in Bucks County, Pennsylvania, dispatchers kept working by hand while CAD was down. The technology failed. Dispatch did not. Every minute spent hoping CAD comes back is another minute emergency calls continue to stack up. Radio dispatch, paper run cards, or mutual aid dispatch will do it if CAD can't. Pick at least two your department can run today, print the cards, and confirm the person on shift tonight has actually filled one out before, not just been shown one.

Communications: If the primary radio system goes down, crews on scene still need to talk to each other and to command. Every department needs a second path already chosen: a specific backup channel, cell or satellite where coverage allows it, a runner if nothing else works. Confirm

every crew already knows that channel number, and that they've used it, not just heard about it in a briefing.

Station alerting: Tones don't drop — whatever knocked out the alerting system, crews still have to get moving. A backup method needs to already exist: a phone tree, a runner from dispatch to the apparatus bay, a manual page over a PA system that doesn't share the network. Confirm every station knows its fallback, and that it's actually been used once, not just posted on a wall.

Command: If the incident management platform disappears, the incident is still running. A tactical worksheet and a grease pencil can track who's on scene, what they're doing, and who's accounting for them, the same way they did before any of this was digital. An incident without accountability doesn't just run less efficiently. It runs unsafely. Every officer who could take command should already know how to run that board by hand, not find out how during the incident that took the platform down.

RECORDS & DOCUMENTATION

Incident documentation: RMS goes down and incidents still have to be recorded for legal and insurance purposes. Paper incident reports need to be on hand at every station, and someone needs to remember how to fill one out completely, not just where the forms are kept.

EMS documentation: ePCR platforms go down and patient care still has to be documented and handed off. Paper PCR forms need to be stocked at every station, and crews need to have actually completed one in the past year, not just been issued the pad.

BUSINESS CONTINUITY

Some capabilities must survive the first operational period. Others become critical only after days of sustained disruption, and continuity depends as much on the places a department operates from as on the systems it runs.

Staffing: Scheduling software goes down and shifts still have to be filled. Know who can build tomorrow's schedule on a whiteboard, and how vacancies get communicated without the app.

Payroll: The payroll system goes down and people still have to get paid on time. Payroll isn't just about checks. It's about trust — miss it once during a prolonged disruption, and rebuilding that confidence takes far longer than the outage did. Know whether payroll can run from a manual process or a recent backup export, and how many pay periods that buys before it becomes a real problem.



Logistics: Ordering and inventory systems go down and stations still need supplies. Know who can place an order by phone, and which vendors will take one without the portal.

Fleet: Maintenance tracking and fueling systems go down and apparatus still has to stay in service. Know how maintenance gets scheduled and fuel gets tracked without the software, even if it's a clipboard for a week.

COMMUNITY & COORDINATION

Mutual aid: Your systems are down and a neighboring department's aren't. Mutual aid dispatch and coordination still work by phone and radio. Confirm your partners know how to reach you if your normal channels are the ones that failed.

Public information: Your website and CAD-fed alert systems go down and the public and elected officials still need accurate information. Know your fallback channel — a phone tree, local media contacts, social media posted from a backup device — before you need it.

Inspections and prevention: Inspection software and plan review systems go down and life-safety

inspections still have to happen. Paper checklists and paper permit tracking keep the work moving until systems return.

Investigations: Case management systems go down and origin-and-cause work still has to hold up in court. Chain of custody and documentation discipline don't change because the software did — they just move to paper.

None of these fallbacks are complicated. Most existed long before the software they replace. The challenge is not inventing them during an incident. It is validating them beforehand.

Every capability in this phase can be tested without waiting for a cyberattack. Turn off the system. Run the operation anyway. Learn what breaks while the consequences are small enough to fix.

Sustaining operations is only half the mission. Once the incident is contained and the immediate disruption has stabilized, the department turns to restoring systems deliberately, documenting lessons learned, and improving resilience before the next disruption.

III



PHASE IV RESTORE

How does the department safely retire contingency operations and return to normal?

IV

CAD comes back online at 1400, after six hours running on paper. Nobody in dispatch is celebrating yet. The question isn't whether the system works. It's whether anyone is ready to trust it again.

Technology returning is not the end of the incident. IT restores systems. Leadership decides when normal operations actually resume — which

manual workarounds stay in place a little longer, which systems get trusted immediately, what needs validation before crews depend on them again, and how that transition gets communicated across the department.

The mission never stopped during Phase III.

Restoration isn't about getting it back. It's about safely retiring the alternate methods that were keeping it going.

Normal operations should be restored in the same order the department prioritized them before the incident — not whichever system happens to get fixed soonest. As each one returns, validate it before removing the manual workaround behind it. Coming back online and being trustworthy are not the same event, and treating them as the same is how new risk gets introduced by the recovery itself.

Then comes the part that's easy to skip past: operational reconciliation. A contingency process isn't finished when the software returns. It's finished when every action taken under that contingency has been accurately carried forward into the department's permanent record. Paper run cards, paper PCRs, a handwritten accountability board, a manual payroll adjustment — none of those are scratch paper. They are the authoritative record until someone reconciles them into the system that replaces them. CAD

coming back at 1400 doesn't mean the incident is over. It means someone still has to make sure every call between 0800 and 1400 exists in the permanent record, correctly.

Chiefs don't direct the technical recovery. They oversee it — what vendors are restoring, what has and hasn't been validated, what remains degraded despite appearing operational. Coordination with insurance, legal counsel, and law enforcement continues through this phase, and nothing about restoring systems should compromise evidence that was preserved earlier or complicate a claim that's still open.

The incident is over when the department has confidence, not simply functionality: mission-essential systems validated, manual processes intentionally retired rather than just abandoned, records reconciled, personnel clear on the return to normal, and any remaining risk known and accepted rather than quietly ignored.

That declaration belongs to leadership, informed by IT — not the other way around.

That declaration belongs to leadership, informed by IT — not the other way around.

Every workaround used during the incident is now evidence. Some of them worked exactly as intended. Others exposed an assumption that

turned out to be false. The next phase asks how those lessons become preparation for the next incident.

Technology returning is not the end of the incident.



PHASE V

IMPROVE

What changes before the next incident?

CAD is back. Payroll is caught up. Every paper PCR has been entered. The insurance carrier has closed its file. The phones have stopped ringing. Somebody asks, “Can we finally put this behind us?”

That question is exactly where improvement gets skipped. Not because anyone is negligent — because the pressure that made the incident urgent is gone, and urgency was the only thing keeping the phase before this one moving. Every incident leaves two outcomes behind: the services your department delivered, and the lessons it earned. One is complete when the emergency ends. The other is only complete when those lessons change how the department prepares for the next one.

This phase isn’t about becoming a better department in general. It’s narrower than that: how does this incident permanently improve your ability to preserve mission capability the next time something takes the technology away?

Start with questions, not a form. Which assumptions proved true? Which proved false? Which workaround worked better than anyone expected? Which capability turned out to be more fragile than the department believed? What surprised the people who lived through it? Every workaround used in Phase III and reconciled in Phase IV is an experiment your department didn’t intend to run, and the answers to those questions are the data it produced.

The lessons that come out of those questions don’t all carry the same weight. Some change behavior — a habit, a checklist, a thing a crew now does differently without needing a policy to tell

V

them to. Some change policy — a decision about who has authority, formalized so it doesn't depend on memory next time. Some change investment — a system, a contract, a piece of infrastructure that costs money and takes longer than either of the first two. Behavior changes first, because it's free and it's immediate. Investment changes last, because it should be justified by what the first two already proved matters. A department that waits for budget approval before it changes anything has confused the cheapest fix with the hardest one.

Before closing the incident, return to the Mission Capability Map. The version completed in Phase I reflected what the department believed about itself. The incident just tested every one of those

beliefs against reality. Update the map to reflect what is now actually known — which manual alternatives held up, which ones didn't, which downtime estimates were accurate and which were optimistic, which Validated? entries can honestly move from Never Tested to Real-World Event. The map doesn't get replaced. It gets more accurate.

Only then should the incident be considered complete. The objective was never to survive one cyber incident. It was to become a department that performs better during the next one. The next incident should begin with a more accurate understanding of your department than the last one did.

The map doesn't get replaced. It gets more accurate.

CONCLUSION

This guide has one practical purpose: helping you find out, before an incident forces the question, whether your department can continue its mission when the technology behind it stops working.

Turn off the system. Run the operation anyway. That's the one thing every phase in this guide has been pointing toward — a specific, answerable question about your own department that most chiefs have never actually asked.

The Mission Capability Map you began in Phase I provides a way to answer that question, one capability at a time. Some of it will hold. Some of it won't. Better to find out now, on a Tuesday like any other, than during the one that isn't.

Turn off the system. Run the operation anyway.



DIGITAL CAPABILITIES RESILIENCE TOOLKIT

A PRACTICAL FRAMEWORK FOR
CAPABILITY CONTINUITY DURING DIGITAL DISRUPTION

DIGITAL CAPABILITIES RESILIENCE TOOLKIT

This toolkit exists for one reason. Reading a guide about operational resilience is not the same as being able to prove your department has it. The five phases of this publication teach a way of thinking about mission-essential capabilities and the technology that enables them. This toolkit is where that thinking becomes something you can print, fill out, and use.

Six tools make up the toolkit. The Mission Capability Map is provided in both a completed sample and a blank working version, which is why the tools that follow are labeled Tool A through Tool F rather than one through six.

The order below is the order you actually use them in.

Start with Tool A, the Mission Capability Map. Building it is a one time size up. List out every mission essential capability your department depends on, and give each one a first pass entry. Nothing gets tested at this stage. You are building the inventory that tells you what exists and what it depends on.

Once the Map exists, pick one capability from it and run Tool B, the Mission Capability Validation Exercise. This is where the manual alternative actually gets used, for real, on a defined date, not narrated or pretended.

After the exercise, complete Tool C, the Mission Capability Validation Record, for the capability you just tested. The Record documents exactly what happened during the exercise and updates the relevant row on the Map.

Repeat that sequence, one new capability each quarter, until your department has a baseline across every mission essential capability. Tier 1

capabilities get revisited at minimum annually after that.

Tool D and Tool E are not planning tools. They are what you reach for during an actual incident. The First 60 Minutes Checklist structures the first hour after Digital Disruption is declared, and it is not IT's checklist, it is the operational one. The Capability Continuity Decision Matrix answers a narrower question. When more than one capability fails at once, which gets attention first.

Tool F, the Digital Disruption Tabletop Exercise, runs on its own separate calendar, outside the quarterly cycle above. It brings in outside stakeholders, fire, police, EMS and hospital partners, emergency management, IT, mutual aid, and federal partners where warranted, to test coordination across agencies rather than a single department's own capability.

WHERE EACH TOOL LIVES.

Planning Toolkit, kept in a preparedness binder. Mission Capability Map. Mission Capability Validation Exercise. Mission Capability Validation Record. Cyber Incident Tabletop Exercise.

Operational Job Aids, kept in the command vehicle. First 60 Minutes Checklist. Capability Continuity Decision Matrix.

None of this is new. Most of it existed in some form before any of this was digital. The work is not inventing these processes. It is proving they still work.

TOOL A

MISSION CAPABILITY MAP (SAMPLE)

A

Confirm the manual alternative does not depend on the same power source, network, vendor, or authentication system as the primary one. A backup that shares the dependency that just failed is not actually a backup.

MISSION-ESSENTIAL CAPABILITY	SUPPORTING SYSTEMS	MANUAL ALTERNATIVE	MAX ACCEPTABLE DOWNTIME	VALIDATED?	IN POLICY?
911 Call Processing	911 system, CAD interface	Direct line to backup PSAP	Minutes	☐ Never Tested	☐ Yes ☐ No
Dispatch Resources	CAD	Paper dispatch cards	Minutes	☒ Validation Exercise	☐ Yes ☒ No
Station Alerting	Automated tone and alerting system	Phone tree, runner to apparatus bay	Minutes	☐ Never Tested	☐ Yes ☐ No
Crew Communications	Primary radio system	Secondary channel, runner if needed	Minutes	☐ Never Tested	☐ Yes ☐ No
Incident Command and Accountability	Incident management software	Tactical worksheet, grease pencil	Minutes to hours	☒ Tabletop	☐ Yes ☐ No
Mutual Aid and Interagency Coordination	Shared radio and CAD interoperability	Direct phone lines to partner agencies	Minutes to hours	☐ Never Tested	☐ Yes ☐ No
Incident Documentation	RMS	Paper incident reports	72 hours	☒ Tabletop	☒ Yes ☐ No
Patient Care Documentation	ePCR platform	Paper PCR forms	72 hours	☐ Never Tested	☐ Yes ☐ No
Staffing and Scheduling	Scheduling software	Whiteboard, phone tree	24 hours	☒ Validation Exercise	☐ Yes ☒ No
Payroll	Payroll and HR system	Manual process or backup export	One pay period	☐ Never Tested	☐ Yes ☐ No
Logistics and Supply	Ordering and inventory system	Phone orders to known vendors	72 hours	☐ Never Tested	☐ Yes ☐ No
Fleet Readiness	Maintenance tracking and fueling system	Manual maintenance log, paper fuel log	24 hours	☐ Never Tested	☐ Yes ☐ No
Public Information	Website, CAD fed alert system	Phone tree, local media contacts	Hours	☐ Never Tested	☐ Yes ☐ No
Inspections and Prevention	Inspection software, plan review system	Paper checklists, paper permit tracking	One week	☐ Never Tested	☐ Yes ☐ No
Investigations	Case management system	Paper case files, chain of custody log	One week	☐ Never Tested	☐ Yes ☐ No

Max Acceptable Downtime assumes the manual alternative is already in use and the capability is continuing by other means. For documentation entries specifically, the interval is how long the paper record can stand in before it must be reconciled into the permanent system, not how long the underlying work itself may be delayed.

Next step. Select one mission-essential capability, run a Mission Capability Validation Exercise (Tool B), and complete a Mission Capability Validation Record (Tool C) with the result.

TOOL A

MISSION CAPABILITY MAP (BLANK TEMPLATE)

A

MISSION-ESSENTIAL CAPABILITY	SUPPORTING SYSTEMS	MANUAL ALTERNATIVE	MAX ACCEPTABLE DOWNTIME	VALIDATED?	IN POLICY?
				☐ Never Tested ☐ Tabletop ☐ Validation Exercise ☐ Real-World Event	☐ Yes ☐ No
				☐ Never Tested ☐ Tabletop ☐ Validation Exercise ☐ Real-World Event	☐ Yes ☐ No
				☐ Never Tested ☐ Tabletop ☐ Validation Exercise ☐ Real-World Event	☐ Yes ☐ No
				☐ Never Tested ☐ Tabletop ☐ Validation Exercise ☐ Real-World Event	☐ Yes ☐ No
				☐ Never Tested ☐ Tabletop ☐ Validation Exercise ☐ Real-World Event	☐ Yes ☐ No
				☐ Never Tested ☐ Tabletop ☐ Validation Exercise ☐ Real-World Event	☐ Yes ☐ No
				☐ Never Tested ☐ Tabletop ☐ Validation Exercise ☐ Real-World Event	☐ Yes ☐ No

Max Acceptable Downtime assumes the manual alternative is already in use and the capability is continuing by other means. For documentation entries specifically, the interval is how long the paper record can stand in before it must be reconciled into the permanent system, not how long the underlying work itself may be delayed.

Blank working version. Print or duplicate this page and complete one row per mission-essential capability.

TOOL B

MISSION CAPABILITY VALIDATION EXERCISE

B

Internal. Fast. One capability, one department, no outside stakeholders. The goal is not to test whether a backup system activates. It's to test whether people can adapt when the failure doesn't match the plan exactly.

SCHEDULING IT

- Assign a set date each quarter. Pick one mission-essential capability from the Mission Capability Map.
- On that date, the department operates using the manual alternative for a defined period. If the capability is dispatch, dispatch works from paper cards for the defined period. If the capability is documentation, crews complete paper PCRs and incident reports for that shift's calls, then reconcile them afterward.
- Put it on the schedule the same way any other proficiency requirement gets scheduled.

RUNNING IT

- Confirm at the start of the shift that everyone knows the manual alternative is in use for the defined period.

- Let people work the way they actually would if the system were down.
- Note where the manual alternative was slow, unclear, or missing something it needed.

AFTER THE SESSION

- Which parts worked as expected. Which did not.
- Anything discovered that isn't already reflected on the Mission Capability Map gets corrected there.
- Complete a Validation Record for the capability tested.

FREQUENCY

- Test one new capability each quarter until the department has a baseline across every mission-essential capability, and revisit Tier 1 capabilities at minimum annually after that.

Exercise output. Complete a Mission Capability Validation Record (TOOL C) and update the Mission Capability Map (TOOL A).

TOOL C

MISSION CAPABILITY VALIDATION RECORD

C

This is where a Validation Exercise becomes proof rather than something that just happened and got forgotten. Every time a capability is tested, whether through a scheduled drill, a tabletop discussion, a coordinated exercise, or a real incident, this record captures what actually happened, who was involved, what fell short, and what changes before the next test. Completing one is what allows the Mission Capability Map to move from an assumption to an honest answer.

CAPABILITY.

The mission-essential capability being tested, pulled directly from the Mission Capability Map. One record per capability, not one record covering several.

MANUAL ALTERNATIVE.

The specific fallback being validated today. If a capability has more than one fallback, complete a separate record for each rather than validating them together.

ASSIGNED TO.

Tracks the validation status of this capability. Accountability for all mission capabilities remains with the Fire Chief.

WHO PERFORMS IT.

The role or position expected to actually execute the manual alternative during a real incident. Often different from who's Assigned To.

WHERE MATERIALS ARE KEPT.

Physical location, specific enough that someone unfamiliar with the station could find it.

WHEN LAST TESTED.

The date of this test. If this is the first evaluation, record today's date rather than leaving the field blank.

METHOD.

☐ Tabletop ☐ Validation Exercise ☐ Real-World Event

Tabletop means the capability, policy, or coordination process was discussed but not physically performed.

Validation Exercise means the department performed the manual alternative for this single capability, live.

Real-World Event means an actual disruption required the alternative to be used, and is the strongest possible answer.

WHAT ACTUALLY HAPPENED.

A factual account, not a summary judgment. "Dispatcher located paper cards in 40 seconds, correctly logged three calls, missed the fourth" is useful. "Went fine" is not.

WHAT FAILED OR FELL SHORT.

Specific enough that someone who wasn't in the room understands exactly what to fix.

CORRECTIVE ACTION.

What will change before the next test. If nothing needs to change, say so explicitly.

NEXT VALIDATION DATE.

A specific date, not "annually." A date on a calendar gets scheduled.

EVALUATOR.

Whoever observed and is vouching for what's written above, ideally not the person Assigned To this capability.

After completing this record. Update the Validated? column on the Mission Capability Map (TOOL A) and schedule the next Mission Capability Validation Exercise.

C

TOOL D

FIRST 60 MINUTES CHECKLIST

DONE	MINUTES	ACTION	WHAT THIS CONFIRMS
☐	0-10	Confirm what's actually down, not suspected, confirmed	Prevents committing to manual operations for a system that's actually fine, or missing a second system that's also down
☐	0-10	Notify the officer or supervisor in each affected function	Every affected function needs its own person aware before that function can respond correctly
☐	0-10	Determine whether the incident requires Unified Command or another multi-agency coordination structure	Check which agencies share jurisdictional or functional responsibility for this incident, and which need coordination, liaison, or notification without becoming part of Unified Command
☐	0-10	Make the call to shift to manual procedures now, or hold and monitor	Check against the Max Acceptable Downtime for the affected capability, and don't wait if downtime is measured in minutes
☐	10-30	Confirm every affected station or unit has what it needs to operate manually	Checks against the Manual Alternative column, confirming the fallback validated on paper is actually present right now
☐	10-30	Confirm the secondary communications path is in use, not just available	"Available" and "in use" are different, and this confirms people have actually switched
☐	10-30	Assign someone to track what's happening, not to fix it	Without a dedicated tracker, no one can accurately complete the Validation Record or Phase IV's reconciliation later
☐	10-30	Identify who's talking to IT and who's running operations, and confirm they are not the same person	A cyber incident is two incidents at once, and one person can't run both without one suffering
☐	30-60	Notify command staff not yet looped in	Confirms notification reached everyone with a need to know
☐	30-60	Determine whether this affects mutual aid, police, or hospital partners	Checks against known mutual aid and interagency dependencies. A disruption involving shared or connected infrastructure may affect partner agencies before they realize it.
☐	30-60	Begin the public information conversation internally	Confirms PIO is prepared before pressure to release information increases
☐	30-60	Confirm legal, insurance, and law enforcement notification requirements	Some reporting obligations have time limits that start running now
☐	End of hour	Confirm every capability still needed today has an assigned manual method and a responsible person	Final check against the Mission Capability Map
☐	End of hour	Set a specific check-in time to reassess	"When it's fixed" isn't a time

D

TOOL E

CAPABILITY CONTINUITY DECISION MATRIX

This tool exists for the moment more than one thing fails at once. It answers a single question. Which capability gets attention first, right now.

Work down the tiers in order. If the failure delays help or puts crews or the public at risk, it's tier one, and everything else waits. If it doesn't rise to that level, move to the next tier and ask its question, continuing down until one applies. If two capabilities land in the same tier at the same time, the tie break rule at the bottom settles it, whichever one has the shorter Max Acceptable Downtime on the Mission Capability Map gets handled first.

1. LIFE SAFETY

Does the failure of this capability stop 911 processing, dispatch, or station alerting, so crews cannot even begin moving toward the emergency?

2. INCIDENT COORDINATION

Does the failure of this capability show once crews are already moving or already on scene, and keeps them from staying in contact with each other or with command?

3. MISSION CONTINUITY

Does the failure of this capability threaten operations over the next hours or days, without an immediate life safety impact.

4. ADMINISTRATIVE CONTINUITY

Does the failure of this capability affect the organization without affecting today's response?

TIE BREAK RULE

If two capabilities fall in the same tier, address the one with the shorter downtime first.

E

TOOL F

DIGITAL DISRUPTION TABLETOP EXERCISE

Internal validation asks whether your department can perform a capability. This exercise asks a different question. Can your community sustain coordinated operations when a cyber incident spans multiple agencies at once?

WHO SHOULD BE IN THE ROOM

- Fire Chief, operations, IT liaison
- Police
- EMS and hospital partners
- Emergency Management
- IT and cybersecurity, internal or contracted
- Mutual aid partners
- Public information officer
- Legal counsel
- Vendor representatives, where a shared system is involved
- Federal partners, FBI or CISA, where the scenario warrants it

If a name can't be attached to a chair for one of these, that's a finding before the exercise even starts.

BUILDING IT

- Whenever possible, build from an existing HSEEP-compliant exercise package rather than starting from a blank page. Several federal and state partners publish free tabletop exercise packages that can be customized to local

systems and dependencies. CISA's Tabletop Exercise Package, or CTEP, is one example.

- Customize the scenario to reflect systems and dependencies specific to your department and community, using the Mission Capability Map as the source of what actually matters to test.

RUNNING IT

- Plan for two to four hours, discussion-based.
- Introduce the scenario in stages. An initial disruption, then a complication, then a longer-term consequence.
- Ask what each stakeholder would actually do, not whether the room agrees on a plan in the abstract.

AFTER THE EXERCISE

- Complete an After-Action Report identifying what worked, what didn't, and what wasn't tested because nobody thought to ask.
- Update the Mission Capability Map and Validation Records for any capability the exercise exposed a gap in. This counts as a Tabletop Exercise on the Method field.
- Set a date for the next one.

This exercise validates relationships and interagency plans. It does not replace the Mission Capability Validation Exercise (TOOL B). A department still needs to test its own capabilities on its own schedule.

