A Guide to Building Organizational Resilience:
How to Navigate Emergencies and Disruptions to Maintain Business Continuity
Notes

This document is provided for informational purposes only. It represents the current product offerings and practices from AWS as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers, or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.
Contents

Introduction

Lessons learned from COVID-19

Building a resiliency framework: Technology and cultural best practices
  Part one: Five organizational pillars of resiliency
  Part two: Building a culture for organizational resiliency

Five technology pillars for resiliency and customer case studies
  Remote workforce enablement
  Standing up emergency call centers
  Building trust with real-time communications
  Real-time data analytics for crisis prioritization
  Emergency backup and recovery of mission-critical systems

A prioritization checklist for leaders

Conclusion

Additional Resources
  AWS Partners
  AWS Tools
  Additional customer stories
Introduction

This eBook serves as a guide for public sector organizations that are looking to build a long-term plan for organizational resiliency and business continuity despite unplanned emergencies. While disruptive events are challenging for any organization, sudden and large-scale incidents such as natural disasters, IT outages, pandemics, and cyber-attacks can expose gaps in technology, culture, and organizational resiliency. Even smaller, unexpected events such as water damage to a critical facility or electrical outages can negatively impact your organization if there is no long-term resiliency plan in place. These events can have significant consequences for your employees, stakeholders, and mission. It can result in a loss of finances, productivity, and trust with citizens and customers, creating lasting reputational damage.

For organizations serving the public, disasters and emergencies can derail missions and critical emergency response, public safety, and public health services. Unfortunately, many organizations move from crisis to crisis with short-term fixes, without addressing the long-term strategy for resilience and business continuity.

This guide highlights lessons learned from the COVID-19 pandemic, top areas of disruption to mitigate with long-term planning, and the steps and frameworks necessary to build a more durable organization. The eBook also shares the latest cloud-based IT technologies to support resiliency with customer examples and additional resources from Amazon Web Services (AWS).
Supporting employees and tapping expertise

Managing IT and telecommunications often depends on always-on infrastructure, which is more costly and challenging to build without the use of cloud computing – the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. What happens when employees are unable to address the emergency and do their jobs? If some of your employees are specialists whose expertise is hard to replace, staffing concerns compound the problem. Certain government systems still run on the legacy 60 year-old IT technologies called mainframes, which rely on aging software languages such as COBOL. What happens if the mainframe software engineer managing your social assistance program database or health benefits database is stranded in high water or out sick?

Most public sector organizations do not support 24/7 staffing, with many essential workers lacking telework equipment such as laptops, headsets, and the software and identity verification tools to work through an emergency. These variables must be considered in your long-term plan as you build resiliency into your organization’s workforce.

Access to data for real-time situational awareness

During a disruption, key decision-makers require access to real-time data in order to prioritize decisions and funding. For example, local fire departments, hospitals, and police need data-insights to prioritize resources. With budgets under a microscope, financial agencies may need new data streams to look for fraud in areas such as loan applications, financial aid requests, or unemployment claims. Stakeholders tracking and sharing this data, and those using this data, may be internal or external and may lack access to it when they need it most.
Organizations should test data sharing and inter-system data sharing (or data interoperability) before a crisis. In addition, organizations should test auditing requirements mandated by agencies that fund emergency management so administrators can access funding when needed. Systems that house data and the data itself should be prioritized and ranked by all departments collaboratively, prior to an emergency, so that organizations can build resiliency for the most critical systems first.

**Lack of financial agility**

A challenge that is unique to public sector organizations is the lack of financial agility. Public sector organizations run on pre-determined annual budgets. Gaining access to incremental or emergency funds can take an act of congress. For educational institutions, funds may require an emergency bond and vote to free up capital for an emergency, while state and federal agencies might need to wait for legislation to release funds. The latter may also have to deal with political decisions that may not align with the priorities presented by the data. Public sector organizations should look to carve out funds for resiliency projects to help address emergencies before they happen.

**Lack of planning**

Despite many emergencies throughout the years, it is uncommon to find an organization that has strategized, planned, tested, and implemented a purpose-built resiliency plan. Most organizations have incomplete, dated, or fragmented plans, and some may not have a plan at all. An important aspect of resiliency planning is to remember that projects started today may not be ready for months, and in some cases years, but starting somewhere is an essential part of building a plan.
Let’s examine the COVID-19 pandemic through the lens of resiliency planning. COVID-19 brought to light fissures in IT infrastructure throughout government, education, nonprofit, and healthcare. Public sector organizations struggled to meet the demands of their constituents, citizens, and employees while trying to maintain operations and continuity. Implementing remote workforce solutions, responding to online inquiries, finding insights across data streams, enabling virtual call centers and 1-800 numbers, and supporting online learning were all areas of focus. However, effectiveness in crisis response varied, as no institution had anticipated the spike in demand for these services and shift in resourcing needed to tackle it.

For example, New York City’s fire department call volumes jumped from 4,000 to 6,000 per day, and the city’s medical help hotline calls grew by 1,600 percent during the first few weeks of the COVID-19 crisis. Business shutdowns and unemployment filings with state agencies shattered previous records. Health and safety agencies found it difficult to track the virus in real-time, and schools and colleges struggled to rapidly deploy remote learning solutions. IT departments had to quickly implement solutions to address the sudden increase in demand. Overall, decades of technical debt suddenly came due, and public sector organizations were unprepared to respond. While there is no way to start again and address COVID-19 with a plan now, organizations can improve the next emergency response if these events are anticipated and planned for properly.

Lessons learned from COVID-19:

“Unless a commitment is made, there are only promises and hopes... but no plans.”

– Peter Drucker - Management Consultant, Educator, and Author
Digital trust and communications platforms

Organizations must expect and plan for a high volume of inquiries from their constituents, citizens, customers, and employees. Communicating effectively during a crisis requires a multi-channel communications platform that is capable of receiving and pushing out real-time alerts and updates across a variety of mediums: mobile phone, chat, text, television, radio, email, social, and more. A protocol for ranking and disseminating vital and official external-facing and internal-facing information should also be negotiated internally, as a central part of your resiliency plan.

System modernization

Organizations must have durable and flexible IT and telecommunications infrastructure that can go live, stay online, and support critical applications while being able to scale up capacity when demand for services peak. Organizations should not build rigid infrastructure that depends on purchasing compute, storage, and networking hardware, as legacy technologies are incapable of supporting the unanticipated demand caused by an emergency. In addition, modern systems in the cloud offer pay-as-you-go pricing so funds can shift from nice-to-have systems to mission-critical systems, saving money and providing flexibility in emergency response. A strong resiliency plan modernizes IT assets and tools before a crisis happens.

Remote workforce enablement

A workforce that lacks mobility or cannot work from anywhere will prevent your organization from delivering 24/7 and performing triage activities when a disruption occurs. Make sure your workforce has the employee hardware, purchasing
mechanisms, supplier relations, tested virtual and physical network connections, and access to on-demand cloud IT services you can turn on when needed, so your organization stays online and remains effective during an emergency. Lastly, providing cybersecurity protection and fraud detection is critical during a crisis. For example, during the COVID-19 crisis, hacking threats increased 15 percent a month since the beginning of 2020. In another example, Washington state halted unemployment payments for two days after finding $1.6 million in fraudulent claims during the pandemic. In addition, identity verification and access controls for virtual workers is also important, since a crisis can bring on a surge in the demand for virtual services.

Build team-wide critical skills

Work to proactively to make sure a variety of employees have specialized skills and train each other prior to an emergency. The cloud can be your best option to spin up emergency IT infrastructure and productivity tools like virtual video chats, online learning solutions, and document sharing websites. But your organization must still have the technical skills to make use of these technologies, so have your entire IT team take AWS Cloud training.
Build a data-driven war room

As part of your resiliency plan, emphasize data management, security, analytics, and dashboards for visualization. You will need visibility into the health of business operations, financials, stakeholders, IT resources, and potentially the inventory levels of resources such as food, shelter, transportation, medical supplies, and capital. You will also need to monitor constituent requests and sentiments to provide a positive customer experience during an emergency. In some cases, citizen science and reporting applications detect patterns across populations by empowering users to report findings in real-time from their mobile phones. These systems show lawmakers and managers what is trending during an emergency. Proactively begin the process of documenting your data flows and the dashboards necessary to mitigate disruptions. Where appropriate and feasible, develop models for data sharing across departments and delivering multidirectional communications with other organizations to share best practices and gain valuable time. In addition, be certain that all steps in your data life cycle (ingestion, consolidation, analysis, visualization, and retention) are part of your disaster recovery strategy. For example, is having your employee management systems up immediately if your data center goes down important? Did you back up your most critical systems, with citizen health information for example, in the same location as your main IT assets, meaning both could be lost in the event of an emergency?
Building a resiliency framework: Technology and cultural best practices

According to executives polled in March 2020, one-third (32.4 percent) rarely update their operating model.

Source: Accenture and Oxford Economics, 2020

The COVID-19 pandemic and other emergencies have made it clear that public sector organizations of all sizes must be prepared to continue operations at all times. AWS can help you build a more resilient organization by:

- Modernizing outdated IT resources
- Upgrading technology at the lowest possible cost
- Improving the speed with which you scale up or turn down IT services to address a disaster
- Providing pay-as-you-go pricing to help you funnel funds where they are most needed during a crisis
- Delivering technology that provides 24/7 uptime for customers and employees
What is a resiliency plan?

What is a resiliency plan? An organization’s resiliency and continuity plan outlines a range of disaster scenarios and the steps the organization will take to return to a regular state. Key staff and multiple departments write plans ahead of time with the goal of creating contingencies that minimize potential harm and negative impacts to the organization.

A strong resilience strategy combines two factors: operational and cultural resilience. Operational resilience includes five pillars:

1) Remote workforce enablement
2) Constituent engagement
3) Process and systems modernization
4) Real-time analytics
5) Operational continuity

A resilience plan also addresses cultural resiliency, defined as best practices that prepare your team for any disruption.
AWS Public sector resiliency framework:

Five Organizational Pillars of Resiliency

Remote Workforce Enablement
Constituent Engagement
Operational Continuity
Real-Time Analytics
Process Systems & Modernization

Suggested Technology Priorities

Virtual Desktop Infrastructure
Collaboration & Productivity Tools
Application Streaming
Private Network Expansion
Identity Verification & Network Access

Multi-Channel Call Center
Internal & External Communication Portals
Chatbot Enablement
Sentiment Analysis
Video Streaming

AWS Disaster Recovery
Data Backup and DR
Elastic Compute Infrastructure
Elastic Networking Infrastructure
Threat Detection & Monitoring
Data Protection & Security

Analytics Dashboard
Database Infrastructure
Data Warehouse Infrastructure
Streaming Analytics
Visualization Tools

Mainframe Modernization
Enterprise Resource Management (ERP)
Business Intelligence (BI)
Supply Chain Management (SCM)
Human Resource Management (HRM)

Value

Virtual Desktop Infrastructure

Multi-Channel Call Center

AWS Disaster Recovery

Analytics Dashboard

Mainframe Modernization

Collaboration & Productivity Tools

Internal & External Communication Portals

Data Backup and DR

Database Infrastructure

Enterprise Resource Management (ERP)

Application Streaming

Chatbot Enablement

Elastic Compute Infrastructure

Elastic Networking Infrastructure

Supply Chain Management (SCM)

Private Network Expansion

Sentiment Analysis

Threat Detection & Monitoring

Data Warehouse Infrastructure

Human Resource Management (HRM)

Identity Verification & Network Access

Video Streaming

Data Protection & Security

Streaming Analytics

Visualization Tools

Up to 30 days

Up to 60 days

Up to 100 days

Up to 300 days
Part One: Five Organizational Pillars Of Resiliency

Pillar One: Remote Workforce Enablement

Having a mobile workforce that is productive from anywhere, 24 hours a day if necessary, is essential for public sector organizations serving mission-critical functions in society. A distributed workforce is viable with the advent of cloud-based software and mobile phone applications. Here are some considerations when evaluating your mobile workforce capabilities:

- Take inventory of your teams’ productivity tools, assuming that most employees will need to work from home. Assess if they have the necessary equipment such as laptops, headsets, VPN software, virtual meeting tools, file sharing tools, identity verification software and devices, video conferencing software, and more. Pilot a small, scoped scenario, where a team works from home for a month to test your plan. Your employees must be able to duplicate their access to key systems and typical performance levels experienced when in the office. Your plan will address document breakdowns.

- Evaluate your teams’ skillsets and make sure there are no gaps or single points of failure. Assign a team member to teach others their skill and pre-assign owners and backup employees for every emergency function in your plan. Assume 100 percent of your team will not be available during a crisis and plan accordingly.

- Approximately 90 percent of organizations use at least one cloud-based productivity tool. Some of your team members may work on large, collaborative projects, and cloud applications make working remotely on these projects viable. For example, during times of disruption you may need to deploy a customer-facing mobile application on short notice. In software development environments, design and development teams often need to work together to accelerate time to market. Successful collaboration leads to better results, fewer misunderstandings, less rework, and smarter delivery of products. Developers rely on task and workflow management tools to help organize projects and track the status of jobs. These tools also enable solution delivery teams to stay on track with a roadmap of project milestones. Lastly, with cloud technologies, teams can chat, make calls, share files, and track workflows. Additional tools for consideration include Amazon WorkDocs for content and file sharing, Amazon Chime for chat, video calling, and virtual meetings, and Amazon Honeycode, which helps teams manage tasks and projects to accelerate the delivery of mobile applications.

- The key to achieving a supportive culture for a remote team is to maintain connections. Create a culture where resiliency is part of every discussion and major plan at the outset where everyone across departments has a role and part of the plan they own and have helped build. Reward nimbleness and employees who experiment with pilot projects that support your resiliency plan. Reward the sharing of information and test telework options throughout the year so there are no
surprises during an emergency. Share your communications on resiliency more than once throughout the year, so that your team has comfort with expectations before an emergency takes place.

**Pillar Two: Constituent Engagement**

For many public sector organizations, meeting their mission means serving citizens, patients, employees, students, suppliers, agencies, and other stakeholders 24/7. People rely on hospitals, schools, and public safety agencies in particular during emergencies. These organizations must innovate with remote learning and telehealth platforms. Never before have digital communications via mobile phones, websites, emails, and texts been more important. Even government agencies with robust communication mechanisms have turned to cloud technologies to improve their capacity to speak with, learn from, and administer benefits to citizens during a crisis. Therefore, upgrading outbound and inbound communications mechanisms requires continual testing and updates over time.

Organizations can build a strategy that effectively leverages their websites as mass, real-time communication tools so that they can communicate through different channels and reach the most number of recipients. Look for communications solutions that:

- Scale intelligently to support large spikes in usage.
- Purchase pay-as-you-go solutions (not solutions with high upfront fixed costs) that you can activate specifically during an emergency, and turn off after an emergency.
- Push content out and poll notifications for all channels: online forms, text messages, online chat transcripts, email, 1-800 voice calls and even social media posts.
- Provide self-service delivery models in order to free up resources to address inquiries that are more serious.
- Since maintaining user trust is paramount during a crisis, provide privacy and security of user data with secure cloud solutions that come with battle-tested security built-in.
- Process constituent data in real-time and pre-build dashboards for department heads and executives too see and address patterns and trends.
- Make sure you have a solution comparable to your external solution for your internal teams and stakeholders.
Most government agencies, mission-critical systems are often dependent on legacy technology that does not work during an outage, disruption, or disaster. That is why the U.S. Government Accountability Office (GAO) has repeatedly warned about the use of legacy programming languages for critical systems. Therefore, modernizing vulnerable, legacy technology such as mainframes computers can change how well you respond to a disaster. Here are some question to ask your IT leadership:

- Where are customer-facing systems housed? Is this system in need of modernization? When did it need an upgrade/refresh (1, 5, 10, or 15+ years ago)?
- Are other systems and your ability make decisions dependent on this system?
- Is this system only administered by a limited number of subject matter experts, or employees with rare skill sets (single point of failures)?
- Was your system built on a closed architecture, such as proprietary hardware or custom software that cannot be readily supported?
- Does the system have the ability to scale up if needed? How long would that take and how much would that cost?
- Is the system consuming an inordinate amount of your operational budget? For example, legacy technology like mainframe computer systems can consume up to 40 percent of an IT budget (e.g. consisting of software licensing, service contracts, and operational inefficiencies).

Making the decision to update a legacy system or business application is not easy, but outdated or poorly performing applications can amplify issues during a crisis, and impact customers. Therefore, building a strategy for system modernization is critical for any resiliency plan and your ability to execute it.

Data is the new currency. Data analytics play a big role in supporting decision making during an emergency by providing the right information at the right time. An advanced analytics platform supports crisis mapping, resource re-allocation, health and safety prioritization, and can even connect families with loved ones. Your data analytics platform is the life-blood of your crisis war room, so it should be durable, backed-up properly, and tested often.
Non-technical leaders should consider these key factors when considering data analytics:

- Your platform should ingest, store, and analyze data from many sources to support situational awareness, since up to 80 percent of an organization’s data may be composed of unstructured data created by newer sources such as websites, searches, social media feeds, and mobile devices.
- Your platform should support large spikes of data streaming in during an emergency, since systems will be flooded with requests for information, support, and service.
- Strategic decision-makers will require clear and concise dashboards during an emergency to visualize what’s happening on the ground, ease decision making, and quickly isolate gaps.
- Make sure to properly secure and back up your data. Cloud technologies can help you access or restore data quickly from anywhere.
- Be certain that your data analytics platform is not dependent on a single subject matter expert.

Regardless of an organization’s mission, operational continuity—or keeping the organization operating like normal—is the goal of any resiliency plan. The first step in operational continuity planning is deciding what functions are essential and allocating time, staffing, and budgets accordingly so that failover mechanisms are in place. Key considerations for providing ongoing operations include:

- Assign acting CIOs to backup existing CIOs and Chief Technology Officers (CTOs) and train both in maintaining IT infrastructure that is resilient and durable, backed up to multiple locations.
- Assign Chief Supply Chain Officers (CSCOs) to develop a short-term action plan to reduce risk and financial impact due to supply chain disruptions, creating a backup suppliers list and agreements that are pre-negotiated and can be activated any time as needed.
- Assign Chief Financial Officers (CFOs) to lead budget reallocation towards resiliency gaps before a disaster takes place, and to make sure budget is liquid and available when needed.
- Assign a chief resiliency officer with the ability to continually monitor and isolate risks and the authority to activate your plan and communicate it up or down through your organization.

Envision your resiliency plan as a hub and spoke model. It must be inclusive and bring in stakeholders from all lines of business or you risk having gaps that can derail your organization during times of crisis.
Part Two: Building a culture for organizational resiliency

Employees are the engines that drive organizations. A strong resiliency plan puts employees at the heart of the plan and involves employees early and often. During emergencies, research shows that employees often feel anxious, which affects productivity and engagement—the ability to act during an emergency. Your resiliency plan should identify employee risks, just as it identifies technology, customer, and financial risks. Beyond pandemics or natural disasters, changing market conditions, mergers, or general restructuring can adversely affect organizations. Regardless of the type of disruption, an employee’s alignment to organizational objectives is most at stake during emergencies. Other elements that influence employees during crisis include the existing organizational culture, leadership, and one’s work environment, which can include technologies, tools, physical space, and processes.

Best practices to help build a culture of resiliency:

When building your resiliency plan make imperfection acceptable and use the plan as a framework rather than a rigid rule imposing negative consequences on those who offer to help.

Treat employees as frontline emergency workers that customers are counting on, and include them in decisions, so they see their role as valuable.

Empower employees with flexible emergency-only policies around working from home, changing their schedules, and other factors that impact morale, inclusion, and engagement.

Share what you know often and treat employees as leaders, not followers, so they own problems during an emergency. If employees feel invested, or that their contribution delivers value, they are more likely to go the extra mile when called upon.
Build into your plan a pre-defined network of connections with cross-functional teams, outside agencies, vendors, and technology partners.

Avoid having a single point of failure with an employee that holds unique skills or access rights. Encourage and reward employees who receive training to mentor other team members to establish a culture of growth and trust. For key staff members, implement a backup policy and program.

Revisit your resiliency plan to keep it aligned with your evolving culture.
Five technology pillars for resiliency: customer case studies

When an emergency or disruption occurs, elements and processes that made the organization successful in the first place can get in the way. For example, cost cutting while instinctive, may be ill-timed during a crisis, even if it is perceived as necessary. Leaders should be open to shifts that are counter-intuitive so their organization can survive emergencies. Let us look at the example of the American Red Cross. The American Red Cross serves the community by assisting citizens in the wake of hurricanes, fires, earthquakes, and disease outbreaks, including COVID-19. Like many nonprofits, the pandemic impacted the American Red Cross, who had to modify their operations to deliver on their charter.

First, they realized that distancing does not equal disengagement, and the nonprofit developed an online training program using cloud technologies to quickly implement a virtual learning platform to train volunteers before they head into the field. The nonprofit also used cloud-based collaboration and data-analytics tools to bring data and decision makers together virtually to prioritize which disasters to address first and what resources would be required.

The American Red Cross was proactive, and in 2017, the organization turned to AWS and APN Partner VoiceFoundry to deploy a cloud-based call center. The call center strategy resulted from lessons learned from Hurricane Harvey, as the nonprofit was inundated with calls for help by impacted citizens. Within 48 hours of the hurricane, the call center was in operation and employees were taking calls supporting Hurricanes Irma, Maria, and Nate. To learn more about the American Red Cross and their lessons learned during the COVID-19 surge, watch the interview with Linda Mathes, chief executive officer (CEO).
AWS Public sector resiliency framework continued:

Five Organizational Pillars of Resiliency

Remote Workforce Enablement
Constituent Engagement
Operational Continuity
Real-Time Analytics
Process Systems & Modernization

Suggested Technology Priorities

Virtual Desktop Infrastructure
Multi-Channel Call Center
AWS Disaster Recovery
Analytics Dashboard
Mainframe Modernization

Collaboration & Productivity Tools
Internal & External Communication Portals
Data Backup and DR
Database Infrastructure
Enterprise Resource Management (ERP)

Application Streaming
Chatbot Enablement
Elastic Compute Infrastructure
Elastic Networking Infrastructure
Business Intelligence (BI)

Private Network Expansion
Sentiment Analysis
Threat Detection & Monitoring
Streaming Analytics
Supply Chain Management (SCM)

Identity Verification & Network Access
Video Streaming
Data Protection & Security
Data Protection & Security
Human Resource Management (HRM)

AWS End User Computer Services
AWS Customer Engagement Services
AWS Compute Services
AWS Analytics Services

AWS Media Services
AWS Storage Services
AWS Machine Learning Services

AWS Content Delivery Services
AWS Backup Services
AWS Database Services
AWS Database Services

AWS Solutions
AWS Migration & Transfer Services
AWS Disaster Recovery
AWS Disaster Recovery

AWS Migration & Transfer Services
AWS Compute Services
AWS Storage Services
AWS Database Services

AWS Analytics Services
AWS Machine Learning Services
AWS Database Services
AWS Machine Learning Services
To get ahead of the next disruptive event, it is important that your workforce is agile, mobile, and can telework. The ability to scale up or scale down on demand for IT help desk or employee health services that let employees be productive from anywhere is important. Traditional computer desktops and even virtual desktops (VDI) cannot scale instantly for peak usage if all employees must work remotely. They require capacity planning and guesswork upfront and for organizations to pay hardware licensing capital expenses prior to an emergency, so you need to build the system before it is needed.

Cloud-based remote work solutions like Desktop-as-a-Service, application streaming, secure mobile access, storage, and collaboration tools let employees turn on services and allow the organization to only pay for services used, scaling from one employee virtual desktop to 100M+ instantly. In other cases, you can support bandwidth-intense programs like CAD design programs, MATLAB, CES EduPack, ANSYS FLUENT, and SOLIDWORKS with cloud-based licenses so they infinitely scale as needed.

Common remote workforce solutions to consider testing in your organization, include:

**AWS end user computing (EUC)**  services give you the agility to make your workforce remote instantly, so you don’t have to pre-purchase hardware and set up months in advance. AWS EUC services such as desktop as a service DaaS solutions, application streaming services, and collaboration solutions are fully managed by AWS, so you onboard new users with a few clicks and remove them just as simply without hardware. AWS EUC services also free you from unwieldy licensing fees and contracts. You can add and remove users on demand and pay only for what you use, when you use it. You no longer need to over-buy hardware and licenses for peak user capacity. AWS solutions are built with security in mind, meeting stringent compliance requirements that do not need to be custom-built from the ground up. With cloud-based workforce solutions, your organization’s data is no longer stored on users’ devices, and you control access with fine-grained permissions and identity verification tools.

**Amazon WorkSpaces**  Amazon WorkSpaces lets employees work on their mobile device or laptop and this DaaS solution gives them access to their computer desktop from anywhere around the world. You can pay for their access either monthly or hourly, and there’s no hardware to patch, update, and secure.

**Amazon AppStream 2.0**  lets you stream software like CAD, SOLIDWORKS, Photoshop, or CES EduPack to any device, so your remote workforce can securely access software typically used in the office. Schools can provide every student with access to the learning applications outside the classroom. Hospitals can give doctors access to diagnostics tools and even technical teams who use computer-intensive modelling software have the same experience from home as they do in the office.
Amazon Chime lets you meet, chat, and place business phone calls with a single, secure application. You do not need to switch between applications to collaborate and can instantly go from a chat to a call, share your screen, and even invite more people to join your meeting. With Amazon Chime, you have the flexibility to choose the communication option that fits with your organization’s needs.

Customer case study: Mt. San Jacinto College enables remote work during COVID-19 with Amazon AppStream 2.0

With the emergence of COVID-19 social distancing mandates, Mt. San Jacinto Community College District (MSJC) needed to quickly transform to support a remote workforce, so faculty and staff could continue to provide vital services to students. As time was of the essence, MSJC engaged their most trusted partners to discuss, design, and assist in implementing the tools needed: InterVision and AWS.

Learn more

Customer case study: Humber College enables remote education on AWS

With over 30,000 full-time students, Humber is Canada’s largest college based in Toronto, Ontario. As a result of COVID-19, Humber needed to develop a remote access solution for academic software and applications to enable education continuity for students amidst social distancing regulations. Learn how Humber College worked with APN Partner Onica and AWS to deploy AppStream 2.0 to enable remote access to a portfolio of over 300 academic applications through any device.

Learn more

Customer panel: Minimize Cybersecurity Risks in a Remote World

Hear from a panel of experts, including Scott Gilhousen, CIO for Houston Independent School District, as they discuss solutions for deploying remote learning and workforce cloud services, and security best practices.

Watch the video
As students and teachers are waking up to a new reality due to COVID-19, Impartus and CareerLauncher, and partners like Intel are using AWS to quickly and securely enable remote learning solutions at scale, so students can continue their education anywhere, anytime. Working together and leveraging the power of the cloud, AWS, its customers, and partners are demonstrating how a combination of resources, expertise, technology, and human ingenuity can solve future challenges around health education, disease transmission, and public resources management.

Learn more

With tens of thousands of students of all ages across Australia and New Zealand now learning from home, there’s no doubt our educators have done a remarkable job of adapting to engage students using online tools. Managing the rapid growth of online learning has been critical for New Zealand-based Education Perfect (EP), a digital education platform that provides transformative online teaching and learning experiences.

Learn more
During emergencies, citizens, students, and patients rely on public sector organizations and agencies for vital information on everything from transportation changes, unemployment benefits, and medical guidance to school openings and other life-impacting services. At the same time, employees tax 1 800 numbers, seeking technical support while working from home. Overall, the volume of calls into call centers spikes and organizations will need to factor supporting existing customer service agents remotely in their homes as well as newly hired agents needed to handle higher call volumes. Using a cloud-based contact center can make these tasks simpler and less costly. For example, Amazon Connect helps you set up an emergency or new contact center in minutes without a contract, and it supports mobile texts, website chats, and phone conversations, and it’s used by Amazon’s retail business to power millions of customer conversations. With Amazon Connect, you can scale your contact center up or down to any size, onboarding tens of thousands of agents in response to normal business cycles or unplanned events.

Customer case study: The cloud helps Rhode Island manage an unprecedented surge in UI claims

When the US economy ground to a halt during the COVID-19 outbreak, states experienced a dramatic surge in unemployment claims. Rhode Island was no exception. The Rhode Island Department of Labor and Training (DLT), which manages unemployment insurance (UI) claims for state residents, received more than 140,000 initial claims for the UI program alone in the first 45 days after the governor declared a state of emergency. Learn how Rhode Island DLT was able to address the surge in call volume by turning to AWS to create and deploy a cloud call-center.

Learn more
Customer case study: LA County call center achieves 60 percent cost savings and 17 percent call reduction using Amazon Connect

When LA County was looking to update its call center, it needed a solution that would reduce hold times by automating simple requests, provide automated information about outages without requiring a voice-over-IP engineer. The county also wanted to improve agent productivity, job satisfaction, and retention by allowing agents to focus on more complex, higher-value calls. In addition, the county needed to ensure agent mobility and flexibility, like spinning up a remote contact center in an emergency or offering the option of telework to employees to help ease traffic congestion. To address these requirements, LA County looked to AWS to help architect and deliver a cloud-based call-center.

Learn more

Customer case study: Accelerating the response to West Virginia’s workforce needs through the cloud

In the first three weeks of the COVID-19 pandemic, sixteen million people filed for unemployment insurance, overwhelming states’ systems. To modernize their contact center, Workforce West Va. turned to AWS Partner Network (APN) Premier Partner Smartronix, one of their existing cloud service providers. Understanding the agency’s need for a secure, reliable, and scalable modern contact center that was simple to set up, Smartronix deployed Amazon Connect, an omnichannel cloud contact center. They created and implemented the contact center within 72 hours.

Learn more
Customer case study: Transforming citizen services through technology

The need to maintain communication with citizens has been vital through the crisis, especially with so many new health and economic measures being brought into effect. But with call centre staff unable to attend their usual places of work, solutions to enable them to continue their work from home are essential. For example, The West Australian (WA) Department of the Premier and Cabinet and WA Police Force led a multi-agency effort to deploy Amazon Connect, a cloud-based contact centre within two weeks to create their 13COVID hotline. The call centre receives an average of 1,200 calls each day and agents answer a range of questions from the community about COVID-19 including the impact of the virus, questions about restrictions, prevention tips, and directions to relevant sources of information.

Learn more

Pillar Three: Process and System Modernization

Communicating important information updates to constituents and employees during a crisis impacts how fast an organization recovers. Whether you must communicate detailed instructions to citizens or provide simpler updates to employees, a multi-channel communication approach is necessary to make sure the majority of your audience hears and understands you. We recommend multi-channel communications platforms that work with your database and inputs to alert audiences via website chatbots, phone, email, mobile text, and social media channels. Chatbots are “conversational agents” on your website that use artificial intelligence (AI) and machine learning (ML), so it appears like users are having a live conversation with a real person. For example, hospital chatbots offer triage hotlines that collect information from patients and help route them to the right caregiver based on their answers. Consider building and deploying chatbots to elevate the value of your digital communications platform by supplementing your customer service representatives. Some cloud-based solutions to support multi-channel communications include:

Amazon Lex lets you convert speech into text using natural language understanding (NLU) to recognize the intention of texts for a life-like interaction akin to Amazon Alexa conversations.

Amazon Polly turns text into lifelike speech, so you can pre-build conversations and answer common questions.

Amazon Cognito lets millions of users sign in to your systems with their Facebook, Google, and Amazon account logins.
Amazon Comprehend uses AI from ML to find insights and relationships in text like doctor’s notes, patient records, and social media accounts so you know what’s trending during a crisis. It even detects and analyzes sentiments such as mentions, comments, likes, or specific text in social media, call logs, video, and web chat data for large populations of customers, patients, and stakeholders.

Amazon Transcribe makes it simple for developers to add speech-to-text capability to their applications. Audio data is virtually impossible for computers to search and analyze. Therefore, organizations need to convert recorded speech to text before using it in applications. AWS Elemental MediaLive is a broadcast-grade live video processing service that lets you create high-quality video streams for delivery to broadcast televisions and internet-connected like connected TVs, tablets, smart phones, and set-top boxes.

AWS Elemental MediaConvert lets you create video on demand (VOD) content for broadcast and multiscreen delivery at scale.

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, and applications to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

Now that you have an overview into the services, let’s look at a scenario where these services can come together to help you address a challenge during a disruption. If your organization provides services to citizens, you may come across scenarios where a constituent does not speak English. For example, a healthcare provider may need to respond to urgent questions coming into their portal from a patient who only speaks Tagalog. As the key service provider, how do you address this issue to make sure that you provide the best support possible? The answer can come in the form of a translation chatbot.

Start by using AWS Lambda for a serverless compute foundation, as it will offer the greatest flexibility and cost benefits. Amazon Cognito will act as your authentication gateway and Amazon CloudFront will serve as your content delivery mechanism. Amazon Polly and Amazon Lex will be your speech-to-text conversion engines that will engage with Amazon Translate to receive content in one language and convert it to the secondary language. Cached translations will reside in Amazon DynamoDB to help the model learn and improve accuracy over time. The chatbot will be housed in Amazon Simple Storage Service (Amazon S3) to take advantage of its elastic storage capability. In this scenario, a patient can use their mobile device to speak or text in their native language. The system then translates the input and determines intent. Next, the system will determine an appropriate reply and translate the response back into the patient’s language. This multi-language or translation chatbot can help your organization by providing incremental support to larger audiences in your community and keep emergency lines free for more critical inquiries. The following customer use cases, provide examples of how public sector customers use AWS media services to deliver educational content and disaster response updates at scale.
As schools closed due to the COVID-19 pandemic, the government of Jordan wanted to quickly help students across the country reconnect with their teachers and classmates to resume their education. Multiple entities came together to deliver the end-to-end, cost-efficient platform including Jordan’s Ministry of Education, Ministry of Digital Economy and Entrepreneurship, and AWS. Since the platform went live on March 22, it has seen more than 35 million views of classes and made a positive impact on education by providing more than 2 million Jordanian students with the tools necessary to continue their education online, from the safety of their homes.

Learn more

Customer case study: Jordan develops eLearning platform for 2 million students with AWS

Pillar Four: Real-Time Analytics

Becoming data driven can help you with constituent engagement, process automation, and cost optimization – in the short term and long term. Cloud IT services have lowered the costs, complexities, and burdens of managing, storing, and analyzing vast amounts of data. These tools can help decision-makers get ahead of a crisis, better support advanced research to resolve a crisis, and result in greater organizational resiliency (Amazon Athena, Amazon Kinesis, etc).

Amazon Athena lets you query structured data like databases and unstructured data like chats on your website without long lead times.

Amazon Kinesis lets you collect real-time data feeds such as video, audio, application logs, website clickstreams, or sensor data for processing now or later.

Amazon QuickSight lets you create and publish interactive dashboards that are accessible to your executives from their mobile phones, or desktops from anywhere. AWS Lake Formation lets you create one main data repository for data from any source including a structured CRM database or new sources like log files, data from click-streams, social media, and internet connected devices. A data lake allows all your data to be housed in a single place, instead of siloed in multiple databases, files, and systems.

AWS Deep Learning solutions allow large datasets to be stored and managed in Amazon EMR, the industry-leading cloud big data platform for processing vast amounts of data using open source tools such as Apache Spark, Apache Hive, Apache HBase, and Presto.
Amazon Comprehend is a natural language processing (NLP) service that uses ML to find insights and relationships in text.

Amazon Textract uses optical character recognition (OCR) technology to automatically detect printed text and numbers in a scan or rendering of a document, such as a legal document or a scan of a book.

Customer video: Wadhwani Institute for Artificial Intelligence Builds Innovative Health Solutions Using AWS

Amazon Web Services helped Wadhwani Institute of AI scale and securely process their government sensitive data as they built multiple solutions for large-scale societal problems.

Learn more

Pillar Five: Operational Continuity

Business continuity requires that systems normally counted on continue to work as expected during an emergency. Whether because of natural disasters, human error, or technical failures, even a brief lapse in operations can lead to financial losses and compromise customer trust. Determine which systems can be down for how long (recovery objectives and recovery time objectives) to prioritize disaster recovery and backup objectives in your resiliency plan. The AWS Cloud gives you the option to recover systems rapidly. As soon as an existing system fails in one facility, the replica is turned on so that no one perceives a disruption. In other scenarios, you can intentionally delay recovery time to lower costs. No lease agreements, physical hardware costs like tape media, or contracts are required. If a backup of your systems is already in the cloud, you can simply turn it up when you need it. For example, with AWS CloudEndure Disaster Recovery, any IT team can shift systems and operations from a physical workplace to a virtual data center in the cloud within seconds with no downtime. Your organization can even select to house its mission-critical databases, websites, and assets in a cloud location in another
A prioritization checklist for leaders

Now that you have a snapshot of key frameworks and technologies to build a more resilient organization, below is a checklist to consider:

**Business impact analysis (BIA)**
Use a systematic process to determine, evaluate, prioritize, and predict the potential effects of an interruption to business operations as a result of a disaster, accident, or emergency. Identifying and evaluating the impact of disasters on day-to-day operations provides the basis for investment in recovery strategies, prevention, and mitigation strategies.

**Leadership**
Does each department know what to do in a mild, medium, and urgent emergency scenario? Have you assigned plan owners tasks? Do they update regularly?

**Human resources**
Does your organization have a way to identify, train, and maintain the personnel required to deliver the necessary level of critical services? Do you have temporary employee contracts in place to activate additional workforce capabilities in the event of an emergency? Have you addressed skills gaps? Is your technology team trained on modern technologies like cloud computing?

**Facilities**
Can your organization easily communicate urgent safety information to its employees and customers?
Stakeholder communications and alerting
Can your organization communicate in real time across multiple channels to the public or its customers and receive information back quickly at a massive scale?

Remote work technology
Can your employees work remotely and collaborate with each other and the public on short notice? How will they get the equipment in an emergency? Have you tested a remote work scenario to isolate and fix any bugs?

Situational awareness
Does your organization have the right technologies and real-time information feedback loops in place to make data-driven decisions and detect patterns with customers during a crisis.

Emergency funding
Does your organization have the procurement and emergency funding mechanisms to address a crisis? Are you using pay-as-you-go models for IT resourcing so mission-critical.

Supply chain risk mitigation
Are you able to assess the health of your suppliers? Is their geographic location going to impede their ability meet increased orders or demand? Are you able to re-negotiate new terms if under financial strain? Do you have supplier diversity policies in place?

Legacy infrastructure
What legacy systems house mission-critical data such as customer databases or support functions that you need to upgrade in 6, 12, and 24 months?
Conclusion

It is time to start building a baseline resiliency plan. Having a plan in place improves your organization’s odds of minimizing the impact of an emergency on your employees, customers, and partners. The severity and extent of a major disruption can challenge even the most tech-savvy and mature organization. As a leader, you have the opportunity to determine your organization’s future state by leveraging lessons learned from past emergencies and the latest technology tools. If your organization identifies a technological gap, the cloud offers the fastest route to remediation and preparedness at the lowest possible cost. In particular, cloud-based IT solutions such as compute, storage, and data management services, like Amazon Elastic Compute Cloud (Amazon EC2), Amazon S3, and databases on AWS, can quickly give you the capacity to withstand a crisis. AWS and our partners are dedicated to supporting your road to creating a resilient organization. Please visit the organizational resiliency and continuity help center to start your journey.
ServerCentral Turing Group (SCTG), an advanced AWS MSP Consulting Partner, provides cloud, disaster recovery, and colocation services, including AWS consulting, cloud migrations, and managed data center services. Customers love being able to offload any IT infrastructure management project to a single provider knowing it gets taken care of as well as or better than their in-house team. See the video of SCTG helping a customer transform their business with AWS. For more information, contact SCTG through their website or the AWS Partner Network.

Enquizit was founded in 2002 with the vision of empowering good. We are an AWS Advanced Consulting Partner that provides human-centered design (HCD) solutions to higher education, federal, and nonprofit organizations. Our core competencies are in cloud migration and cloud-native application development. Our focus in these areas allowed us to develop a cloud migration tool named SkyMap™ that determines the optimal path to the cloud with less risk. SkyMap™ brings stability, consistency, and efficiency to migration and disaster recovery projects through automation and machine learning. We are also an Authorized AWS Reseller with Migration, DevOps, Government, Nonprofit, and Education Competencies. For more information contact Enquizit through their website or the AWS Partner Network.

InterVision is an AWS Premier Consulting Partner with a decade of cloud experience and a twenty-five-year legacy of supporting clients in their datacenters. As a strategic services provider, our consultative approach, comprehensive solution portfolio and deep bench of certified AWS experts helps close the knowledge gap between legacy and cloud systems that stalls many cloud initiatives while mitigating the risk of poor cyber hygiene and cost sprawl. For more information contact InterVision through their website or the AWS Partner Network.

Presidio is a leading IT solutions provider assisting clients in harnessing technology innovation and simplifying IT complexity to digitally transform their businesses and drive return on IT investment. Our Digital Infrastructure, Cloud and Security solutions enable our almost 7,000 middle market, enterprise, and government clients to take advantage of new digital revenue streams. For more information, contact Presidio through their website or the AWS Partner Network.
Additional Resources

- Cloud 101 for Public Sector
- AWS Project Resilience
- AWS Disaster Response
- AWS Free Tier
- AWS Cost Optimization Help Center
- AWS Professional Services
- How Governments Can Build Resilience in a New Normal: Emerging Practices from Europe, Middle East, and Africa
- Maintaining Critical Transportation Operations in Times of Crisis

Tools

- AWS Cloud Adoption Readiness Tool (CART)
- AWS Cloud Champion
- AWS Simple Monthly Calculator
- AWS Total Cost of Ownership (TCO) Calculator

Additional customer stories

- Mission: Connection and access for all
- Case Study - Using Amazon Sagemaker to combat school dropout and failure in Brazilian Education (In Portuguese)
- Highline Public Schools: Building the business case: How districts can save, be flexible, and innovate during times of uncertainty
- The State of Utah balances its COVID-19 response with Domo
- Accenture: New Mexico Human Services
- ECS: Department of Health and Human Services (HHS) Program Support Center (PSC)