AWS Cloud Adoption Framework for Continuity of Government IT (CAF-CGIT)

Introduction

Citizens expect public services to be as accessible and available as the banking, livestreaming, and shopping apps on their mobile devices. Public sector organizations, however, face a variety of threats that can prevent them from providing the availability and services that users need. Public sector IT leaders must prepare for potential emergencies that traditional backup systems or facilities can't mitigate. These include weather events, natural disasters, infrastructure failures, cyberattacks, and hostile geopolitical actions.

The AWS Cloud Adoption Framework (AWS CAF) leverages AWS experience and best practices to help you accelerate successful digital transformation. Use the AWS CAF to identify and prioritize transformation opportunities, evaluate and improve your cloud readiness, and evolve your transformation roadmap.

The Cloud Adoption Framework for Continuity of Government IT, as described in this document, extends AWS CAF with updated and new organizational capabilities that allow government agencies to safeguard citizen data and digital services from large-scale disruptions. This guide has been written for public sector IT leaders who seek to build resilient digital societies.

Continuity and value chains

Protecting critical public data and services is essential for national security. The number of yearly significant cyber incidents has tripled since 2016, according to statistics by the Center for Strategic and International Studies.

The war in Ukraine has underscored the need to secure critical digital infrastructure. According to the Sophos 2024 Ransomware Report, 68 percent of central and federal government organizations were hit by ransomware. Governments must also address the impacts of climate change, such as flooding and fire, on digital infrastructure.

Citizens expect public services to be available and secure, especially during crises when demand may surge. The COVID-19 pandemic drove a digital surge across geographies and sectors, especially for healthcare and welfare. As an owner of critical digital assets, from tax records to land ownership, you need to know how to create secure backups and plan for recovery from large-scale impacts. This must be cost-effective and enable your assets to evolve and create more value.

Attaching a monetary value to the risk and cost of rare, high-impact events is a daunting task as there is little data available to use statistical methods. It's simpler to assume these events will occur and to focus on recovery point and time objectives, and total cost of ownership of continuous value delivery and fulfilling of RTO/RPO objectives.

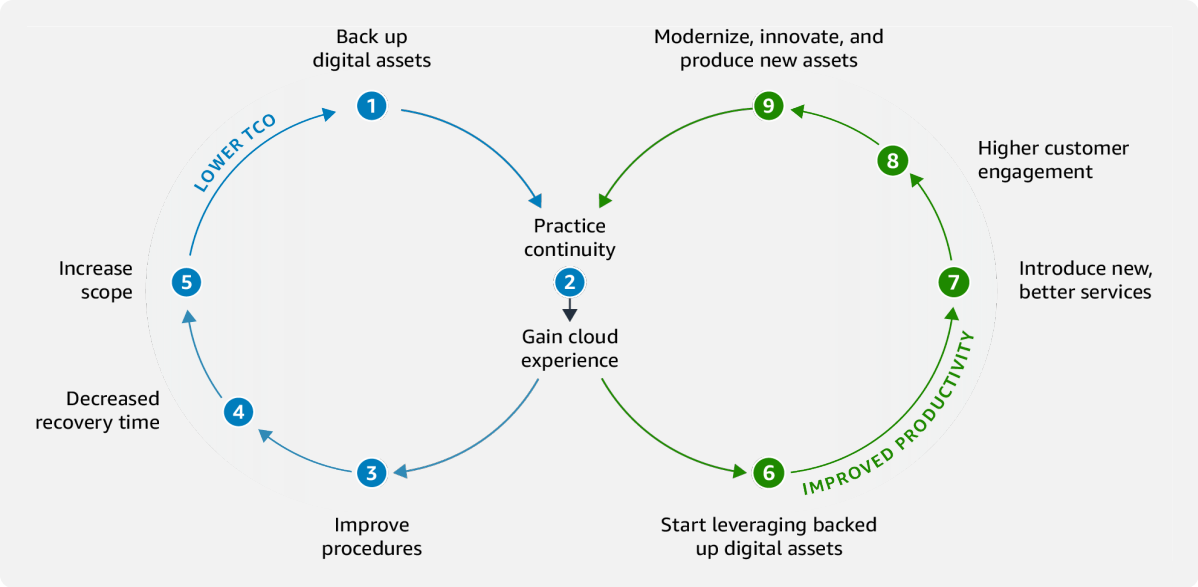
Continuity can be thought of as the ability to direct assets to deliver value to customers (citizens), and for customers to communicate their needs. Resilient assets and communication channels support this value chain.

Your continuity-first transformation journey

Building continuity improves cloud adoption by demonstrating the operational and cost benefits for government. For some organizations, these benefits will motivate the cloud journey.

Continuity is not a static end state. You'll iteratively build best practices, and improve these with repeated use. You'll learn to measure your ability to expect the unexpected, use feedback loops for process improvement, and balance your business outcomes with best practices for continuity. Continuity should never hinder or replace your day-to-day business goals or innovation.

Some organizations start by backing up digital assets for disaster recovery, then use the cloud experience as a springboard for innovation, as shown in the continuity flywheel (Figure 1).



The flywheel illustrates a customer journey with corresponding benefits. The story puts you in the role of a customer who wants to protect their digital assets against adverse events by backing these up to highly available secure cloud.

You start the journey in the top-left corner, aiming to back up critical digital assets such as files, documents, databases, or whole services and configuration. By doing so, you have already improved your assets' survivability (1), which can be measured against your Recovery Point Objectives (RPO). RPO measures the amount of data loss you can tolerate in an event, often measured in time between the last known state of your assets and an event. The more often you back up, the better (shorter) your RPO can be. You also need to be able to recover from a backup after an adverse event occurs.

A recurring practice routine validates your ability to recover so your organization gains true confidence (2). You can avoid overconfidence and false confidence by varying your practice conditions and challenges in every practice run.

Repeated mindful practice increases cloud experience and so improves your organization's skill level both vertically (in-depth knowledge in resilience, benefit 3) and horizontally (general cloud knowledge, benefit 6).

In-depth skills allow your organization to improve resiliency procedures, take advantage of automating cloud operations and thus decreasing the time to recover (4), which can be measured against your Recovery Time Objectives (RTOs). Through confidence, improved knowledge and procedures, you gain bandwidth to increase the scope of your continuity journey to new types and larger volumes of digital assets.

As scope increases, you start taking advantage of a lower total cost of ownership (TCO) (5) of the cloud, thanks to reduced need to build and maintain your own duplicate infrastructure. Over time, this lower TCO translates to more budget available for innovation - the differentiating element of your organization.

As your digital footprint in the cloud grows, together with cloud knowledge (#6) of your workforce, and with better TCO freeing up resources to innovate, you can start taking advantage of digital assets that have been already backed up in the cloud. Using cloud services that would be costly to replicate in your on-premises environments, such as machine learning, large data warehouses, flexible compute and virtually unlimited storage, you can start designing and experimenting with new use cases that leverage your digital assets. This improves the productivity of your assets (7), as it results in your organization being able to introduce new and better services to your customers.

A better service experience results in higher customer engagement (8), in turn allowing new kinds of digital assets to emerge through customer interactions. Through this process your organization not only modernizes itself, but also starts gaining benefits of value-add of the cloud (9), such as agility, flexibility, improved security, and better sustainability. Over time, your focus can shift from the initial continuity journey on the left side of the illustration, to a cloud-based innovation and transformation journey, while the best continuity practices that were rooted into the organization at the beginning, grow into modern continuity and resiliency practices in the cloud. Over time, the focus shifts from the initial continuity journey to a cloud-based innovation and transformation journey, while continuity best practices are embedded into the organization.

As your digital footprint in the cloud grows, together with cloud knowledge (6) of your workforce, and with better TCO freeing up resources to innovate, you can start taking advantage of digital assets that have been already backed up in the cloud. Using cloud services that would be costly to replicate in your on-premises environments, such as machine learning, large data warehouses, flexible compute and virtually unlimited storage, you can start designing and experimenting with new use cases that leverage your digital assets. This improves the productivity of your assets (7), as it results in your organization being able to introduce new and better services to your customers. A better service experience results in higher customer engagement (8), in turn allowing new kinds of digital assets to emerge through customer interactions.

Through this process your organization not only modernizes itself, but also starts gaining benefits of value-add of the cloud (9), such as agility, flexibility, improved security, and better sustainability. Over time, your focus can shift from the initial continuity journey on the left side of the illustration, to a cloud-based innovation and transformation journey, while the best continuity practices that were rooted into the organization at the beginning, grow into modern continuity and resiliency practices in the cloud.

Business perspective

Strategy management

Government IT and digitalization should drive long-term benefits of convenience, accessibility, and security for citizens and civil servants. Continuity of IT assets and operations should be integral, as falling back to non-digital operations may become unviable. The first goal is to create disaster recovery mechanisms.

Consider strategic cost optimization targets. What do you want to invest in managing IT infrastructure? How much reserved capacity do you need to become resilient? How rapidly is your digital footprint growing? Align continuity and innovation goals. You can start with a goal to have disaster recovery mechanisms. Once your digital assets are in the cloud, you can use technologies that would be prohibitively costly or time-consuming to implement in traditional IT environments. Make continuity and preparedness a normal part of long-term operations, using cloud technologies to improve this.

Business perspective

Portfolio management

Understand the parts of your product or service portfolio that are most critical to protect. This will help prioritize efforts and clarify your continuity journey. Map cloud resource investments you need using the 7 Rs, a common migration strategy.

Work backwards from customer needs before, during, and after a crisis, to create a continuity-oriented view of your asset portfolio. Consider dependencies on other organizations and their resilience. These questions help categorize assets:

1. What data, products, and services do your end users or dependent organizations most rely on?
2. Will they also rely on these during a crisis?
3. Can similar citizen outcome (for example social security payment or example online advice) be delivered through other means?
4. Which additional assets need to become available during crises?
5. What parts of your portfolio depend on other organizations?
6. How resilient are these organizations?
7. Do you share common dependencies with these organizations during an impact?

Business perspective

Innovation management

Everything will eventually fail over time. An organization where preparedness and resilience are implicitly parts of the mindset, skillset and toolset, is capable of moving faster without the fear of falling. Mistakes made during innovation are acceptable and provide useful learnings. For example, the Correction of Error (COE) process dives deep into failures, analyzes the impact and identifies actions to avoid repeat mistakes. A COE creates visibility into how organizations can improve. Tolerating mistakes and providing ways to recover motivates teams to move faster, experiment, and innovate.

Product management

While an organizational continuity strategy can and often should be driven centrally, tactical and operational responsibility is best shifted close to product and service owners. This increases agility when continuity plans need to be implemented, tested and executed. Delegating continuity ownership does not have to mean relinquishing control over how or when continuity plans are executed. Continuity strategy can prescribe guardrails and mechanisms for reacting to large-scale continuity events. When service owners have the power to make the best implementation decisions for their services, reaction and recovery times will accelerate. Decentralize where you can. Allow your organizations to self-regulate through cross- organization competence sharing, forming guilds or appointing leaders and evangelists for particular technologies. You don’t necessarily have to have all required competencies available centrally, but can nurture a collaborative environment that has a critical mass of knowledge that gets spread across the organization.

Business perspective

Strategic partnership

Achieving end-to-end continuity expertise is rare. Selecting the right partners is critical: they can drive innovation while assisting with delivery and providing trusted guidance. This includes knowledge of local legislation. Maintain a sense of organizational responsibility, as partners may also be impacted during large-scale events.

In addition to assisting your organization through delivery of continuity outcomes, partners can be trusted advisors in the process of building your continuity strategy, guiding you on your journey, and helping your organization stay up-to-date in skills and procedures. Relying on strategic partners to perform security or continuity testing helps your organization stay alert and make continuity drills a normality in your daily workflow. It is however critical to retain the sense of responsibility for continuity within your organization, as large-scale adverse events can also disrupt the partner resources that are available during everyday activities.

Strategic partnership assumes trust and transparency. Continuity can be a very sensitive topic and we see a natural tendency to reduce information sharing to a need-to-know basis. This can result in seeking solutions to irrelevant or partial problems (XY problem) and not surfacing critical problems until failure occurs. Be open about the expectations to the partner as well as the circumstances and conditions under which you'll share information. A strategic partnership for improving continuity throughout your organization should not be viewed as a customer-vendor relationship, as there is no well-defined good to vend.

People perspective

Culture evolution

"A culture of resilience entails everyone making it part of their job, considering anything non-resilient as poor quality, and collectively addressing potential failure conditions and working to mitigate them." (M.Schwartz, A Culture of Resilience, AWS Cloud Enterprise Strategy Blog)

Incentivize ownership by allowing teams to come up with their own best practices for resiliency that align with the cross-organizational strategy, enable teams to make practicing resiliency a common activity. Allow for independence in tactical decision-making during crises. Promote rapid feedback when potential problems are spotted anywhere in the organization, and steer away from placing blame. Evaluate the state of the organization to understand behaviors, attitudes, cultural norms, and other factors that attribute to the willingness and readiness to adopt best continuity practices in the cloud. Draw attention to the potential friction points and generate momentum by addressing the recurring concerns.

People perspective

Transformational leadership

As a cross-organizational feature, continuity needs strong top-down support from leadership, from both a technological and an organizational perspective. Make sure that technology and business leaders co-develop and co-lead continuity of IT in the organization. If you have an established digital transformation office, use it to evangelize and drive the efforts throughout the organization through prescriptive patterns and advice. Examples of cross-government top-down support include the UK's Government Cyber Security Strategy 2022-2030 and The Singapore Cybersecurity Strategy 2021.

Having strong leaders who are available during adverse events, helps an organization through the crisis. While you want to build a culture where teams are independent in reacting to crisis, there is high value in having empathic strategic leaders to both support the workforce and shield the organization from unnecessary external pressures, while building communities of practice to support the development of other leaders. Leaders act as single points of contact during a crisis, and are in the best position to retroactively evaluate, how well the organization as a whole was able to react and recover.

People perspective

Cloud fluency and skills transformation

Use continuity as a driver to upskill your cloud workforce in best practices in security, compliance, automation, observability, and cost management.

Capability and skills can be hard to hire, train or retain. There are resources such as the AWS Training & Certification resources to support skills development. This assessment tool can help identify learning needs. In the UK, the government-funds the Digital Skills campaign.

If you have chosen to work with partners, you can leverage their expertise as a way to train and develop people in the organization who work alongside them. As you progress, build an inclusive team with technical and non-technical skills to align technology and business needs.

Organization design

Ensure your structure and capabilities fully support continuity goals. Consider a Cloud Center of Excellence to own continuity mechanisms and event handling. Identify who will make decisions about specific elements of your crisis response and include managed service providers and partners as well as internal individuals or teams.

Governance perspective

Program and project management

Manage your continuity program with agility. Set clear objectives, validate progress, and stay flexible on details. Keep stakeholders informed of course corrections.

Regulatory compliance management

Align your continuity objectives and mechanisms with the regulatory context you operate in. Leverage AWS services and partners to establish robust compliance controls. You can find information on the AWS shared responsibility model; AWS compliance programs; AWS security products and Partner solutions. AWS Professional Services can also help you establish mechanisms.

The AWS Digital Sovereignty Pledge describes how digital sovereignty is and will continue to be built in to AWS Cloud by design. At the same time, you want to encrypt everything, everywhere and leverage confidential computing directly to build additional layers of control over your environments, giving you even more levers to address regulatory requirements.

Platform perspective

Platform architecture

A well-architected cloud environment facilitates continuity through standards, guardrails, and blueprints. Consider workloads with different continuity requirements, for example simple data backup at one end of the scale to entire infrastructure backup or duplication at the other end.

Data architecture

Resilient data is core to continuity. Implement mechanisms to validate data authenticity and integrity, and manage dependencies between data sources through data taxonomies.

Platform perspective

Data lifecycle management

Define policies for data retention, archiving, and deletion based on sensitivity, compliance, and business needs. Implement automated mechanisms to manage the full data lifecycle, including backups.

The elements of data lifecycle management:

- Legal and regulatory requirements around data retention
- Policy around retention of that data type
- Data deletion policies around that data type
- Business operation needs

Data classification provides a way to categorize data, based on criticality and sensitivity in order to help you determine appropriate protection and retention controls. Data classification policies determine how long the workload should retain the data and backups. They ensure organization-wide compliance with regulation. More information on data retention can be found in this resource about data sustainability .

Defining the archival and deletion policies enable cost-effective data storage so that for example data isn't stored beyond its deletion date. Data loss due to corruption, natural disasters, or malicious internal employee can occur at any time.

Consider distributing your backups to at least two different regions if allowed by European Union's (EU) General Data Protection Regulation (GDPR), Brazil's Lei Geral de Protecao de Dados (LGPD), China's Personal Information Protection Law (PIPL), and Japan's Act on the Protection of Personal Information (APPI) among others.

These AWS resources help automate backup, cost-effective archiving throughout the data lifecycle.

Platform perspective

Software development lifecycle resilience

There are a number of ways to incorporate resilience into the software development life cycle (SDLC). AWS have many articles that speaks about SDLC and what kind of steps that you can implement to improve your resilience posture. In this section we will talk about common recommendations and pattern that any leader needs to be aware of to create a resilient environment

There are five steps that needs to be implemented before any organization can start to fully incorporate resilience into their SDLC. The steps that need to be implemented are:

1. Detection: An organization needs to be able to recognize that there is an outage or a disaster taking place. You can only recognize the outage even if you are able to observe and monitor your system.
2. Evaluate: An organization needs to be able to evaluate the and quantify the outage/disaster event.
3. Response: An organization needs to be able to respond or mitigate different outage/disaster events.
4. Recover: An organization needs to be able to recover from outages/disaster events.
5. Confirmation: An organization needs to be able to confirm that their systems have return to their standard operating behavior.

Implementing many of the above steps will require any organization to implement observability in every corner of their environment. It all starts with setting up the right environment and how are you going to architect your organization. Almost every organization will be using more than one account to deploy their workloads. If that is the case then it's very important to understand how this is done in AWS in the easiest possible way. AWS Organizations is a service that can allow you to create and structure your accounts to match your actual units (also called organization units) in reality. It allows you to set boundaries and to define organizational units within your own organization.

Structuring your organization in the right way can make all the difference when you need to understand how your organization operates. Also, it can give your organization visibility into the activities and common patterns that takes place across the entire organization. This is very important during a disaster event because it allows you to control the whole organization from one place. Embed resilience throughout your SDLC, from detection and evaluation to response, recovery, and confirmation. Use services to help you. For example, AWS Organizations to create and structure accounts to match organization units; AWS Control Tower to control who can create new accounts; and AWS CloudWatch to observe and monitor resources and applications whether on the cloud or on premises.

The ability to recover from outages/disasters and how you can respond to such events can be done by using a number of reference resilience architectures. AWS has been developing a number of architectures that allow us to mitigate those events for our clients and we openly share architectures with our customers. Some of these strategies are:

- Infrastructure As a Code (IaC): defining your infrastructure as a code, backing up those scripts in multiple zones or regions allows you to redeploy your compromised environment components in a very short time. Using IaC scripts in deploying your environment takes the human error out of the equation and provides and standardized way to define your systems.
- Cell architecture: this type of architectural design limits the disaster blast radius.
- Leveraging AWS services: over the years AWS has rolled out a multitude of services that can help you in accomplishing your resiliency goals. AWS Resilience hub, AWS Backup and AWS CloudEndure are just some of the well-known services that can really help any organization to realize their resiliency goals. AWS incorporates resiliency in most of our services and has many customers that require resilient systems and as such we have built our knowledge over years of joint customer collaboration to achieve the highest standards of resiliency.

Security perspective

The AWS CAF security perspective helps achieve confidentiality, integrity, and availability of your data and workloads. Its capabilities include identity and access management, detective controls, infrastructure security, data protection, and incident response.

AWS CAF helps you increase program maturity and efficacy, while shortening timelines and reducing costs. The difference in using the cloud is fundamental and impactful - you no longer manage physical security of your data centers, nor the related design, implementation, training, deployment, or maintenance of them. AWS provides and secures the data centers and manages all physical upgrades and maintenance. You can use software-based security tools to monitor and protect the flow of information into and out of your cloud resources. As an AWS customer, you reap the benefit of all the best practices of AWS policies, architecture, and operational processes that satisfy the requirements our most security-sensitive customers.

Security perspective

The security perspective focus is on an organization's ability to respond and restore; the visibility of resources, monitoring, ability to react, contain and recover. Large-scale disruptive events illustrate how important it is for public sector organizations to respond rapidly to keep essential services running, as well as to quickly pivot to offer new services. This agility, along with the security and flexibility needed to respond to change and disruption, are the foundations of digital resilience and why we see digital resilience as a key factor in the digital transformation of government.

Digital resiliency is the ability of an organization to rapidly adapt to business disruptions by leveraging digital capabilities that both restore business operations in a timely manner, and also capitalize on the changed conditions

Security perspective

Strong security is a core enabler of digital transformation, helping organizations adopt machine learning (ML), artificial intelligence (AI), big data, and the speed and scale of the cloud to meet changing g business conditions and evolving customer needs. The key is that digital resiliency is not just defensive as in disaster recovery or cybersecurity; digital resiliency is also proactive in that government and education organizations use technology to improve services in response to changing circumstances and/or disruptions.

Strong security is a core enabler of digital resiliency, helping organizations adopt machine learning (ML), artificial intelligence (AI), big data, and the speed and scale of the cloud to meet changing business conditions and evolving customer needs. Each organization's cloud journey is unique. To succeed in your transformation, you'll need to envision your desired target state, understand your cloud readiness, and adopt an agile approach to closing the gaps. Organizations can accelerate their journey by leveraging resources that are architected to align with AWS best practices and country-specific compliance frameworks.

- Landing Zone Accelerator: A foundational infrastructure for deploying mission-critical workloads across a centrally-governed multi-account environment.
- Customer Compliance Guides (CCGs) cover 100+ services and features offering security guidance mapped to 10 different compliance frameworks.
- The AWS control without compromise pledge shows that AWS services have no mechanism through which AWS could access your data.

Operations perspective

Availability and continuity management

Through the implementation of automated performance testing, running game days, and the incorporation of chaos testing, organisations can proactively detect potential failure scenarios in their systems prior to their manifestation, thereby preventing any further downtime. This enhances the reliability and resilience of the system.

Chaos engineering is the discipline of experimenting on a system in order to build confidence in the system's capability to withstand turbulent conditions in production.

Chaos engineering does not introduce chaos into your systems, rather, it uncovers the chaos that is already there. By definition, chaos experiments should be fail-safe and tolerated by the system. It is therefore key that you use tools that allow for controlled experiments. A controlled experiment possesses a well-defined scope of impact, which includes rollback mechanisms, and is tightly integrated with monitoring systems that offer comprehensive real-time analysis of the experiment's impacts.

Chaos engineering allows teams to gain knowledge from failures and systematically assess, quantify, and enhance the ability of their workloads to withstand disruptions. By consistently implementing chaos engineering, you can identify and resolve shortcomings in your workloads to avoid a detrimental impact on availability and operation.

Chaos engineering tools

AWS Fault Injection Simulator (AWS FIS) is a fully managed service for running fault injection experiments. These faults include termination of resources, forcing failovers, stressing CPU or memory, throttling, latency, and packet loss. Since it is integrated with Amazon CloudWatch alarms, you can set up stop conditions as guardrails to rollback an experiment if it causes an unexpected impact. Third party tools include open-source tools such as Chaos Toolkit, Chaos Mesh, and Litmus Chaos, as well as commercial options like Gremlin. To expand the scope of faults that can be injected on AWS, AWS FIS integrates with Chaos Mesh and Litmus Chaos, allowing you to coordinate fault injection workflows among multiple tools.

Operations perspective

Emergency preparedness management

Conduct regular game days to test systems, processes, and team responses. Implement emergency levers to ensure critical components can withstand failures of non-critical dependencies.

Game day features

1. Game days test services where operational failure could result in significant consumer or citizen impact and/or reputational impact to the government.
2. Game days are holistic events. You will create an elaborate map to show how people and processes in technical and non-technical spheres interact and what technologies they use.
3. Define and execute failure scenarios to see how systems respond and adjust to prepare for real-life situations.
4. Observe and document people, process, and technology reactions in the face of failure.
5. Integrate the lessons learned into system design.

Tools

AWS Fault Injection Simulator is a fully managed service that runs fault injection experiments on AWS, which makes it easier to improve an application's performance, observability, and resiliency.

Amazon CloudWatch is a monitoring and observability service that provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. Organizations can enable automatic recovery using a variety of AWS services, including Amazon CloudWatch metrics Amazon CloudWatch Events, and AWS Lambda.

AWS X-Ray helps you analyze and debug production and distributed applications (such as those built using a microservices architecture). X-Ray helps you understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors

Operations perspective

Emergency levers

Implementing emergency levers can help build reliable procedures to improve the continuous availability of critical components in your workload.

1. Identify business-critical components in your workload. Each technical component in your workload should be mapped to its relevant business function and ranked as critical or non-critical. For examples of critical and non-critical functionality at Amazon, see Any Day Can Be Prime Day: How Amazon.com Search Uses Chaos Engineering to Handle Over 84K Requests Per Second.
2. Design and architect the critical components in your workload to withstand the failure of non-critical components. During dependency analysis, consider all potential failure modes and verify that your emergency lever mechanisms deliver critical functionality to downstream components.
3. Test to validate the behaviour of your critical components. Try to avoid bimodal behaviour; for more detail, see REL11-BP05 Use static stability to prevent bimodal behavior.
4. Define the right metrics to monitor for the workload. Some example metrics are latency or the number of failed requests to a dependency.
5. Define the procedures, manual or automated, that comprise the emergency lever, such as load shedding, throttling requests, or implementing graceful degradation.

Conclusion

In this document we gave an overview of the Cloud Adoption Framework for Continuity of Government IT, a map of how government IT organizations can organize and structure their continuity journey, which capabilities they need for success, and how to think about continuity as an integral part of the organization's life cycle.

The foundational capabilities in this document tie into the AWS Cloud Adoption Framework and are presented as an extension of the framework to the continuity and resiliency space.

Further reading

For additional information, refer to:

- AWS Cloud Adoption Framework (CAF)
- Continuity of Government IT on AWS (CGIT)
- AWS Well-Architected
- AWS Architecture Center
- AWS Prescriptive Guidance
- AWS Whitepapers & Guides

Contributors

Contributors to this document include:

- Yuliya Linetskaya, Principal TAM, Enterprise Support
- Rovan Omar, Principal TAM, Enterprise Support
- Mohamed Ismail, Sr. Solutions Architect, WWPS Solution Architecture
- Bill Ohlson, Principal Executive Security Advisor, WWPS Solution Architecture
- Tõnis Pihlakas, Technical BDM Continuity, WWPS Industry