McKinsey & Company

Public Sector Practice

# How US states can protect coronavirus-benefits programs

Fiscal-relief programs are straining state governments as they try to meet demand, opening systems to risks of all kinds. Several short-term actions can help state agencies combat risks.

*by Juan Aristi Baquero, Sean Christiansen, Adrian Murphy, and Eric Schweikert*



May 2020

**As COVID-19 sweeps through** the United States, state governments are responding by rolling out new or modified fiscal-relief programs amid substantial funding from federal aid packages. Child-nutrition programs, for instance, have transitioned operations to pickup and delivery models, and eligibility for unemployment-insurance (UI) benefits has been expanded via the Pandemic Unemployment Assistance program under the Coronavirus Aid, Relief, and Economic Security (CARES) Act, offering relief for laid-off or furloughed workers. These programs help safeguard the standard of living for many Americans.

However, the unprecedented scale at which state governments are disbursing benefits is putting pressure on the system. Outdated IT systems are straining to process surging benefit applications as quickly and accurately as possible. Service delivery is stressed by overwhelming demand brought on by crisis conditions and remote-work operations for which many state government agencies and functions were not prepared. To meet demand, states are rapidly rethinking service operations across people, processes, and technology, causing strain and creating opportunities for fraud of various kinds. And for newly created programs such as the Pandemic Unemployment Assistance program, the lack of existing processes and well-understood criteria is itself a source of risk.

As states aspire to achieve their service-delivery objectives (speed, scale, integrity, and efficiency), they have ten common types of risks—including fraud, cybersecurity, and data privacy, as well as error liability, technology, and those from third parties—to manage and balance (Exhibit 1). Risk-prone service delivery can undermine the effectiveness of economic-assistance programs and prevent critical services from reaching eligible recipients.

To provide people with lifesaving services and address associated risks in the short term, states can take a number of actions, including thoroughly testing, upgrading, and patching software applications to mitigate cybersecurity issues; pursuing process improvements and new technologies to manage fraud; and increasing quality control. Actions taken now to address these most common issues can help states establish long-term risk operating models.

## Mitigating and preventing risk: Short-term actions states can consider

Fiscal-relief packages help governments meet three goals. First, they protect the well-being of individuals and households, minimizing income loss and reducing the number of people who fall below the poverty line. These packages also help employers weather the crisis and avoid failing due to a liquidity crunch and temporary revenue shocks. Finally, they help the financial system maintain stability and avoid a wider economic recession or crisis.

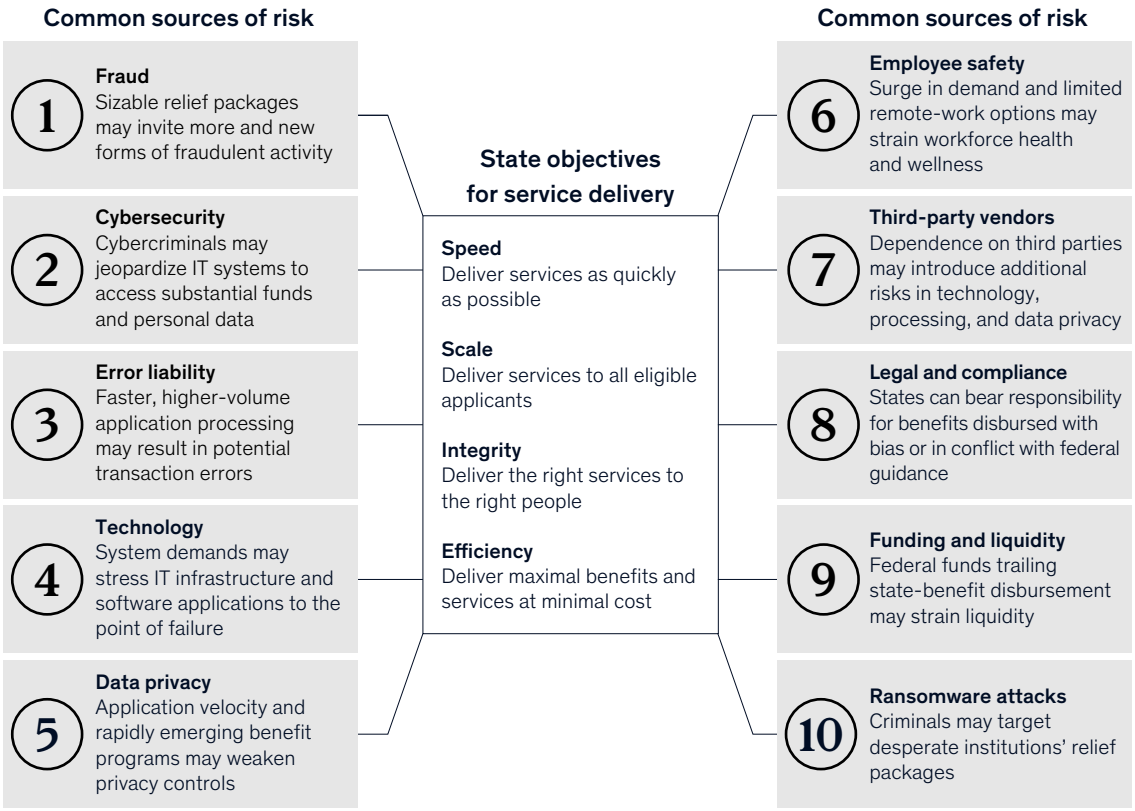
However, the administration of emergency relief packages heightens the risk of fraud and associated problems as states face pressure to execute these services quickly, often before they are ready to support new requirements. This can result in overloaded internal infrastructures.

State programs have always been susceptible to various types of risk. In July 2019, for instance, the state of Maryland was the target of hackers who illegally accessed personal information about residents stored in older databases. Today, the sheer volume of funding and requests for benefits arguably increases the likelihood of security problems.

**To meet demand, states are rapidly rethinking service operations across people, processes, and technology.**

Exhibit 1

## States have to balance managing common risks while achieving service-delivery objectives.




To achieve their objectives, states can break down the citizen journey[1] to identify the likelihood of risk incidents at each step, focus on mitigating actions, and determine the likely impact of risks (Exhibit 2).

Consider fraud, one of the most pervasive risks in relief programs. This risk typically manifests in three scenarios: when identity thieves apply for benefits using stolen identities, when people intentionally provide false eligibility information to qualify for benefits, or when someone provides false information to receive more benefits. To address this issue, states might increase controls for threat detection or triage applications based on risk factors and trends. After-the-fact fraud and abuse analyses could also mitigate risk through automated or deep manual review of cases to validate decisions made quickly at the time of application.

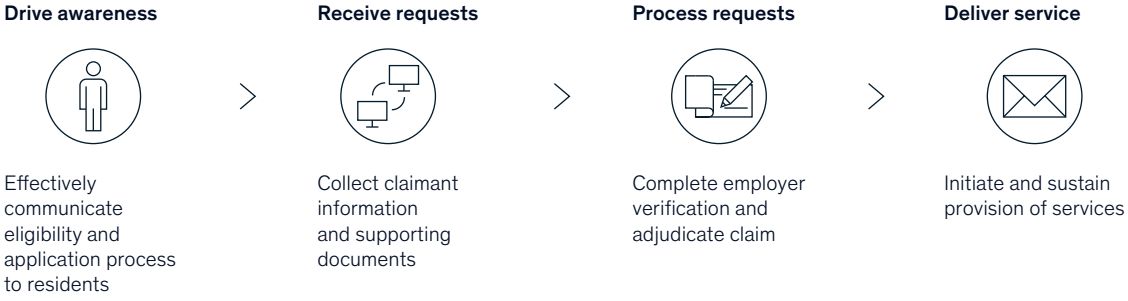
Cybersecurity risks can happen across all steps in the service-delivery journey. They could be addressed by educating employees and service

[1] The customer service–delivery process consists of four phases: raise awareness (communicate eligibility and application process to residents), receive requests (accept claimant information and supporting documents), process requests (complete employer verification and adjudicate claim), and deliver service (initiate and sustain provision of services).

Exhibit 2

## State agencies can manage unemployment-insurance risks at each step of a resident's service-delivery journey.

**Steps in service-delivery journey**




beneficiaries about schemes and how to avoid common scams through techniques such as phishing testing. For employees who work remotely, states could provide preconfigured IT equipment that protects sensitive information. Exhibit 3 details other short-term mitigation tactics for these and for the other eight common types of risk.

To illustrate how state governments can take short-term actions to address common risks, we've provided two examples of programs supported by the CARES Act: unemployment-insurance provisions and the Coronavirus Relief Fund.

## Unemployment-insurance provisions

The COVID-19 crisis has created an unprecedented surge in demand for UI benefits. In response, the federal government has introduced relief packages to expand funding availability and flexibility.[2] The Pandemic Unemployment Assistance program, part of the CARES Act, has also expanded eligibility to include new groups of people, such as self-employed individuals and other workers who do not file Form W-2. However, many workers are at risk of not receiving unemployment insurance as many states have outdated technology systems, often dating back to the 1970s and '80s. This creates acute logistical challenges for states as they try to implement new rules and processes.[3]

States need to meet the surge in applications and new benefits programs while managing administrative costs (scale and efficiency) and getting cash to residents more quickly. Agencies can manage risks at each step of the service-delivery journey, from raising awareness to receiving requests, processing requests, and delivering services.

An assessment of the service-delivery journey for unemployment benefits shows that the most relevant risks for states are fraud, error liability, third-party vendors, and legal and compliance. Below are some examples of why those risks might occur, as well as the actions states could take.

### Fraud

The huge volume of unemployment benefits being processed today could increase the prevalence of identity theft—which in turn might be more difficult to uncover as state agencies move quickly to process requests. States could also receive multiple applications across multiple state and federal UI programs, resulting in duplication of benefits given the difficulty of verifying whether someone has already received benefits in another jurisdiction. There may also be risk that people will duplicate and cash multiple versions of the same check or commit first-party deposit fraud.

[2] Ramsey Fahs, Nehal Mehta, Jim Pallotta, Rachel Riley, Sarah Tucker-Ray, Hrishika Vuppala, and Rob Whiteman, "COVID-19: How American states can manage the surge in unemployment services," March 2020, McKinsey.com.
[3] Caroline George, Annelies Goger, and Tracy Hadden Loh, *Unemployment insurance is failing workers during COVID-19. Here's how to strengthen it,* Brookings Institution, April 2020, brookings.edu.

Additionally, some states are considering self-certification of income for independent contractors and self-employed applicants, because work history is harder to verify for this population than for traditional employees. As individuals file for unemployment benefits, state agencies could clearly communicate the risk of prosecution to deter potential acts of fraud. State agencies can also gather income-verification documentation, such as 1099s or prior-year tax returns, up front to deter fraud attempts.

Once agencies have received and processed requests, they could attempt to improve identity- and information-validation processes and risk-assessment tools to ensure that the right people are applying for the right benefits (and only doing it once).

Randomized after-the-fact validation can also help identify potentially fraudulent acts. Using statistical analysis to identify questionable activity, such as multiple beneficiaries sharing the same bank account, can help focus investigations. Agencies can also cross-reference applications across UI programs and follow relevant procedures and controls closely to minimize fraud risk.

**Error liability**

Agent- or applicant-caused errors, such as incorrect personal information, can result in people getting UI benefits they do not quality for. This could affect recipients' finances if the benefits are to be repaid later.

To reduce the possibility of error across the service-delivery journey, state agencies can perform

Exhibit 3

## Several actions can help states prevent and mitigate risks.

| Risk area | Actions for states to consider (select examples) | |
|---|---|---|
| **Fraud** | ✓ Triage applications based on risk factors and trends<br>✓ Use objective formulas or algorithms to reduce reliance on judgment or manual processing<br>✓ Apply relevant controls (eg, identity verification, fraudulent IP[1] addresses and device IDs, known stolen identities) | ✓ Increase quality-control sampling and drive process improvements<br>✓ Perform ex post facto fraud and abuse analyses<br>✓ Increase controls for insider threat detection<br>✓ Share intelligence as needed with partner agencies |
| **Cybersecurity, including ransomware attacks** | ✓ Thoroughly test, upgrade, patch software applications<br>✓ Educate vulnerable groups on cyber best practices (eg, avoidance of common scam techniques)<br>✓ Verify user identity via two-factor or multifactor authentication | ✓ Use captchas to filter and block large-scale automated attacks<br>✓ Provide preconfigured IT equipment for remote work<br>✓ Monitor for cybercrimes and share intelligence as needed |
| **Error liability** | ✓ Surge staff to the most critical or high-risk processes<br>✓ Triage applications based on complexity<br>✓ Thoroughly test new processing solutions and automation algorithms | ✓ Establish clear procedures and train staff on them, especially for steps requiring manual judgment<br>✓ Establish quality-control processes (eg, closed-file reviews) for manual application processing |
| **Technology** | ✓ Scale IT capacity to meet expected demand volume<br>✓ Perform technology-capacity testing at off-peak times | ✓ Redeploy IT resources to most-critical systems<br>✓ Develop IT dashboards to monitor critical systems |

[1] Internet protocol.

Exhibit 3 (continued)

## Several actions can help states prevent and mitigate risks.

| Risk area | Actions for states to consider (select examples) | |
|---|---|---|
| **Data privacy** | Minimize the amount of sensitive data requested; request essential data only | Limit access to sensitive data for essential purposes only |
| | Maintain strong protections of stored sensitive data | Update and reinforce privacy policies |
| **Employee safety** | Identify essential and high-risk workforce segments | Stagger work shifts to maintain physical distancing |
| | Implement remote-work options, with regular check-ins | Expand and emphasize healthcare benefits |
| **Third-party vendors** | Contract reputable vendors, adhere to robust due diligence and onboarding | Review and reinforce data-sharing and privacy policies |
| | Propagate expected demand to size needed capacity | Increase communications to better monitor performance |
| **Legal and compliance** | Obtain clear understanding of federal guidelines | Update procedures for petitions and disputes |
| | Establish audit trail to ensure proper handling | Maintain close contact with federal or state administrators |
| **Funding and liquidity** | Determine expected availability of relief packages | Establish agreements with federal government for financial reimbursement timelines |
| | Estimate benefits delivery and cash-flow timelines | |

robust, end-to-end testing of new processes and technology. This might mean clarifying application forms and eligibility instructions to steer applicants correctly, establishing clear quality-assurance and quality-control processes for new programs or highest-risk cases, flagging answers that are inconsistent with known information about a user, and prepopulating data from state sources when possible.

**Third-party vendors**

States that rely on third-party vendors run the risk that those organizations' technology systems might fail or be unable to adjust to the increased demand of applicants. To eliminate vendor risk, state agencies can pursue a few actions. First and foremost, states can ensure that vendors have strong testing capabilities and a track record of operating at scale. They can also lean on their

States that rely on third-party vendors run the risk that those organizations' technology systems might fail.

vendor-management policies and contracts to enforce quality requirements and achieve the urgency needed for technology modifications during the crisis. Should any issues arise, operational managers can call on agency executive leadership to help manage vendor relationships.

**Legal and compliance**
State-agency employees can ensure they clearly understand federal guidance and legal and compliance requirements from the US Department of Labor. Doing so significantly reduces the risk of potential bias or conflict while disbursing benefits. In the case of ambiguities, employees can ask the agency or seek counsel. Maintaining a traceable audit trail of UI-benefit approvals and approval processes is a good way to ensure all state-agency employees are on the same page and working in a consistent manner.

## Coronavirus Relief Fund

As part of the federal government's CARES Act, the Coronavirus Relief Fund (CRF) provides $150 billion in funding for state and city government expenditures related to the COVID-19 emergency response.[4] The intent of the fund is to allocate critical funding to COVID-19 response efforts, making sure that limited funding goes to cases of highest need. States have discretion for where and how to spend this money, though spending must follow CARES Act and subsequent guidance on eligible uses.

But the funds are already subject to risks. The FBI has issued warnings about COVID-19 stimulus-package scams, and hackers and scammers have ramped up online attacks to take advantage of the coronavirus pandemic.[5] A McKinsey analysis of the current situation shows that the most relevant risks for states are in legal and compliance, technology, error liability, fraud, and funding and liquidity risk.

**Legal and compliance**
State agencies are responsible for ensuring that funding is allocated fairly and without bias, adhering to federal guidance regarding use of CRF funds. To avoid accusations of bias or unfairness, agencies can design the service-delivery journey to provide transparency to stakeholders around compliance requirements. An example might be publishing a report or holding virtual public hearings.

Establishing proactive communications with the US Department of the Treasury and the CRF program management office can reduce the risk of compliance issues. Keeping detailed audit records on use of funds is also helpful. Agencies are likely already doing this for other programs, but because the CRF is a new program, states need to make sure their records align with federal guidance and satisfy relevant monitoring and oversight from the Treasury's inspector general. Further, state agencies can establish and monitor KPIs that measure inequities across geography, race, and class to better identify and provide funding to those who need it most.

**Technology**
When faced with a significant volume of requests for funding, states need to be able to rely on the technologies used to process applications and distribute funds. Performing tests on these tools can mitigate the risk of funding-transfer breakdowns during transaction or approval processes.

**Error liability**
For state agencies to process applications, disburse money, and keep records without error, they will likely need to improve procedures for receiving, processing, and allocating funding disbursements. Agencies will need to understand the processes involved in this new program so that they can train employees appropriately. Even employees who have been involved in disbursements before will need to learn new protocols and be tested before they can begin work.

**Fraud**
Many of the current fraud controls in place are very manual in nature, can put a high onus on the applicant, and may inhibit disbursement. These controls may need to be adapted to allow money

[4] Bill is still subject to regulatory updates.
[5] Alfred Ng, "FBI issues warning about COVID-19 stimulus-package scams," CNET, March 26, 2020, cnet.com.

## Protecting against fraud in the long term

**When developing** a long-term risk operating model, state agencies can plan for three phases in parallel: investing in medium-term fraud intervention tools, setting clear fraud aspirations, and making strategic shifts in how fraud management is handled.

For the medium term, agencies can invest in fraud intervention and mitigation tools to help them better protect service beneficiaries. Examples of tools are SMS authentication, automated-ID document review, validation of income and employment verification through tax returns, and comparison to third-party reporting via 1099s and W-2s. These tools can be used to mitigate short-term risks as well.

Agencies could set clear goals for different parts of the organization—such as operational efficiency, talent and capacity, and speed of response—to help focus their efforts and their responses to fraud. For instance, to reduce fraud while maintaining the speed of response, agencies could focus on improving their ability to detect fraud and make decisions quickly and develop clear guidelines on how to make decisions during attacks. The ultimate goal is to achieve a near-instant response rate for transaction monitoring and rapid decision making for applications.

Over time, changes in fraud management could be based on strategic shifts that address pressing trends and ladder up to a long-term vision. For example, a state agency might decide to focus on prevention through design backed by use cases. In practice, this means continuously examining current and emerging entry points for attacks across operational and customer journeys to reduce the likelihood of a successful fraud event, rather than mitigating losses after an attack.

to get to where it is needed. At the same time, states do need to consider new, more-streamlined, effective controls since risk remains. To ensure that funding distribution follows procurement standards and is used as intended, states could establish control personnel and tools within the state's fiscal-recovery and procurement offices. Employees could measure the efficacy of allocations and monitor for uncompetitive pricing or fraud, waste, and abuse. Setting strict rules on who has the authority to make reimbursement decisions—and how—is another way to reduce or eliminate fraud risk.

**Funding and liquidity**

To meet demand, states need a plan for quick disbursement and reimbursement so that they can maintain a workable cash-flow balance. State agencies could synchronize reimbursement and disbursement timelines with federal and state treasury departments and receiving agencies and municipalities to speed up their work while ensuring that they do not transfer money before they have it. Once states have a short-term action plan in place, they will be better prepared to mitigate risks and meet their core objectives of speed, scale, integrity, and efficiency. This is not the end of the journey for state agencies, however. Once they have achieved stability in the immediate term, states can progress toward building a risk-and-fraud operating model that will protect service delivery in the long term (see sidebar, "Protecting against fraud in the long term").

---

The short-term fraud interventions that state agencies build today can feed into a longer-term strategy for fraud mitigation. As state governments build a stable of effective short-term actions, they can find breathing room to focus on medium- and longer-term risk-mitigation strategies, helping them better protect beneficiaries of fiscal-relief programs.

**Juan Aristi Baquero** and **Adrian Murphy** are partners in McKinsey's New York office, and **Sean Christiansen** is a consultant in the Washington, DC, office, where **Eric Schweikert** is a senior expert.

The authors wish to thank Dan Ward for his contributions to this article.