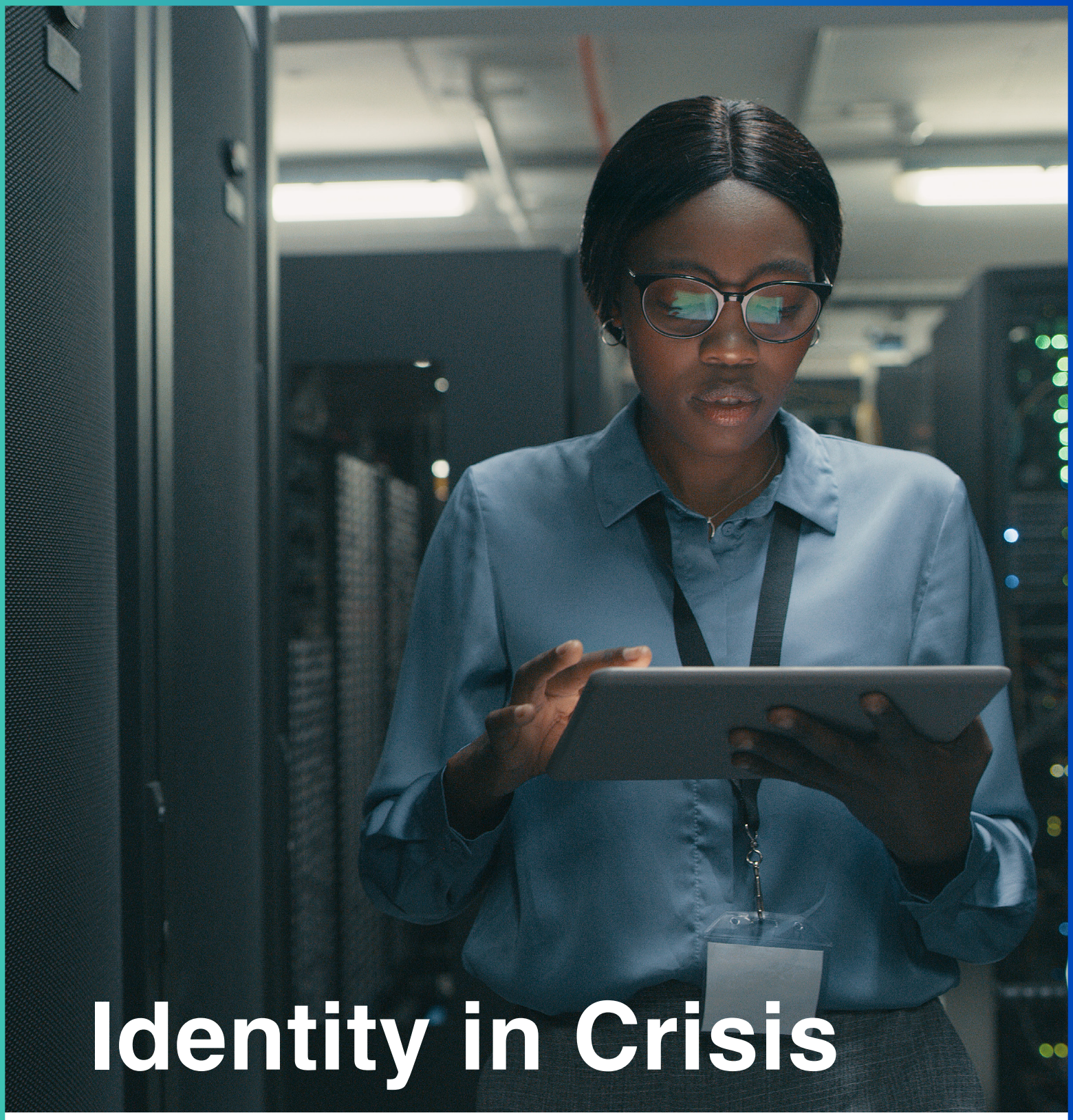

Identity in Crisis

Why Governments Must Build Disaster Recovery Centres for Identity Documents

Whitepaper

TOPPAN

TOPPAN Security

Introduction

Ensuring access to legal identity documents is a fundamental responsibility of governments worldwide. However, disruptions such as system failures, cyberattacks, political instability, and natural disasters can compromise the ability of citizens to obtain or replace essential identification. Without valid identity documents, individuals may be unable to access government services, travel, or conduct financial transactions, leading to severe social and economic consequences.

Identity Disaster Recovery Centres (DRCs) provide a vital solution to this challenge, ensuring continuity in identity services when traditional government operations are compromised. These centres play a crucial role in disaster preparedness by offering identity document replacement, verification services, and public assistance programs. This whitepaper explores the significance of Identity DRCs, the risks of disrupted identity services, and best practices for their establishment and operation.

Consequences of Lacking Legal Identity Documents

When unforeseen disruptions occur, many citizens find themselves without valid identification, making it nearly impossible for them to travel internationally or relocate to safer areas. The inability to prove one's identity restricts access to essential services such as healthcare, banking, and housing, delaying recovery efforts and deepening vulnerabilities. Moreover, individuals without legal identification may struggle with proving property ownership, claiming insurance, or asserting citizenship, which can lead to statelessness and long-term socio-economic hardships.

Proactive Government Initiatives

Recognizing these challenges, some governments have implemented proactive measures to ensure that citizens can quickly recover lost identity documents.

The Republic of Barbados has created an offsite disaster recovery centre, in response to the country being hit by numerous severe weather incidents in the past few years, ensuring that citizens can always acquire passports and identity cards.

Other nations such as Kuwait, the UAE, and Ghana are also cited for proactive disaster readiness strategies in the identity space.

$2.97 trillion
in global economic losses from disasters between 2000 and 2019.

$2 trillion
in damages from extreme weather between 2014 and 2023.

50%
Economic rebound in countries with strong disaster recovery plans, according to the World Bank and International Monetary Fund.

Levels of Disaster Recovery for Identity Documents

Governments can implement disaster recovery solutions at different levels depending on their risk assessments and operational capabilities:

- **Level 1:** *Data Recovery*

  This foundational level ensures the backup and recovery of citizen identity data in an offsite, secure location. Typically, this could be to a secure storage server in a that is used to hold replicated production data. The use of system-to-system data transfer removes the risk of data loss, or compromise, and is more reliable than physically moving media (tapes, hard drives, etc.) between sites. While a system based solely on data recovery does not allow for document production in case of an emergency, it does provide an essential safeguard to authenticate passport and ID information when necessary.

- **Level 2:** *Data Recovery & Operational Capability*

  This level includes both data backup and a limited set of operational stations for enrolment, adjudication, and quality assurance. Even with a minimal setup, having at least one of these processes in place allows a Disaster Recovery Center to function independently and reproduce a small volume of identity documents in case of an emergency.

- **Level 3:** *Full Business Continuity*

  The most comprehensive level, full business continuity ensures that if one identity issuance site goes down, another site can immediately take over operations. This could involve just data recovery in the case of digital credential issue, but more likely will include operational stations and a well-planned supply chain, trained personnel, and the necessary infrastructure to maintain seamless service delivery under any circumstances.

Recovery Objectives for Disaster Preparedness

When establishing a Disaster Recovery Center, governments must define their Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO):

- **Recovery Point Objective** (RPO): How much data a government is willing to lose in case of a disruption. The more frequent the data backups, the smaller the data loss.

- **Recovery Time Objective** (RTO): The acceptable timeframe for restoring full operational capacity. A well-structured DRC should aim for minimal downtime to avoid service disruptions for citizens.

These considerations highlight the need for a tailored disaster recovery approach, allowing governments to build resilience while ensuring their citizens always have access to identity services.

Guidelines for Establishing Identity Disaster Recovery Centres

To effectively set up DRCs for identity documents, governments should consider several key factors. First, selecting the right location is essential. The location must be well removed from the primary issuance centre to ensure that it is not affected by any localised issues e.g. weather events, fires or civil unrest. It should also be located where issuance of new documents to civilians can be easily facilitated. A DRC should be isolated as much as possible from the primary site in terms of using different power sources, transport routes and with completely firewalled IT systems to ensure protection from cyber-attack. Airports and major transportation hubs are often chosen where the government want to use the secondary facility to offer additional or premium services such as expedited document issuance.

Comprehensive service offerings are also crucial. Identity DRCs should facilitate the swift issuance of passports, national IDs, and other vital records. Strong verification processes must be implemented to prevent identity fraud, particularly in periods of mass document issuance.

Operational preparedness plays a key role in ensuring the effectiveness of these centres. A documented procedure for failing over to DR (the Invocation Plan). This would include defined communication channels for engaging with staff and initiating the failover, as well as plans for redeploying the operations staff and blank stock from primary to DR. A good plan also includes a virtual DR team, with named individuals who have defined roles in the event of a disaster. These procedures not only need to be defined but also practiced. Round-the-clock availability is essential, particularly during crises, and staff should be trained in emergency response protocols, customer service, and fraud detection. Investment in secure, resilient IT systems is necessary to handle high demand while protecting sensitive citizen data. Secure backup systems and cloud-based storage can also ensure continued access to identity services in case of major disruptions.

Public awareness and communication strategies must also be part of the equation. Governments should launch public awareness campaigns to educate citizens on available services and the necessary steps to obtain replacements for lost documents. Establishing feedback mechanisms ensures continuous improvement in service delivery and responsiveness.

Conclusion

Ensuring access to legal identity documents is crucial in maintaining societal stability and individual freedoms. Governments must proactively establish Disaster Recovery Centers to mitigate the effects of identity document loss due to natural disasters, cyberattacks, or infrastructure failures. By implementing strategic locations, comprehensive services, and robust operational frameworks, authorities can safeguard citizens' rights and access to essential services. Forward-thinking initiatives, such as those implemented in Barbados, Kuwait, the UAE, and Ghana, provide valuable models for other nations looking to enhance their disaster preparedness efforts.

Copyright © 2025 TOPPAN Security. All rights reserved.

TOPPAN

TOPPAN Security

www.toppansecurity.com
info@toppansecurity.com