.infront

The Hybrid Cloud Company

DISASTER RECOVERY AS A SERVICE

Infront is transforming the way IT is built, consumed and managed with our 'as a service' offerings.

Business Continuity Management

Business continuity management (BCM) in Australian Government entities is governed by the Protective Security Policy Framework (PSPF).

For entities subject to the PSPF, the key mandatory requirement relating to BCM is GOV 11.

Mandatory Requirement

GOV 11   Agencies must establish a business continuity management program to provide for the continued availability of critical services and assets when warranted by a threat and risk assessment.

Protocols, standards and guidelines have been developed to support the mandatory requirements in the PSPF in relation to GOV 11. This includes an expectation that an entity's BCM program should comprise of the following five components:

1. A governance structure that establishes authorities the responsibilities for the BCM program, including the development and approval of business continuity plans (BCPs)

2. An impact analysis to identify and prioritise an entity's critical services and assets

3. Plans, measures and arrangements to ensure the continued availability of critical services and assets

4. Activities to monitor an entity's level of overall preparedness

5. The continuous review, testing and audit of BCPs

In addition to these specific requirements, Australian National Audit Office (ANAO) advices that entities should seek to adopt a BCM approach that is relevant, appropriate and cost-effective.

Disaster Recovery as a Service

The importance of Disaster Recovery

IT systems and their continued availability are essential to the smooth running of the commonwealth. Any interruption to these critical systems can effectively halt the ability of a department to deliver critical citizen services.

Business Challenge

Departments of all sizes are exposed to risk from unplanned outages, and face the challenge of operating 'non-stop' to ensure the smooth running of government and delivery of vital services.

Interruptions due to unexpected system failure, software corruption, maintenance windows, human error, outside threats or disasters have the potential to embarrass the agency and undermine the confidence business has for IT.

Moreover, with so many projects and business as usual tasks pulling vital resources from the more mundane, such as Disaster Recovery (DR) testing, an affordable, fully managed service is required.

The Solution

Our Disaster Recovery as a Service (DRaaS) solution is a subscription based, managed outcome that enables critical services to be replicated from virtual or physical environments to a secure highly-available cloud infrastructure.

With more than a decade of disaster recovery expertise, we go beyond simple backup to ensure all key workloads are protected – and the business continuity plans are tuned to your business priorities and compliance needs.

> "Many services delivered by public sector are essential to the economic and social wellbeing of the society—a failure to deliver these could have significant consequences for those concerned and for the nation."
>
> **– ANAO**

What is Disaster Recovery as a Service?

Disaster recovery as a service (DRaaS) is a fully managed outcome that enables you to rest easy knowing that your critical business systems will be recoverable in the event of disaster. DRaaS is the essential service for todays overworked, undermanned IT as it ensures that all BCP plans are continuously reviewed, tested and monitored for compliance against GOV11.

How it works

We work with you to classify your services in terms of criticality and recovery objectives, so that we can help you achieve the right service level agreement for your business critical systems.

To ensure your organisation is prepaered in the event your BCP is enacted, we offer to continually test your BCP plan for individually protected services on a period defined by you – monthly, quarterly or annually. These tests are non-disruptive and result in an audited event that can be used to report against GOV11.

The process to initiate a BCP is strictly governed. Only authorised individuals have the ability to failover a protected service. In the event that a BCP is initiated, authorised users will be able to securely access the system from any device, anywhere, ensuring seamless business continuity.

Why not just use backups?

Backup is a critical first step towards data preservation and restoration. But you should not rely on it for disaster recovery.

Under normal conditions, your backup is protecting your data. But what would happen if you lost access to your production environment due to hardware failure, human error or some other disaster? Would your agency end up in front of Senate Estimates? This makes DR a necessity, not a 'nice to have', as you run the risk that a single event could put your agency on the front page of every national newspaper.

To truly protect your data, you need a secure secondary storage location and a fully tested, automated way to initiate business resumption. This means dedicating a recovery environment solely for this purpose.

	Disaster Recovery	Backup
Recovery Point	Seconds	12+ Hours, Long Term Retention
Recovery Time	< 4 hours	Days
Replication	Continuous	Scheduled
Reputation	Stella	Cautious Optimism
Business Service	App + Data	Data only
Remote Connectivity	Yes	No

How we help

Failover
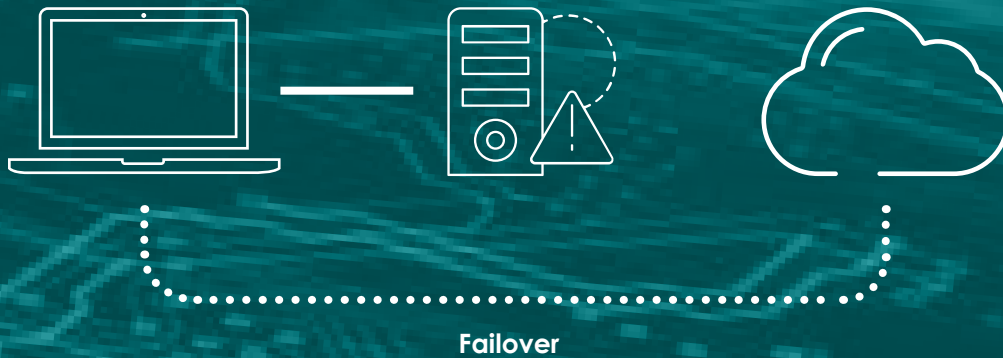
Advisory Services

From business impact and risk analysis to defining your business continuity strategy, we help you identify vulnerabilities that could impact your operations, and define a roadmap for increased BCM preparedness.

Our advisory services include:

• **Business Impact and Risk Analysis:** We help you identify critical business processes and systems that could be affected by an unplanned outage and analyse the effects of losing them. Furthermore, we examine all vulnerabilities and weaknesses that could contribute to a disaster.

• **Business Continuity Planning:** Our experts can recommend options for resilient and recoverable architectures that align with your business impact and risk analysis findings, business policies, budgets, and IT capabilities.

Disaster Recovery Services

Our Disaster Recovery Services provide managed replication services covering a multitude of hybrid cloud use cases including physical to virtual (P2V), virtual to virtual and virtual to cloud (V2C) infrastructure with custom recovery time objectives and 24/7 recovery options.

Our Disaster Recovery Services include:

• **Disaster recovery plan development:** We help you enable quicker, more cost-effective business resumption through the development of disaster recovery plans that are aligned with your business goals.

• **Disaster recovery programme management:** Expertise and best practices developed over 15 years will ensure your BCP plan is ready to go when you need it most.

Benefits

Fully managed offering for peace of mind

Our DRaaS is a turn-key offering that ensures compliance to GOV11 with a fully tested and automated BCM service.

Business outcome-driven consulting

We can help you shape your strategy and implementation with industry leading practices and align it to your specific business requirements.

Seamless operational resiliency

We take responsibility for creating, executing, and maintaining the disaster recovery plan to keep up with your changing operational requirements while you focus on strategic initiatives.

Relevant, appropriate and cost effective

We support you in making the most effective use of cloud-based disaster recovery. Our DRaaS offering removes all capital investments needed to establish a traditional DR service and allow you to only pay for the business critical services you need to protect.

Modular and standardised services

Our services map to ISO 22301 standards. It abstracts the complexity of business continuity management from you, while addressing your requirements in a modular and scalable fashion, and offering a holistic service.

Help power innovation

Our DRaaS frees up valuable resources allowing your team to focus on more strategic initiatives, while we take care of planning, maintaining, and implementing your business continuity plans.

> "We take responsibility for creating, executing, and maintaining the disaster recovery plan"

**DTA
APPROVED**

DTA Approved Service

Infront's DRaaS can be procured through the DTA's Cloud Services Panel, available to all federal, state and territory government agencies.

The Cloud Services Panel provides a platform for agencies to acquire pre-evaluated services with a standard set of terms and conditions, reducing the time and effort of procurement. Agencies can browse and procure this service through the ICT Procurement Portal and searching Service Number: **CSP0002145**

Why Infront?

For 20 years, Infront has been committed to providing you with the best IT solutions to deliver better business outcomes.

We align people, processes and technologies for a fast, cost-effective way to transform IT and realise the benefits of Hybrid Cloud. We partner with you to make your journey to the cloud a success.