

**Certitude**

TECHNOLOGY RISK SERVICES

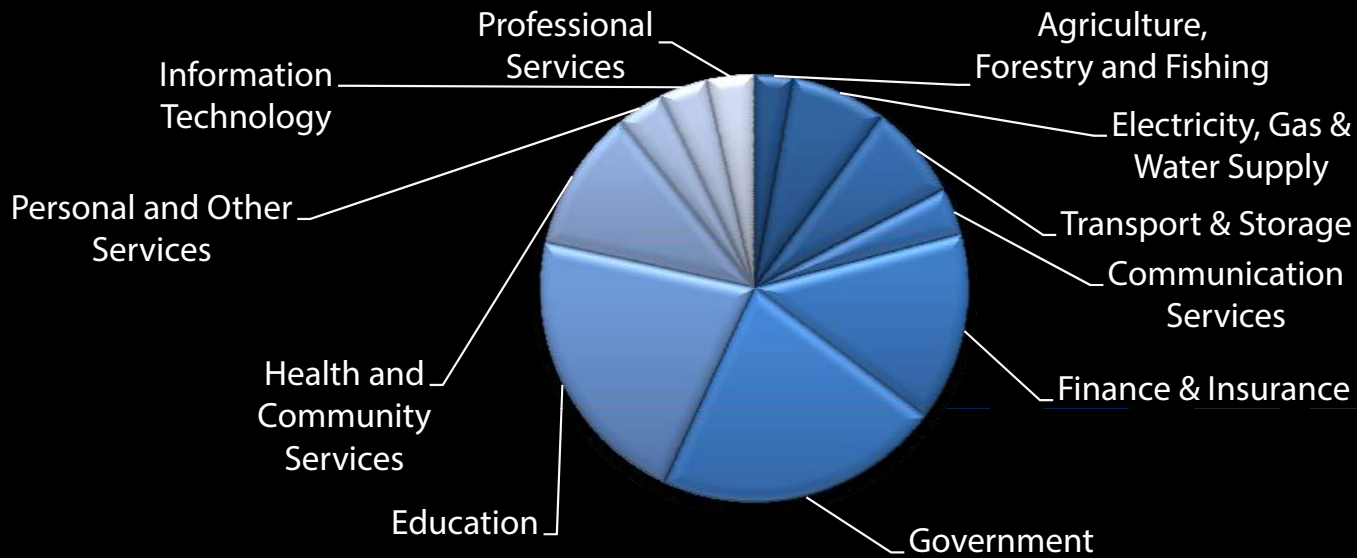
2015  
IT  
DISASTER  
RECOVERY  
SURVEY  
UPDATE

18 Nov 2015

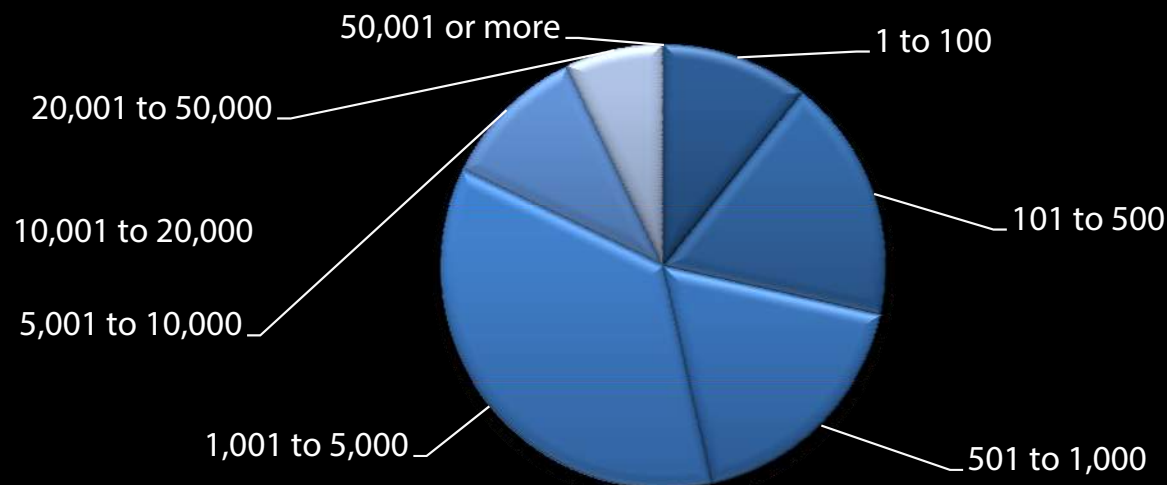


# DEMOGRAPHICS

## Industries



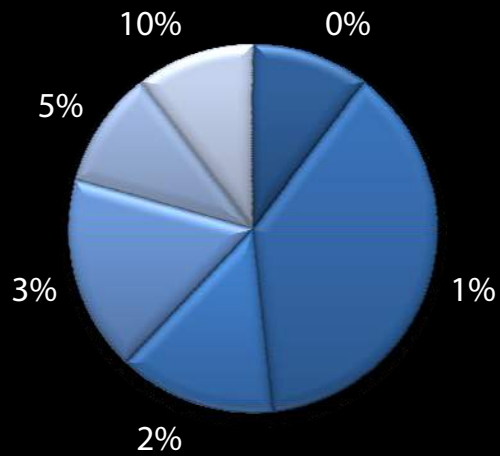
## Employees



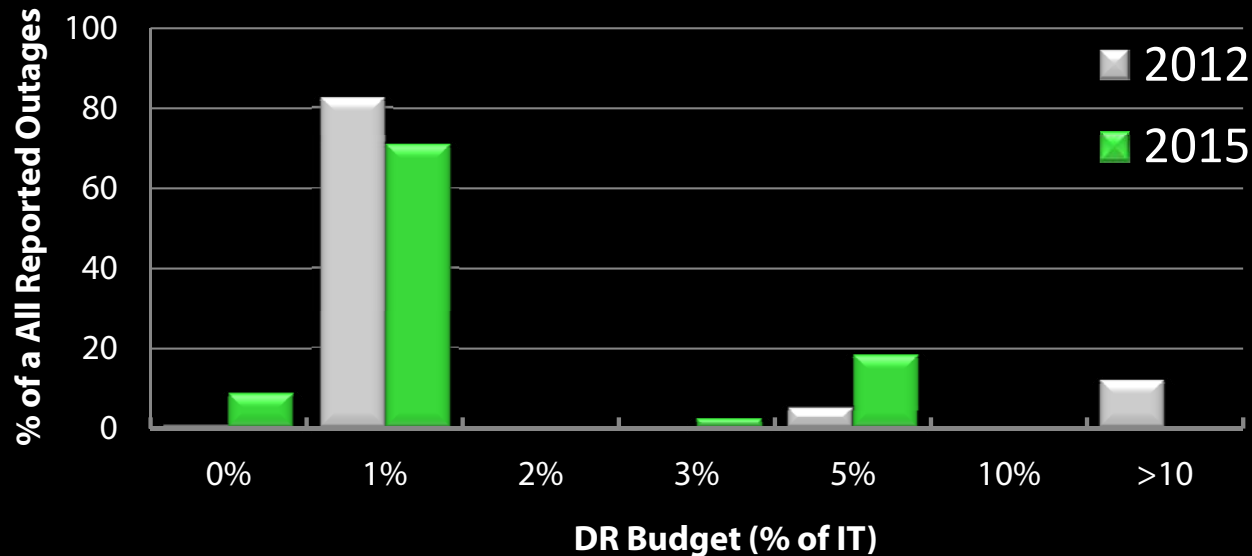
- Organisations operating in **Australia**
- 11 of the 19 ANZSIC **Industries**
- Representation of all **employee** sizes
- All **annual IT spend**, majority \$5m to \$20m

# BUDGET

## DR Budget (% of IT)



## Outages vs DR Spend

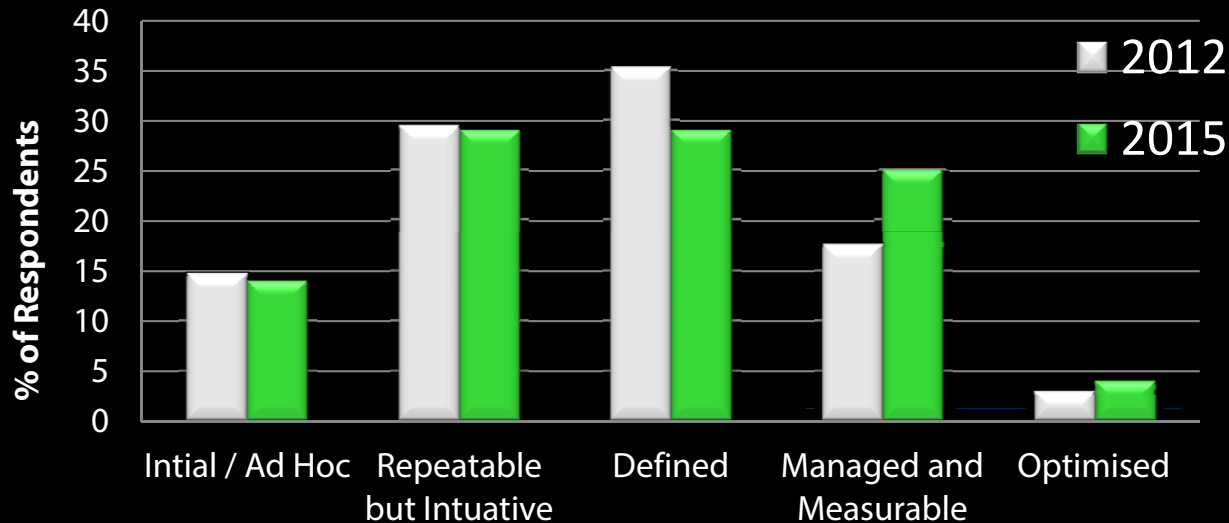


*Respondents who spend at least 2% to 3% of their IT disaster recovery are less likely to incur outages.*

- Most respondents spent ~1% of their IT budget on DR, and incurred the highest % of all outages reported.
- Those who spend 2% to 3% on DR appear to have the least number of outages.

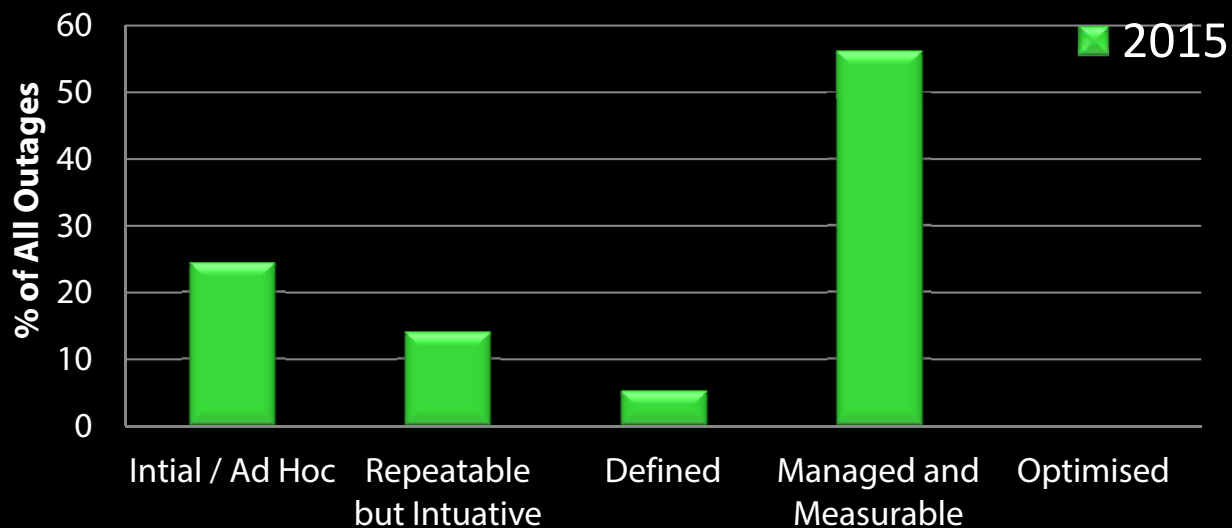
# MATURITY

## Maturity



*Higher levels of disaster recovery maturity can reduce system disruption or provide better statistics.*

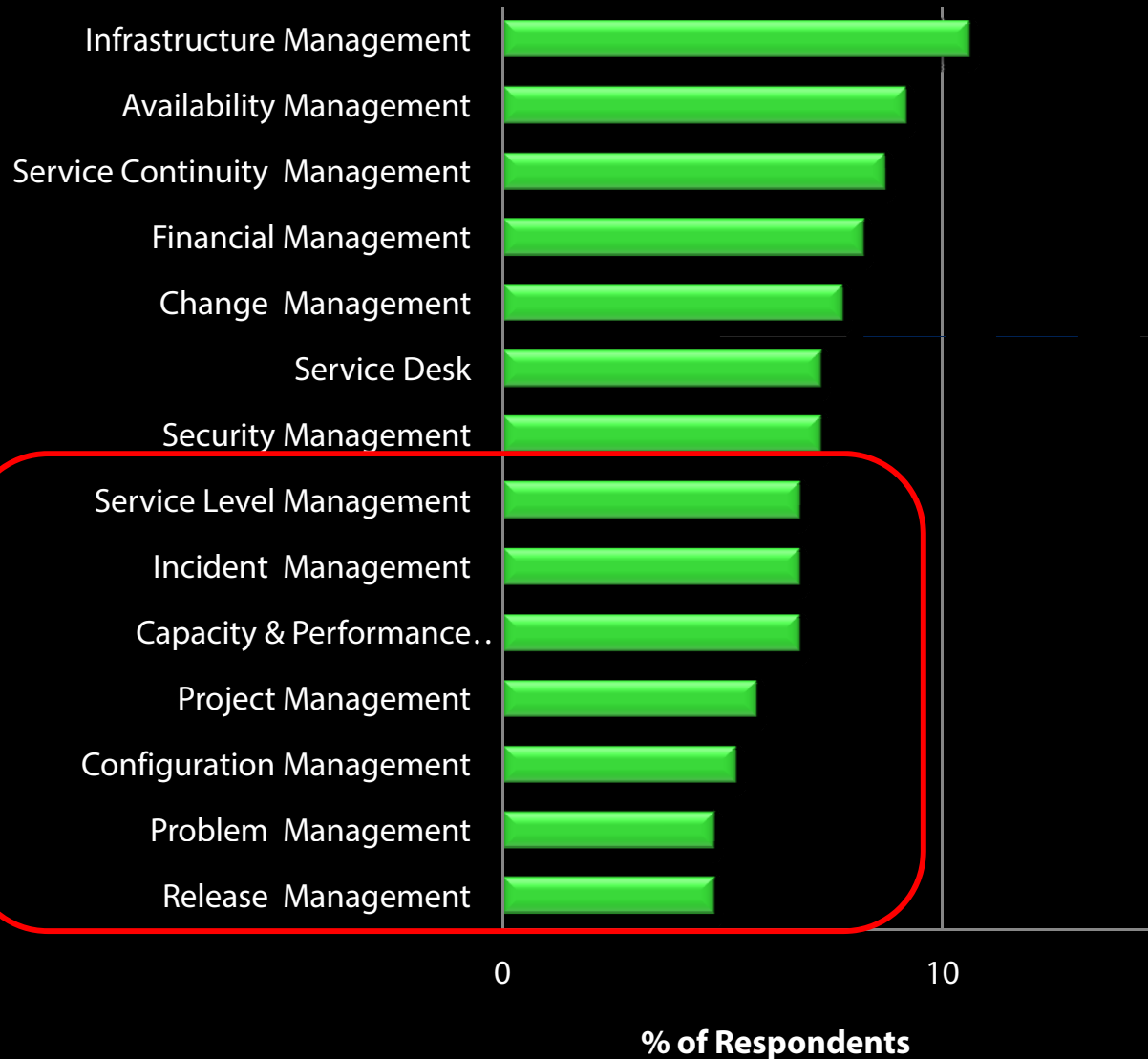
## Outages vs Maturity



- Most describe their DR maturity as **‘repeatable, but intuitive’**, or **‘defined’**
- Whilst low maturity incurred ~38% of all outages, the higher maturity incurred to most. This may be due to better incident recording and reporting.

# PROCESS INTEGRATION

## Where DR is Embedded



*Disaster recovery is poorly embedded into many processes.*

- Most have DR embedded into IT Service Continuity, ICT Infrastructure, Availability, Change, Financial Management
- Few have DR embedded into important processes e.g. Incident, Release, Capacity, Project and Service Level Management!

# DISRUPTIONS

## Outages



Average (hrs)

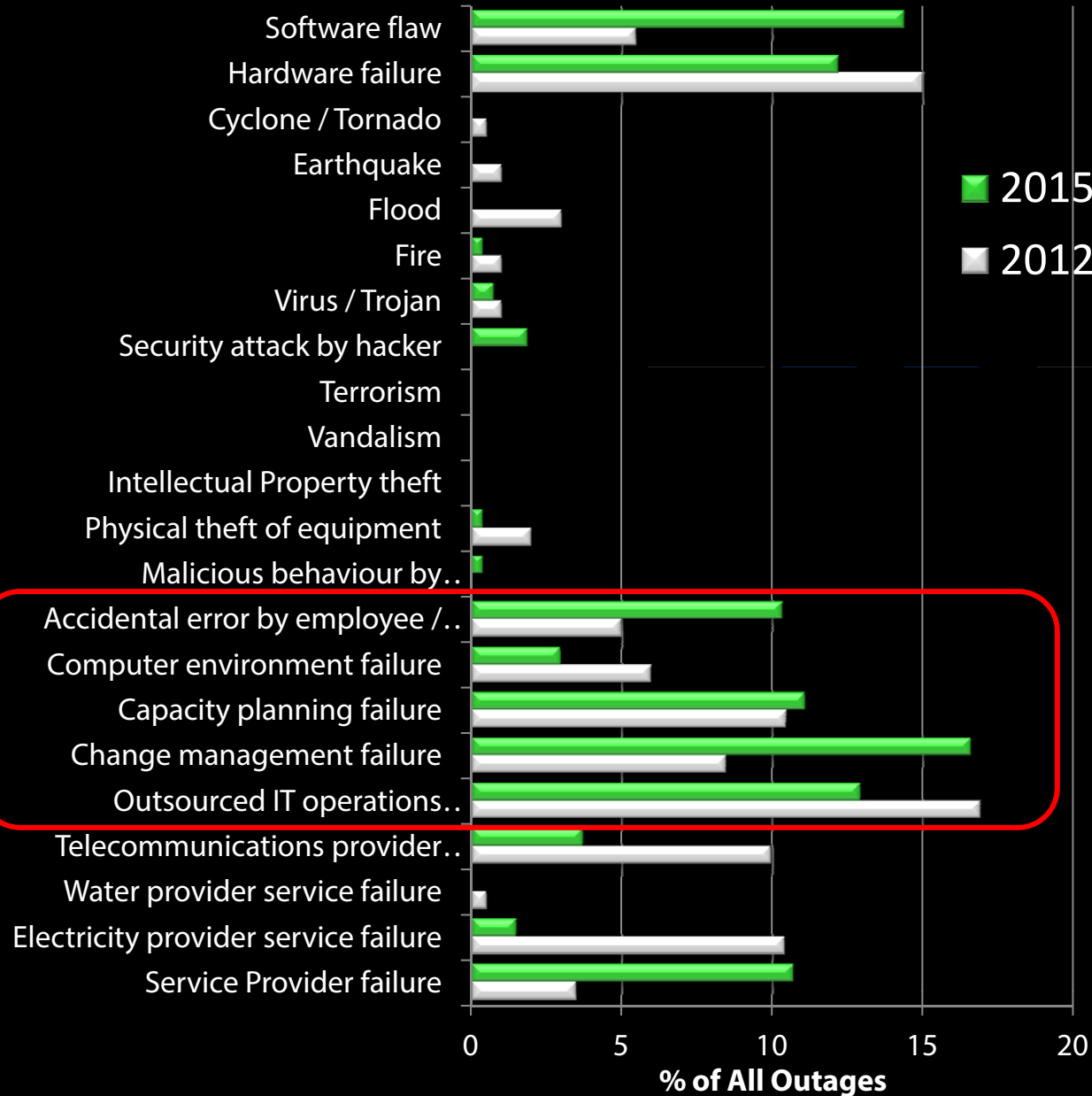


Longest (hrs)

- About a **third** experienced unplanned outages in the past 2 years
- Average length of outages was **2 to 5 hours**.

# DISRUPTIONS

## Root Causes



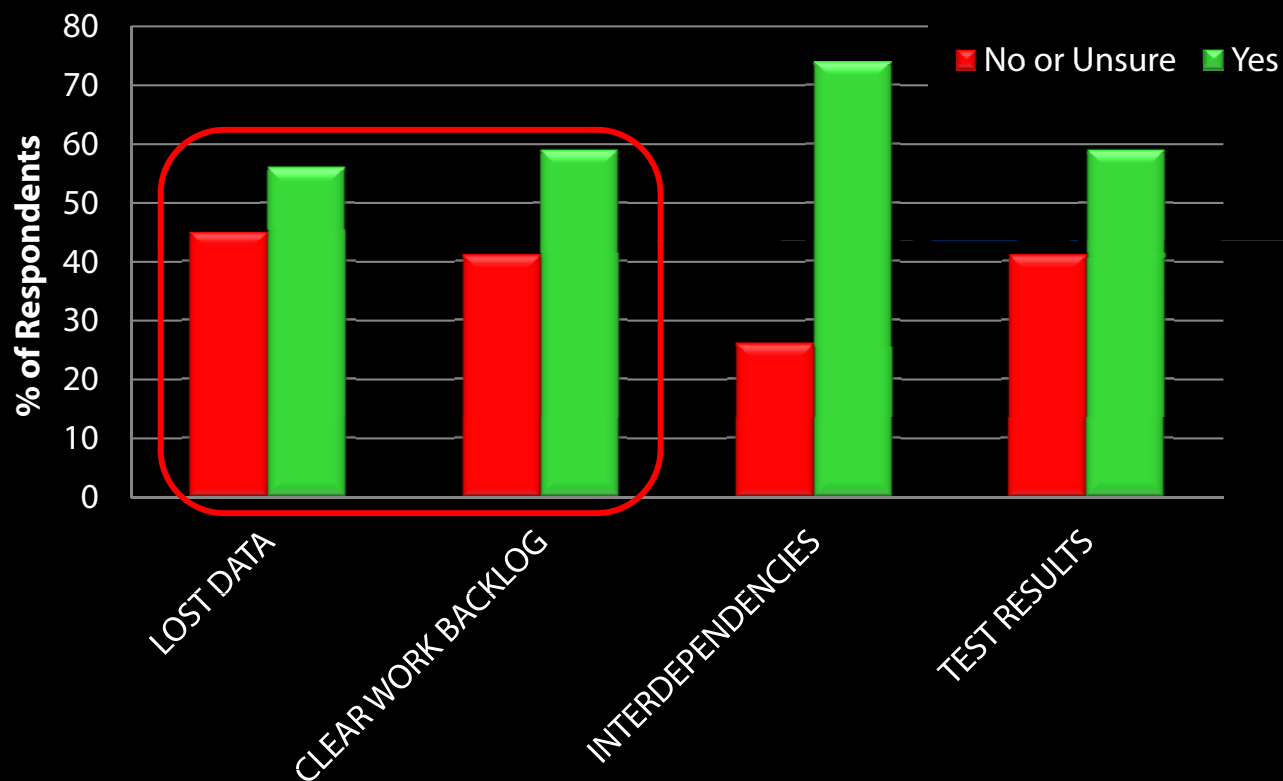
*Many system disruptions are still essentially "self-inflicted".*

- Many causes of disruption can be controlled by processes that are in the **direct control** of the organisation
- Processes that help manage 3rd-parties are neglected even though many outages are caused by third-parties

# RECOVERY REQUIREMENTS

*RPOs are not well Considered.*

## RPO Considerations



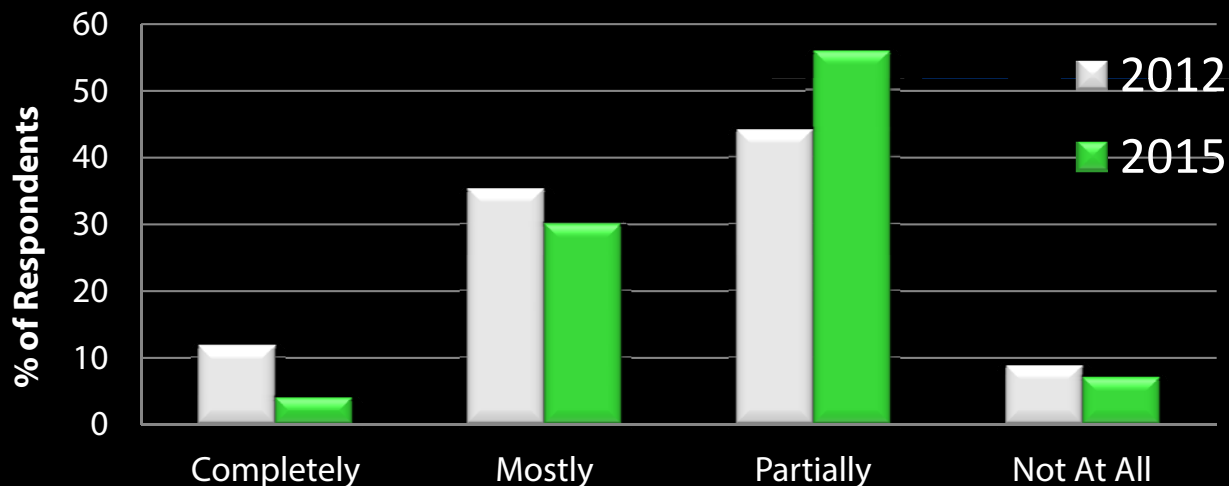
- Work-arounds, and system dependencies are well considered for RTOs
- The **re-entry** and processing of lost data, and the clearing of any work **backlog** is not well considered for RPOs



# EXPECTATIONS & IMPACT

*User recovery expectations are still not well managed.*

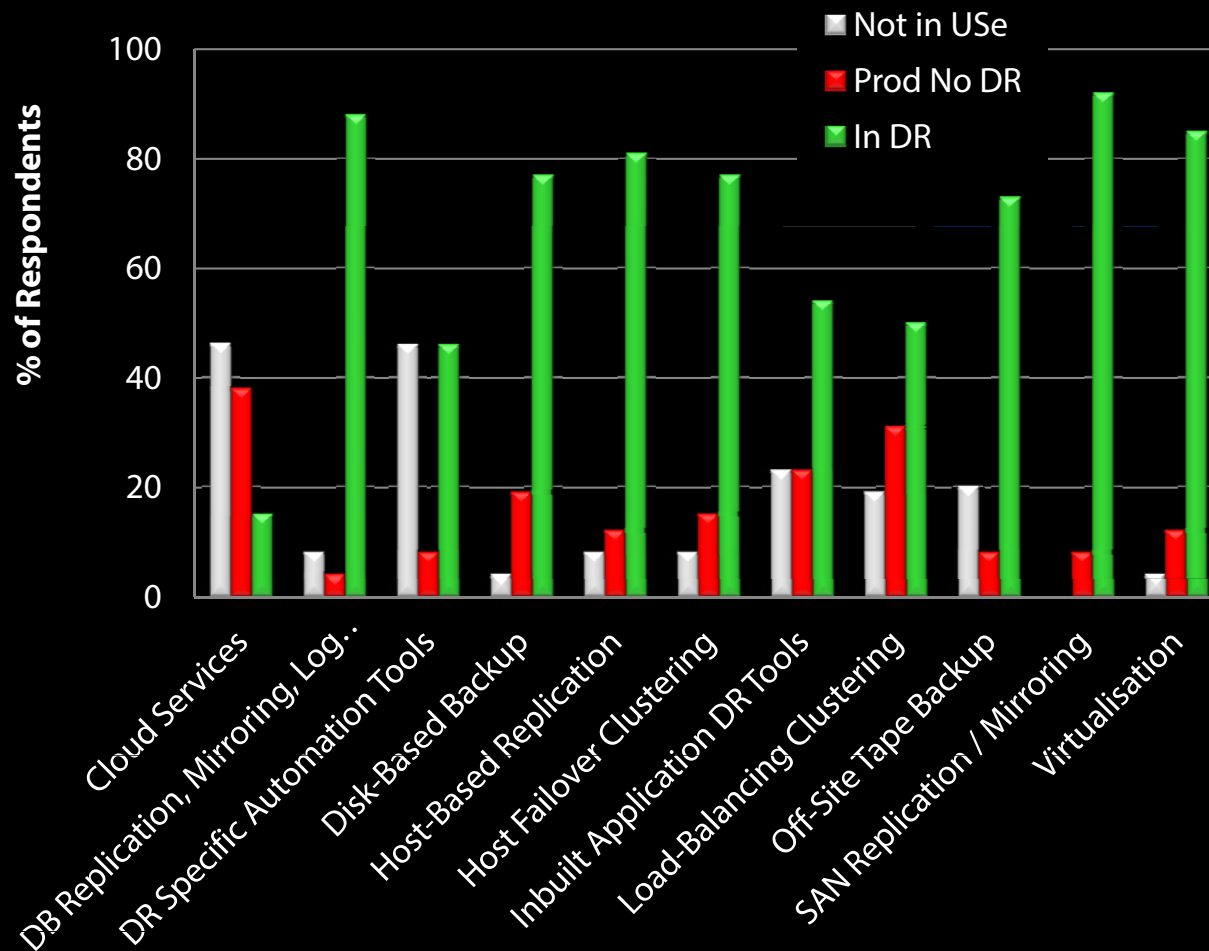
## Expectation Management



- Users are involved but expectations are not well managed
- **Reputational** damage was of high concern, and is the most difficult to actually measure, and quantify
- **Operational** and **financial** impacts also ranked highly

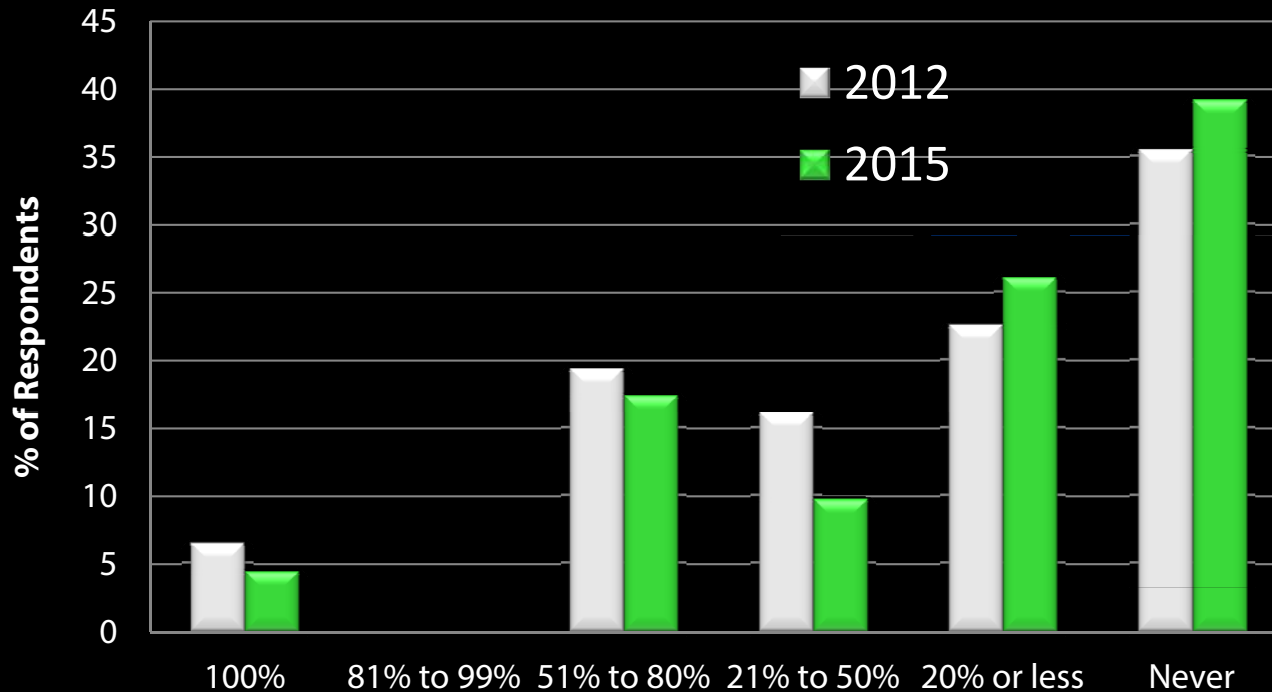
*Technologies in production are well utilised for recovery capability. However, use of DR architecture is not wide spread.*

## Use of Production Technologies



- 38% have **no formal DR architecture**
- Most make good use of **existing technologies** in their production environment
- **Cloud-based** services are starting to become popular

## Testing By Independent Parties



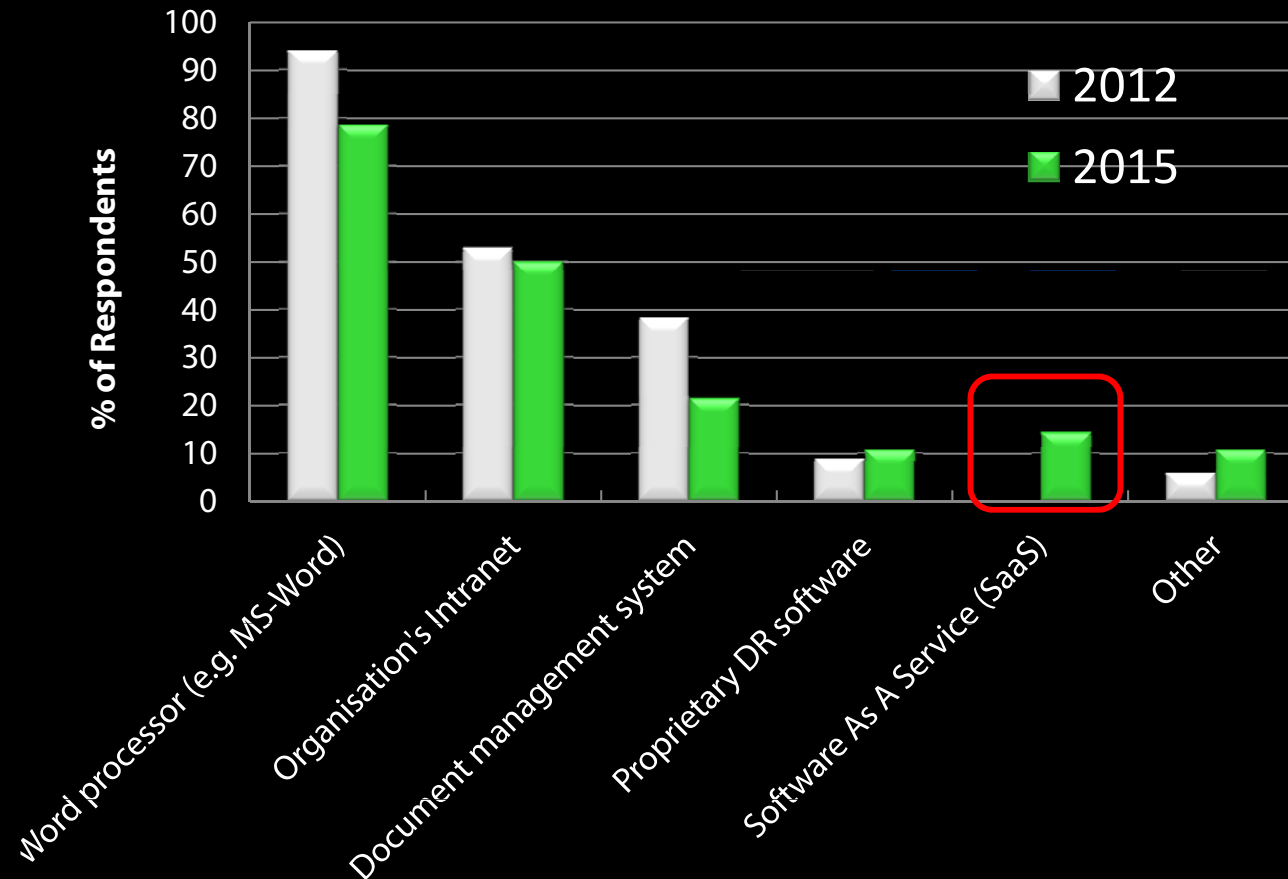
*Near half of the respondents don't have their recovery tests independently evaluated and reported.*

- Many never have their tests independently evaluated

# DOCUMENTATION

*Plans are often out of date, and supporting documentation is often unidentified or unavailable.*

## Documentation Tools



- Many review or update their documentation at least once every year.
- Most use generic word processing, but SaaS is on the rise.
- Accessibility to supporting documentation is often neglected

**PREVAIL<sup>TM</sup>**

**BCM / DR Management System**

# The Issues

Restrictive user access

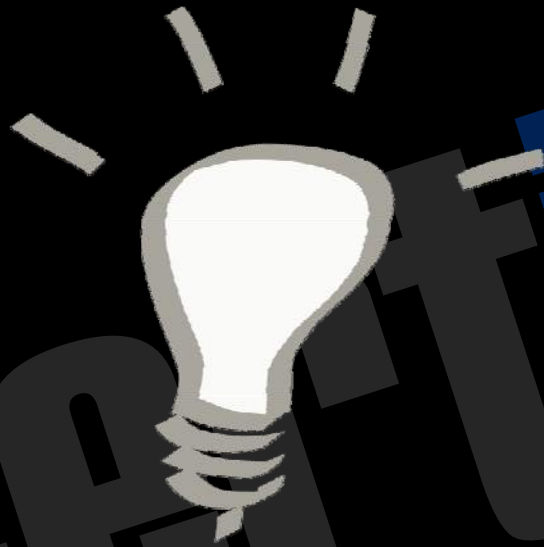
Just a document template

Poor business case for requirements

Hard to govern and audit

No on-site support

# Expert System

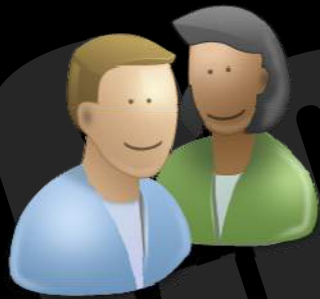


expertise



methodology

# Ubiquitous Access



anyone



any device



any time

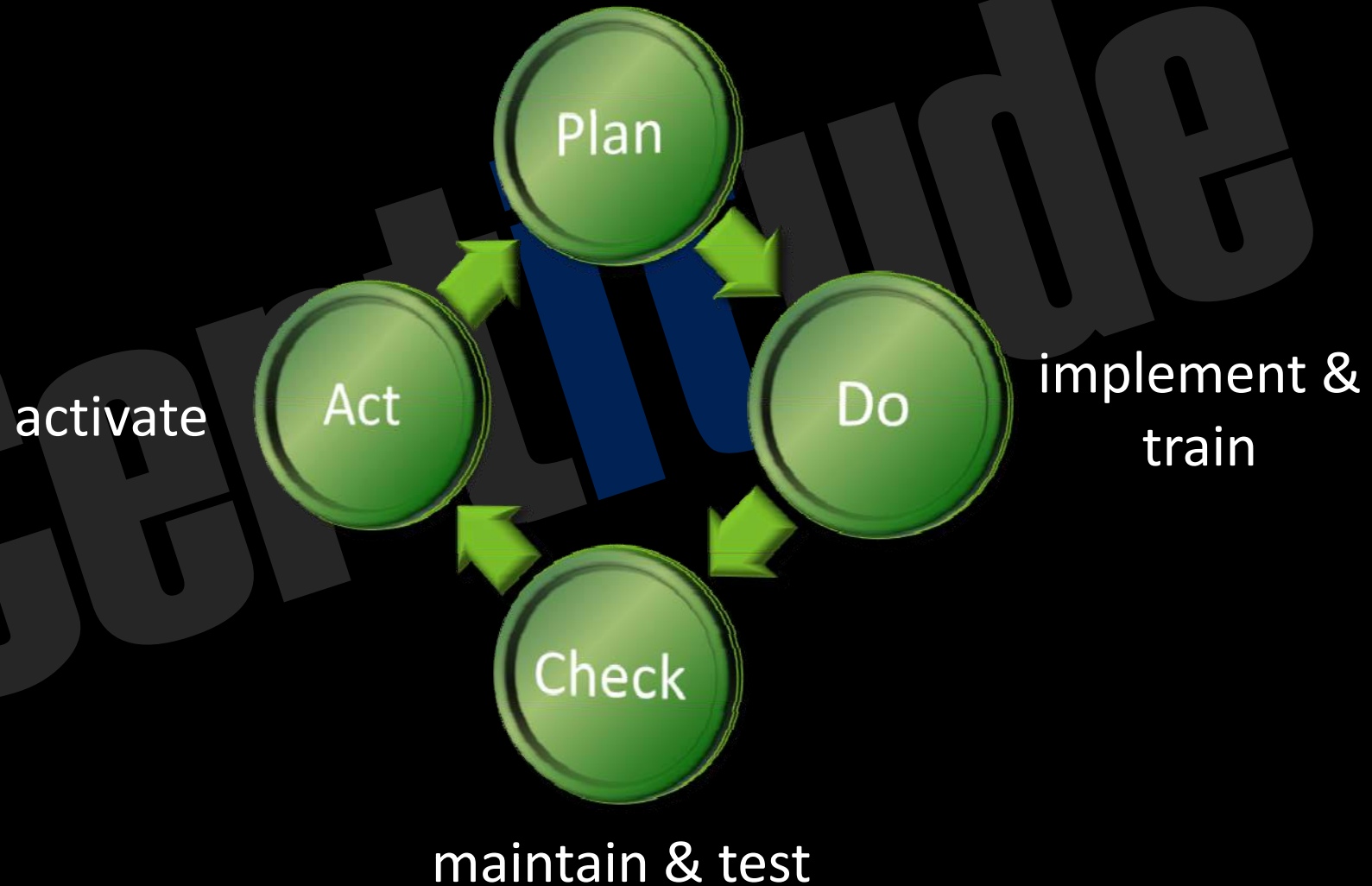


any where



# Full Life-Cycle

requirements & strategy



# Smarts



requirements



mapping

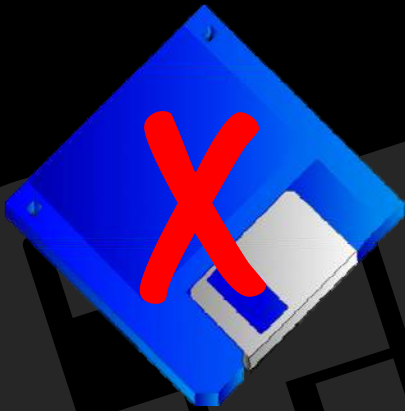


test



activation

# Self-Maintained



nothing to install



onsite support



auto upgrades

[certitude.com.au](http://certitude.com.au)

certitude