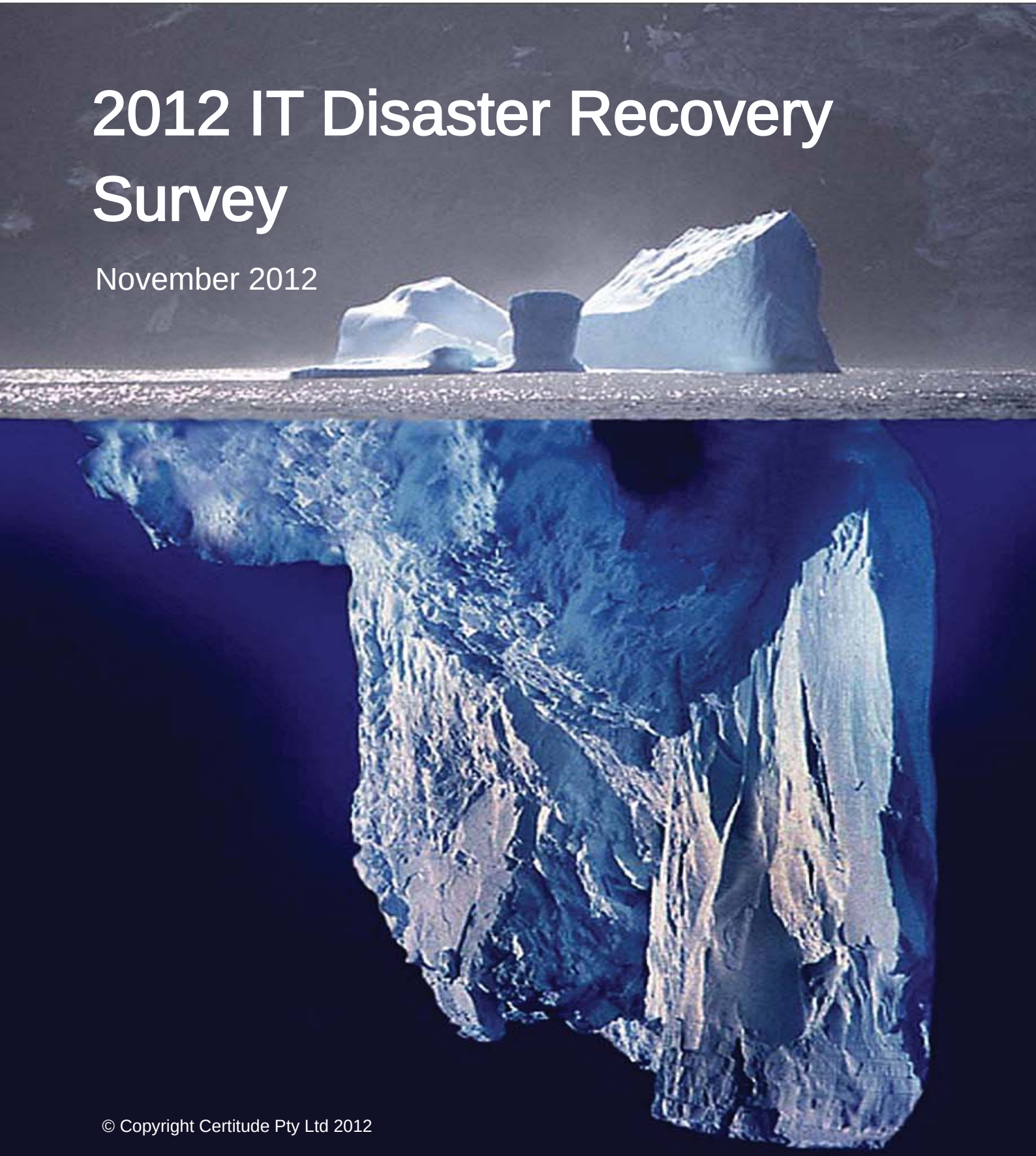
Certitude
TECHNOLOGY RISK SERVICES

2012 IT Disaster Recovery Survey

November 2012



About the Survey

This is the first information technology disaster recovery survey (the Survey) that Certitude has conducted.

Certitude surveyed numerous organisations in Australia from a wide range of industries. The Survey specifically focused on the disaster recovery practices of Australian organisations, and therefore presents findings that are most relevant to the Australian market.

In August and September 2012, respondents completed the online Survey which asked a number of questions concerning Information Technology Disaster Recovery (DR) in their organisation.

Depending on individual respondent answers, additional questions were asked to obtain further detail, and suggestions for improvement were given.

This report presents a summary of the responses, analysis of the data (including correlation across questions), and commentary from Certitude's principal disaster recovery consultants.

In most cases, the findings are presented in charts. To make the pie charts easier to read, individual slices are presented from largest to smallest in a clockwise direction starting from the top of the chart.

In some cases, values have been rounded to the nearest second decimal place and therefore the total of all percentage values (where only one answer was allowed) may not total exactly 100%. Some charts present values where multiple answers were permitted. In these cases, the total of the percentage values could be more or less than 100%.

We thank all the organisations that gave their time to complete the Survey.

We hope you find this report interesting, and helpful in your efforts to manage your organisation's IT disaster recovery and business continuity solutions.

Certitude
TECHNOLOGY RISK SERVICES

Executive Summary

The results of the Survey indicate that, broadly, disaster recovery in Australian organisations is well managed. However, with many organisations currently focused on cost reduction, opportunities exist that could enable organisations to achieve their disaster recovery objectives more economically. Some of these opportunities are illustrated in the key findings of the Survey.

On average, respondents spend about 3% of their annual IT budget on disaster recovery. Most system outages were reported by those organisastions that spent around 1% of their IT budget on disaster recovery. However, spending well above the average on disaster recovery does not necessarily provide protection against system outages. Some respondents spend more than 10% of their annual IT budget on disaster recovery, and still experienced system outages (about 12% of all outages reported in the past two years).

There was no apparent correlation between reported disaster recovery maturity and the size of an organisation. However, there were certain industries that were more mature in this area than others. The most mature industries were; financial service, education, health and community services, and professional services. The less mature industries were; mining, manufacturing, transport and storage, and communication services.

Embedding disaster recovery into everyday IT processes can help achieve cost effective disaster recovery objectives, and improve disaster recovery awareness across an organisation. Generally however, the Survey found that disaster recovery is poorly embedded into project management, service level management, the service desk, and third-party management processes.

The majority of reported system disruptions were caused by failure of third-party service providers (e.g. electricity, IT operations, or telecommunications providers). This highlights the need to further, and more effectively, embed disaster recovery into organisations' service level and third-party management processes. Other reported causes of system disruptions could have been prevented by good internal controls. These causes were often related to failures in change management, capacity planning, and IT environmental management processes, all of which are usually within an organisation's direct control.

Whilst most respondents involve their users in the determination of disaster recovery requirements, most failed to adequately consider the re-entry and processing of lost data, and the clearing of work backlog. This indicates that, while users were involved, their level of engagement or understanding of disaster recovery may have been inadequate.

Technologies available in production environments are well utilised to build recovery capability. However the use of specific disaster recovery architecture is not widespread.

Many respondents use disaster recovery testing as the primary method of training, rather than other direct training methods.

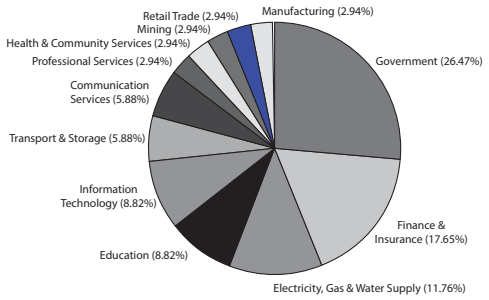
Certitude
TECHNOLOGY RISK SERVICES

Participant Demographics

A large variety of organisations participated in the Survey. Surveyed organisations spanned the range of Australian and New Zealand Standard Industrial Classifications (ANZSIC) industries and sizes, except for those with an annual IT spend of $500,001 to $1m (AUS). Respondents held C-level positions and other strategic roles including: IT operations, application support, general counsel, risk and compliance, and program management.

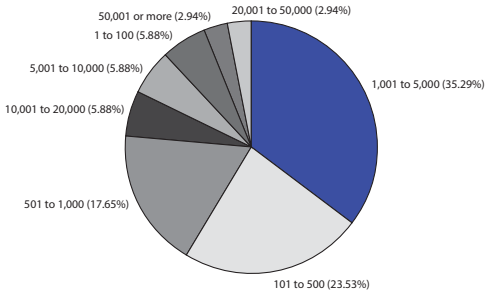
Industry

Which one of the following best describes your organisation's INDUSTRY?



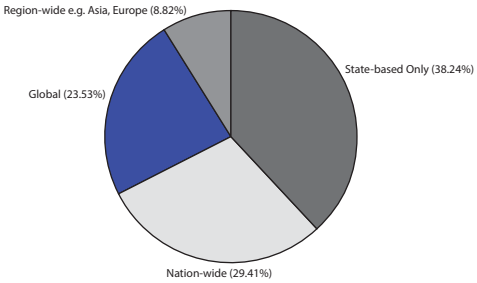
No. of Employees

Which one of the following best describes the NUMBER OF EMPLOYEES in your organisation?



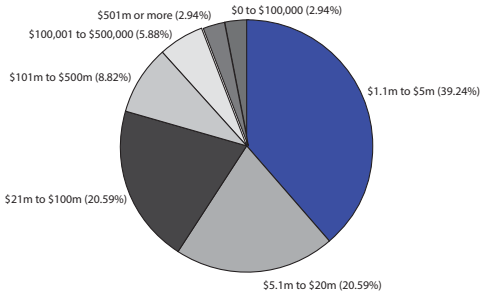
Geographic Presence

Which one of the following best describes your organisation's GEOGRAPHIC PRESENCE?



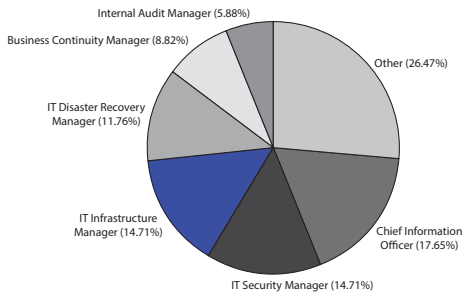
Annual Information Technology Spend

Which one of the following best describes your organisation's approximate ANNUAL INFORMATION TECHNOLOGY BUDGET ($AUD)?



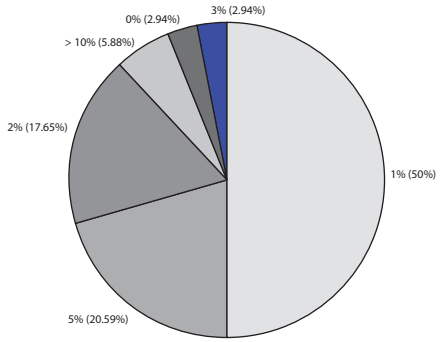
Role

Which one of the following best describes YOUR ROLE in your organisation?



Budget

Which one of the following best describes your organisation's approximate ANNUAL DISASTER RECOVERY (DR) BUDGET as a percentage of annual information technology budget?

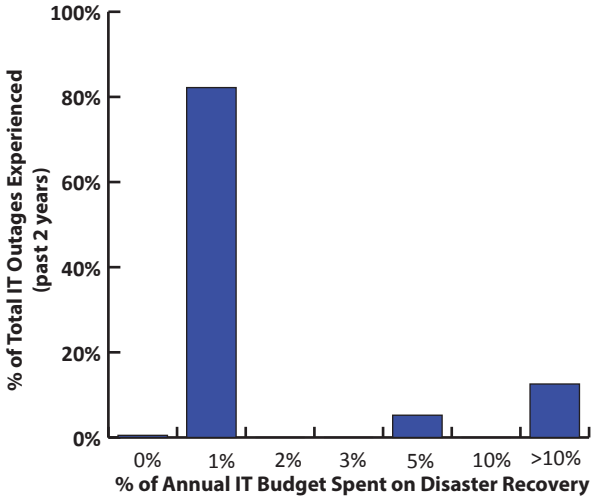


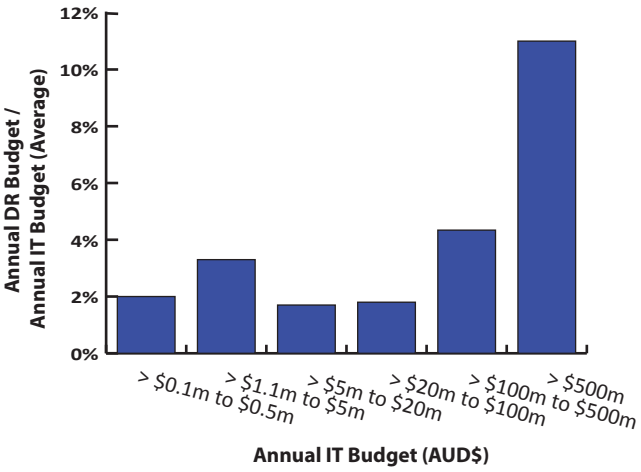
Respondents spend around 3% of their IT budget on disaster recovery. However money doesn't necessarily buy fewer IT outages.

The majority of the total IT outages reported in the past two years were experienced by respondents who spent around 1% of their IT budget on disaster recovery. However, a substantial number (around 12%) of the total outages reported were experienced by respondents who spent a relatively large proportion of their IT budget (more than 10%) on disaster recovery.

Of the respondents with an annual IT budget of less than or equal to $100,000, close to 0% of the annual IT budget was spent on disaster recovery. In comparison, respondents with an annual IT budget of more than $500m spent over 10% of their annual IT budget on disaster recovery.

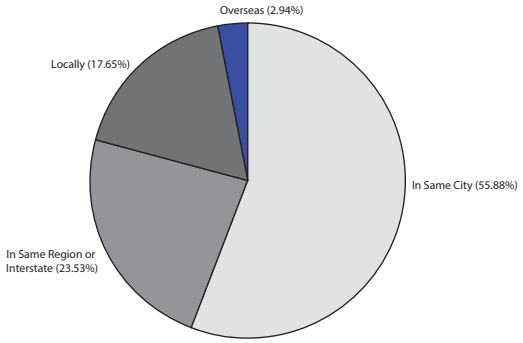
On average, the percentage of annual IT budget spent on disaster recovery is around 3%.





Recovery Location

Which one of the following best describes WHERE your organisation's production systems would be RECOVERED in the event of their loss or unavailability?

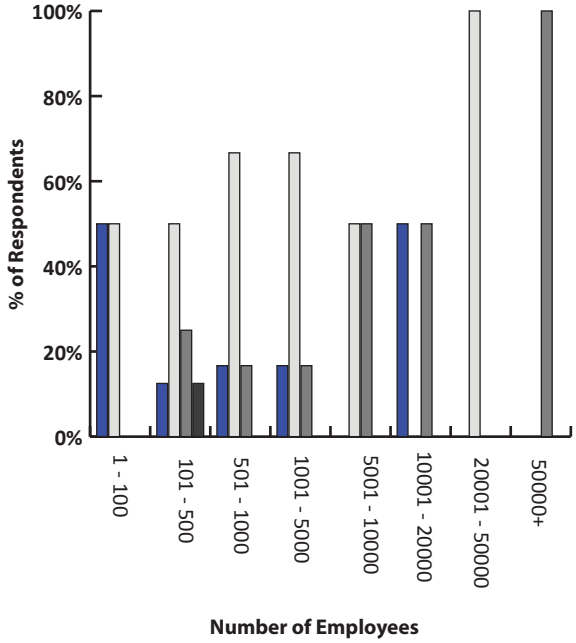


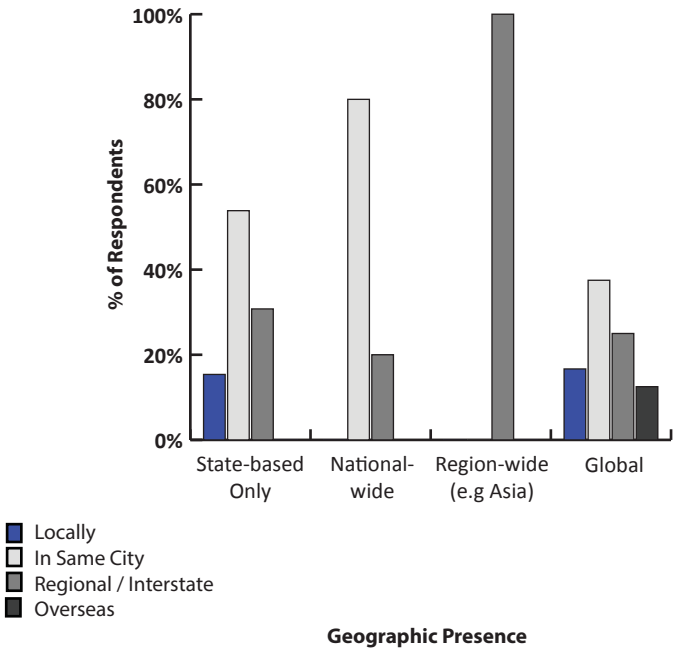
Small and/or geographically non-dispersed organisations are having difficulty finding suitable recovery locations.

The majority of respondents (55.88%) recover their systems to a location within the same city.

Organisational size (i.e. by number of employees) and geographical presence appear to have a significant influence on recovery location. Small organisations typically recover locally or within the same city. This illustrates a problem that small and/or geographically non-dispersed organisations encounter. They do not own, and therefore have no easy access to, other suitable recovery locations, and the cost to subscribe to third-party recovery facilities may be prohibitive for these organisations.

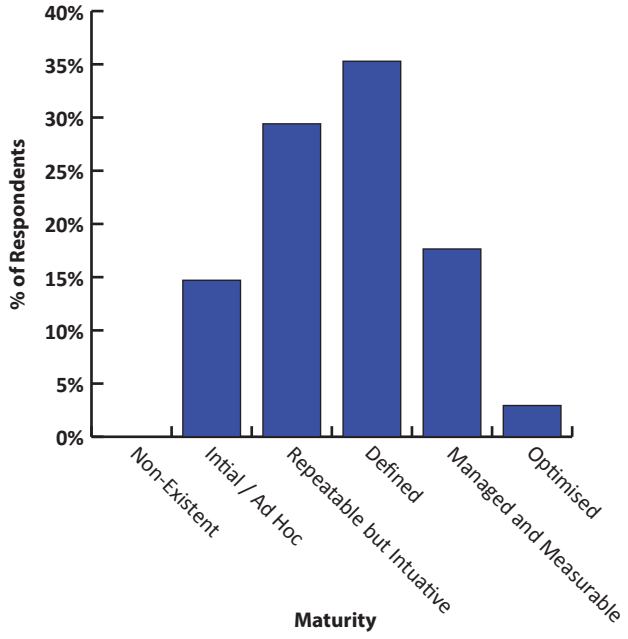
In contrast, respondents who have a regional presence appear to be taking full advantage of their geographical diversity by recovering to facilities they own in other locations.

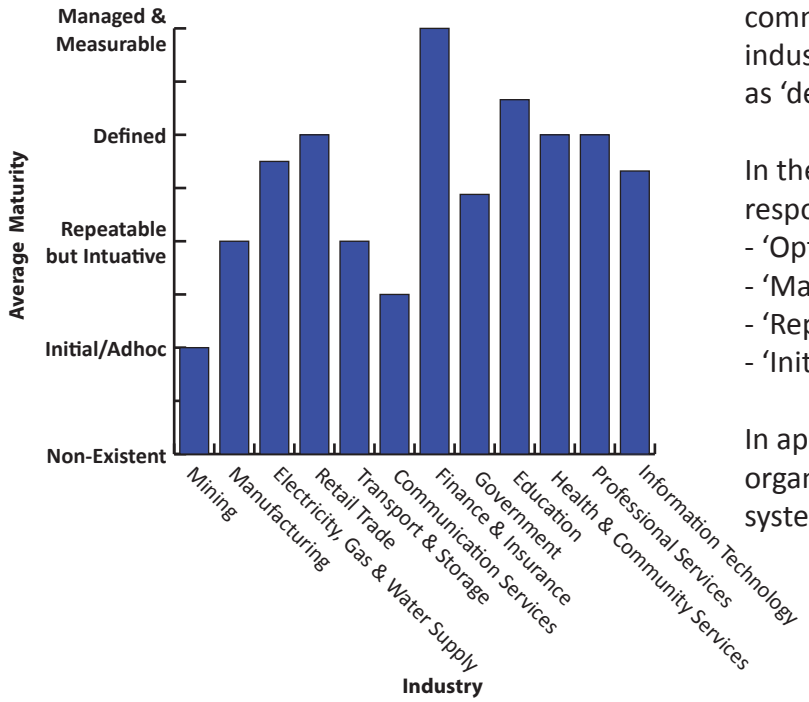




Maturity

Which one of the following best describes the MATURITY of your organisation's Disaster Recovery?





The majority of respondents described the maturity of their disaster recovery as 'repeatable, but intuitive', or 'defined'. Around 2.5% of respondents described the maturity of their disaster recovery as 'optimised'. The size of an organisation does not appear to influence maturity.

Higher levels of disaster recovery maturity can reduce system disruption.

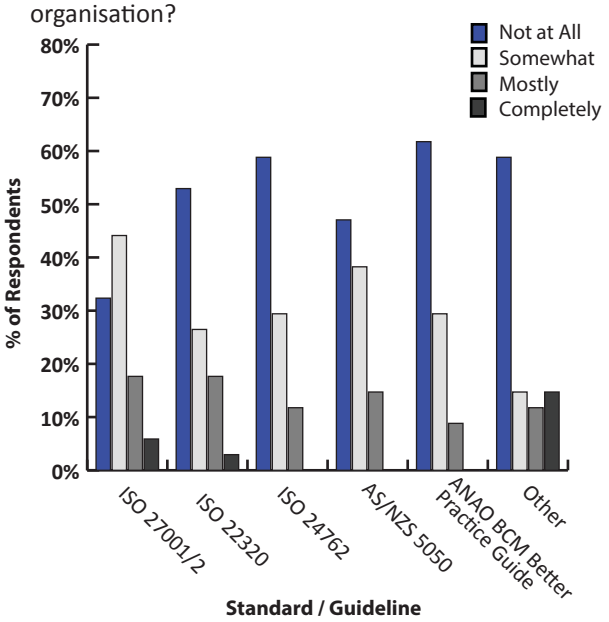
However, there were notable differences in maturity across different respondent industries. Respondents from mining, manufacturing, transport and storage, and communication services, on average, described their maturity as 'repeatable, but intuitive' or lower. The financial services, education, health and community services, and professional services industries, on average, described their maturity as 'defined' or higher.

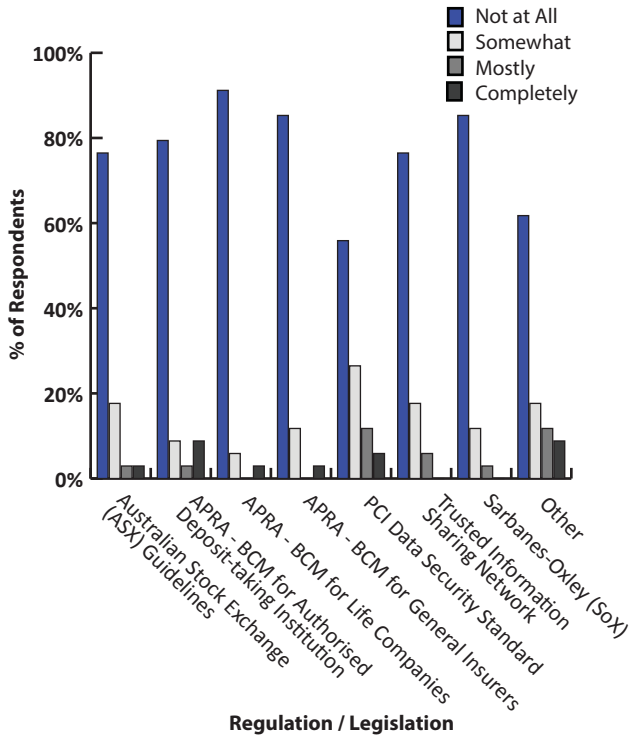
In the past two years, the following percentage of respondents, by maturity, experienced an outage:
- 'Optimised' = 0%
- 'Managed and Measurable' or 'Defined' = 33.3%
- 'Repeatable, but Intuitive' = 50%
- 'Initial/Adhoc' = 100%.

In appears that improving the maturity of an organisation's disaster recovery is likely to reduce system disruption.

Standards & Regulations

For each of the following STANDARDS / GUIDELINES / REGULATIONS / LEGISLATION, please indicate the EXTENT they have INFLUENCED Disaster Recovery in your organisation?





For the most part, it appears that existing disaster recovery relevant standards, guidelines, regulation, and legislation have no real influence on organisations' disaster recovery.

Particularly interesting, is that broader standards and guidelines such as ISO 27001 and ISO 22320 appear to be of greater influence than disaster recovery and Business Continuity Management (BCM) specific standards and guidelines such as AS/NZS 5050 and the Australian National Audit Office's (ANAO's) BCM Practice Guide.

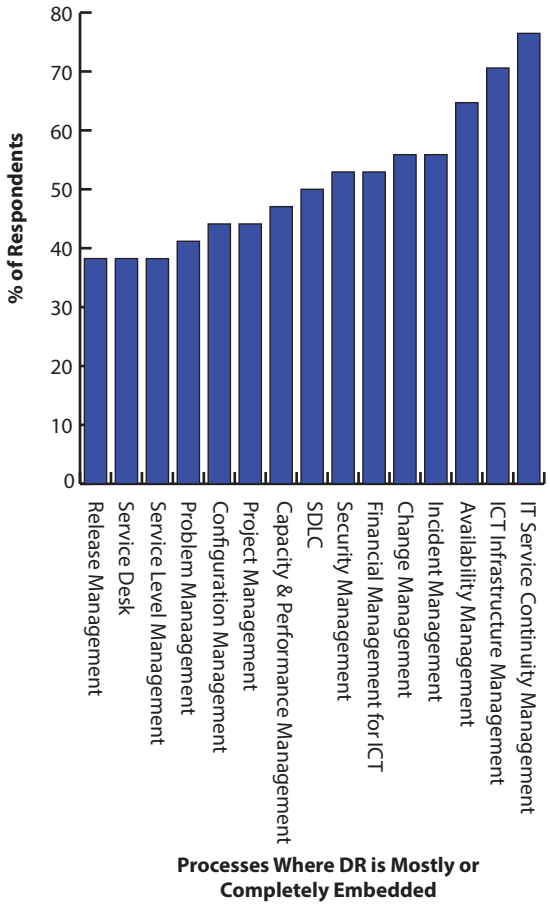
Disaster recovery standards and guides do not significantly influence most organisations' disaster recovery.

Note: APRA's APS / LPS 232 and GPS 222, have all been superseded by CPS 232 as at 1 July 2012. Some of the changes to be aware of include:

a) A regulated institution cannot just perform a BIA for critical business operations. It must perform the analysis for all operations in order to determine which are critical.
b) Clarifications concerning the role and obligations of the board (or equivalent) in complying with the standards.
c) An extension to the standard to include registered life Non Operating Holding Companies (NOHCs).
d) A greater clarity around the application of the standard to foreign branches.
e) A new requirements for life companies to conduct periodic reviews of their business continuity plans using internal auditors or external experts.
f) Under CPS 232, new powers for APRA to request that an external expert undertakes an assessment of BCM arrangement for ADIs and general insurers.
g) A new requirements for Level 2 insurance groups to comply with the Prudential Standard GPS 222 Risk Management: Level 2 Insurance Group BCM requirements.

Process Integration

For each of the following processes, HOW WELL is Disaster Recovery EMBEDDED into these processes in your organisation?



Most respondents (over 50%) have disaster recovery mostly or completely embedded into their IT Service Continuity, ICT Infrastructure, Availability, Change, Incident, Security and Financial Management processes.

Few (around 44%) have disaster recovery embedded into their Project Management processes. Fewer still (less than 40%) have embedded disaster recovery into other important processes such as Release, Management, Service Desk and Service Level Management processes.

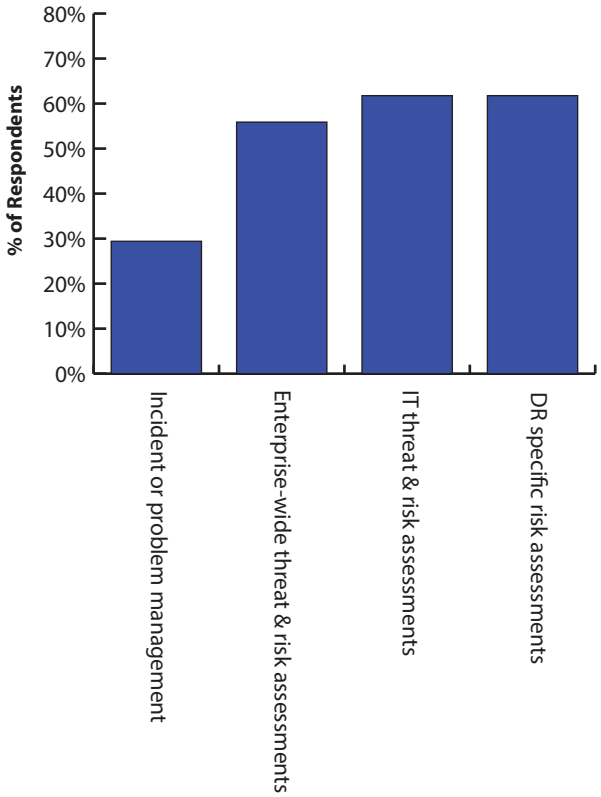
Disaster recovery is poorly embedded into project and service level management, as well as service desk processes.

Embedding disaster recovery activities into everyday IT processes, can help achieve disaster recovery objectives in a very cost efficient manner, and improve disaster recovery awareness across the organisation.

Embedding disaster recovery into existing IT processes, may negate the need to maintain a standalone disaster recovery process that may become neglected over time. For example, embedding disaster recovery considerations and sign-off in change requests, may reduce the possibility that a production change will reduce the disaster recovery capability. Doing this may also prevent a new system being commissioned without an established disaster recovery solution.

Threats

Which one or more of the following best describes how THREATS to IT SERVICE CONTINUITY are identified in your organisation?



The majority of respondents identify threats to IT service continuity by using disaster recovery specific risk assessments, broader IT risk assessments, or enterprise-wide risk assessments.

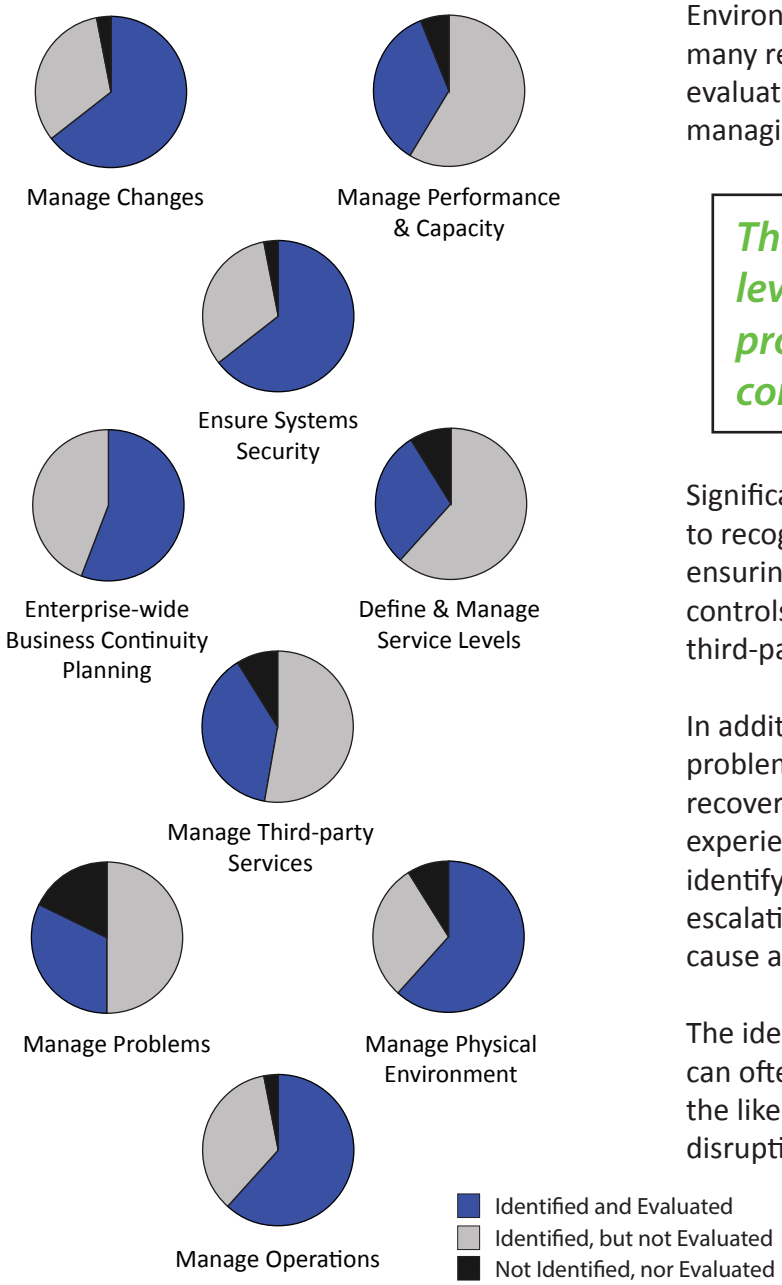
Few (less than 30%) used information recorded by their incident and problem management processes to identify threats.

This represents a missed opportunity to analyse past threats and then to improve risk mitigation activities in order to prevent future reoccurrence.

Trends learned from incident and problem management are not often used to identify disaster recovery threats and opportunities to prevent future system disruption.

Key Controls

For each of the following potential controls for protecting against unplanned system disruption, please select those that you have IDENTIFIED as key controls, and which you have EVALUATED for operational effectiveness.



Most respondents identify and evaluate several key controls that can protect against unplanned system outages. These include; Manage Changes, Ensure System Security, Enterprise-wide Business Continuity Planning, Manage the Physical Environment, and Manage Operations. However, many respondents had only identified, but not evaluated, other important key controls such as managing performance, capacity and problems.

The management of service levels and third-party service providers is being missed to control disaster recovery risk.

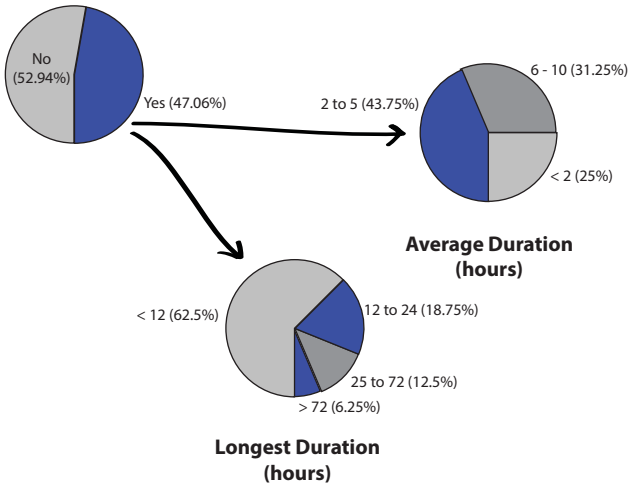
Significantly, many respondents did not appear to recognise the importance of having and ensuring the operational effectiveness of key controls related to managing service levels, and third-party providers.

In addition, some respondents do not identify problem management as an important disaster recovery control. These respondents may experience unnecessary harm, due to not identifying potential causes of disruption, or not escalating minor issues appropriately before they cause a disruption.

The identification and validation of key controls can often significantly, and cost effectively, reduce the likelihood and consequences of system disruption.

Disruptions

In the past two (2) years, has your organisation had any MAJOR & UNPLANNED system disruption(s)?

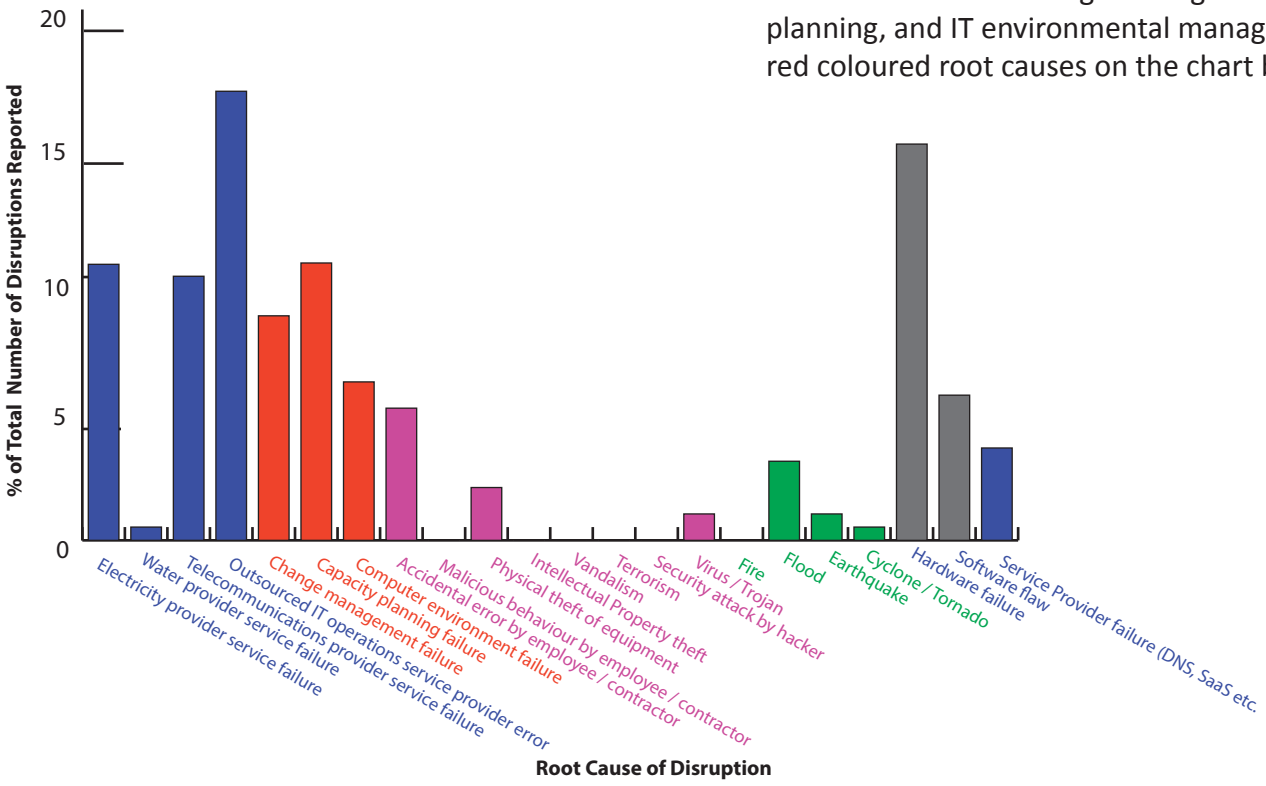


Nearly half of the respondents (47.06%) had experienced a major and unplanned system disruption in the past two years. Of these, most experienced an average outage of one to five hours, and a longest outage of less than 12 hours (half a day). 6.25% of the respondents experienced one or more outages of greater than 72 hours.

Many system disruptions are essentially self-inflicted.

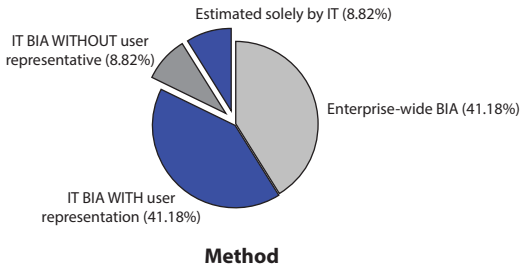
While service providers and vendor hardware failures caused a significant number of the reported disruptions, areas that are predominately in the direct control of an organisation caused a notable number. These could fairly be regarded as 'self-inflicted' as they relate to failures in change management, capacity planning, and IT environmental management (see red coloured root causes on the chart below).

How many times in the past two (2) years have each of the following been the ROOT CAUSE of your organisation's MAJOR & UNPLANNED system disruption(s)?



Recovery Requirements

Which one of the following best describes HOW your organisation DETERMINES DISASTER RECOVERY REQUIREMENTS?



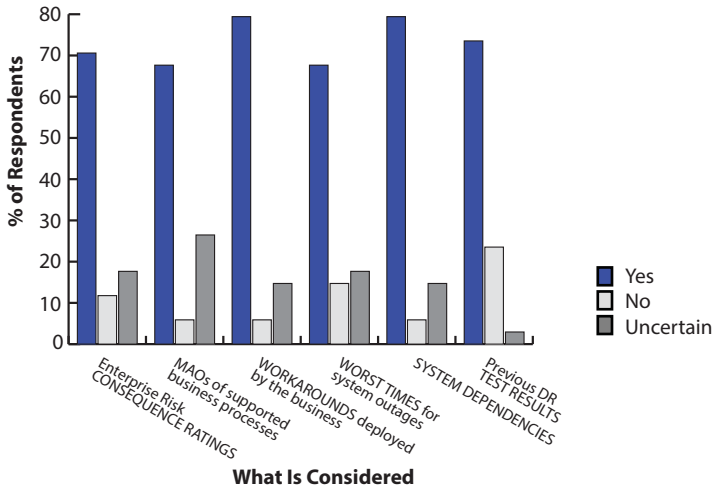
Users are involved in determining disaster recovery requirements.

Encouragingly, most respondents determine their disaster recovery requirements with representation from users through a Business Impact Analysis (BIA). Also, most respondents consider important factors, such as work-arounds, and system dependencies, when determining Recovery Time Objectives and Recovery Point Objectives.

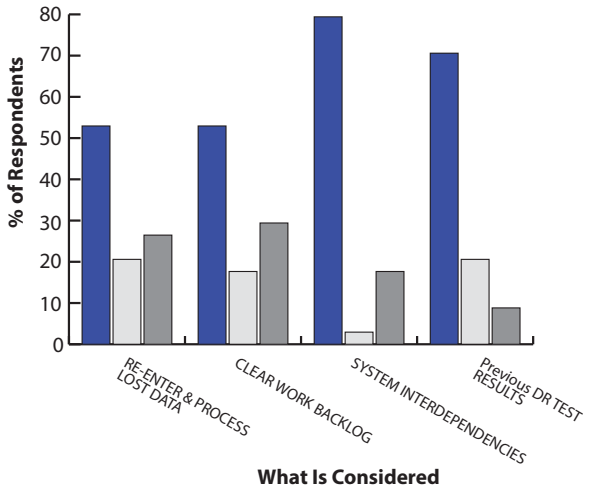
However, nearly half the respondents had not adequately considered the re-entry and processing of lost data, and the clearing of any work backlog. This may indicate that while users were involved in the determination of requirements, their engagement may have been inadequate. This may lead to:

a) A gap between disaster recovery capability and business expectations, and over or under investment in capability;
b) Inaccurate or incomplete MAOs, RTOs and RPOs;
c) Noncompliance with relevant regulations and law.

Have you considered each of the following when determining your RECOVERY TIME OBJECTIVES (RTOs)?



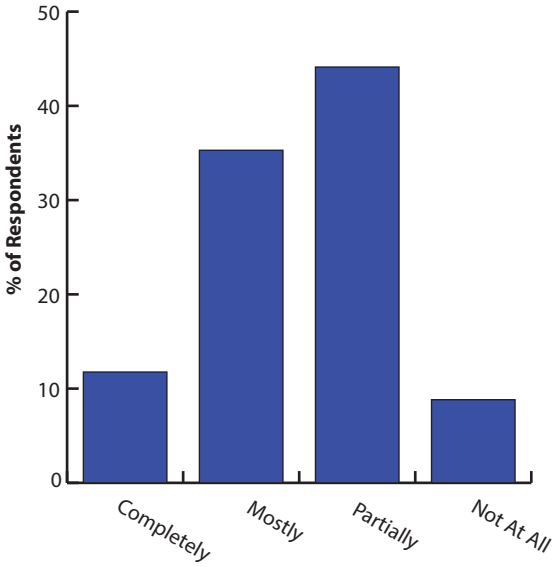
Have you considered each of the following when determining your RECOVERY POINT OBJECTIVES (RPOs)?



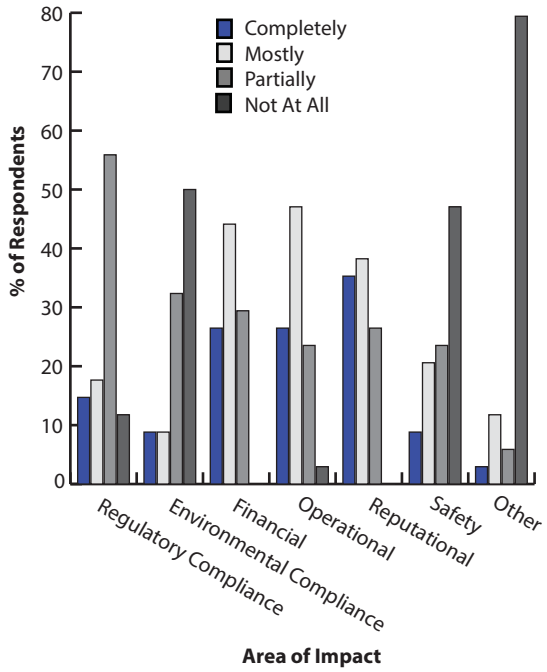
RTO = Recovery Time Objective is the period in which a given system must be recovered following its unavailability or loss, before the consequence becomes unacceptable.
RPO = Recovery Point Objective is the amount of data that can be acceptably lost (expressed as a period of time e.g. one day's worth of lost data), before the consequence becomes unacceptable.
MAO = Maximum Allowable Outage is the period in which a given business process must be re-established following its disruption (whether due to system outages or other reasons), before the consequence of the outage becomes unacceptable.

Expectations & Impact

Which one of the following best describes how well your organisation MANAGES UNREALISTIC RECOVERY EXPECTATIONS, when determining Disaster Recovery requirements?



For each of the following areas, rate the damage an UNPLANNED SYSTEM DISRUPTION would cause your organisation?



Despite a high participation of users in the determination of disaster recovery requirements, overall user expectations appear to be poorly managed. Over half the respondents thought that they partially managed unrealistic recovery expectations, if at all.

Failing to manage unrealistic expectations may lead to dissatisfied users, and unnecessary expenditure on disaster recovery implementation and maintenance. It can also diminish the importance of user responsibilities in minimising the harm caused by system disruption (e.g. through the deployment of work-arounds).

The most difficult area of harm to quantify, reputation, is of the greatest concern.

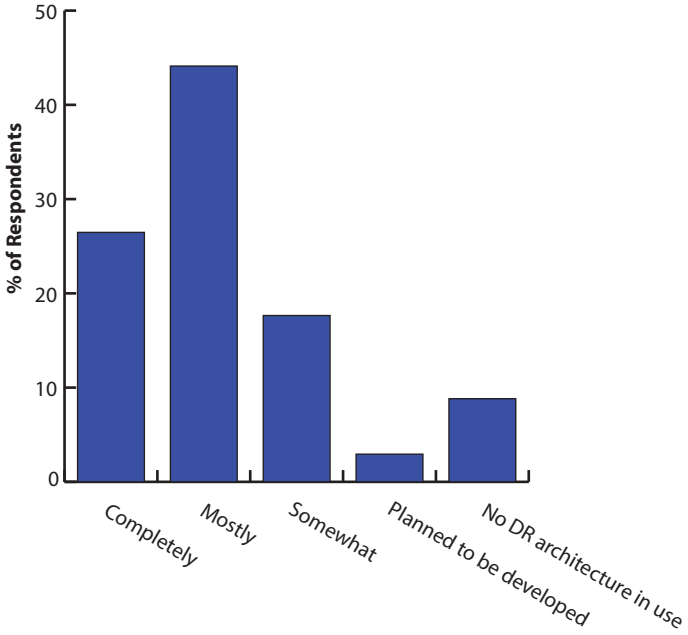
Of all the potential areas of damage caused by unplanned system outages, reputational damage was of high concern for the greatest number of respondents. Approximately 72% stated that their organisation's reputation would be either completely or mostly harmed if an unplanned system disruption occurred.

The recognition that reputational damage is significant to many organisations presents a small problem in building a business case for disaster recovery. Unlike other typical areas of harm, reputational damage is the most difficult to actually measure, and quantify.

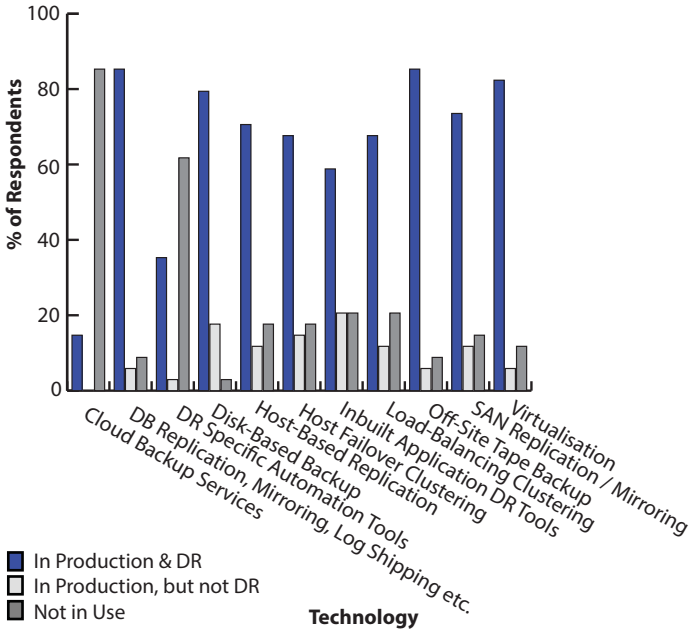
Reputational harm was closely followed by the operational and financial impacts that could cause the most harm to the respondents' organisations.

Design & Technology

Which one of the following best describes how your organisation's Disaster Recovery ARCHITECTURE can be used to DESIGN Disaster Recovery solutions appropriately, consistently, and cost effectively?



For each of the following technologies, please indicate if they are USED in your organisation and if they are USED for Disaster Recovery?



Most respondents (approximately 70%) have some form of disaster recovery architecture, however only around 75% of these make good good use of it. Around 12% of respondents either had no disaster recovery architecture, or were intending to develop one.

Technologies available in production environments are well utilised to build recovery capability. However, the use of specific disaster recovery architecture is not widespread.

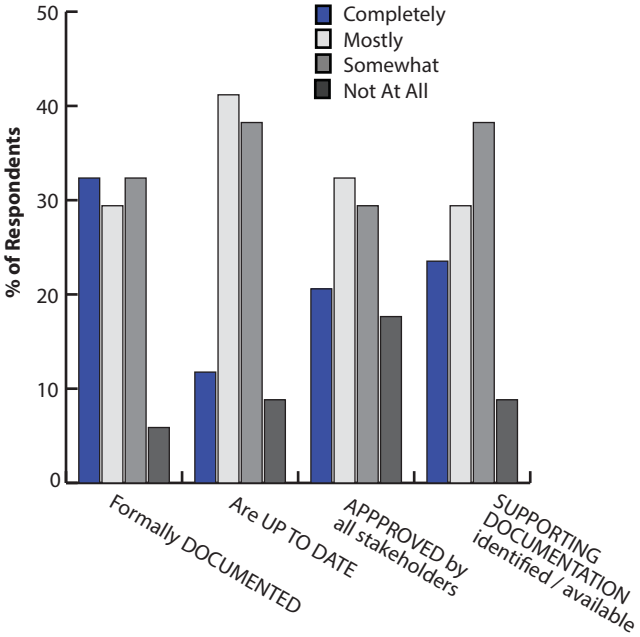
Despite the availability of cloud services, most respondents do not use cloud-based backup services. Automation tools specific to disaster recovery are also not widely used.

.

Leveraging technologies that already exist in an organisation's production environment can provide improved and cost effective recovery capability. Of all the technologies presented in the survey, the majority of respondents (80% or more) have made use of technologies that already exist in their production environments. These include: database replication, off-site tape backup, and virtualisation. Other technologies widely used to aid recovery include; disk/host-based backup, host failover clustering, in built application recovery tools (e.g. Exchange 2010, SharePoint), load-balancing, and SAN replication.

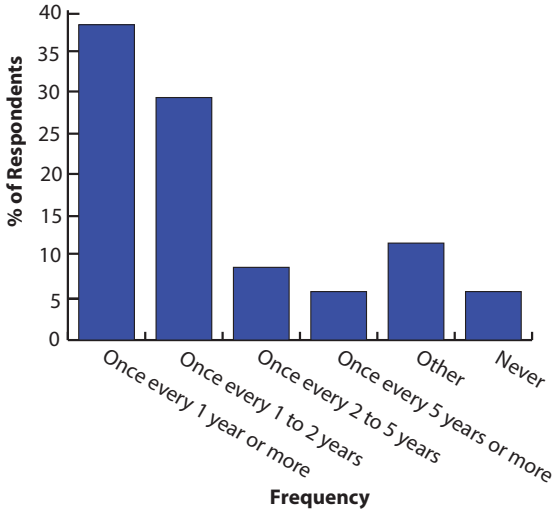
Documentation

For each of the following quality attributes, please RATE your organisation's disaster recovery plans.



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

Which one of the following best describes HOW OFTEN your organisation REVIEWS and / or UPDATES its Disaster Recovery documentation (e.g. plans, supporting doco.)?

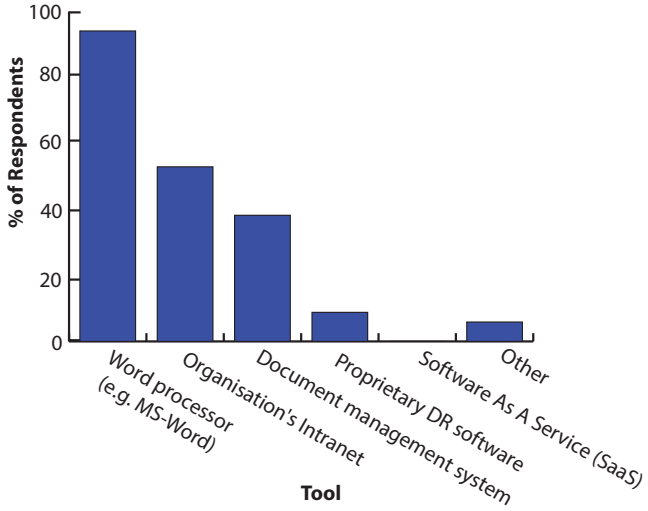


Around 6% of respondents said that they have never reviewed or updated their disaster recovery documentation. In contrast, about 38% of respondents review or update their documentation at least once every year. Some respondents also review or update their disaster recovery documentation as a continuous part of their change management process, either bi-monthly, or when specified by their customers.

The majority of respondents (around 94%) use generic word processing tools to document their disaster recovery plans and associated documentation. Around half of the respondents also use generic systems such as their intranets and document management systems to publish and maintain their documentation.

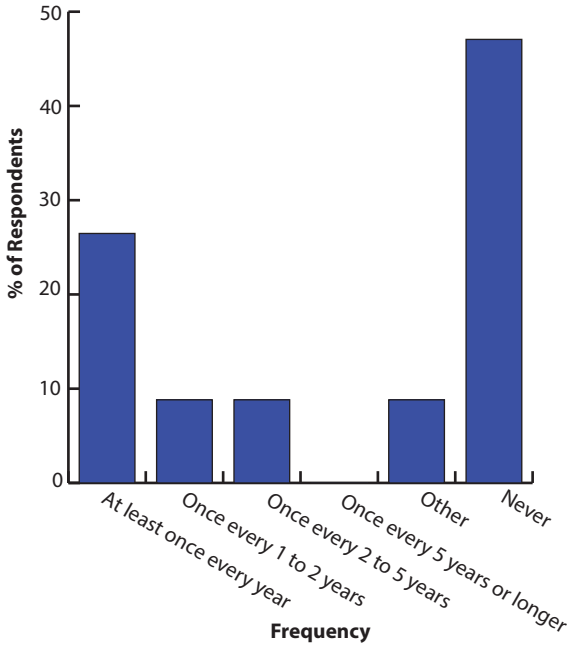
Cloud based services have not gained popularity, with no respondent reporting using services to store and disseminate disaster recovery documentation . About 6% of respondents use other tools such as their CMDB and Service Management Software.

Which one or more of the following does your organisation use to DOCUMENT and MAINTAIN its disaster recovery documentation?



Training

Which one of the following best describes HOW OFTEN your organisation CONDUCTS DISASTER RECOVERY TRAINING?



Surprisingly, about 47% of respondents said that they have never conducted disaster recovery training. This may be because some respondents considered regular disaster recovery testing to be the best form of training.

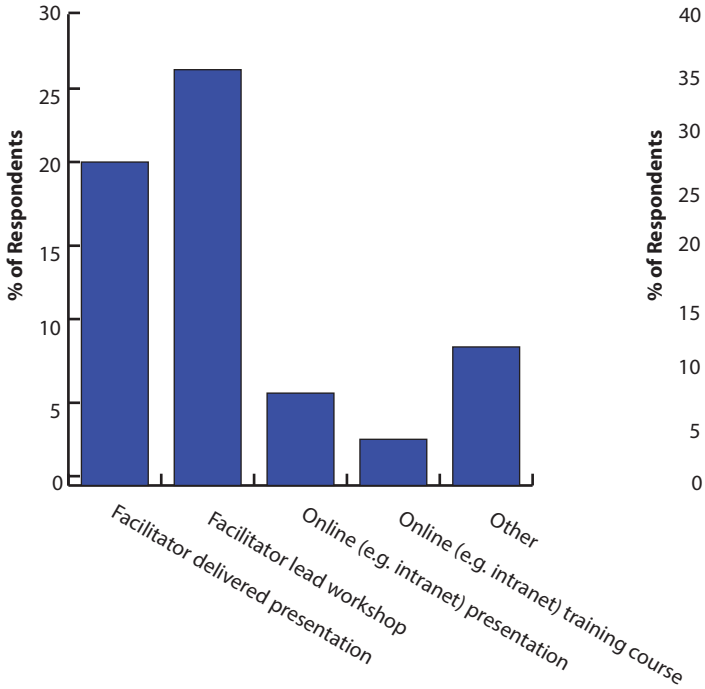
In contrast to the above, one respondent said that they conducted training bi-monthly.

Some respondents conducted on-the-job training.

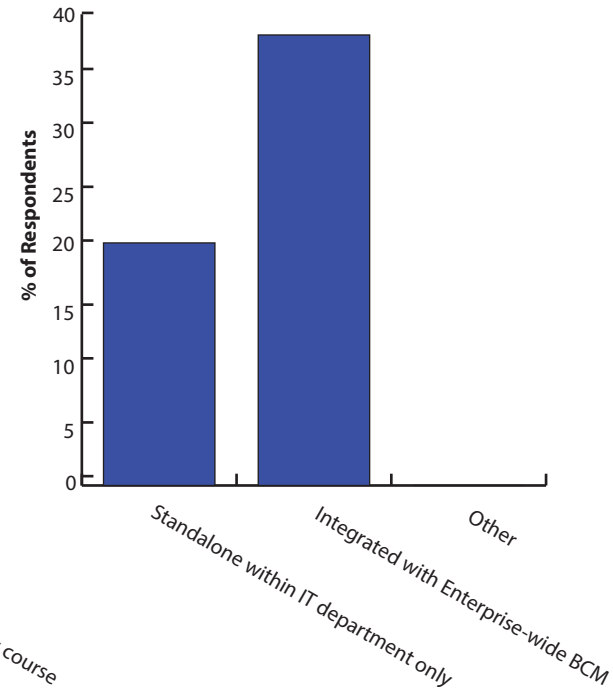
Many respondents use disaster recovery testing as the primary method of training.

The questions below were only asked if a respondent did not answer 'never' to the above question.

Which one of more of the following best describes HOW your organisation CONDUCTS DISASTER RECOVERY TRAINING?



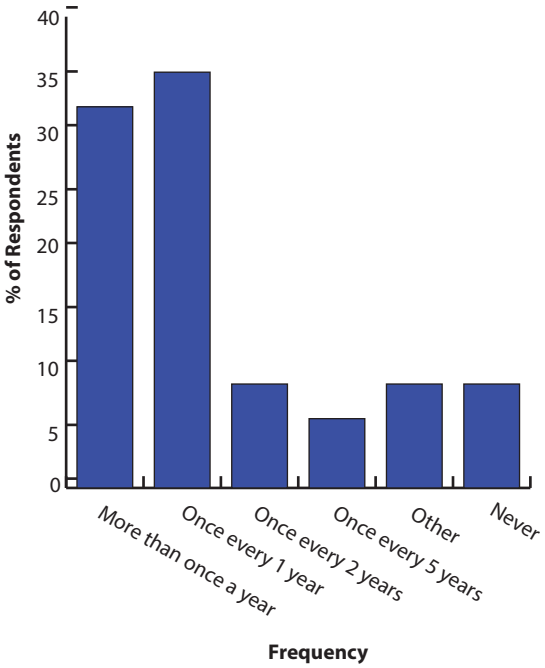
Which one or more of the following best describes how your DISASTER RECOVERY TRAINING is integrated within your organisation?



Certitude
TECHNOLOGY RISK SERVICES

Testing

Which one of the following best describes how OFTEN you perform Disaster Recovery TESTING?



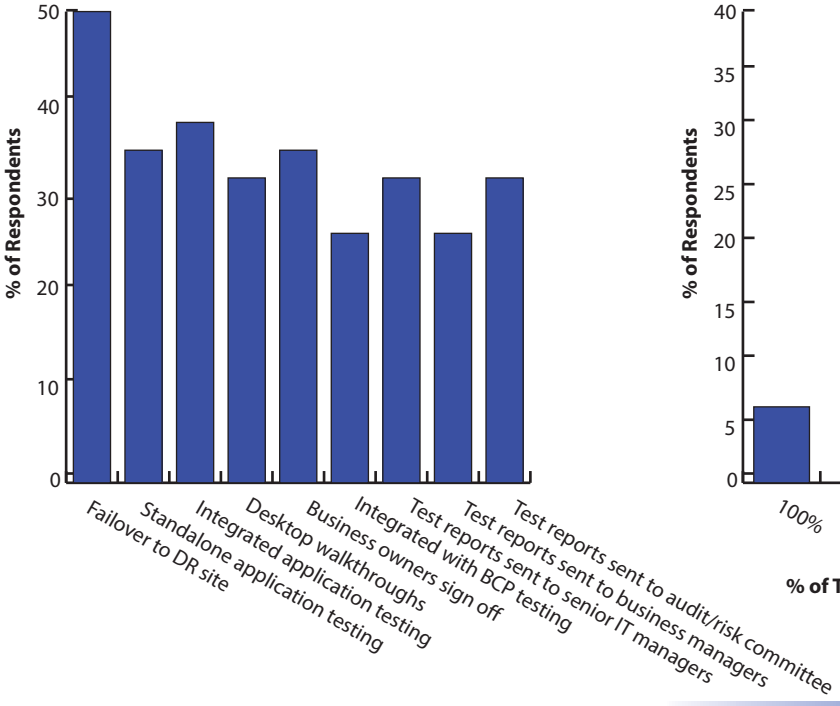
About 9% of respondents said that they have never conducted disaster recovery testing. Of those, 100% never conduct training either. In addition, of those that never conduct testing, about one-third had also not experienced a system outage from which they could validate their recovery capability. In contrast, about 67% of respondents conduct testing at least once per year. Some respondents conduct testing bi-monthly, after IT environment changes, and at various frequencies depending on the service they provide and their type of customer.

Respondents conduct testing in a wide variety of ways, with fail-over to the disaster recovery site (about 50%) being the most commonly used method. About 64% of respondents have their tests independently evaluated and reported.

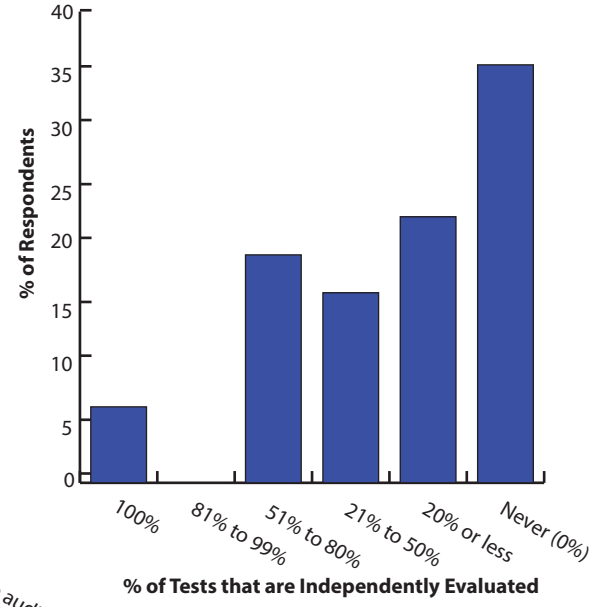
Note: Authorised Deposit-Taking Institutions (ADIs) should be aware that APRA has clarified that 'annual' testing means within 12 calendar months rather than at 'sometime' in the following calendar year.

The questions below were only asked if a respondent did not answer 'never' to the above question.

Which one or more of the following best describes HOW your organisation TESTS its Disaster Recovery capability?



Which one of the following best describes HOW OFTEN your organisation has its Disaster Recovery TESTS EVALUATED & REPORTED BY INDEPENDENT PARTIES?



About Certitude

Certitude is a niche professional services company specialising in assisting senior business managers identify and control risks associated with people, processes and technology.

Our consultants are qualified and experienced risk specialists who maintain a high degree of professionalism, and offer quality and value to their clients.

We are independent of vendor and product alliances, allowing us to provide impartial assessments and advice.

Certitude was established out of the recognition that risks need to be presented in a way that is easy to understand. This allows business managers to balance risks against costs and business opportunities, and to make informed decisions. To provide real value we:

- Take a **business process driven approach** to understanding real operational needs and risks.
- Clearly relate identified risks to the **real impact** to the business.
- **Bridge the gap** between technical details and business management's notion of risk.
- Provide **practical recommendations** that are cost effective and suitable for your organisation to manage identified risks, rather than just quoting 'best practices'.

Services

Certitude delivers all of its services using consultative, comprehensive, evidence based, and independent methodologies. these are based on our experts experience and Certitude's Service Delivery Frameworks (SDFs).

We provide services in:

- Information & IT Security
- Business Continuity Management & IT Disaster Recovery
- IT Project Governance & Assurance
- IT Audit and Assurance
- Computer Forensics & Analysis

Go to www.certitude.au.com for more information about us.

Certitude

TECHNOLOGY RISK SERVICES

Contact us

Melbourne (Head Office)

Main: +61 (0) 3 8610 6700
Fax: +61 (0) 3 8610 6334
Address: Level 3
480 Collins Street
MELBOURNE VIC 3000
AUSTRALIA

Sydney

Main: +61 (0) 2 9994 8981
Fax: +61 (0) 2 9994 8008
Address: Level 14
309 Kent Street
SYDNEY NSW 2000
AUSTRALIA

WWW.CERTITUDE.AU.COM