Certitude
TECHNOLOGY RISK SERVICES

2015 IT Disaster Recovery Survey Update

November 2015

About the Survey

In 2012, Certitude conducted its first Information Technology Disaster Recovery (DR) survey (the Survey).

The Survey included participants from 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 2015, Certitude conducted an online update to the Survey (the Update). This 2015 Update highlights significantly different outcomes compared to the 2012 Survey, along with supporting analysis and commentary from Certitude's BCM and disaster recovery professionals.

When reading this Update, readers should also refer to the original 2012 Survey, available from the downloads section of the Certitude website at www.certitude.com.au.

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

In November 2015, Certitude also launched **PREVAIL**, our whole of life cycle expert BCM/DR Software-as-a-Service (SaaS). Prevail was developed by our BCM/DR professionals based on many years of experience, and outcomes from the 2012 Survey and the 2015 Update. To find out more about **PREVAIL**, go to http://www.certitude.com.au or contact us directly.

We thank all the organisations that gave their time to complete the Update. We hope you find this report interesting, and helpful in your efforts to manage your organisation's IT disaster recovery and business continuity capability.

Certitude
TECHNOLOGY RISK SERVICES

Executive Summary

The results of the 2015 Update (the Update) show that there are some noteworthy changes since the 2012 Survey (the Survey).

The Update indicates that disaster recovery in Australian organisations is generally managed, however there remain opportunities for organisations to achieve their disaster recovery objectives more effectively and economically, as well as reduce the number and impact of outages.

The key findings of the Update are as follows.

1. Respondents who spend around 3% of their IT Budgets on disaster recovery were most cost effective in reducing the number IT outages. Also, increasing the DR maturity level to 'defined' was associated with a reduction in the number and consequence of IT outages.

2. Because the majority of reported outages were caused by failures in areas predominantly within the control of the organisation, organisations should concentrate on improving the design and effectiveness of controls related to *change management*, *capacity & performance management*, *training*, and the *management of third-parties*.

3. Greater engagement with stakeholders can avoid problems when determining DR requirements, especially regarding re-entry of lost data and the clearing of work backlog when determining Recovery Point Objectives (RPOs).

4. Economies of scale and simplification of recovery strategies can be achieved by leveraging existing technologies used in production, as well as the use of cloud services for recovery if there is no desire for maintaining a data centre and IT resources, e.g. for Small / Medium Businesses (SMBs).

5. Boards, audit committees, third parties and insurers increasingly want assurance that the organisation's DR capability is adequate and can meet business requirements. Evaluation and reporting of DR plans and tests by third-parties can assist in providing such comfort.

6. Around one fifth of respondents have started using SaaS to document, maintain, distribute and use DR documentation. SaaS tools have the advantage that they can provide ubiquitous access, as well as greater assistance with plan development and activation.

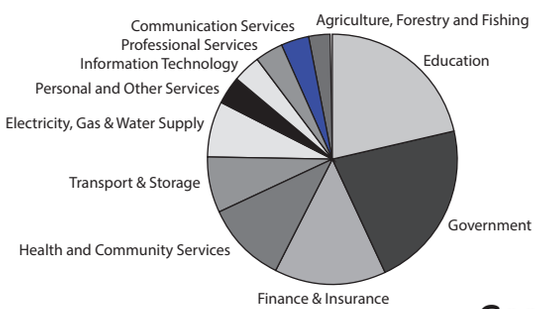
Certitude
TECHNOLOGY RISK SERVICES

Update Participant Demographics

Surveyed organisations spanned the range of Australian and New Zealand Standard Industrial Classifications (ANZSIC) industries and sizes, with the Update now including organisations with an annual IT spend of $500,001 to $1m (AUS). Like the 2012 Survey, Update respondents held C-level positions and other strategic roles, however the Update had a greater percentage of respondents who held IT managerial roles.

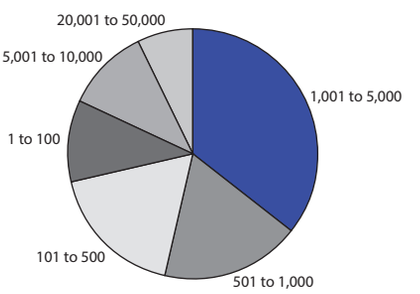
Industry

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



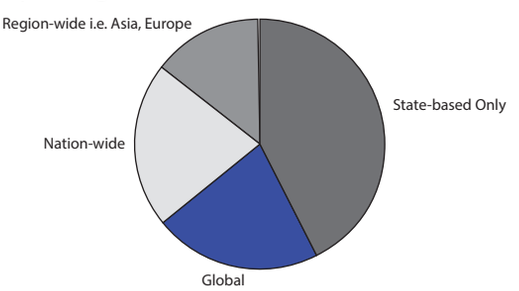
No. of Employees

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



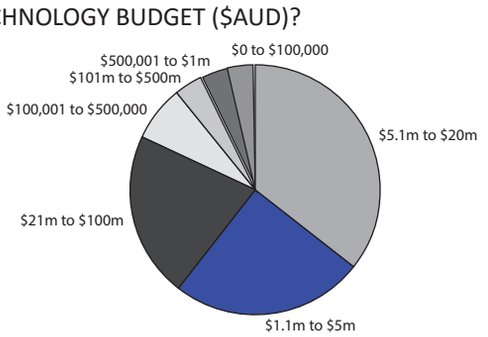
Geographic Presence

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



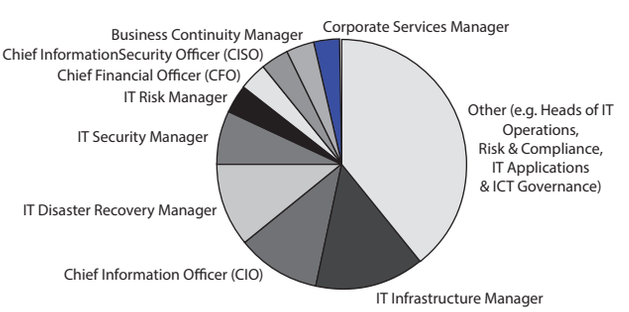
Annual Information Technology Spend

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



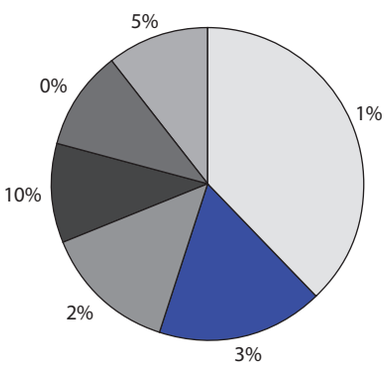
Role

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?

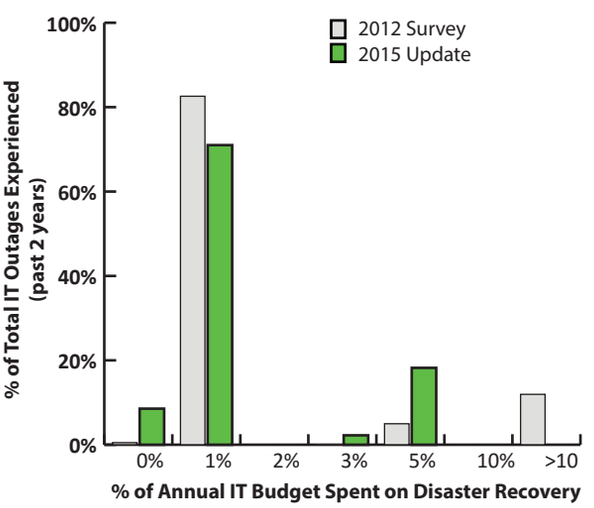


Respondents still spend on average 3% of their IT budget on disaster recovery, and those that do have the least number of outages.

A greater number of respondents (~11%) compared to 2012 Survey (~3%) spend 0% of their IT budget on disaster recovery, with the majority still spending about 1%.

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

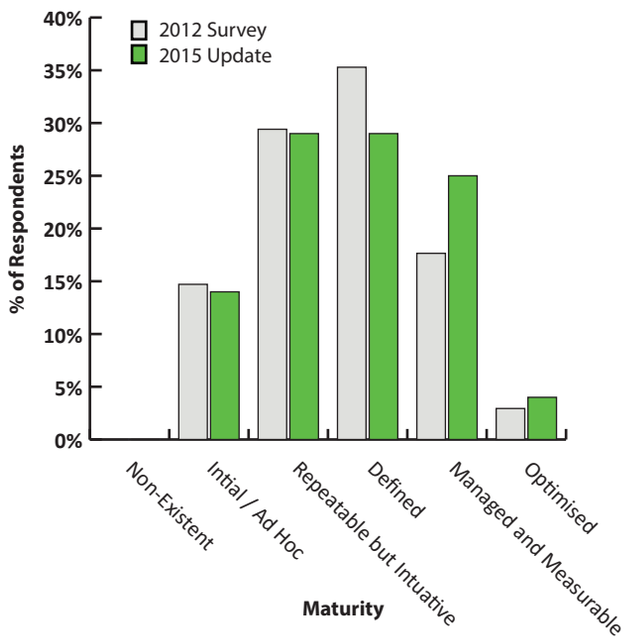
The majority of the total IT outages reported in the past two years (~80%) were experienced by respondents who spent around 1% or less of their IT budget on disaster recovery.

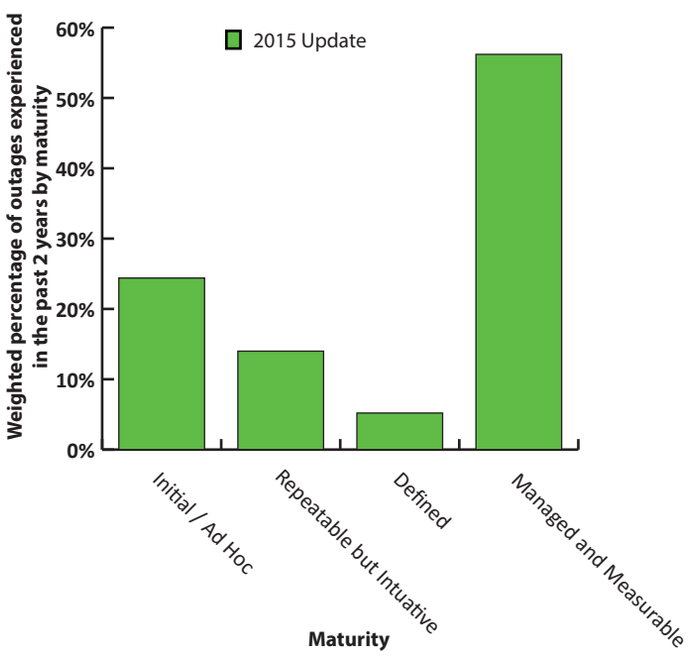


Certitude
TECHNOLOGY RISK SERVICES

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 3% 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.

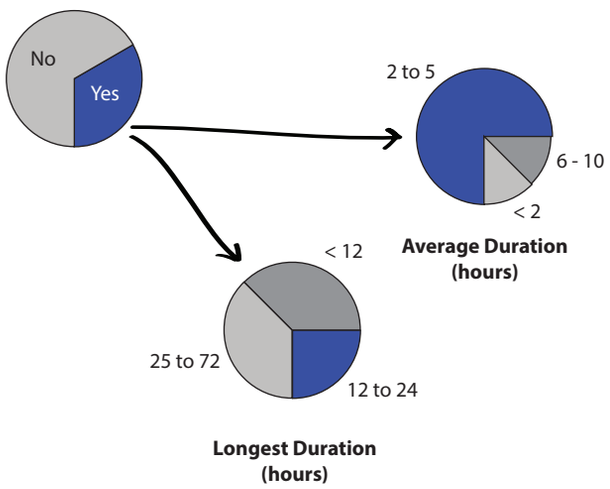
However, there were notable differences in maturity across different respondent industries. Respondents from mining, manufacturing, transport and storage, and communication services, on average described their maturity as 'repeatable, but intuitive' or lower. The financial services, education, health and community services, and professional services industries, on average described their maturity as 'defined' or higher. In the past two years, the weighted percentage in each level of maturity, who experienced an outage, were as follows:

- 'Initial/Adhoc' ~ 25%
- 'Repeatable, but Intuitive' ~ 14%
- 'Defined' ~ 5%
- 'Managed and Measurable' ~56%
- 'Optimised' = 0%

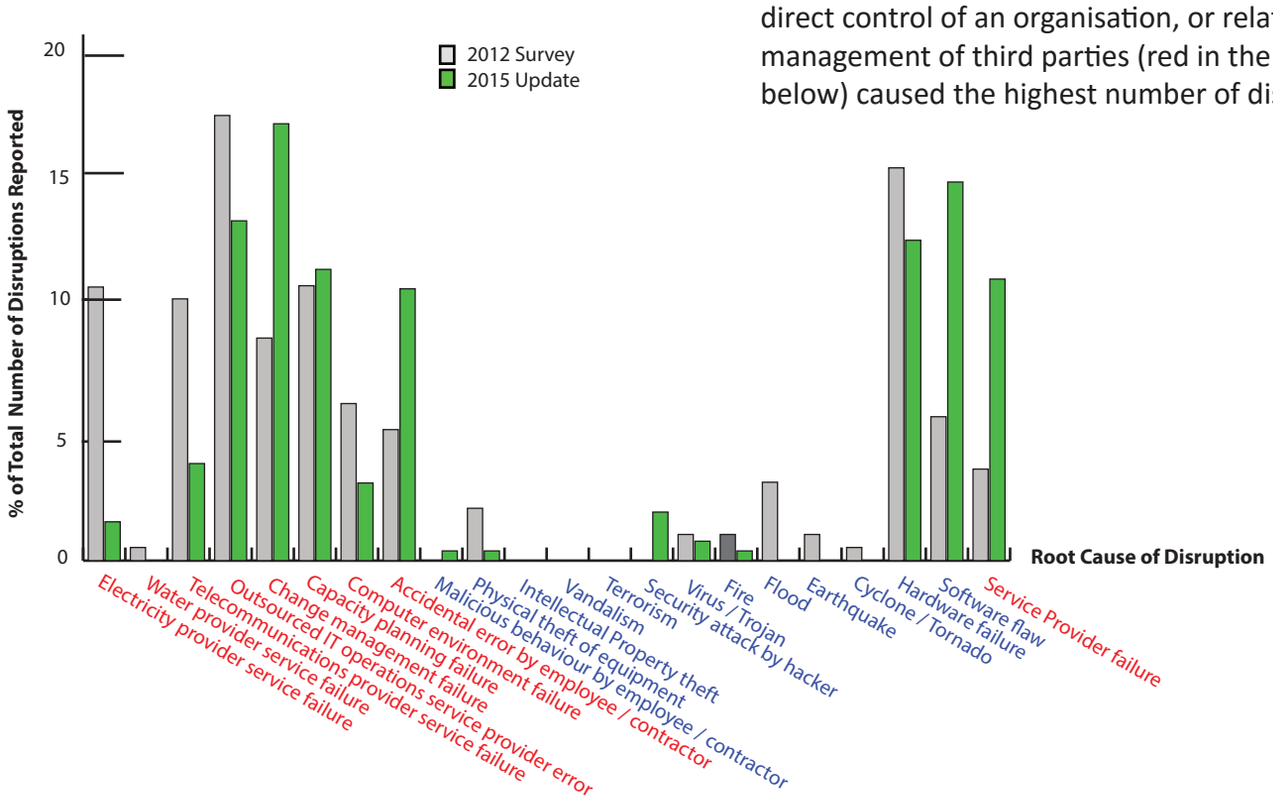
Where respondents have rated themselves as 'Managed and Measurable' and incurred a high percentage of the total outages reported, this may be due to unidentified weaknesses in their risk assessment process, particular in the organisation's ability to identify and address threats that may increase the likelihood of outages.

Threats & Disruptions

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



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)?



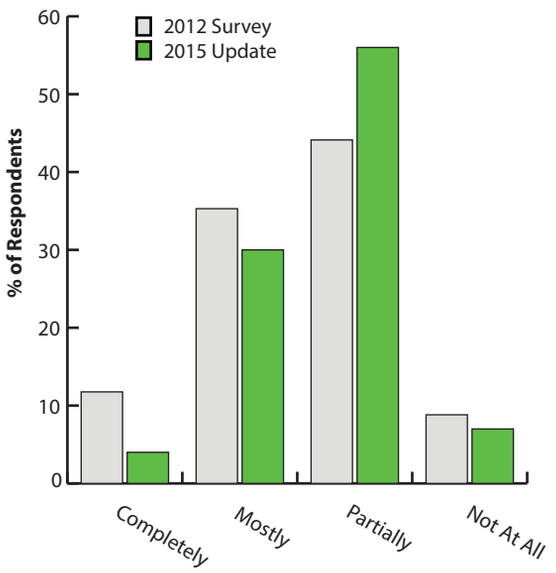
About a third (~32%) of respondents experienced a major and unplanned system disruption in the past two years. As in the 2012 Survey, most experienced an average outage of two to five hours. However the average longest outage had increased from less than 12 hours, to about 28 hours. None of the Update respondents experienced an outage of greater than 72 hours.

Many system disruptions continue to be essentially self-inflicted.

While service providers, hardware failures, and software flaws continue to cause a significant number of the reported disruptions, like in the 2012 Survey, areas that are predominately in the direct control of an organisation, or relate to the management of third parties (red in the chart below) caused the highest number of disruptions.

Expectations & Requirements

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



As in the 2012 Survey, despite a high participation of stakeholders in the determination of disaster recovery requirements, expectations appear to be poorly managed. Over half the respondents still thought that they partially managed unrealistic recovery expectations, if at all, and there was a material decrease in the number of respondents who thought they were completely managing unrealistic stakeholder expectations.

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.

Similar to the 2012 Survey, the 2015 Update respondents indicated that of all the potential areas of damage caused by unplanned system outages, reputational and operational damage were of the highest concern. The recognition that reputational damage is significant to many organisations presents a 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.

Like the 2012 Survey, most of the 2015 Update respondents, encouragingly, determine their disaster recovery requirements (MAOs etc.) 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, like in the 2012 Survey, nearly half the respondents had not adequately considered the re-entry and processing of lost data, and the clearing of any work backlog when determining Recovery Point Objectives (RPOs). Doing so may lead to:

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

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.

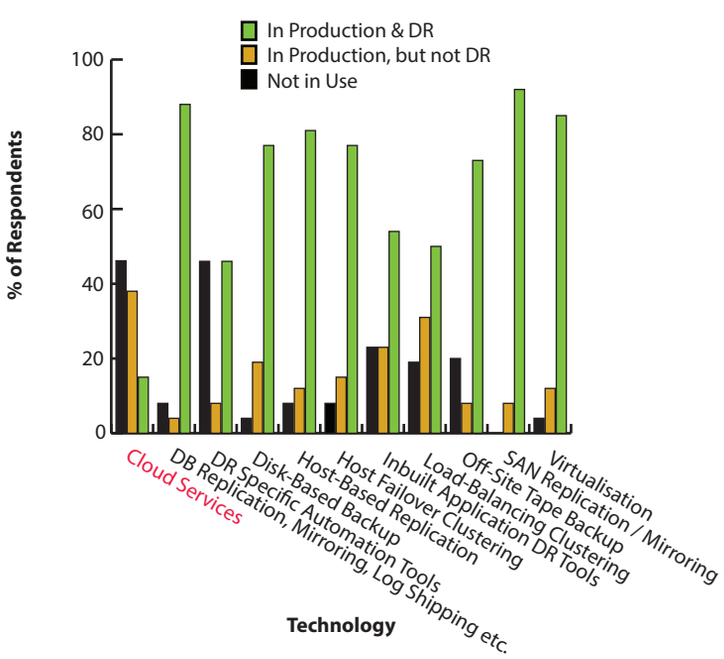
Design & Technology

In the 2012 Survey, despite the availability of cloud services, most respondents did not use cloud-based backup services. However, in the 2015 Update around 38% were using cloud services for production only, and 15% also for recovery.

Cloud-based disaster recovery is still incipient, SMBs especially are beginning to leverage DR cloud services. These services may be of benefit to organisations with limited IT resources, as having a recovery site in the cloud reduces the need for data centre space, IT infrastructure and IT resources.

However, organisations should be aware that there are some challenges still to overcome when using DR cloud services.

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



These challenges relate to:

- The security of the data when transferred and stored in the cloud.
- The strength of user authentication to protect against unauthorised access.
- The cloud service provider's ability to support and maintain the organisation's regulatory requirements, such as privacy.
- Provisioning adequate network band-width, not just for moving data into the cloud, but also when making data accessible once recovered, e.g. ensuring sufficient network capacity to provide an acceptable level of service from remote locations.
- The time it takes to restore from the cloud to on-premises infrastructure.

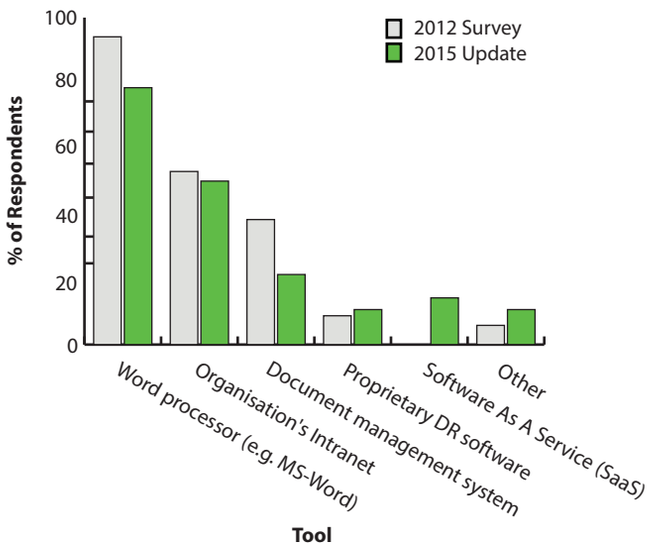
The use of cloud services for recovery is increasing.

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 Update, the majority of respondents 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 & Testing

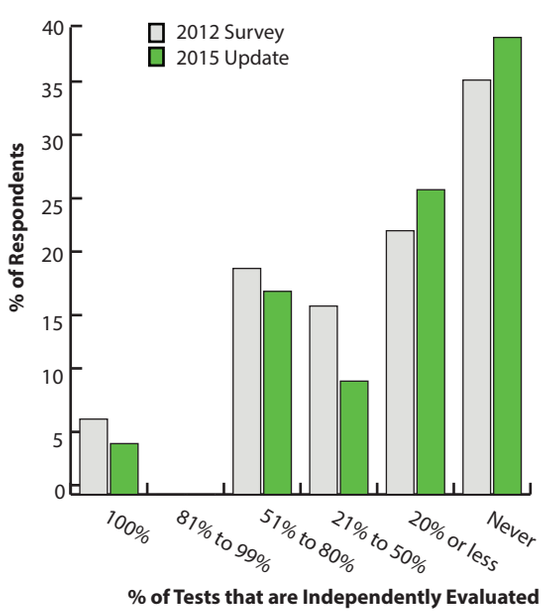
Which one or more of the following does your organisation use to DOCUMENT and MAINTAIN its disaster recovery documentation?



As per the 2012 Survey, the majority of respondents 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. However, cloud based documentation services have gained in popularity, with about 20% of respondents reporting using services to store and disseminate disaster recovery documentation .

Plans documented using traditional word processing tools are problematic to distribute, maintain and use during recovery.

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



The independent evaluation and reporting of tests by independent parties has remained essentially the same. However since the 2012 Survey, a greater percentage of respondents (~39% versus ~31%) never have their Disaster Recovery tests evaluated and reported by independent parties. In addition, for those that do have their tests independently evaluated, they do so for a smaller number of tests.

Increasingly, boards, auditors and insurers are seeking greater assurance of organisation's disaster recovery capability. Organisations that engage independent parties to evaluate their capability, can more easily provide such assurance, as well as potentially benefit from favourable business disruption insurance premiums.

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, and evidence based approaches, as well as methodologies that support independent advice.

We provide services in:

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

Certitude is the provider of the **PREVAIL** expert Business Continuity Management (BCM) cloud software service. Information at http://www.certitude.com.au.

Go to www.certitude.com.au 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.COM.AU