Singapore Standards Council

SS 507 : 2015
(ICS 35.040)

SINGAPORE STANDARD

Information and communications technology disaster recovery services

Published by
Enterprise Singapore

SS 507 : 2015
(ICS 35.040)

SINGAPORE STANDARD

Information and communications technology disaster recovery services

ISBN 978-981-4726-04-7

This Singapore Standard was approved by the Information Technology Standards Committee (ITSC) on behalf of the Singapore Standards Council on 14 September 2015.

First published, 2004
First revision, 2008
Second revision, 2015

The ITSC, appointed by the Standards Council, consists of the following members:

		Name	Capacity
Chairman	:	Mr Yap Chee Yuen	*Member, Standards Council*
Deputy Chairman	:	Mr Chak Kong Soon	*Member, Standards Council*
Secretary	:	Ms Ho Buaey Qui	*Infocomm Development Authority of Singapore*
Members	:	Assoc Prof Chan Mun Choon	*National University of Singapore*
		Mr Cheong Tak Leong	*SPRING Singapore*
		Mr Robert Chew	*Individual Capacity*
		Assoc Prof Benjamin Gan	*Singapore Management University*
		Mr Harish Pillay	*Internet Society (Singapore Chapter)*
		Dr Derek Kiong	*Individual Capacity*
		Mr Karl Kwan	*Singapore Polytechnic*
		Mr Lee Kee Siang	*Information Technology Management Association*
		Mr Kelvin Ng	*Nanyang Polytechnic*
		Mr Patrick Pang	*National Research Foundation*
		Mr Victor Tan	*Defence Science Technology Agency*
		Prof Tham Jo Yew	*Institute for Infocomm Research*
		Mr Thomas Ting	*Association of Small and Medium Enterprises*
		Mr Yow Tau Keon	*Singapore infocomm Technology Federation*

The Technical Committee on Security and Privacy Standards, appointed by the ITSC and responsible for the preparation of this standard, consists of representatives from the following organisations:

		Name	Capacity
Chairman	:	Mr Chan Kin Chong	*Individual Capacity*
Secretary	:	Mr Ho Kee-Vin	*StarHub*
Members	:	Mr Calvin Chan	*SIM University*
		Mr Ronald Chan	*Individual Capacity*
		Mr Aloysius Cheang	*Cloud Security Alliance*
		Mr Hoo Chuan Wei	*BT Singapore*
		Mr Kang Meng Chow	Cisco Systems
		Mr Lau Soon Liang	*Network for Electronic Transfer (S) Pte Ltd*
		Mr Lin Yih	*Digital Applied Research and Technology Pte Ltd*
		Mr Albert Pichlmaier	*Infocomm Development Authority of Singapore*
		Mr Philip Sy	*Professo Consulting Pte Ltd*
		Mr Wong Onn Chee	*Resolvo Systems Pte Ltd*
		Mr You Cheng Hwee	*Maximus International LLC*
		Mr Zhou Jianying	*Institute for Infocomm Research*

The Working Group, appointed by the Technical Committee to assist in the preparation of this standard, comprises the following experts who contribute in their *individual capacity*:

		Name
Convenor	:	Mr Lau Soon Liang
Deputy Convenor	:	Mr Edward van Leent
Members	:	Mr Ba Thein Naing
		Mr Ronald Chan
		Mr Chen Jie
		Ms Carolynn Lock
		Mr Sam Loong
		Mr Low Liang Ngien
		Mr Marc Ng
		Mr Frankie Phee
		Mr Sasanka Sekhar Sahu
		Mr Philip Sy
		Mr Jasper Tan
		Mr Wong Tew Kiat

The organisations in which the experts of the Working Group are involved are:

1-Net Singapore Pte Ltd
Acclivis Technologies and Solutions
Enterprise Products Integration Pte Ltd
Hewlett-Packard Singapore (Sales) Pte Ltd
Hitachi Data Systems Pte Ltd
IBM Singapore Pte Ltd
NCS Pte Ltd
Network for Electronic Transfers (Singapore) Pte Ltd
Organisation Resilience Management Pte Ltd
Professo Consulting Pte Ltd
StarHub
TÜV SÜD PSB Pte Ltd

(blank page)

Contents

		Page
Foreword		7
0	Introduction	9
1	Scope	12
2	Normative references	14
3	Definitions	14
4	Abbreviated terms	15
5	ICT disaster recovery	15
5.1	General	15
5.2	Asset management	16
5.3	Proximity of site	17
5.4	Proximity of services	17
5.5	Shared services	17
5.6	Vendor management	18
5.7	Outsourcing arrangements	19
5.8	Information security	20
5.9	Activation and deactivation of disaster recovery plan	21
5.10	Training and competency	22
5.11	Business continuity planning for ICT DR service providers	23
6	ICT disaster recovery facilities	24
6.1	General	24
6.2	Location of recovery sites	24
6.3	Physical facilities security	25
6.4	Dedicated areas	28
6.5	Environmental controls	29
6.6	Telecommunications	30
6.7	Power supply	31
6.8	Cable management	32
6.9	Fire protection	33
6.10	Emergency operations centre (EOC)	35
6.11	Non-recovery amenities	36
6.12	Facility equipment life cycle	36
7	Outsourced service provider’s capability	38
7.1	General	38
7.2	Review user organisation disaster recovery status	38
7.3	Logical access control	38

Page

7.4 ICT equipment and operation readiness 39
7.5 Simultaneous recovery support 39
7.6 Levels of services 39
7.7 Types of services 40
7.8 User organisation testing 40
7.9 Changes in capability 41
8 Continuous improvement 41
8.1 General 41
8.2 Internal audit 41
8.3 Performance measurement 41
8.4 Nonconformity and corrective actions 42
8.5 Management review 42

Annexes

A Guidance on planning and provision of ICT disaster recovery facilities 43
B Guidance on selection of recovery sites 52

Figures

1 ICT DR service provision framework 11

Bibliography 54

Foreword

This Singapore Standard was prepared by the Working Group appointed by the Technical Committee on Security and Privacy Standards which is under the direction of the Information Technology Standards Committee.

This standard is a revision of SS 507 : 2008. The 2008 edition was a modified adoption of ISO/IEC 24762 : 2008 which has since been withdrawn.

The revised standard incorporates industry feedback and updates industry practices. The changes in the revised edition include the following:

- Introduced management system elements into the revised standard including internal audit, corrective action and management review.

- Incorporated the clause on physical access controls into the clause on physical facility security to cover physical security holistically.

- Incorporated the clause on testing into the clause on facility equipment lifecycle to cover testing as part of the management of facility equipment lifecycle.

- Included concept and practices covered in the previous clause on restricted facilities into various clauses on facility (Clause 6).

- Streamlined and/or re-grouped requirements throughout the standard so as to provide precise and concise requirement statements and improve readability.

The awareness of information and communications technology disaster recovery (ICT DR) services has grown due to threats from terrorism and geopolitical tension. There are increased threats to the resilience of companies' IT and telecommunications infrastructure worldwide. Enterprises are looking at alternative locations for recovery purposes in the event of disruptions.

There is a strong value chain of service providers supporting the ICT DR cluster in Singapore. ICT DR service providers face challenges such as a need to differentiate themselves to retain competitive advantage and a need to maintain and constantly improve service levels.

Some concerns faced by the user organisations include the lack of clarity over the different type of service providers and the risk involved in outsourcing arrangements, especially for ICT DR functions.

It is targeted at ICT DR service providers (internal and outsourced) that wish to get certified under the standard as well as at ICT DR service providers and organisations that use the standard as a reference document.

This standard also provides a basis to certify and differentiate the outsourced ICT DR service providers, helps the user organisations in selecting the best-fit service providers and provides quality assurance. It also establishes industry best practices to mitigate outsourcing risks.

In preparing this standard, references were made to the following publications:

ISO 9001 : 2008	Quality management systems – Requirements
ISO/IEC 27001 : 2013	Information technology – Security techniques – Information security management systems – Requirements
ISO/IEC 24762 : 2008	Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services

Acknowledgement is made for the use of information from the above publications.

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions.*

2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR.*

3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

Singapore Standard for information and communications technology disaster recovery services

0 Introduction

0.1 General

This standard is aimed at specifying the requirements of an information and communications technology disaster recovery (ICT DR) Services Management System to which service providers shall conform in their provision of ICT DR services in order to achieve certification. The management system can be implemented on its own or be part of an integrated management system including information security management system (ISMS), business continuity management system and risk management system.

Information security management is the process by which management aims to achieve effective confidentiality, integrity and availability of information and service. When an organisation implements an ISMS, the risks of interruptions to business activities for any reason shall always be identified and mitigated.

ISO/IEC 27001, ISO/IEC 27002 and ISO 22301 include a control objective for information security aspects of business continuity management the implementation of which will reduce those risks. That control objective is supported by controls to be selected and implemented as part of the ISMS process.

Business continuity management is an integral part of a holistic risk management process that safeguards the interests of an organisation's key stakeholders, reputation, brand and value creating activities through:

a) identifying potential threats that may cause adverse impacts on an organisation's business operations, and associated risks;

b) providing a framework for building resilience for business operations; and

c) providing capabilities, facilities, processes, action task lists, etc., for effective responses to disasters and/or failures.

In planning for business continuity, the fallback arrangements for information processing and communication facilities become beneficial during periods of minor disruption(s) of service and essential for ensuring information and service availability during a disaster and/or failure for the (complete) recovery of activities over a period of time. Such fallback arrangements may include arrangements within the organisation, with third parties in the form of reciprocal agreements, or commercial subscription services.

0.2 Structure

This standard specifies requirements for the ICT DR services of a user organisation. It covers facilities and services capability and provides fallback and recovery support to an organisation's ICT systems. It includes the implementation, testing and execution aspects of disaster recovery. It does not include other aspects of business continuity management.

The requirements are applicable to both "in-house" and "outsourced" ICT DR service providers of physical facilities and services in varying degrees. ICT DR service providers shall interpret the intent of these requirements within the context of the services they offer.

This standard include the requirements for implementing, operating, monitoring and maintaining ICT DR services, divided into two areas:

- ICT DR (Clause 5); and

- ICT DR facilities (Clause 6)

"Outsourced service provider's capability" - Clause 7 specifies the capabilities which outsourced ICT DR service providers shall possess, and the practices they shall follow, for them to be able to provide basic secure operating environments to facilitate organisations' recovery efforts. The capabilities required are specified in terms of the infrastructure and services needed to enable organisations to implement and execute their ICT DR plans[1].

"Continuous improvement"- Clause 8 specifies requirements for ICT DR service providers for ensuring continuous improvement to their ICT DR services through a set of practices. These practices enable service providers to continuously maintain and improve the level of their services thus providing an additional level of assurance to organisations engaging these services.

Annexes A and B are informative and provide further guidance.

Annex A – "Guideline for implementation of ICT DR services management system", provides further consideration in the implementation of the management system.

Annex B – "Selection of recovery sites", provides guidance for:

- user organisations that are in the process of selecting an external recovery site as part of their ICT DR practices; and

- ICT DR service providers who are in the process of building (additional) recovery sites to expand their operations.

0.3 Framework

0.3.1 ICT DR service provision framework

This standard is based on a multi-tier framework comprising different elements in the ICT DR services provision, as illustrated in Figure 1. The "foundation" layer comprises the important aspects of ICT DR services, namely "Policies", "Performance Measurement", "Processes" and "People". This layer helps to define the supporting infrastructure and services capability. The "Continuous Improvement" layer highlights practices that help to improve ICT DR activities in specific areas, and represents an added level of p5rovision to the services provided. Thus the standard is drawn from a composite view of these layers, and with a balance between cost effectiveness and standard rigorous considerations.

0.3.2 Policies

"Policies" enable ICT DR service providers to set the direction in the other, related areas of their ICT DR services and also enable clear communication to the relevant parties on the requirements that can be met by ICT DR service provider facilities.

The "Policies" aspect is elaborated on in Clauses 5 to 8 . An established policy is usually expressed as "the system shall include the following policies …" or "there shall be documented policies and procedures …".

[1] It should be noted that although this clause is targeted at outsourced service providers, the requirements it contains are also applicable to service providers in general.

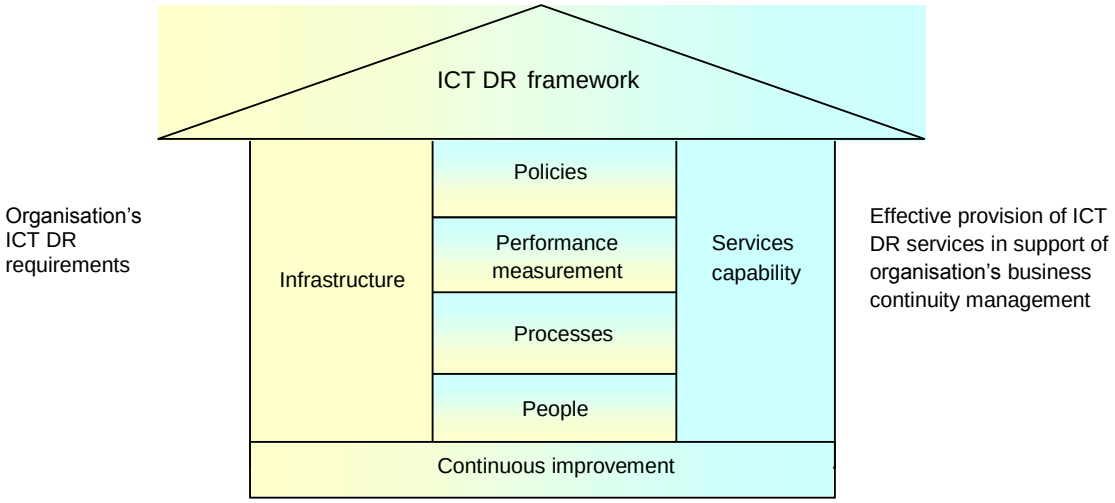

Figure 1 – ICT DR service provision framework

0.3.3 Performance measurement

"Performance Measurement" enables ICT DR service providers to review and improve their services whilst providing a means for them to demonstrate that their services meet user organisation requirements. This will in turn help to promote the ICT DR industry service level as a whole.

The "Performance Measurement" aspect is elaborated on in 8.3, which explains the need for measuring the performance of ICT DR services and illustrates some examples of measurement metrics that service providers can select.

0.3.4 Processes

"Processes" ensures that a consistent approach will be adopted in the other areas of ICT DR services, making possible the continuous maintenance of service levels and the ease of training of ICT DR personnel.

The "Processes" aspect is elaborated on in Clauses 5 to 8. An established process is usually expressed as "..according to appropriate established procedures.", "establish a set of procedures to ensure …", or "there shall be documented policies and procedures …".

0.3.5 People

"People," relates to the pool of skilled and knowledgeable service providers, organisation and where relevant, third party personnel needed to help operate, uphold and maintain ICT DR practices. Further, the safety and welfare of personnel is also one of the aspects which ICT DR service providers will need to take care of.

The "People" aspect is elaborated in various clauses of this standard. Subclause 5.10 covers the general training and competency requirements and 6.9 and 6.11 cover personnel health and safety.

0.4 Interpretation of clauses

0.4.1 Statements on capability expectations

Statements on capability expectations typically contain the phrase – " . . . service providers shall be capable of providing organisations with . . . " - meaning that service providers shall possess certain capabilities. Such capabilities can be a latent potential that can be swiftly activated by service providers if there is organisational demand. For example, additional resources could be readily channelled from another unit (e.g. from elsewhere in the region or country or from overseas) in response to an organisational requirement. Obviously the actual provision of a particular stated capability to any organisation would be subject to contract negotiations between the service provider and user organisation.

0.4.2 Service level agreement (SLA) / Service level commitment (SLC)

Certain subjects raised in this standard can be SLA/SLC issues. However, they do not dictate the content of the SLA/SLC between service providers and user organisations. The subjects raised are intended to build common understanding and expectation between the service providers and user organisations. In particular they serve to draw the organisations' attention to the typical items that could be included in SLA/SLC negotiations.

1 Scope

1.1 General

This standard describes the basic practices which ICT DR service providers, both in-house and/or outsourced, should consider.

It covers the requirements that service providers shall meet, recognising that individual organisations may have additional requirements that are specific to them (which would have to be addressed in their agreements/contracts with service providers). Examples of such organisation requirements may include special encryption software and secured operation procedures, equipment, knowledgeable personnel and application documentation. Such additional organisation specific requirements, if necessary, are generally negotiated on a case-by-case basis and are the subject of detailed contract negotiations between organisations and their ICT DR service providers and are not within the scope of this standard.

1.2 Exclusions

This standard does not:

a) provide any requirements on business continuity management as a whole for organisations;

b) take precedence over any laws and regulations, both existing and those in the future;

c) have any legal power over the SLAs included in negotiated contracts between user organisations and service providers;

d) address requirements, legal or otherwise, governing normal business operations to be adhered to by service providers. Examples of such requirements include detailed regulations covering building and fire safety, occupational health and safety, copyright regulation and prevailing human resource practices;

e) provide an exhaustive list, and thus technical security controls are not covered. Readers shall refer to ISO/IEC 27001 and ISO/IEC 27002, vendor literature and other technical references, as necessary.

1.3 Audience

This standard applies to:

a) all organisations requiring the ICT DR services as part of their business (whether in-house and/or outsourced);

b) ICT DR service providers in their provision of ICT DR services; and

c) communities of organisations with reciprocal or mutual arrangements relating to ICT DR services.

1.4 Certification

1.4.1 Certification categories

ICT DR service providers to be certified can be divided into two distinct categories: disaster recovery facility provider and disaster recovery service provider. Certification of the former examines physical infrastructure while certification of the latter examines its service capability.

1.4.2 Disaster recovery facility provider certification

The following clauses apply to disaster recovery facility provider certification:

a) Clause 5;

b) Clause 6; and

c) Clause 8.

1.4.3 Disaster recovery service provider certification

The following clauses apply to disaster recovery service provider certification:

a) Clause 5;

b) Clause 6;

c) Clause 7; and

d) Clause 8.

1.4.4 Exemption for internal service providers

For internal service providers, the following clauses are not applicable if they only provide services to one production site:

a) Clause 5.4;

b) Clause 5.5;

c) Clause 7.6;

d) Clause 7.7;

2 Normative references

The following referenced documents are indispensable for the application of this standard. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27001 *Information technology – Security techniques – Information security management systems – Requirements*

ISO/IEC 27002 *Information technology – Security techniques – Code of practice for information security management*