Singapore Standards Council

TR 62 : 2018
(ICS 35.020; 35.210)

TECHNICAL REFERENCE

Guidelines for cloud outage incident response (COIR)

Published by
Enterprise Singapore

TR 62 : 2018
(ICS 35.020; 35.210)

TECHNICAL REFERENCE

Guidelines for cloud outage incident response (COIR)

ISBN 978-981-47-8491-7

This Technical Reference was approved by the Information Technology Standards Committee (ITSC) on behalf of the Singapore Standards Council on 20 March 2018.

First published, 2018

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

		Name	Capacity
Chairman	:	Mr Yap Chee Yuen	*Individual Capacity*
1st Deputy Chairman	:	Mr Chak Kong Soon	*Singapore Computer Society*
2nd Deputy Chairman		Ms Samantha Fok	*Infocomm Media Development Authority of Singapore*
Secretary	:	Mr Yip Mann Fai	*Infocomm Media Development Authority of Singapore*
Members	:	Mr Chau Chee Chiang	*Government Technology Agency*
		Mr Cheong Tak Leong	*SPRING Singapore*
		Assoc Prof Benjamin Gan Kok Siew	*Singapore Management University*
		Mr Kendrick Lee	*Information Technology Management Association*
		Mr Lim Soon Chia	*Cyber Security Agency*
		Mr Kelvin Ng	*Nanyang Polytechnic*
		Mr Ni De' En	*National Research Foundation*
		Mr Harish Pillay	*Internet Society (Singapore Chapter)*
		Mr Tan Boon Yuen	*Singapore Polytechnic*
		Mr Victor Tan Hein Kiat	*Defence Science Technology Agency*
		Dr Henry Wong Chuen Yuen	*Agency of Science, Technology and Research*
		Mr Wong Wai Meng	*SGTech*

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

		Name	Capacity
Chairman	:	Mr Robert Chew	*Individual Capacity*
Secretary	:	Mr Steven Tan	*Infocomm Media Development Authority of Singapore*
Members	:	Dr Calvin Chan	*Singapore University of Social Sciences*
		Mr Chan Kin Chong	*Individual Capacity*
		Mr Hammad Rajjoub	*Individual Capacity*
		Dr Kang Meng Chow	*SGTech*
		Dr Ryan Ko	*Individual Capacity*
		Mr Kwa Kim Chiong	*Information Technology Management Association*
		Mr James Loo	*Information Technology Management Association*

		Name	Capacity
Members	:	Mr Kelvin Ng	*Nanyang Polytechnic*
		Ms Ng Lay Ngan	*National University of Singapore*
		Mr Harish Pillay	*Internet Society (Singapore Chapter)*
		Mr Raju Chellam	*SGTech*
		Dr J Anton Ravindran	*Singapore Computer Society*
		Dr Suriya Priya Asaithambi	*Institute of Systems Science*
		Mr Tao Yao Sing	*Infocomm Media Development Authority of Singapore*
		Mr Wong Onn Chee	*Resolvo Systems Pte Ltd*
		Mr Martin Yates	*Individual Capacity*

The Cloud Outage Incident Response Working Group, appointed by the Cloud Computing Standards Technical Committee to assist in the preparation of this technical reference, comprises the following experts who contribute in their *individual capacity*:

		Name
Convenor	:	Prof Alex Siow
Deputy Convenor	:	Mr Raju Chellam
Members	:	Mr Suresh Agarwal
		Mr Michael Chua
		Mr Paul Lee
		Ms Lim May-Ann
		Mr Lim Soon Tein
		Mr Edwin Lim Tai Huat
		Mr Paolo Miranda
		Mr Prem Prakash
		Dr J Anton Ravindran
		Mr David Siah
		Mr Tao Yao Sing
		Mr Adrian Toh
		Ms Evelyn Widjaja
		Mr Wong Tew Kiat

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

Asia Cloud Computing Association
Cloud Security Alliance Singapore Chapter
Defence Science & Technology Agency
Infocomm Media Development Authority of Singapore
Information Technology Management Association
National University of Singapore
SGTech
Singapore Computer Society

(blank page)

Contents

Foreword

This Technical Reference (TR) was prepared by the Cloud Outage Incident Response Working Group appointed by the Cloud Computing Standards Technical Committee (CCSTC) which is under the direction of the Information Technology Standards Committee (ITSC).

This TR is a provisional standard made available for application over a period of three years. The aim is to use the experience gained to update the TR so that it can be adopted as a Singapore Standard. Users of the TR are invited to provide feedback on its technical content, clarity and ease of use. Feedback can be submitted using the form provided in the TR. At the end of the three years, the TR will be reviewed, taking into account any feedback or other considerations, to further its development into a Singapore Standard if found suitable.

In preparing this TR, reference was also made to the following publications:

1. Cloud Outage Incident Response Guidelines 1.0 (Feb 2016), Infocomm Development Authority of Singapore (now known as Infocomm Media Development Authority of Singapore)

2. SS 584 : 2015 Specification for Multi-Tiered Cloud Computing Security

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

This TR is expected to be used by both Cloud Service Customers (CSCs) and Cloud Service Providers (CSPs).

Attention is drawn to the possibility that some of the elements of this TR may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

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.*

Guidelines for cloud outage incident response (COIR)

0 Introduction

0.1 Cloud outage risks

Cloud outages result in the unavailability of subscribed cloud services. This can adversely affect cloud service customers' (CSCs') accessibility to data and impact their business operations. It is imperative that these business disruption risks are mitigated so that CSCs can continue their operations whilst working with cloud service providers (CSPs) to rectify the cloud outage incident.

Cloud outages also adversely affect CSPs in terms of reputation and financial loss. Hence, it is also important that the associated risks are mitigated to minimise reputational and financial impact to the CSPs.

There are a variety of issues that can lead to a cloud outage. Some examples of such issues are listed below.

- Capacity and planning:
  - cloud service failure due to oversubscription in peak usage periods;
  - single-points-of-failure due to addition of complex technology components;
  - inability to verify cloud infrastructure resiliency;
  - inadequate physical and environmental safeguards for cloud hosting sites;
  - lack of continuity plan for cloud service failure, provider acquisition, or change in service strategy;
  - inadequate cloud migration planning.

- Operations and maintenance:
  - cloud service failure due to power or network outage;
  - inadequate monitoring of cloud resource utilisation;
  - lack of coordination of system maintenance resulting in conflicting changes and difficulty in troubleshooting;
  - inability to test cloud continuity and disaster recovery (DR) plans.

- External factors:
  - inability to troubleshoot performance issues due to continuous environment changes;
  - interruption of cloud services due to critical subcontractor failure.

Due to the above issues, CSCs could experience a varying degree of outage severity from limited usage, loss of functionality, cloud service degradation or unavailability of cloud services.

0.2 Motivation

CSPs' responses to cloud outages and service levels vary and often, their different approaches in handling cloud outage incidents will require CSCs to spend more time to understand and work out an outage plan with the CSP to enable timely remedial action. The lack of a common cloud outage incident response (COIR) framework is a hindrance for CSCs, regardless of their business size, to plan and take necessary preventive and mitigating measures to reduce damages and losses caused by cloud outages.

The main objective of this TR is to provide a COIR framework for CSCs to choose an appropriate outage protection measure to complement their own business continuity/IT DR capabilities through:

- a set of common parameters and guidelines for CSCs for identification, evaluation, and negotiation of protection needs with CSPs to incorporate into the SLAs;

– sharing of COIR practices by CSPs via the same set of common parameters to facilitate discussion, comparison and matching of outage protection needs with provisions.

This TR benefits CSCs in that it provides a mechanism for CSCs to work with CSPs to gain confidence in CSPs' ability to meet minimum outage protection requirements specified for their services. It provides guidance for CSCs to work with CSPs to both avoid or mitigate unnecessary business risks and reduce the negative impacts of cloud outages. On the other hand, CSPs benefit from having a mechanism to communicate their outage incident response measures for their cloud offerings.

These guidelines are built on recognised Singapore and international standards on cloud computing, IT security, business continuity management, and IT disaster discovery. A list of references is provided in Bibliography of this technical reference.

1 Scope

1.1 General

This TR describes a COIR framework that details different types of cloud outage protection needs, provides guidelines for CSCs on cloud outage mitigation, handling and post-management, and provides suggestions on what and how CSPs' COIR practices may be shared using the common framework.

The guidelines specified in this TR focus on cloud outage directly associated with operational mistakes, infrastructure or system failures and environmental issues (e.g. flooding, fire.) This TR is meant to provide recommendations on steps to be taken in managing cloud outage incidents. It can be used for all businesses regardless of their size, types of cloud service models as well as cloud deployment models.

This TR complements the ISO/IEC 19086 series of international standards with the generic title "Information technology – Cloud computing – Service level agreement (SLA) framework" and is intended to assist CSCs when they compare outage protection measures for cloud services from different CSPs.

This TR does not specify any conformance requirements. Besides, it does not make recommendations on handling of data breaches by CSPs as those are already specified in ISO/IEC 27035 series of international standards on information security incident management, ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, ISO/IEC 19086-4 Service Level Agreement (SLA) framework – Part 4: Security and privacy, and respective countries' legal and regulatory requirements. Consequently, this TR is not intended to be used for resolving issues due to cyber security, malicious act or breach of personal data protection laws.

1.2 Target audience

The main audience of this TR are CSCs and CSPs.

Cloud Service Customers (CSCs) – This TR provides clarity, at the onset of engagement of cloud services, to help CSCs develop appropriate incident response plan as part of their negotiations with CSPs to fulfil both legal and contractual obligations to their own customers and regulatory compliance in the event of a cloud outage. CSCs are the key beneficiaries who can choose the appropriate category for each parameter of outage protection needs to complement their own business continuity/IT DR capabilities including applicable legal and regulatory duties to fulfil.

Cloud Service Providers (CSPs) – This TR provides considerations for CSPs to support the business continuity and IT DR needs of the CSCs. Potentially, this helps not only cut down the client engagement time and sales cycle, but also minimise or avoid future disputes with CSCs in managing cloud outages. In addition, CSPs can utilise these COIR guidelines for any cloud outage investigation as the cause of outage may not be apparent initially till it is later confirmed/established.

2 Normative references

There are no normative references in this TR.