Feb 2016

FACTSHEET
Cloud Outage Incident Response Guidelines

Background

The Cloud Outage Incident Response (COIR) Guidelines continues Singapore's strong commitment to Business Continuity Management (BCM) and Disaster Recovery (DR) Plans by bringing clarity on how to respond to outages in the cloud. This will strengthen transparency, trust and resilience of cloud service providers (CSPs) in a Smart Nation.

It builds upon previous standards around BCM and DR plans and form part of IDA's drive to ensure standards keep pace in the changing landscape of emerging technologies such as the cloud, the Internet of Things and Big Data.

The guidelines enable CSPs to address the challenge of preparing for and mitigating the thread of cloud outages – whether for business-critical uptime or data sensitivity. CSPs which have completed COIR Guidelines can clearly state the scope and scale of resilience measures they have in place in the event of cloud outages.

Such clarity on capabilities has gained urgency as emerging technologies disrupt businesses. Cloud computing, with its off-premises and always-on capabilities; have created new questions around how enterprises should respond should the worst occur, both during and after an outage.

Research from the Cloud Security Alliance (CSA)[1] in 2014 has shown that the most common cloud outages result from situations such as power outages, natural disaster, traffic and DSN routing, software bugs, human error, failed storage, and network connectivity.

Adoption of COIR Guidelines will help address such concerns and, together with other cloud-related standards such as the Multi-Tier Cloud Security Singapore Standard, help drive adoption of cloud services. The "Cloud Adoption, Practices and Priorities" survey report released by the CSA in Jan 2015 indicated that 74% of enterprises are ready or hopeful to migrate to the cloud, or realize the need for a move to this new business model.

About COIR Guidelines

The COIR Guidelines sets out clear requirements which will help enterprises/cloud users and CSPs plan for and mitigate the threat of cloud outages – whether for business critical uptime or data sensitivity. It covers all cloud services and deployment models and is intended to aid in Singapore's Smart Nation cloud ecosystem resiliency.

The Guidelines address an urgent need for clear guidelines on how to respond to changing conditions around cloud outages both as and after they have occurred. To meet this need, COIR has been released as a set of Guidelines to allow for faster takeup and implementation in tackling the most common forms of cloud outages arising from non-security causes (e.g.

[1] Raj Samani, Brian Honan, Jim Reavis, 2014. Cloud Security Alliance Guide to Cloud Computing: Implementing Cloud Privacy and Security. Syngress. pp 45, figure 3.2.

power outages, hardware failure). It **does not** cover premeditated outages. COIR will now be further worked on together with the IT Standards Committee to be turned into a Singapore Standard.

Assessing appropriate COIR Tiers

COIR assesses CSPs based on two broad groupings (See table) spread across 17 criteria namely:

Group One:

Readiness, preparation & detection for outage such as sharing and testing of COIR plan and monitoring of health status of cloud services

Group Two:

Support and recovery from outage such as notification/communication plans and service restoration commitments

Group One	Group Two	
Preparation Before Outage	During an Outage	After an Outage

The COIR Guidelines help CSPs to assess and put in place plans for cloud outages such as:

- An appropriate communications plan;
- Activation of pre-planned processes and team(s) such as a senior management executive team and pre-installed command centre;
- Mobilization of additional emergency resources (including activation of third party services if necessary);
- Prioritisation levels for recovery and restoration of affected cloud services for risk and impact mitigation based on COIR tier.
- Monitoring a CSP's uptime via a third-party hosting service to detect outages
- Implementation of clear means for either CSPs or enterprises to notify the other regarding outages.

CSPs should also be capable of catering for various stress testing scenarios during exercises to validate their COIR plan.

The guidelines propose four tiers of response levels CSPs can choose to prepare for based on projected impact of outages, ranging from most to least severe:

- Tier A - Systemic / Life-Threatening Impact – cloud services hosting functions which directly affect human safety or stability of economy, market or an entire industry at large. Immediate restoration is essential. E.g. Air traffic management controls

- Tier B - Business Critical Impact – cloud services hosting functions that are critical to an organization's operations. Businesses may be severely impacted should restoration not occur within hours. Restoration should occur within four hours. E.g. Payment gateways, E-commerce portals.

- Tier C - Operational Impact – cloud services hosting functions that are essential to an organization's operations. Outage of these would result in significant impact to efficiency and effectiveness. Restoration within eight hours to a day is expected. E.g. Corporate emails.

- Tier D - Minimal Impact – cloud services hosting functions that are considered least important to an organization's operations and where longer duration of outages are tolerable. Restoration should generally occur within two working days. E.g. General information websites, development or testing environments.

Dependent on an enterprise's needs, they would decide upon which tier their cloud services should be prepared for. For example, an enterprise which relies heavily on official emails for business might require a Tier B-ready CSP, while those with alternative communication options may prefer Tier C.

About COIR Working Group

The COIR Working Group was formed in September 2013 comprising representatives from IDA, Defence Science & Technology Agency, Asia Cloud Computing Association, IT Management Association, Singapore Computer Society and Singapore IT Federation. Focus Groups comprising representatives from cloud users, CSPs and sectorial regulators were also formed to solicit their views and feedback.

For media clarification, please contact:

Eugene NEUBRONNER (Mr)
Manager, Corporate and Marketing Communication
Tel: +65 6211 1182
Email: Eugene_neubronner@ida.gov.sg

LIN Mei Jun (Ms)
Assistant Director, Corporate and Marketing Communication
Tel: +65 6211 3817
E-mail: lin_mei_jun@ida.gov.sg