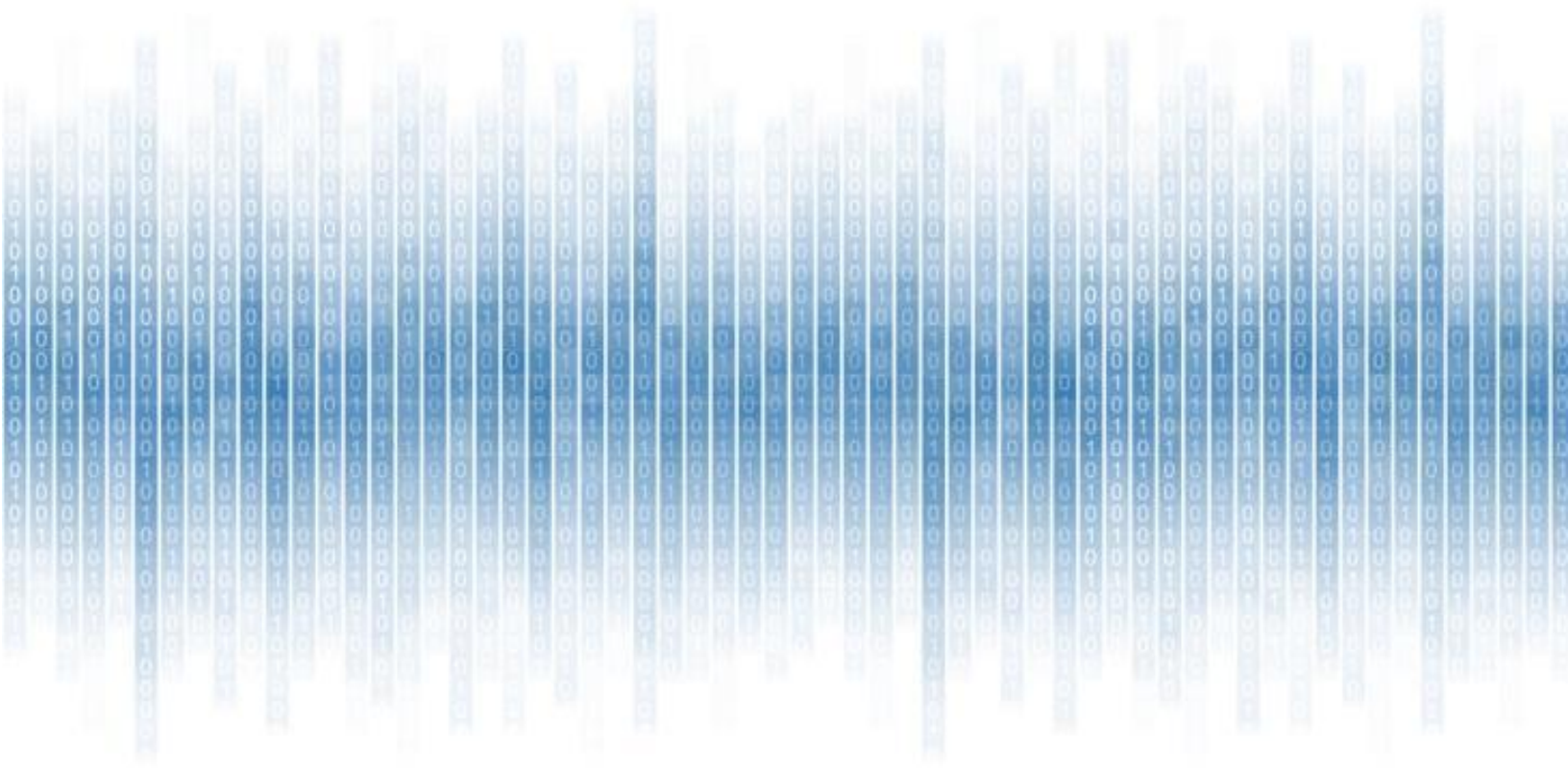

Cloud Incident Response Working Group

Charter

August 2018

WORKING GROUP EXECUTIVE OVERVIEW

- Working Group Scope and Responsibilities

Working Group Membership

- Working Group Structure
  - Co-Chairs
  - Committees
  - Sub-Work Groups

Alignments with Outside Groups

Operations

- Advisory
- Research Lifecycle
- Peer Review

Communications Methods

- Infrastructure & Resource Requirements
- Work Group Conference Calls and In-person Meetings

Decision-making Procedures

Deliverables/Activities

Duration

Charter Revision History

WORKING GROUP EXECUTIVE OVERVIEW

Mission Statement: To develop a holistic Cloud Incident Response (CIR) framework that comprehensively covers key causes of cloud incidents (both security and non-security related), and their handling and mitigation strategies. The aim is to serve as a go-to guide for cloud users to effectively prepare for and manage the aftermath of cloud incidents, and also a transparent and common framework for Cloud Service Providers to share with cloud customers their cloud incident response practices.

In February 2016, the former Infocomm Development Authority (IDA) – now the Infocomm Media Development Authority (IMDA) completed the development of Cloud Outage Incident Response (COIR) Guidelines. The Guidelines was subsequently submitted to Singapore's IT Standards Committee (ITSC) to be developed into a Singapore Technical Reference (TR), released in April 2018.

The COIR TR is an authoritative framework by the Singapore Government that brings clarity to cloud users on how to respond to outages in the cloud. It covers cloud outages directly associated with operational mistakes, infrastructure or system failure, and environmental issues such as flooding and fire are within scope. The scope for cloud outages caused by cyber security incidents and malicious acts had been excluded in part due to its complexity and expansive scope, and the fact that most cloud outages had not been attributed to cyber security-related causes[1].

With today's fast-evolving threat landscape, the Cloud Security Alliance (CSA) opines that cyber security incidents and malicious acts are imperative factors of cloud incidents that should be considered in a holistic cloud incident response framework. Exclusion of this within the COIR TR's scope represents an opportunity for CSA's volunteer community to play a role to bridge the gap. To do this, inputs can be drawn from Domain 9 (Incident Response, aka D9) of CSA's 'Security Guidance For Critical areas of Focus In Cloud Computing v4.0', which details response lifecycle in incidences of cyber security incidents and malicious acts.

This Cloud Incident Response (CIR) working group aims to develop a holistic CIR framework by merging and establishing of the complements – COIR TR + CSA D9, along with inputs from international standard frameworks such as National Institute of Standards and Technology Computer Security Incident Handling Guide (NIST 800-61rev2 08/2012), ISO/IEC 27035 and ENISA Strategies. The resulting whitepaper creates a comprehensive guideline to readers by collating and recommending best practices for effective management in events of cloud incidents. This will help CSPs align to market demand on service expectations, and regulators to standardise BCM

[1] Ko, Ryan, Stephen Lee, and Veerappa Rajan. "Cloud computing vulnerability incidents: A statistical overview." *Cloud Security Alliance* (2013).

requirements for CSPs. This framework will also help cloud users opt for the appropriate level of incident protection to complement their BC/DR capabilities.

This initiative is propelled with the ultimate goal of feeding the resulting whitepaper to steer international standards development, emulating the success of the joint project between SPRING and CSA - the 'Best Practices for Mitigating Risks in Virtualised Environments' whitepaper contributed to the ISO/IEC DIS 21878 efforts.

CSA initiatives that may be relevant for this work will be referenced in this work. Furthermore, alignment to global standards can be achieved through the CSA International Standardization Council.

Working Group Scope and Responsibilities

The CSA CIR Working Group will be the primary decision-making body relative to the reference architecture and the defined deliverables. A majority of the members will make decisions.

The scope for the CIR working group includes, but is not limited to:

- Develop a holistic CIR framework by merging of the complements – COIR TR + CSA D9
- Provide guidance for how the cloud shared responsibility model applies to the IR space for different incident scenarios (who is first to detect)
- Develop more situational awareness for cloud incident due to cyber security and/or malicious acts.
- Enlightenment of C-level
- Provide insights to the various reasons for cloud incidents and importance of having an incident response lifecycle
- Develop industry specific standard and regulations
- Holistic cloud incident response lifecycle

WORKING GROUP MEMBERSHIP

The working group is chaired by **Professor Alex Siow, Raju Chellam** and **Lim Soon Tein**.

Principal attendees will be designated representatives from an entity and any alternative to be designated by each principal.

The chair may appoint others as necessary to assure the effective execution of the defined work.

Other individuals may be invited to attend meetings by the principals as deemed necessary to provide inputs to topics under discussion.

Working Group Structure

Chair

The working group will be led by co-chair in addition to the selected leadership. The co-chair will assist with the leadership responsibility of the working group. The co-chair may appoint others as necessary to assure the effective execution of the defined research.

Committees

The working group may designate and organize subcommittees to aid in research with the initiatives pertaining to the subject matter of the working group.

Sub-Work Groups

Ad hoc sub-work groups comprised of subject matter experts may be formed to plan or execute any related outreach, awareness or research opportunities. Such sub-working groups shall report directly to the main working group.

ALIGNMENTS WITH OUTSIDE GROUPS

The working group may also choose to allow resource sharing between CIR and cyber security communities focused on CIR and other CSA working groups to assist in the timely completion of projects, programs and other activities needed to support/enable the working group's defined body of work, on demand basis. The working group will share research and standards that align with other CSA Working Groups, advisory groups, and industry partners (i.e SDOs, gov).

OPERATIONS

Advisory

The CSA Working Group will be advised by the CSA Subject Matter Expert (SME) Advisory Council, International Standardization Council (ISC), and CSA Executive Team to ensure that the research under the working group is within the scope of the CSA and aligns with other industry partner research. The research will remain unique to industry and make reference to any redundant or replicated works.

Research Lifecycle

The CSA Working Group will follow the development of the CSA research lifecycle for all projects and initiatives:

https://downloads.cloudsecurityalliance.org/initiatives/general/CSA_Research_Lifecycle_FINAL.pdf

Peer Review

We will seek CSA's help in reaching out to peers for reviewing our charter, publications, and other documented activities of the working groups.

COMMUNICATIONS METHODS

Infrastructure & Resource Requirements

The working group will be composed of CSA volunteers; it will have co-chairs and/or committee(s). The working group will require typical project management, online workspace and technical writing assistance.

Work Group Conference Calls and In-person Meetings

The working group will hold conference calls no less than quarterly. Attendance or participation in the online workspace by the Principal or Alternate is required. The Alternate must have full authority to act on behalf of the Principal if the Principal is absent. In-person meetings will happen in a location to be determined.

DECISION-MAKING PROCEDURES

A. Definition of a majority

1. A majority shall consist of more than half of the members present and voting.
2. In computing a majority, members abstaining shall not be taken into account.
3. In case of a tie, a proposal or amendment shall be considered rejected.
4. For the purpose under this Charter, a "member present and voting" shall be a member voting "for" or "against" a proposal, including proxy representative.
5. Proxy where authority is delegated through a written statement or non-repudiated email should be declared and inspected for validity by the working group leadership before voting starts.

B. Abstentions of more than fifty percent

1. When the number of abstentions exceeds half the number of votes cast (for votes, plus against votes, plus abstention votes), consideration of the matter under discussion shall be postponed to a later meeting, at which time abstentions shall not be taken into further account.

C. Voting procedures

1) The voting procedures are as follows:
    a) By a show of hands as a general rule, unless a secret ballot has been requested; if at least two members, present and entitled to vote, so request before the beginning of the vote and if a secret ballot under b) has not been requested, or if the procedure under a) shows no clear majority
    b) By a secret ballot, if at least five of the members present and entitled to vote so request before the beginning of the vote (online voting is applicable)
2) The Chair(s) shall, before commencing a vote, observe any request as to the manner in which the voting shall be conducted, and then shall formally announce the voting procedure to be applied and the issue to be submitted to the vote. The Chair(s) shall then declare the beginning of the vote and, when the vote has been taken, shall announce the results.
3) In the case of a secret ballot, the working group leadership shall at once take steps to ensure the secrecy of the vote.

DELIVERABLES/ACTIVITIES

Q2 2019

Publish a whitepaper covering the following:

- Merging of the complements – COIR TR + CSA D9
- Analysis of cloud incidences
- Analysis of current cloud incident response and recovery
- Holistic guideline for cloud incident response for Cloud Users and CSPs

DURATION

The working group will operate until Q1 2020 for its chartered deliverables, and at that time consider charter renewal.

Charter Revision History
