Title of Deliverable

Cloud Incident Response Framework

Objective of Deliverable

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.

Scope of Deliverable

This CIR framework seeks to provide guidelines to plan and prepare for cloud incident, mitigation strategies and post-mortem processes based on the following documents:

1. Technical Reference (TR) 62 – Cloud Outage Incident Response (COIR)
2. CSA 'Security Guidance For Critical areas of Focus In Cloud Computing v4.0'
3. NIST 800-61 Computer Security Incident Handling Guide
4. ISO/IEC 27035
5. ENISA Strategies
6. Other relevant documents (suggested by WG members)
    a. ISO 223220:2011 Societal Security - Emergency Management - Requirements for Incident Response
    b. FedRAMP Incident Communications Procedure

This framework focuses on and should be applicable to all cloud incidents that affect the regular operations of cloud services. These incidents can be a result of both security and non-security related causes, including but not limited to operational mistakes, infrastructure or system failure and natural disasters. It provides guidelines on developing an effective incident response procedure, but the essential focal point of this document is detecting, analysing and handling incidents.

Principles provided are intended to be sufficiently-generic so that it is applicable to all organizations regardless of size or industry. Customisations and additions to the framework for specific industry sectors' are recommended and can be addressed in the Working Group (WG)'s future deliverables in the form of addendums to the generic framework.

The framework aims to help CSPs align to market demand on service expectations, and regulators to standardise BCM requirements for CSPs. This framework will also help cloud users opt for the appropriate level of incident protection to complement their BC/DR capabilities.

The WG may consider in its first deliverable to work on a high-level and concise document to give an overview of the CIR framework, before diving into next-level details in subsequent deliverables.

Skeletal Structure

1. Foreword
2. Introduction
    a. Purpose and Scope
    b. Audience
3. Normative References
4. Definitions, Abbreviations and Acronyms
    a. Definition of ‘incident’
    b. Incident risks
5. CIR Framework
    a. Preparation
    b. Detection and Analysis
        i. Security-related
        ii. Non-security related
        iii. Incident classification scale
    c. Containment, Eradication, and Recovery
    d. Post-Mortem
    e. Coordination and Information Sharing
6. Guidelines for CSCs
7. Guidelines for CSPs
8. Using the COIR framework
9. Annex

Timeline

Phase I: Open all clauses for discussion except Guidelines for CSPs/CSCs.
Phase II: Guidelines for CSPs / CSCs to be discussed.
Phase III: Phase I & II combined.