Contents

1.0 Problem Statement ..............................................................................................................................................4
2.0 Working Group Purpose .......................................................................................................................................4
3.0 Core Values...........................................................................................................................................................5
4.0 Scope ....................................................................................................................................................................5
5.0 Deliverables ..........................................................................................................................................................6
6.0 Membership & Structure of the Working Group .................................................................................................7
7.0 Advisory Roles ......................................................................................................................................................7
8.0 Communications Methods ...................................................................................................................................8
9.0 Duration ................................................................................................................................................................8
Working Group Executive Overview

1.0 Problem Statement

Security incidents that involve cloud computing environments can present significant challenges to responders. There are technical and legal hurdles to detecting and investigating information security incidents when computing environments span geographical, jurisdictional, and organizational boundaries. Similar issues are present in the realms of legal compliance and electronic Discovery (“eDiscovery”).

Although many of the underlying technologies involved in provisioning cloud computing have been in existence for years, they are being combined in novel ways. This creates both opportunities and challenges for the collection, preservation and analysis of digital forensic evidence. Despite the fact that the fundamentals of incident handling and forensics remain unchanged, the constant innovation that is a hallmark of the industry requires that we keep pace in developing technical and procedural capabilities.

2.0 Working Group Purpose

The working group intends to serve as a focal point for the examination of incident handling and forensics in cloud environments. Initially, we seek to develop best practices that consider the legal, technical, and procedural elements involved in responding in a forensically sound manner to security incidents in the cloud. Working together with cloud providers, consumers, governments and the legal and academic communities, we hope eventually to lead an effort to define and promulgate standards in this domain.

We intend to promote the use of best practices in this domain by:

- Gaining input and consensus from identified stakeholders
- Defining the problem space accurately by conducting a gap analysis for cloud environments
- Helping to clearly define a conceptual framework that maps the relationships between forensics, incident handling, legal compliance and electronic discovery
- Establishing a roadmap for the creation of standards
- Collecting and indexing current research and sponsoring new research that is driven by real world issues identified by the community
- Providing timely reporting to the community on current state and new developments in incident management and forensics
- Authoring portions of the “Security Guidance for Critical Areas of Focus” and developing supplemental guidance, templates and other useful tools
- Educating the community on issues relating to the domain
3.0 Core Values

It is the intention of the Incident Management and Forensics Working Group to:

- Build upon existing standards, research and other related work
- Be inclusive by seeking input and communicating effectively with all stakeholders
- Provide robust guidance by utilizing sound scientific research

4.0 Scope

The scope of the working group includes, but is not limited to, the following topics:

- Incident Management (IncM) in Cloud Environments
  - The IM lifecycle in cloud environments (preparation, detection, analysis, containment, eradication and recovery, and continuous improvement)
  - General legal and technical issues related to IncM in clouds
    - Types and locations of available evidence such as log data, forensic artifacts, etc.
    - Contractual and general legal issues
    - Collection of evidence
    - Multi-jurisdictional issues
    - Multi-tenancy Issues
  - Command, Control and Communications (C3)
- Cloud Forensics
  - Relationship between cloud forensics and IM in clouds
  - Cloud service provider (CSP) forensics capabilities
  - ISO 27037 mapping (guidelines for identification, collection, acquisition, and preservation of digital evidence)
  - Process for conducting cloud forensic investigations
    - CSP perspective
    - Customer perspective
    - Legal perspective
    - Law enforcement perspective
- eDiscovery
- Legal & technical issues related to cloud forensics
  - Service level agreements (SLA) for forensic support
  - Warrants for evidence from cloud environments
  - Forensic-ready virtual cloud environments
  - Data provenance for forensic evidence
  - Chain of custody
  - Forensics as a Service
  - Privacy and handling of PII
  - Forensics as part of IM lifecycle
  - Best practices for cloud forensics
5.0 Deliverables

Deliverables will be governed by CSA’s intellectual property rights policy.

**Q4 2012**

- Finalize charter
- Identify lawyer with appropriate experience to participate in working group
- Identify cloud providers that may be willing to participate and provide feedback
- Identify academic institutions that may be willing to partner
- Survey cloud consumers and providers to identify their major concerns for IncM and forensics in the cloud
- Cloud Security Congress

**Q1 2013**

- Begin development of a roadmap to industry accepted standards for cloud forensics and incident handling
- Develop a set of research priorities for academia
- Identify any related work produced by other entities, creating a single information repository for IncM/Forensics topics in cloud environments
- Provide content for CCSK examination
- Publish “Mapping of ISO 27035 Controls to Cloud Environments: Gap Analysis” (title not final)
- Initial Draft of “Provider Forensic Support in Public Multi-Tenant Cloud Environments”

**Q2 2013**

- Publish “Provider Forensic Support in Public Multi-Tenant Cloud Environments”
- Published a capability maturity model (CMM) for IncM and forensics in cloud environments

**Q3 2013**

- Conduct first workshop on IncM and forensics roadmap for the cloud. The intention is to bring the industry to a roundtable discussion to shape goals and the short-, mid-, and long- term milestones for an industry roadmap.
- Publish results that have been created by the working group

**Q4 2013**

- Establish discussion, solidify goals and open request for comments
Q1 2014

- Finalize roadmap with milestones and present them to the broad public
- Initiate the discussion for follow-up projects

6.0 Membership & Structure of the Working Group

The working group will be composed of CSA volunteers who meet at least one of the criteria listed below. Individuals who meet more than one of the criteria will be given preference when adding new working group members. Ideally, working group members:

- Are highly motivated and willing to contribute to a non-profit working group
- Have documented experience in the domain either through their current or previous jobs or through conducting academic research of high quality.
- Can provide references as to their bonafides

The Incident Management and Forensics Working Group will have two co-chairs, who will provide updates and seek guidance from the advisory roles. The working group will require typical project management, online workspace and technical writing assistance.

Peer Review

We will seek the CSA’s help in reaching out to peers for reviewing our charter.

7.0 Advisory Roles

Advisory roles will be held by subject matter experts to support the Incident Management and Forensics research efforts. Subject matter experts will help provide:

- Guidance on research projects conducted by the working group
- Suggestions for new projects relevant to the industry
- Input on current research projects, including peer review of materials
- Access to properly sanitized data for research purposes
- Access to cloud provider contacts for research interviews

Advisory roles can be filled through individual subject matter experts, as well as through liaisons for groups such as CloudCERT.
8.0 Communications Methods

Communication will be through bi-weekly phone calls and through online collaboration tools such as the CSA’s basecamp site.

9.0 Duration

The working group will operate until Q1 2014 for its chartered deliverables, and at that time consider charter renewal.