ISO27037 – Requirements Overview:

This document outlines the ISO27037 requirements, as well as showing the way in which these requirements can be interpreted / adhered to in a cloud context.

# General Requirements

## Requirements for Identification, Collection, Acquisition and Preservation of Digital Evidence - ISO 27037

|  |  |
| --- | --- |
| **ISO27037** | **Cloud** |
| **5.3.2 Auditable**  It should be possible for an independent assessor or other authorized interested parties to evaluate the activities performed by a DEFR (Digital Evidence First Responder – “individual who is authorized, trained and qualified to act first at an incident scene in performing digital evidence collection and acquisition with the responsibility for handling that evidence”) and DES (Digital Evidence Specialist – “individual who can carry out the tasks of a DEFR and has specialized knowledge , skills and abilities to handle a wide range of technical issues”). This requires appropriate documentation regarding actions taken, why and how. | While this high-level requirement itself remains the same for cloud environments, execution becomes more difficult as investigations will likely be conducted on dynamic, distributed, and complex systems that can neither be frozen nor easily identified. Thus, the necessity for appropriate qualifications and documentation becomes even more important. |
| **5.3.3 Repeatable**  Repeatability is established when the same test results are produced under the following conditions:   * Using the same measurement procedure and method * Using the same instruments and under the same conditions * Can be repeated at any time after the original test | While standard procedures and methods seem to be achievable even in a SaaS environment, conducting tests “under the same conditions” and “at any time after the original test” becomes more challenging (but not always impossible) within a dynamic, distributed, and complex cloud environment.  For acquisition in current forensic practice regarding imaging memory, an active log file, or other dynamic process, the concept of “snapshot forensics” is used. The analogy is that no two successive snapshots of a running child will capture exactly the same image (since the child is moving) but the snapshot accurately captures the appearance of the child and her background at a moment in time. Assurance of reliability for the snapshot then becomes assurance of its provenance and that it has not been modified since acquisition. Documentation can assure the identity, place and time of the snapshot while traditional techniques such as cryptographic hashes and chain-of-custody processes can provide integrity assurances.  The snapshot process is repeatable as it can be demonstrated that the camera will take an “accurate” photograph each time the shutter release is pressed. Reproducibility can similarly be shown by using a camera of similar capability from a different manufacturer. Thus, the process can be repeatable and reproducible even though no two successive snapshots of the running child will ever produce exactly the same results. |
| **5.3.4 Reproducible**  Reproducibility is established when the same test results are produced under the following conditions:   * Using the same measurement method * Using different instruments and under different   conditions   * Can be reproduced at any time after the original test |
| **5.3.5 Justifiability**  The DEFR should be able to justify all actions and methods used. | No changes for cloud environments. |

## Digital Evidence Handling - ISO 27037

|  |  |
| --- | --- |
| **ISO27037** | **Cloud** |
| **5.4.1 General**  Potential digital evidence should be treated according to the following principles:   * Minimize handling * Account for any changes and document actions * taken * Comply with local rules of evidence * Do not take actions beyond your competence | No changes for cloud environments |
| **5.4.2 Identification**  The search for, recognition and documentation of potential digital evidence should be undertaken according to the following principles:   * Prioritize the evidence collection based on volatility * Minimize the damage to the potential digital evidence * Identify hidden digital evidence * Recognize that identification may be difficult (cloud) | Potential identification of the additional data sources unique to the cloud service model. Specifically:   * SaaS - application level logs like authorization errors, accounting (who did what, when), performance issues, data volumes * PaaS - application specific logs available ideally via an API, patch status, authentication errors, operating system exceptions and warnings, anti-malware software warnings * IaaS - system level logs, Infrastructure: hypervisor events and logs, raw virtual machine files suspend files capturing unencrypted RAM snapshots , Intrusion detection and firewall events, network events and packet capture, storage logs, backups. |
| **5.4.3 Collection**  *“Collection is a process in the digital evidence handling process where devices that may contain digital evidence are removed from their original location to a laboratory or another controlled environment for later acquisition and analysis.”* | Due to the multi-tenant nature of cloud infrastructures, acquisition should usually be preferred over collection to avoid impacts to parties not involved in the matter and the gathering of irrelevant information that must be excluded during analysis. However, the specifics of the legal mandate in a particular situation must be followed. It must be emphasized that collection of digital evidence can often only be performed by the CSP and not by the tenant. |
| **5.4.4 Acquisition**  The process of creating a copy of an item of potential digital evidence. | Because of the virtual nature of the cloud infrastructure, items normally thought of as physical (hard drives, server memory, etc.) will be logical items (a virtual hard disk file, a file that contains the contents of server memory for a suspended virtual machine, etc.) and acquisition must focus on these logical items rather than the physical containers where they reside. |
| **5.4.5 Preservation**  Preservation is the protection of the integrity of potential digital evidence. Potential digital evidence and digital devices must be safeguarded from tampering or spoliation. | No changes for cloud environments. However, the chain of custody must be preserved as well, which is challenging in multi-geographical and multi- jurisdictional environments. |

## Key Components of Identification, Collection, Acquisition and Preservation of Digital Evidence – ISO 27037

xxxxxxxx

# Instances of Identification, Collection, Acquisition and Preservation - ISO 27037

## Computers, Peripheral Devices and Digital Storage Media - ISO 27037

Some sections missing

|  |  |
| --- | --- |
| **ISO27037** | **Cloud** |
| **7.1.1 Identification**  **7.1.1.1 Physical incident scene search and documentation**  This refers mainly to stand-alone systems and is therefore only partially applicable for cloud |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |