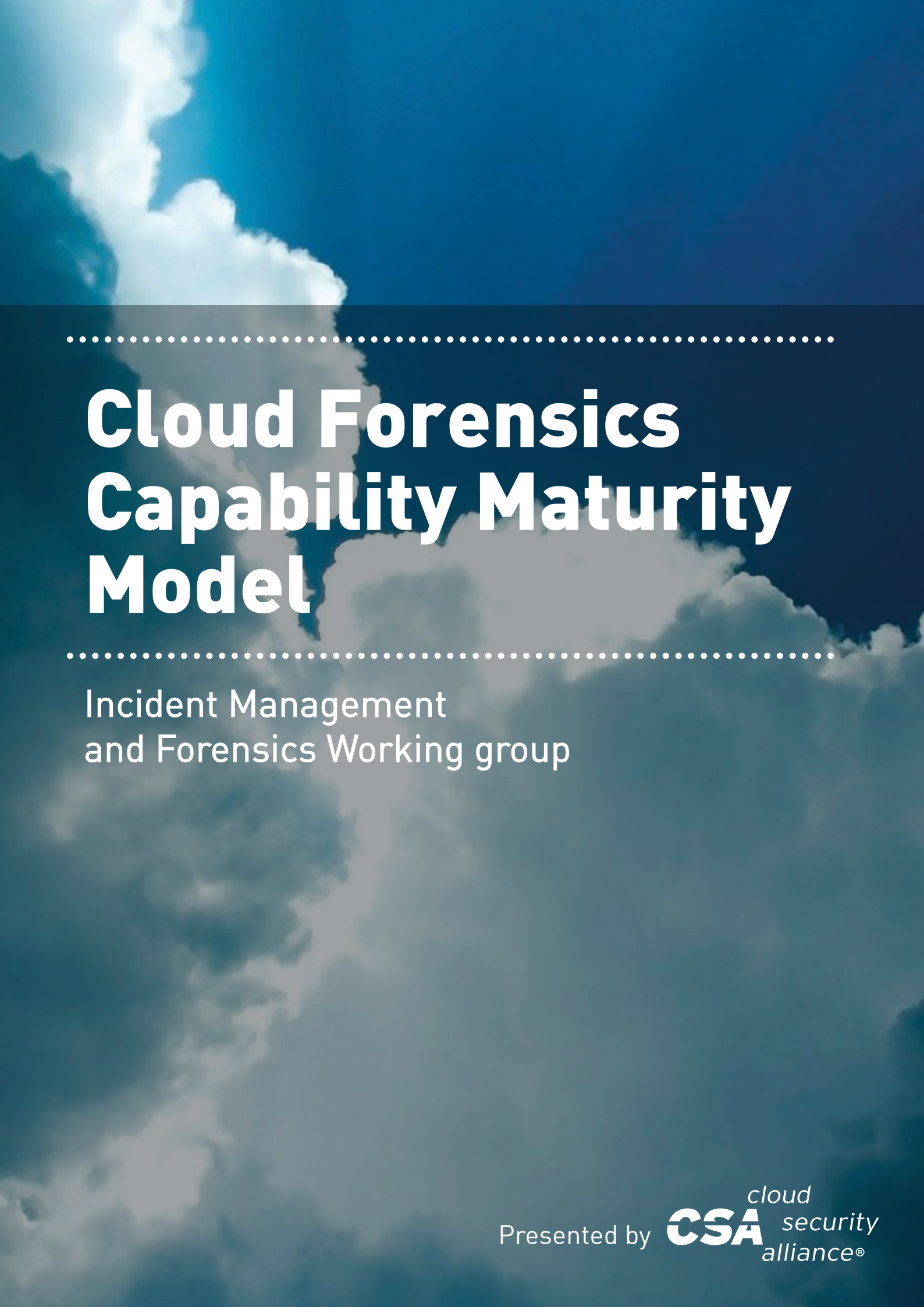

Cloud Forensics Capability Maturity Model

Incident Management
and Forensics Working group

Presented by CSA cloud security alliance®

Contents

Acknowledgments

Authors

Richard Austin
Bernd Jäger
Dominik Birk

Contributors

Curtis Kozielec
Michael Roza
Randy Tangco
Ricci Leong
Samuel Moore
Raymond Choo

CSA Global Staff

Luciano Santos
Ekta Mishra
Frank Guanco
Larry Hughes

Cloud Forensics Capability Maturity Model

This document describes a Capability Maturity Model (CMM) that can be used by both cloud consumers and Cloud Service Providers (CSPs) in assessing their process maturity for conducting digital forensic investigations in the cloud environment.

Intended Audience:
The target audience for this paper is enterprise users that deal with all aspects (technical and organizational) of their forensic processes, and that plan to or have already integrated cloud IaaS services into their IT infrastructure.

The starting point for the model was the Carnegie Mellon University Software Engineering Institute's (SEI) "Software Process Maturity Framework"[1] which identifies five progressive levels of process maturity as shown in Table 1.

Level	SEI Capability	Forensics Question
1	Initial	How are we ever going to do this?
2	Repeatable	Have we ever done this before?
3	Defined	What is our process for doing this?
4	Managed	What resources did this require?
5	Optimizing	How can we do this better?

Table 1. Forensic maturity levels

The following chapter will describe how this model could be mapped to cloud forensics giving some high-level guidance per level. This initial work will focus on the IaaS Cloud usage model to reduce complexity. Other models might be subject to future research.

[1] Carnegie Mellon University Software Engineering Institute (1995) The Capability Maturity Model: Guidelines for Improving the Software Process. Addison-Wesley. pp. 15-17.

Level 1: Initial – How are we ever going to do this?

This level might be considered "chaotic," insofar as it applies to organizations in which there is no defined process, and perhaps even no defined responsibility, for carrying out the forensic process. It is characterized by initial panic followed by heroic[2] efforts by an ad hoc team that manages to carry out some form of investigation. No knowledge capture is employed, and the valuable lessons in how a cloud investigation should be carried out are lost. Unless progress is made to the next level, the next time an investigation is triggered, the same chaotic process will occur.

Level 2: Repeatable – Have we ever done this before?

At this level, the cloud consumer and the CSP have begun to recognize that the need for a digital forensics investigation is a repeating phenomenon, and that they should therefore start preserving their knowledge and experience. Preservation is an important characteristic at this level, as it enables the organization to leverage past experience when faced with similar types of investigations in the future.

Consider the following diagram for a typical security incident that triggers a forensics investigation (for instance, a compromised virtual machine (VM)) in a cloud:

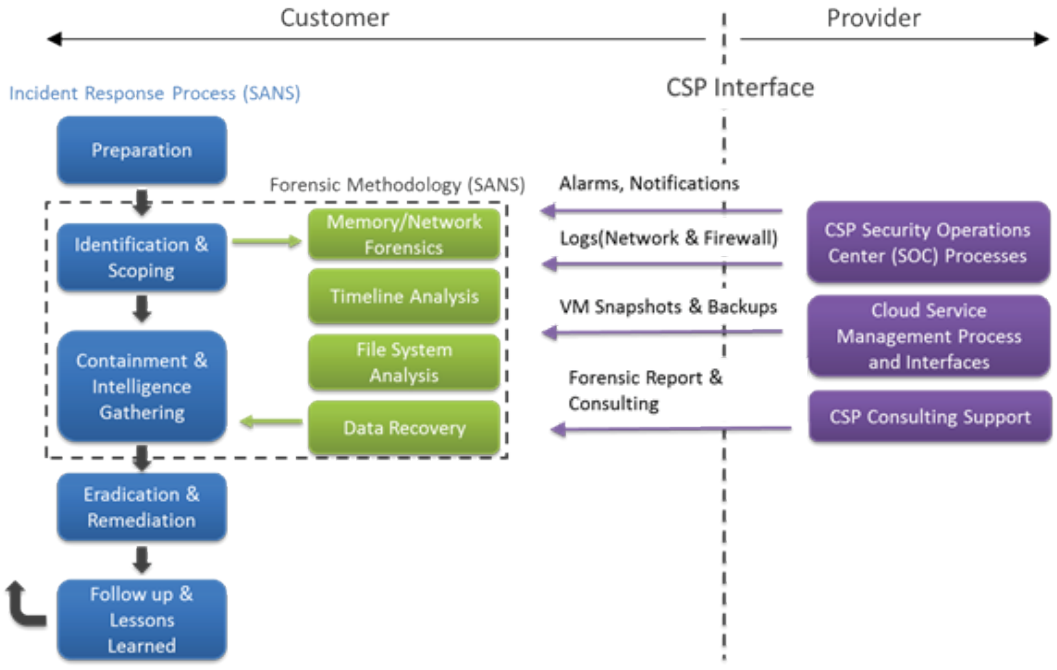

Figure 1: High-Level Cloud Forensic Process

2 "Heroic" does not imply courage but rather the significant efforts of individuals or small, informal groups in carrying out the task at hand.

The left side of the diagram depicts a generic incident response process within an enterprise. The intelligence gathering includes forensic activities like analyzing network captures and timelines of changes to a particular host and its file system. To conduct appropriate forensic activities, it is necessary to trigger certain activities at the CSP side in order to exchange detailed information regarding the incident, as is depicted on the right.

Sometimes the cloud consumer may not be aware that their VM has been compromised until notified by their CSP that the VM is behaving oddly, or perhaps is even being used to attack other hosts[3]. Sometimes the CSP's SIEM (Security Information and Event Management) will automatically trigger the Incident Response (IR) process. In situations like these, the consumer's IR team might determine that it requires access to evidence in the form of, for example, image files or log files that are only available at the CSP's infrastructure. Well-defined and repeatable processes must be put in place at both the consumer and the CSP side to allow this to happen. Being now a mixed party activity, those repeatable processes must still protect the integrity of the evidence and preserve the chain-of-custody in this more complex environment.

To accomplish the objectives of this level, it is important to pre-identify elements that are consistently required and the steps by which knowledge of them should be preserved.

Some of the important elements should include but not be limited to:

- Description of the steps conducted during the forensic investigation
- Description of how the steps were conducted (for instance, tools the investigator used, and how they were used)
- Description of the information that was captured (for instance, network traffic)
- Description of the interactions with the CSP. This would include, for instance, how image files and logs were requested; how they were provided; what credentials were used to access them; etc.

A report should then be written that integrates all of the above information, and the report placed in a secure forensic repository. Access to the repository should be tightly controlled.

In cases potentially involving litigation, separate chain of custody procedures and documentation might be necessary. To avoid the possibility of "contaminating" evidence, legal advice should be sought before the first incident.

[3] The CSP might for instance observe DNS requests from the consumer's virtual machine (VM), asking for name or address resolution of known bot-net controllers, etc.

Level 3: Defined – What is our process for doing this?

At this level, a digital forensic process can be said to exist. One of the differentiating factors between this and preceding levels is that it is more proactive and less reactive.

Ideally this level is accomplished based on a widely accepted standards such as ISO 27037, 27041 and 27042. When confronted with the need to conduct an investigation, the consumer and the CSP must have mutually acceptable documentation and processes already in place.

The need for mutual understanding and cooperation between consumer and CSP is critical, as each will own certain components and capabilities required by the investigation. For example, the consumer will have detailed knowledge of its data, and the CSP will have supplementary data such as access logs, records of virtual machine usage and resource consumption, etc.[4] Only by cooperating and combining their knowledge can a comprehensive and successful investigation be accomplished.

It is therefore necessary for a formal agreement to exist between the parties. It should include clear language regarding responsibilities, processes and procedures, data capture, access controls and data preservation. This agreement commonly takes the form of documented service level objectives in an overall contractual Service Level Agreement (SLA) between the parties. It is important that both parties be able to demonstrate to each other that they are operating at the correct level of maturity. It can be a good idea to perform coordinated tests from time to time.

To accomplish the objectives of this level, it is important to pre-identify elements that are consistently required, and the steps by which knowledge of them should be preserved.

Some of the important elements should include but not be limited to:

- Comprehensive description of the forensic process
- Standard forms, templates, and tools
- If required, any technical infrastructure to support the IR processes (e.g., dedicated workstations, a secure channel for exchanging files, secure disk storage, and so forth)
- People pre-trained on all aspects of the process
- Enumeration of people to engage, and how to engage them
- Means of verbal communication (e.g., conference lines)
- Pre-exchanged keys for encrypted email
- Well-defined and pre-approved technical roles. It should be known in advance who the investigators are, who the operators are, who should support whom and how, who has which privileges who is authorized to access which information, and so on
- Well-defined business and legal roles. It should be known in advance when legal counsel should be engaged, when senior management should be briefed, and so on

[4] For more details see section 2.1 of Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing, available at https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf

It may also be wise to pre-consult with legal counsel on various matters, including when and how to observe evidentiary chain of custody practices, how practices might be affected by cross-national boundaries, and so on.

Level 4: Managed – What resources did this require?

At this level, resourcing goals are established and tracked. Planning and measuring is key to success. One important goal is to apply quality control measures to forensic processes, and to manage variation within acceptable limits.

The consumer and the CSP will need to develop their own processes and goals, and they will likely maintain them separately. However, a consumer could still define goals that includes a combined end-to-end forensic process and then either choose CSP independent key performance indicators (KPI's) or include KPIs only the CSP has control over, in order to measure the CSP's performance. The measurements can then be used to discuss improvements.

Setting Goals

It is important for the cloud consumer and the CSP to work together to define compatible "quality goals" that can be measured using tool-based statistical analysis. Metrics should be documented in the SLA. it makes sense for the consumer and the CSP to spell theirs out separately, and to agree on where they are independent, and where they overlap.

Example Goal:

- Time to acquisition: 30G/h disk-to-disk
- Time for key-word search/hash analysis = f(data volume)
- Time for Timeline Analysis = f_1(size, complexity =f_2[Incident type])
- How many people/man-hours for various forensic tasks
- Time to report
- Time to identify infection path for infected system
- Time for the intrusion path discovery of an unknown hacked system
- What was requested vs. what was received
- % failed hash verification of acquired images
- % properly initiated IR
- etc.

Where "time to" is the metric, it will depend on several variables. How large is the image file? How complex is the processing and analysis of the image data? Is a single system affected or a distributed cloud application? Is data encrypted? How long does it take to

receive the escrow keys to decrypt a volume? Does the encryption need to be broken?[5] It is important to account for the fact that KPIs might need to account for scale in various scenarios. For example, it might be feasible to analyze twenty VM images in parallel, but not one hundred.

The below diagram outlines the process of setting goals and tracking KPIs:

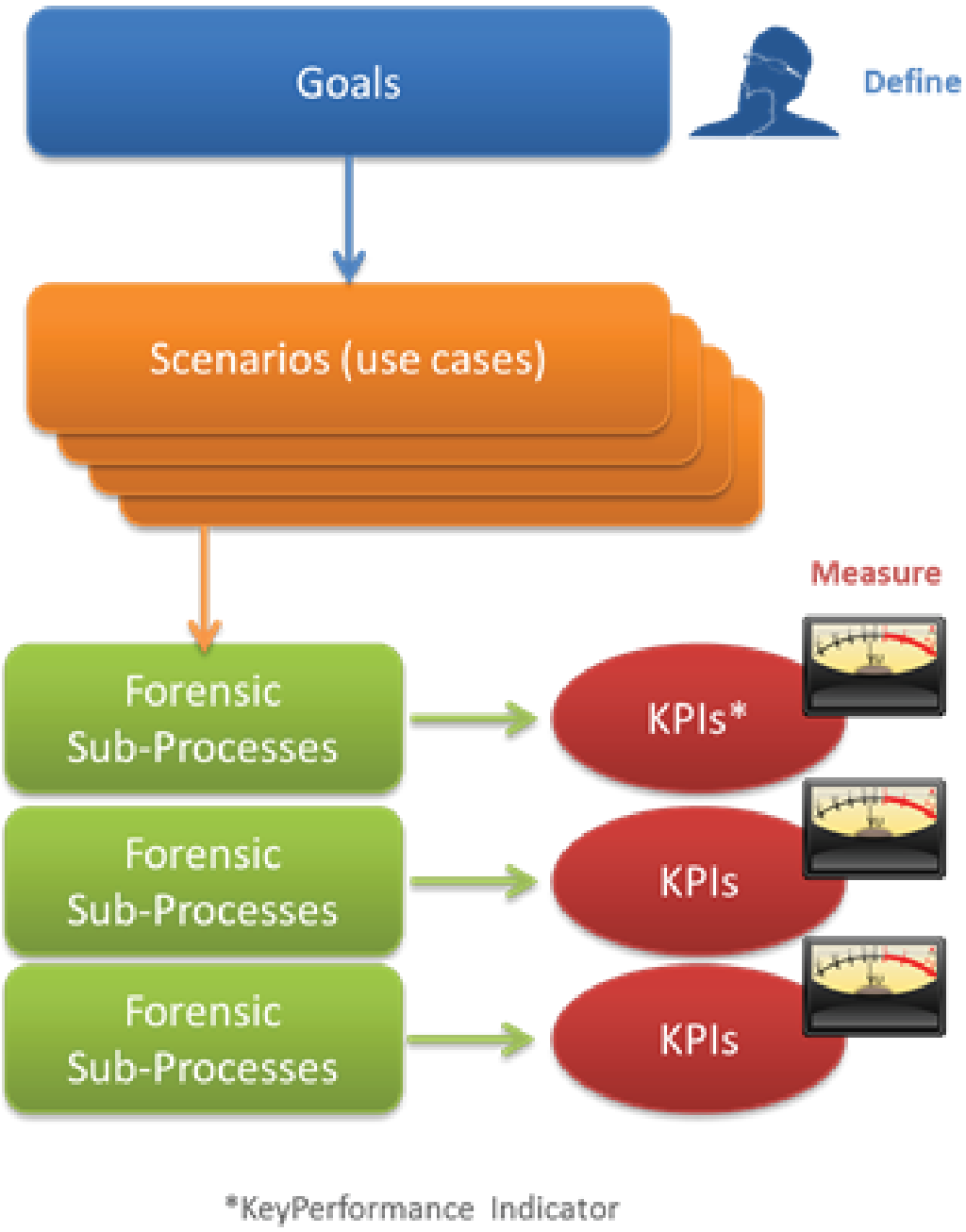

Figure 2: Development of key quality indicators

[5] "Break" refers generally to techniques such as a brute-force attack on the cryptographic implementation, recovery of a stored key phrase, dictionary attack on the key phrase, etc

Start by defining high-level goals that will drive "standard scenarios" to be divided into specific forensic tasks or sub-processes. For example, some scenarios might be:

Scenario	KPI	Acceptable Variation
Incident on a single, mid-size[6] VM in the Cloud	• Time to locate VM + files • Time to acquire all VM files • % of successfully verified image hashes	10 – 30 min 1h – 3h 90% - 100%
Incident regarding a Cloud portal application	• Time to receive incident report • Incident report completeness • Time to receive application logs (e.g., access logs)	4h – 8h 80% - 100% 1h – 2h
Incident involving a mobile device	• Time to locate an online device • Time to wipe sensitive data • Time to analyze a suspicious application	1h – 2h 2h – 3h 2h – 5h

Table 2: Forensic Sub-Process Scenarios

The final step is tracking achievements and variances of KPIs. This requires the continual collection and processing of quantitative (i.e., statistical) data.

Level 5: Optimizing – How can we do this better?

At this level an organization focuses on continual performance improvement. Solid measurement and tracking will identify the opportunities for improvement that will yield the greatest return on investment (ROI). It will also help the consumer derive SLA parameters appropriate for their business.

Tracking Goals and Adapting

One challenge at this level is the continuous capturing and monitoring of KPIs, while at the same time applying changes to optimize the processes. In doing so it is important to identify and define key individual sub-processes that will adapt to step changes.

[6] Future work needs to be done to define what exactly "mid-size" means in each scenario.

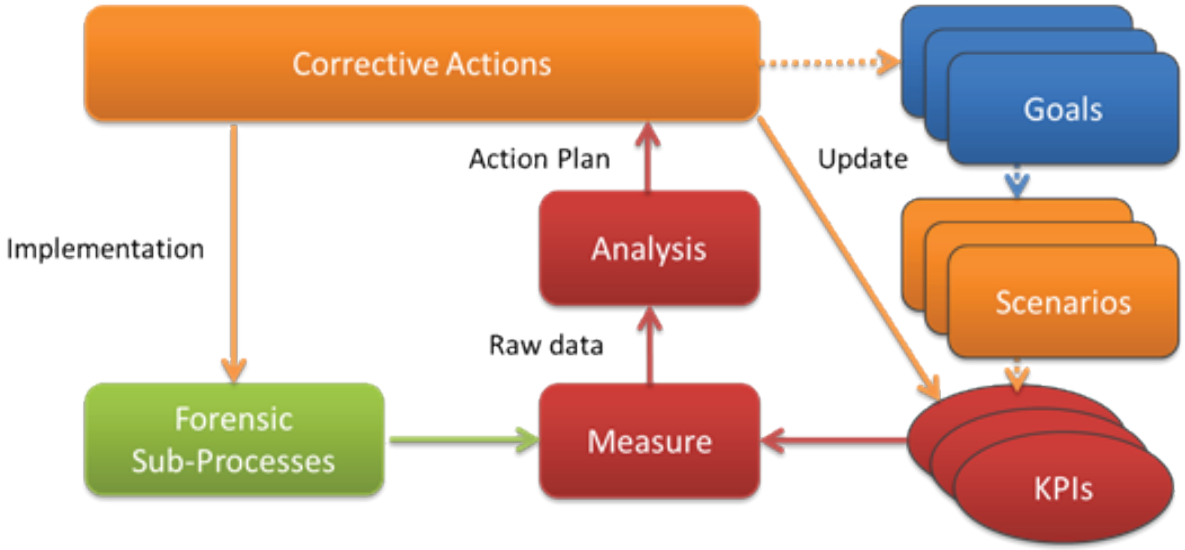

Figure 3: The adaptive process

Each sub-process should be measured according to its own KPIs, and the quantitative data analyzed to determine whether further optimization is required. In some cases this might even lead to revisiting the target values of the KPIs. In any case, action plans should be created, actions items assigned and progress tracked.

Adaptive actions might address:

- Processes and procedures
- Standards
- Management (plan, schedule, team lead, resources, etc.)
- Requirement definition
- Documentation
- Quality goals
- Design
- Engineering
- Code
- Interfaces
- Testing (plans, procedures, etc.)
- Technologies
- Training

Conclusion

The most capable enterprise cannot avoid data breaches entirely. As such, there is a rising need for enterprises to adopt mature forensic security processes. This need will rise at least at the speed at which adversaries improve their attack strategies and techniques.

This situation is even more complex in the world of cloud computing. Only with close cooperation between the cloud consumer (who has given up some control) and the CSP (who has inherited it) can adequate, timely and accurate forensic analysis occur. As such it behooves consumers to be fully prepared for the occasions in which forensic analysis is necessary. It is, in all likelihood, a question of "when" not "if."

Smaller enterprises might not have the resources or skills to drive the cloud forensic process themselves. Even some large organizations might not have the resources required to conduct their own forensic investigations within the cloud. Some CSPs offer forensic support and services, and some consumers account for that in their CSP selection criteria.

The purpose of this document has been to provide general guidance by which both cloud consumers and CSPs can plan for and assess their cloud forensics CMM. Five maturity levels were given, with an attempt to map classic digital forensics to the cloud environment. It has attempted to answer questions like: How do the maturity levels differ from each other? What are the key objectives for each? What is the specific impact on forensic process in the cloud? At the end of the day however, it is up to each individual enterprise to decide upon the guidance and practices that they deem most appropriate for their business.

Future work in this area will provide a greater level of detail that will aid implementation.