# Compliance monitoring of AWS accounts.

As an AWS account owner, you will be aware of certain requirements for AWS accounts, such as tagging and the use of approved AMIs etc.

You should also be aware that there is a published Bayer (ex-Monsanto) standard that applies to all AWS accounts and that all AWS account owners are expected to comply with it. This is

*Cloud (IaaS and PaaS) Security Standard Infrastructure as a Service (IaaS) and Platform as a Service (PaaS)*

which was last revised in April 2019, by the then ISO group (now Cybersecurity Risk Management). You can find this standard here:

<http://portals.monsanto.com/enterprise/informationsecurity/SiteCollectionDocuments/Standards/Cloud%20IaaS%20and%20PaaS%20Security%20Standard%20v2.1.pdf>

## Monitoring and Compliance.

Monitoring of compliance with this standard (and its predecessors) has been going on since at least 2017, particularly by the Compliance group, and by the CSR project, concentrating on the higher risk areas, and certain functions that were relatively easy to check, such as the tagging. These checks were a subset of those set out in the IaaS/PaaS standard. A dashboard of compliance with this subset of the standard is published and is made available to IT leadership, currently on an informational basis.

It should be noted however that Compliance with all parts of the standard is expected, and in addition to the requirements of initial the setup of the AWS assets, there are ongoing requirements such as Change Management, Access Reviews, Patching etc. It is the account owner’s responsibility to ensure compliance with the standard.

If you are not familiar with the requirements of this standard, please read through it.

Over the last 6 months, using various tools, particularly Dome 9 and Cloud Health, the compliance levels have been fed back to a Pilot group of 3 account owners. At the same time the monitoring has been developed and a larger set of checks, based on recommended AWS best practices, has been developed as a rule set in Dome 9 and these results are have also been presented to the Pilot Group of AWS account owners as well as IT management.

## Expansion of the Pilot Project.

The Pilot project is being expanded to full monitoring of AWS assets with the results being fed to all AWS account owners. This is being rolled out in three phases, with those accounts where certain assets have been identified as potentially regulated (i.e. GxP or SOX-relevant) in Phase 1.

Phase 2 will include Prod and Non-Prod accounts and Phase 3 will include all others, including temporary, test and other lower risk accounts.

You are receiving this communication as you are documented as an AWS account owner, and you will shortly start to receive the current version of the AWS dashboard on a weekly basis. This is to inform you of the compliance levels of AWS assets in your own area.

The information is of a general nature giving an aggregated % compliance level of all relevant assets in the account based mainly on Dome9. To see exactly which assets are non-compliant will require the use either of Dome9 itself or other tools. As there are tens of thousands of AWS assets in the more than 100 AWS accounts, a simple dashboard does not allow for the pinpointing of individual non-compliances.

## The Dashboard

The Published dashboard is a simple excel spreadsheet that records the % compliance levels of each account. The number of tests of four rules sets appear on separate sheets and there is overall summary page which divides the Accounts into

* ISO a single account
* Regulated accounts – two accounts where most of the GxP and SOX relevant functions were originally presumed to reside. As this appears to be no longer valid this division will likely be removed soon
* All other accounts.

The Rulesets are:

* Compliance main bundle – the original set of Dome 9 rules reflecting the highest priority requirements from the IaaS/PaaS standard
* Compliance tagging bundle – a check for the presence of the 6 mandatory tags and a check on the content of some tags.
* CIS subset. Based on the CIS 1.1.0 standard, as small set of highest priority requirements.

Recently a fourth ruleset has been added.

* Combined compliance bundle. A large set of 240+ rules based on
  + All of the rulesets above
  + ISO27001
  + CIS 1.1.0 standards
  + Other rulesets in use at Bayer Germany, currently
  + AWS Good Practices as defined by Dome 9.
* This is likely to be the most used ruleset going forward. A historic record of compliance levels is maintained.

In addition, the dashboard includes information on AWS accounts providing logs to the central logging system. This information is not available via Dome 9 and is derived using a Splunk report.

The four rules are visible to all users of Dome9. Please refer to Dome 9 for details of each of the tests.

## What to do with the information on the dashboard.

As noted above, compliance with the IaaS/PaaS standard is expected. The compliance information is currently being rolled out to AWS account owners on an information basis.

The most pertinent information will be that of the combined compliance ruleset, which will be monitored in the longer term with historical data being maintained. This can be used as the starting point for checking and maintaining compliance levels, but to identify individual non-complying assets, more precise tools such as Dome9 itself will need to be used.

## Dome9

Most AWS account owners will have access to Dome9. If you do not, please let the compliance department know and we will ask for you to be added.

The rule sets in Dome9 have good explanations of individual rules, and the dashboards all ow drilling down to the individual asset levels, so you will be able to see what has triggered any non-compliance alerts.