# Secure in the cloud (5 February 2025)

## Introduction

This document is a product of the Cloud Security by Default Stakeholders Group, to support Cloud Service Providers (CSPs) in implementing default secure baselines in their customer environments, as outlined in the Manifesto "Actioning Baseline Cloud Security by Default".[1] The Stakeholders Group includes representatives from industry, public service and sectoral associations, covering a broad range of sectors and levels of maturity. Commercial and cost aspects are kept outside the scope.

## Scope and goal

The work of the Stakeholders Group focuses on identifying, validating and documenting secure baselines (configurations, controls, policies) implementable by default in customer-managed cloud tools and environments (SAAS, PAAS, IAAS). It draws from industry best practices to maintain an appropriate level of security and resilience for the vast majority of organizations, balancing security and practicality.

Numerous commercial, governmental, and community initiatives provide guidance and best practices to secure cloud workloads. The Stakeholders Group has drawn from:

- CIS Benchmarks[2]
- CIS Critical Security Controls[3]
- CSA's Cloud Control Matrix[4]
- FS-ISACs Principles for Financial Institutions' Security and Resilience in Cloud Service Environments[5]
- CRI Profile[6]
- NCSC-NL's Cloud Security Control Framework (SCF)
- CISA BOD 25-01[7]

## Working assumptions and process

The Stakeholders Group has used the experience of their members to weigh and select principles/outcomes, configuration parameters, controls and policies which should be implemented by default. The proposed baselines are a combination of:

- Intended outcomes (principles) which describe at a high level of abstraction the objectives. These intended outcomes are broadly applicable across CSPs.
- Detailed technical recommendations, which are specific for a CSP/product. The technical recommendations are grouped within an intended outcome. The group used the CIS benchmarks as a starting point.

---

[1] https://www.freddydezeure.eu/48-manifesto-actioning-baseline-cloud-security-by-default
[2] https://www.cisecurity.org/cis-benchmarks
[3] https://www.cisecurity.org/controls/cis-controls-list
[4] https://cloudsecurityalliance.org/research/cloud-controls-matrix
[5] https://www.fsisac.com/hubfs/Knowledge/Cloud/PrinciplesForFinancialInstitutionsSecurityAndResilienceInCloudServiceEnvironments.pdf?hsLang=en
[6] https://cyberriskinstitute.org/the-profile/
[7] https://www.cisa.gov/resources-tools/services/bod-25-01-implementing-secure-practices-cloud-services-required-configurations

Technical recommendations are rated using a scoring system with four categories:

| | |
|---|---|
| 1 | Default is fine, deviations from default to be flagged to avoid drift |
| 2 | Default is fine, high priority deviation flagging or time-limited exceptions |
| 3 | Default to be changed, deviations from default to be flagged to avoid drift |
| 4 | Default to be changed, with high priority deviation flagging or time-limited exceptions |

The baseline selection of technical recommendations resulted from an assessment by the group of their added value for the target population in implementing specific options by default rather than by choice. Priority was given to recommendations with the highest impact, considering potential implementation difficulties and friction.

In doing so, the group has made some choices which move the needle to security rather than convenience. The underlying argumentation for this is that the current threat landscape requires our infrastructure to become more resilient and determined choices need to be made in the interest of collective well-being. Security by default should therefore also be seen in the context of policy and regulatory cyber resilience initiatives.

Working from the selected technical recommendations up to the intended outcomes it became clear that not all intended outcomes had corresponding technical recommendations. For certain intended outcomes (asset management, backups…) no CIS benchmark component was available. Additional outcomes were identified to create a comprehensive set.

Gaps were identified, both on the level of the technical recommendations as on the level of the intended outcomes. Several iterations from principles (outcome) to implementation (technical recommendation) and back resulted in the current proposal.

The proposed set of outcomes was compared with existing control frameworks as listed earlier in this paper. This led to additional outcomes and technical recommendations.

**Green field / brown field – avoiding drift**

Implementation of secure baselines at initial launch (green field) risks drifting to a less secure status over time. Exceptions may be made without resetting to the secure status, errors or misconfigurations may occur over time and escape attention.

It is therefore recommended to accompany the implementation of secure baselines with a mechanism to avoid drift or allow for exceptions within a time window. This could be done using policies or a cloud security posture management system.

These drift avoidance solutions could also help to implement default secure baselines in existing infrastructures (brown field). The default secure baseline could serve as a yardstick to adapt controls over time to a more secure intended outcome.

**Avoiding vendor lock in**

The draft secure baselines contain product-specific technical recommendations. This does not mean that the choice of a specific product (SSO, EDR…) would be mandatory

for a secure default baseline. Instead, these product-specific technical recommendations would be triggered by the choice of a specific product.

**Logging and monitoring security alerts**

The Stakeholders Group did not come up with specific recommendations regarding log collection to be included in the default secure baselines. There is a planned CIS track on prioritizing log collection which could serve as an input at a later stage.

To foster consumption and facilitate response, it would be useful, though, that the CSPs offer a simple single pane interface to the alerts produced by different products from the CSP the customer has subscribed to. Most small and medium sized enterprises would not have the means to operate a SIEM. They would need to respond to critical alerts coming from different sources (baseline drift, CSP security alerts, malware detection, risky logins, changes in privileged account etc.).

**Adapting the baselines over time**

The threat landscape is evolving over time, and the secure baselines might become less secure due to new techniques/tactics deployed by adversaries. Also, the infrastructure and products offered to customers also evolve.

It is therefore crucial to keep the default secure baselines up to date. This will require ongoing effort by the community and the CSPs.