AirCyber
General Means of Compliance

This document list the means deployed by BoostAeroSpace to evaluate a company to AirCyber Maturity Levels using the AirCyber questionnaire and give the associate AirCyber Bronze, Silver or Gold level.

It details the different activities performed by BoostAeroSpace and its network of CyberSecurity experts called "Maturity Assessors" in order to allow any company to perform this activity with results trusted by the Shareholders of BoostAeroSpace.

It is important to keep in mind that BoostAeroSpace is performing AirCyber Maturity Analysis as part of the global AirCyber service of security governance deployed to both companies having to be evaluated to reach the AirCyber maturity levels as well as companies asking their suppliers to reach AirCyber maturity levels.

This 2 sides activities of "buy side" and "sell side" companies makes the success of the AirCyber framework, "buy side" companies using AirCyber to help their suppliers to reach AirCyber maturity levels and "sell side" companies demonstrating their maturity level through BoostAeroSpace AirCyber services.

More details about the BoostAeroSpace AirCyber service itself is available publicly on the BoostAeroSpace website: https://boostaerospace.com/aircyber as well as in the detailed AirCyber white paper https://boostaerospace.com/aircyber/aircyberwhitepaper.

Means of compliance list, V1.0 01/01/2023

- ***Scope review of supplier activity to fill "Extended" questions:*** *AirCyber propose a set of "Extended" questions, that must be evaluated to be answered, meaning that the company evaluated shall be aware of the Extended questions categories and select carefully those categories before the maturity assessor onsite evaluation. The categories are associated with some AirCyber extended questions (e.g: do not select AirCyber extended questions associated with Software Development if the company is not performing Software development).*
- ***BoostAeroSpace selection and review of Assessors activities and reports (quality assurance):*** *The maturity assessor must be a certified company performing security audit, by a country cybersecurity government department like ANSSI PASSI qualification, or be a company performing CyberSecurity as principal activity with proven experience in CyberSecurity audits (like ISO27001). The maturity assessor's work shall be reviewed regularly at least the first time the maturity assessor performs a maturity assessment to verify the quality of its security report and evaluation of the AirCyber level of the supplier.*
- ***Physical onsite first review:*** *to get a "validated" label, the assessment must be performed inside the physical site of the company information system evaluated, with preparation of the review with the help of the security questionnaire answers and company context.*
- ***Responsibility of the maturity assessor:*** *The maturity assessor is responsible for the Cybersecurity report production as well as the CyberSecurity evaluation of the company information system, to verify if he estimate the need to any proof of maturity associated to every question of the questionnaire, to validate if questions are not applicable to the evaluated company when company informed that it was the case and to evaluate the urgency of the actions plan resulting of the review by giving High, Medium and Low priority to each question.*
- ***1 assessment / qualification for 1 Physical site of assessed company:*** *AirCyber maturity level is associated to 1 company, having designated 1 physical site associated to the maturity of the company. If the company is composed of multiple physical sites having different cybersecurity maturity levels, every site must be associated to an AirCyber evaluation. If the company is composed of multiple sites having the same cybersecurity maturity level, then, the company is authorized to produce a company document certifying in the name of the company that a defined list of sites have the same AirCyber level as the site associated to the company. This document must be provided with the AirCyber maturity information of the company.*
- ***Full report redaction / validation with Action plan tuning by expert (High Medium Low actions) + Levels "Certificate" creation****: the Cybersecurity expert company must produce a full cybersecurity report to the assessed company, listing all the AirCyber questions answered, with a customized summary of the onsite review a detailed action plan with High, Medium and Low priority associated to each action with regards of the context of the assessed company.*
- ***Annual review of level with expert:*** *The update of the action plan by the assessed company shall be reviewed at least one a year between a CyberSecurity expert and the assessed company, with action to review if the company context has evolved (eg: merge, new IT infrastructure) and with a review of the actions that are still not addressed to reach AirCyber levels.*
- ***Onsite reassessment every 3 Years if Annual review is not performed:*** *if the assessed company is not reviewing every year its action plan progress with a security expert and communicate this to its customer, the customer shall consider that the AirCyber level is valid only for 3 years, and that it shall be associated with a new maturity assessment to be validated after 3 years.*
- ***Tailoring of results to validate the "level" (90%), communication on results:*** *The AirCyber maturity level shall be communicated by the evaluated company by showing it is reaching of 90% of the level's questions to "Yes", with the exact percentage of maturity for Bronze, Silver and Gold. Site name, maturity assessor company name, the assessed company shall also communicate the date of the review.*

Limitations: *The mission of BoostAeroSpace is to ensure that this list of means of compliance is well enforced in the AirCyber Service, with the deployment of maturity assessment platform and process to allow both assessed companies ("sell side") and customers of those companies ("buy side") to spend the less efforts in the associated activities, in a secured collaborative and trusted environment to allow secure collaboration between the 2 entities. The Maturity assessment's activity described in this list of means of compliance is also mostly performed with the help of online automated tools to allow the buy side and sell side company to only support the cost of the intellectual work performed by each party. The time taken by a maturity assessor inside the AirCyber framework and tool is 2 days maximum to perform the onsite review and the maturity assessment report customization and validation, but shall not be taken as mean of compliance as only possible thanks to the usage of the AirCyber maturity platform, and assessment management activities that are part of AirCyber service.*