

Agence nationale de la sécurité
des systèmes d'information

Paris, le 25 SEP. 2023
N° 1690 /ANSSI/SDE

NOTE

**relative à l'évaluation des
Prestataires d'accompagnement et de conseil en sécurité des systèmes
d'information (PACS)
qualifiés Prestataires d'audit de la sécurité des systèmes d'information (PASSI)**

I. Objet

Le présent document est à destination des centres d'évaluation de la conformité des PACS, et des PASSI qualifiés qui souhaitent obtenir une qualification PACS initiale

Il prescrit aux centres d'évaluation de la conformité des PACS les règles à suivre lorsqu'un PASSI qualifié souhaite obtenir sa qualification PACS initiale.

II. Modalités

a) Sécurité du système d'information

Si le prestataire déclare auprès du centre d'évaluation que le système d'information mis en œuvre dans le cadre des missions PACS est identique à celui mis en œuvre dans le cadre de ses missions PASSI, alors il n'est pas demandé au centre d'évaluation de vérifier que le prestataire est conforme aux exigences du chapitre « Protection de l'information » du référentiel PACS, le respect de ces exigences étant attesté par la qualification PASSI.

Le rapport d'évaluation de la conformité du prestataire aux exigences du référentiel PACS élaboré par le centre d'évaluation devra mentionner explicitement si le système d'information mis en œuvre par le prestataire dans le cadre de ses missions PACS est identique à celui mis en œuvre dans le cadre de ses missions PASSI.

b) Evaluation combinée

Le prestataire peut, s'il le souhaite, combiner à terme les évaluations de la conformité PASSI et PACS. La combinaison des évaluations PASSI et PACS offre plusieurs avantages au prestataire : elle facilite la gestion des qualifications PASSI et PACS et permet de réduire les coûts de mise en conformité et d'évaluation de la conformité aux exigences des référentiels PASSI et PACS.

Le prestataire qui souhaite combiner à terme les évaluations de la conformité PASSI et PACS doit le préciser dans sa demande de qualification PACS. L'ANSSI proposera alors au prestataire, en cas d'octroi de qualification PACS, les mesures permettant de synchroniser les qualifications PASSI et PACS, et ainsi de mener à terme des évaluations de conformité PASSI et PACS combinées. Parmi ces mesures, sans que cela ne constitue une liste exhaustive, l'ANSSI peut : réduire une durée de qualification, prolonger une qualification, modifier la date d'une évaluation de surveillance ou annuler une évaluation de surveillance.

c) Examens écrits et oraux

Les évaluations de la conformité aux référentiels PASSI et PACS mettent en œuvre des évaluations individuelles de certains personnels du prestataire à l'aide d'examens écrits et oraux.

Aucun résultat d'examens, écrits ou oraux, menés dans le cadre de l'évaluation PACS ne peut être utilisé dans le cadre de l'évaluation PASSI, et inversement.

Vincent STRUBEL
Directeur général de l'Agence nationale
de la sécurité des systèmes d'information