



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SA-17(05)

Conception simple

Juill. 2026



Acquisition sécurisée des systèmes/services

System and Services

SA-17(05) – Conception simple (PbMM)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de :

- a. concevoir et structurer le matériel, les logiciels et les micrologiciels servant à la sécurité de façon à créer un mécanisme de protection complet, de conception simple et doté d'une sémantique précisément définie
- b. structurer en interne le matériel, les logiciels et les micrologiciels servant à la sécurité, en portant une attention particulière au mécanisme en question

Responsable : Aucun

Discussion :

Le principe de complexité réduite repose sur le fait que la conception du système est aussi simple et petite que possible (voir le contrôle SA-08(07)). Une conception petite et simple est plus facile à comprendre et à analyser, en plus d'être moins vulnérable aux erreurs (voir les contrôles AC-25 et SA-08(13)). Le principe de complexité réduite s'applique à tous les aspects d'un système, mais il est particulièrement important pour la sécurité en raison des diverses analyses réalisées pour obtenir des preuves de la propriété de sécurité émergente du système. Pour assurer la réussite de telles analyses, il est essentiel de faire appel à une conception simple et de petite taille. L'application du principe de complexité réduite aide les développeuses et développeurs de système à comprendre l'exactitude et l'exhaustivité des fonctions de sécurité du système et à faciliter la détermination des vulnérabilités potentielles. La conséquence de la complexité réduite veut que la simplicité du système soit directement liée au nombre de vulnérabilités qu'il contiendra

a. En d'autres mots, les systèmes plus simples contiennent moins de vulnérabilités. Deux avantages importants de la complexité réduite font en sorte qu'il soit plus facile de comprendre si la stratégie de sécurité a bien été intégrée dans la conception du système et qu'il y ait moins de vulnérabilités susceptibles d'être introduites lors du processus de développement technique. Ce principe permet également de rendre des conclusions par rapport à l'exactitude, à l'exhaustivité et à l'existence des vulnérabilités avec un degré élevé d'assurance comparativement aux conclusions formulées dans des situations où la conception du système est fondamentalement plus complexe.