

**CONCOURS INTERNE
POUR L'ACCÈS AU GRADE D'INSPECTEUR DES FINANCES PUBLIQUES
AFFECTÉ AU TRAITEMENT DE L'INFORMATION EN QUALITÉ D'ANALYSTE**

ANNÉE 2023

ÉPREUVE ÉCRITE D'ADMISSIBILITÉ N° 3

Durée : 1 heure 30 – Coefficient : 1

Version anglaise à partir d'un texte issu d'une revue ou d'une documentation informatique

Seuls sont pris en compte les points obtenus au-dessus de 10.

Recommandations importantes

Le candidat trouvera au verso la manière de servir la copie dédiée.

Sous peine d'annulation, en dehors du volet rabattable d'en-tête, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tels que nom, prénom, signature, paraphe, localisation, initiale, numéro ou toute autre indication, même fictive, étrangère au traitement du sujet.

Sur les copies, les candidats devront écrire et souligner si nécessaire au stylo bille, plume ou feutre de couleur noire ou bleue uniquement. De même, l'utilisation de crayon surligneur est interdite.

Il devra obligatoirement se conformer aux directives données.

Le candidat complétera l'intérieur du volet rabattable des informations demandées et se conformera aux instructions données

Nom de naissance

Prénom usuel

Jour, mois et année

Signature obligatoire

Numéro de candidature

À compléter par le candidat

Ne rabattre le cache qu'en présence d'un membre de la commission de surveillance

Concours externe - interne - professionnel - ou examen professionnel ⁽¹⁾

⁽¹⁾ Rayer les mentions inutiles

INTERNE

Pour l'emploi de : **Inspecteur des Finances Publiques affecté au traitement de l'information en qualité d'analyste**

Épreuve n° : **3**

Matière : **051 – Version anglaise**

Date : **2 9 1 1 2 0 2 2**

Nombre d'intercalaires supplémentaires :

Préciser éventuellement le nombre d'intercalaires supplémentaires

RÉSERVÉ À L'ADMINISTRATION

À L'ATTENTION DU CORRECTEUR

Pour remplir ce document :
un stylo ou une pointe feutre
couleur **NOIRE** ou **BLEUE**.



Pour porter votre note, cochez les gélules correspondantes.

Reportez la note dans les zones **NOTE / 20** et dans le cadre **A**

En cas d'erreur de codification dans le report des notes cochez la case **erreur** et reportez la note dans le cadre **B**.

À L'ATTENTION DU CANDIDAT

En dehors de la zone d'identification rabattable, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tel que nom, prénom, signature, paraphe, localisation, initiale, numéro, ou toute autre indication même fictive étrangère au traitement du sujet.

Il est demandé aux candidats d'écrire et de souligner si nécessaire au stylo bille, plume ou feutre, de couleur noire ou bleue uniquement. Une autre couleur pourrait être considérée comme un signe distinctif par le jury, auquel cas la note de zéro serait attribuée. De même, l'utilisation de crayon surligneur est interdite.

Les étiquettes d'identification codes à barres, destinées à permettre à l'administration d'identifier votre copie, ne doivent être détachées et collées dans les deux cadres prévus à cet effet qu'en présence d'un membre de la commission de surveillance.

Suivre les instructions données pour les étiquettes d'identification

Cadre A réservé à la notation				Cadre B réservé à la notation rectificative			
20	19	18		20	19	18	
17	16	15		17	16	15	
14	13	12		14	13	12	
11	10	09		11	10	09	
08	07	06		08	07	06	
05	04	03		05	04	03	
02	01	00		02	01	00	
Décimales				Décimales			
,00	,25	,50	,75	,00	,25	,50	,75
							Erreur

NOTE / 20
| | | |

NOTE / 20
| | | |

EN AUCUN CAS, LE CANDIDAT NE FERMERA LE VOLET RABATTABLE AVANT D'Y AVOIR ÉTÉ AUTORISÉ PAR LA COMMISSION DE SURVEILLANCE

VERSION ANGLAISE À PARTIR D'UN TEXTE ISSU D'UNE REVUE OU D'UNE DOCUMENTATION INFORMATIQUE

Code matière : 051

Les candidates et les candidats peuvent avoir à leur disposition sur la table de concours le matériel d'écriture, une règle, un correcteur, des surligneurs.

In a remote-work world, a zero-trust revolution is necessary

[...]

Last summer, law enforcement officials contacted both Apple and Meta, demanding customer data in "emergency data requests." The companies complied. Unfortunately, the "officials" turned out to be hackers affiliated with a cyber-gang called "Recursion Team."

Roughly three years ago, the CEO of a UK-based energy company got a call from the CEO of the company's German parent company instructing him to wire a quarter of a million dollars to a Hungarian "supplier." He complied. Sadly, the German "CEO" was in fact a cybercriminal using deepfake audio technology to spoof the other man's voice.

One set of criminals was able to steal data, the other, money. And the reason was trust. The victims' source of information about who they were talking to was the callers themselves.

What is zero trust, exactly?

Zero trust is a security framework that doesn't rely on perimeter security. Perimeter security is the old and ubiquitous model that assumes everyone and everything inside the company building and firewall is trustworthy. Security is achieved by keeping people outside the perimeter from getting in.

A UK doctoral student at the University of Stirling named Stephen Paul Marsh coined the phrase "zero trust" in 1994. (Also called "de-perimeterization," the concept was thoroughly fleshed out in guidelines like Forrester eXtended, Gartner's CARTA and NIST 800-207).

Perimeter security is obsolete for a number of reasons, but mainly because of the prevalence of remote work. Other reasons include: mobile computing, cloud computing and the increasing sophistication of cyberattacks, generally. And, of course, threats can come from the inside, too.

In other words, there is no network edge anymore — not really — and even to the extent that perimeters exist, they can be breached. Once hackers get inside the perimeter, they can move around with relative ease.

Zero trust aims to fix all that by requiring each user, device, and application to individually pass an authentication or authorization test each time they access any component of the network or any company resources.

Technologies are involved in zero trust. But zero trust itself is not a technology. It's a framework and, to a certain extent, a mindset. We tend to think of it as a mindset for network architects and security specialists. That's a mistake; it needs to be the mindset of all employees.

[...]

Computerworld, April 22, 2022