DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

CONCOURS INTERNE POUR L'ACCÈS AU GRADE D'INSPECTEUR DES FINANCES PUBLIQUES AFFECTÉ AU TRAITEMENT DE L'INFORMATION EN QUALITÉ D'ANALYSTE ET/OU DE PROGRAMMEUR DE SYSTÈME D'EXPLOITATION

ANNÉE 2020

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, 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. L'utilisation du crayon surligneur est interdite.

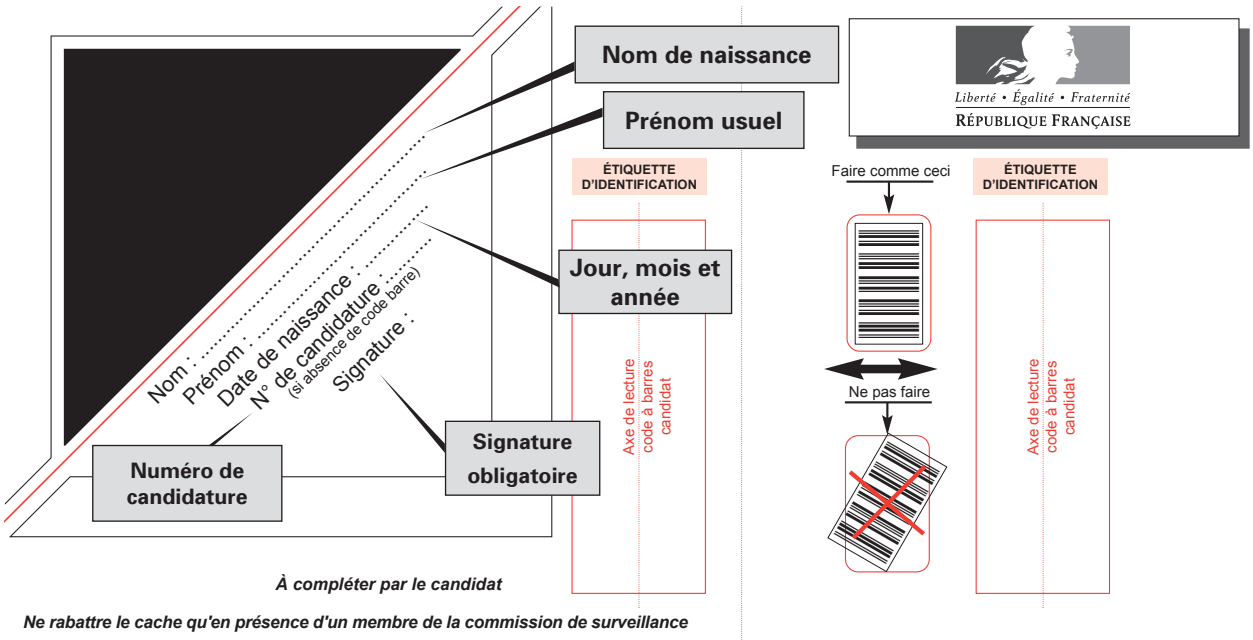
Il devra obligatoirement se conformer aux directives données.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ACTION ET DES COMPTES PUBLICS

Tournez la page S.V.P.

Le candidat devra compléter l'intérieur du volet rabattable des informations demandées et se conformer aux instructions données



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 et/ou de programmeur de système d'exploitation~~

Épreuve n° : 3

Matière : Version anglaise

Date : 13 11 2019

Nombre d'intercalaires supplémentaires :

Préciser éventuellement le nombre d'intercalaires supplémentaires

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

NOTE / 20 ,

RÉSERVÉ À L'ADMINISTRATION

À L'ATTENTION DU CORRECTEUR

Pour remplir ce document :

Utilisez un stylo ou une pointe feutre de couleur NOIRE ou BLEUE.

EXEMPLE DE MARQUAGE : Faire comme ceci — Ne pas faire

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**.

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

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

NOTE / 20 ,

N°140 - IMPRIMERIE NATIONALE 2014 01 51061 PO - Juin 2014 - 145 112

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

DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

SUJET

Code matière : 051

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

Aucun matériel ni documentation spécifiques.

How businesses plan to protect themselves against cyberattacks

Many organizations will spend more to shore up their defenses against cyberattacks this year, says business insurance provider Hiscox.

Cyberattacks continue to rise in both frequency and cost, and businesses are boosting their security budgets to better defend themselves. But more may be required, according to a Tuesday report from Hiscox.

For its annual The Hiscox Cyber Readiness Report 2019, Hiscox surveyed almost 5,400 business professionals across the US, UK, Germany, Belgium, France, Spain, and the Netherlands, all of whom are responsible for their organization's cybersecurity.

A full 61% of the respondents said their business was hit by a cyberattack over the past 12 months, compared with 45% over the year before. Specifically, 24% of the respondents reported a virus or worm, and 17% said they were hit by a ransomware attack. The number of respondents who reported a distributed denial-of-service (DDoS) attack rose to 15% from 10% the prior period.

Among the 3,300 firms hit by attacks, around 2,250 of them calculated the cost to their business. Among those, the median cost for losses as a result of these attacks was $360,000, up from $229,000 from the previous 12 months. Further, the median cost of the largest single incident rose to $200,000, up from $34,000.

To combat the increased number of cyberattacks, 72% of the respondents said their companies plan to boost spending on cybersecurity over the coming year. Only 50% said they plan to spend more on technology, down from 57% the prior 12 months. But the percentage of respondents who plan to spend more this year rose in all other areas, including employee training, security consultants and third-party services, cyber security staffing, and security outsourcing.

Beyond increasing spending, though, companies concerned about cyberattacks need to look at their reliance on the supply chain and the cloud, the report noted. A full 65% of respondents said they suffered one or more cyberattacks due to a weak link in their supply chain. Some 74% said they evaluate the security of their supplier networks at least once a quarter or on an ad-hoc basis. But only 8% said they had increased the frequency of their supply chain valuations due to a cyber incident over the past year.

Some 22% of respondents reported problems due to outages from third-party cloud providers, up from 13% over the previous 12 months. Large enterprise companies were more likely to report a cloud-related incident than were smaller organizations.

Only 16% of those surveyed said they have "no defined role for cyber security," down from 32% the prior 12 months. Most have their own internal head of cyber security or a dedicated team, while 19% said they used an external provider. And only 32% said they changed nothing following a cyber security incident, down from 47% previously. (…)

Companies are increasingly aware of the risks and pouring more resources into cyber protection, and yet, there is still a tremendous gap between awareness of the issue and actually having an effective defense.

Tech Republic, April 23, 2019