

# CAHIER DES CHARGES

---

B.O. n° 42 du 15 novembre 2012

<http://www.education.gouv.fr>

## Règles communes aux deux parcours - 1

1.1 Un contexte est composé d'une organisation cliente et d'un prestataire informatique interne ou externe à l'organisation cliente. Ces organisations sont réelles ou directement inspirées du réel. L'organisation cliente et le prestataire informatique sont décrits à travers leurs principaux processus métier et support, leur système d'information et l'ensemble de leurs relations formalisées (contrats ou catalogue de services, politique de sécurité, charte, etc.).

1.2 Les besoins de l'organisation cliente en matière de création ou d'amélioration de services informatiques sont clairement identifiés dans un ou plusieurs cahiers des charges qui définissent les contraintes techniques, financières et temporelles à respecter.

Les règles communes concernent tous les contextes, s'il y en a deux, ils doivent respecter chacun ces règles communes (cf. 1.6)

## Règles communes aux deux parcours - 2

**1.3** L'environnement technologique d'apprentissage supportant le système d'information de l'organisation cliente **comporte au moins** :

- un service d'authentification pour les utilisateurs internes et externes à l'organisation ;
- un SGBD ;
- un accès sécurisé à internet ;
- un environnement de travail collaboratif ;
- un logiciel de gestion d'incidents ;
- un logiciel de gestion des configurations ;
- deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel open source ;
- une solution de sauvegarde ;
- des ressources dont l'accès est sécurisé et soumis à habilitation ;
- deux types de solution technique d'accès dont une mobile (type smartphone, tablette, ou encore assistant personnel).

**1.4** Les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer à des équipements réels dans l'environnement technologique d'apprentissage.  
**Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.**

1.3 « Le cahier des charges parle de l'environnement technologique d'apprentissage, c'est-à-dire celui que les étudiants ont eu l'occasion d'au moins manipuler dans le cadre de leur PPE et pas seulement d'avoir exploité uniquement en tant qu'utilisateur ou d'avoir regardé de loin. » *Alan Van Sante*.

« Il s'agit de construire des environnements d'apprentissage qui permettent de supporter les contextes et non des environnements réels : dans un contexte dans lequel il y a quinze sites extérieurs comprenant chacun cinquante postes de travail à relier à un siège, un environnement d'apprentissage permettant de simuler deux ou trois sites avec chacun deux ou trois postes de travail est suffisant... » *Alan Van Sante*.

1.4 La virtualisation en tant que réponse à un besoin de l'organisation est justifiée de même que le recours à un logiciel de simulation pour créer une maquette. Mais l'environnement technologique dans lequel évolue l'étudiant est constitué d'équipements réels.

## Règles communes aux deux parcours - 3

**1.5** Tous les documents et ressources qui décrivent un contexte doivent être accessibles en ligne aux commissions de correction à partir d'une date fixée par les autorités académiques :

- documents de présentation des organisations (organisation cliente et prestataire informatique) ;
- description de l'environnement technologique d'apprentissage ;
- tout ou partie des documents de référence utilisés par l'organisation cliente et par le prestataire informatique qui sont utiles pour définir le contexte (référentiels de bonnes pratiques, normes ou standards, processus, données métiers, etc.) et nécessaires pour le déroulement de l'épreuve ;
- les schémas d'infrastructure réseau ;
- la documentation technique des services disponibles ;
- les fichiers de configuration, la documentation technique des équipements matériels et des logiciels disponibles ;
- les éléments financiers et juridiques liés aux services et aux équipements disponibles.

**1.6** Lorsque les **deux situations professionnelles** présentées par un candidat s'appuient sur **deux contextes différents**, chaque contexte et son environnement technologique d'apprentissage doivent respecter les règles communes aux deux parcours. Le respect des règles relatives au parcours du candidat (SISR ou Slam) est mesuré à partir du cumul des caractéristiques des deux environnements technologiques d'apprentissage.

1.5 – Documentation, ressources données avec le contexte.

1.6 – « Il n'est pas nécessaire que le premier contexte de l'année respecte ce cahier des charges, ni que l'étudiant ait installé tout cet environnement à la fin des deux années. C'est bien l'environnement dans lequel il aura "baigné » à l'issue de ses deux années de formation. Car un PPE est essentiellement un travail d'équipe alors qu'une situation professionnelle est personnelle. » *Alan Van Sante*.

## Règles spécifiques au parcours SISR

### 2.1 L'environnement technologique supportant le système d'information de l'organisation cliente **comporte au moins** :

- un réseau comportant plusieurs périmètres de sécurité ;
- une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès ;
- un logiciel d'analyse de trames ;
- un logiciel de supervision système et réseau ;
- trois types de solution technique d'accès dont une mobile ;
- un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité.

- Une DMZ, un réseau local, un réseau de serveurs, un réseau administratif... peuvent constituer ces périmètres dès lors qu'ils sont délimités par des règles de filtrage...
- SSH, RDP sous Windows, certificat, ...
- Wireshark, tcpdump, moniteur réseau Windows...
- Nagios, Cacti, Shinken, ...
- Critères d'appréciation larges : selon le SE, le type de matériel : « [...] tout outil numérique, fixe ou nomade, constitué de composants matériels et logiciels, permettant à un utilisateur d'accéder à des services en ligne. »
- Le résultat de l'action menée par l'étudiant est donc destiné à l'utilisateur final. On répond à un besoin destiné à améliorer le service rendu à l'utilisateur final.

## Règles spécifiques au parcours SISR

2.2 La structure et les activités de l'organisation s'appuient sur **au moins trois solutions d'infrastructures opérationnelles** parmi les suivantes :

- 2.2.1 une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet) ;
- 2.2.2 une solution garantissant la continuité d'un service ;
- 2.2.3 une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion ;
- 2.2.4 une solution permettant la connexion sécurisée entre deux sites distants ;
- 2.2.5 une solution permettant le déploiement des solutions techniques d'accès ;
- 2.2.6 une solution gérée à l'aide de procédures automatisées écrites avec un langage de scripting ;
- 2.2.7 une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des services avec remontées d'alertes ;
- 2.2.8 une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau ;
- 2.2.9 une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion.

2.3 Les solutions d'infrastructure présentes dans le contexte sont opérationnelles et documentées. Elles s'appuient sur des composants matériels accessibles au moment de l'épreuve.

- 2.2.1 – intranet/extranet, sécurisation des accès
- 2.2.2 – Haute disponibilité, identification des risques, plans de reprise informatique, plans de continuité informatique, peut-être QoS.
- 2.2.3 – Haute disponibilité de service (exemple avec Heartbeat) ou d'éléments d'interconnexion (Routeur et HSRP, commutateur et spanning-tree)
- 2.2.4 – VPN.
- 2.2.5 – Par exemple avec un service de déploiement : Ghost, clonezilla, FOG, ...
- 2.2.6 – Langage de scripting en shell, en WSH, ...
- 2.2.7 – Nagios, Cacti, MRTG, Shinken, ...
- 2.2.8 – IDS : *Intrusion Detection System* - NIDS (*Network Based Intrusion Detection System*), qui surveillent l'état de la sécurité au niveau du réseau. On trouve les logiciels : Snort, Bro,...
- 2.2.9 – LVS, IPVS, VRRP, HAProxy, GLBP (Gateway Load Balancing Protocol)...