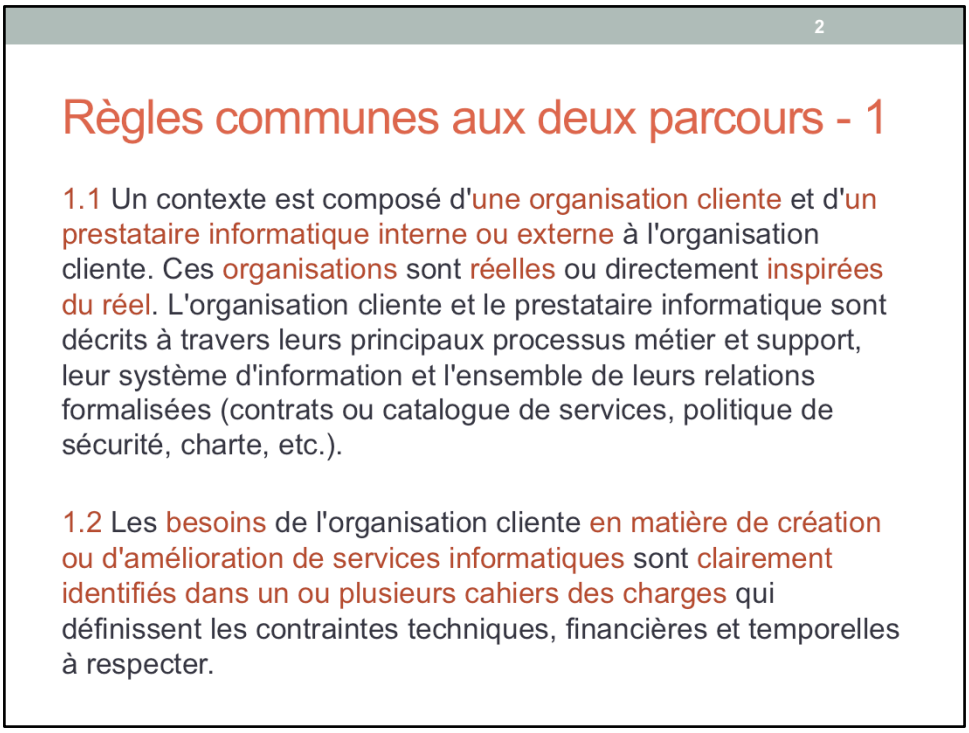
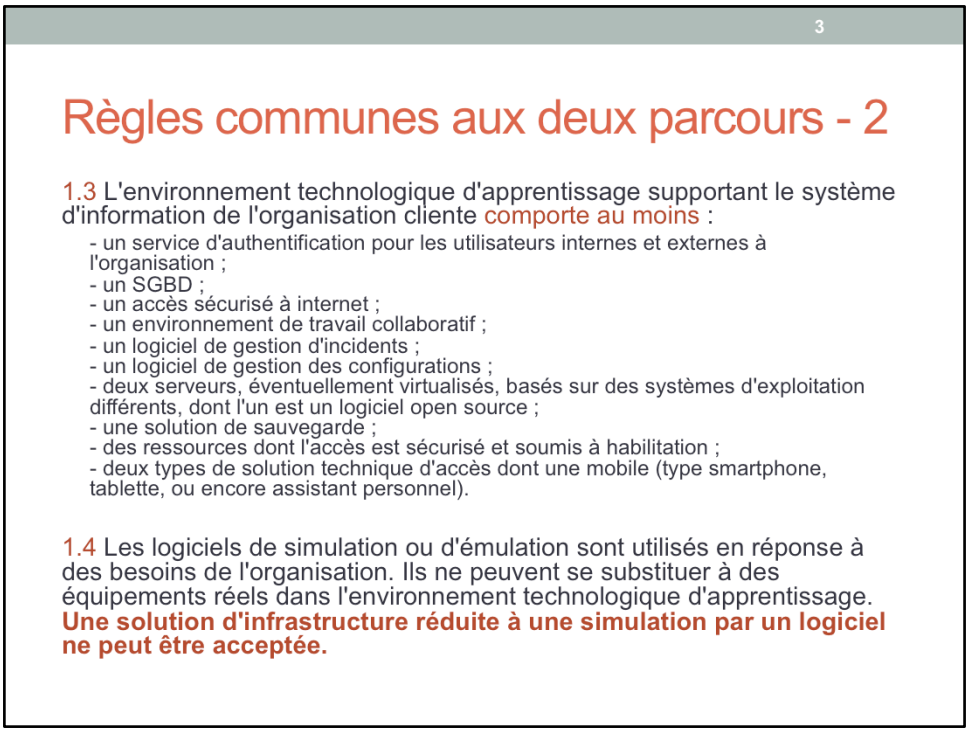
CAHIER DES CHARGES

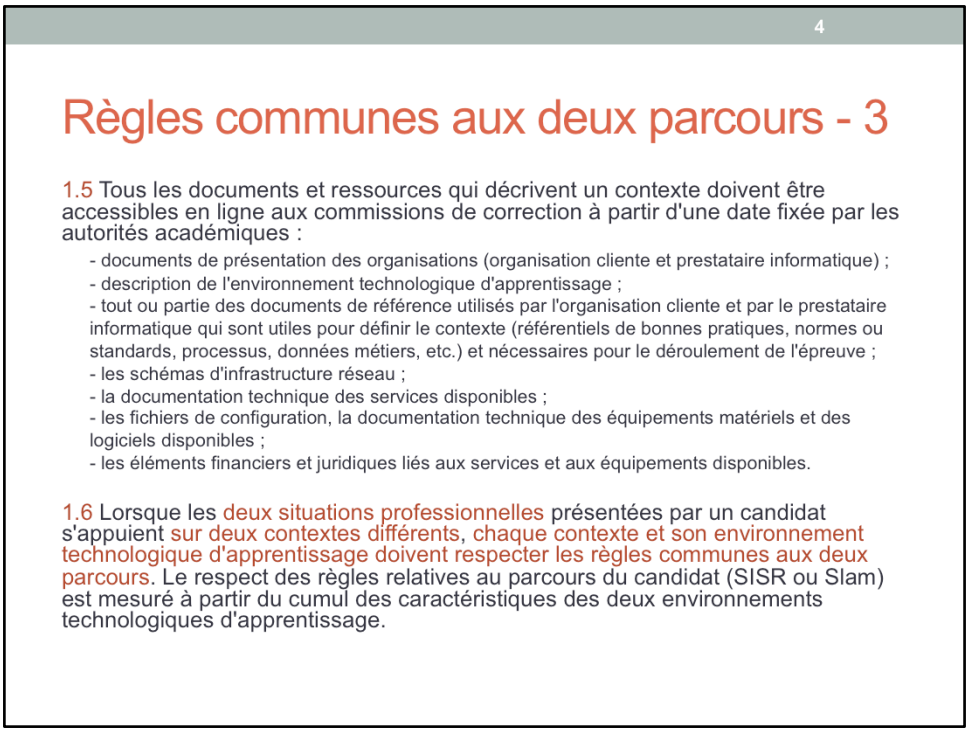
B.O. n° 42 du 15 novembre 2012
http://www.education.gouv.fr



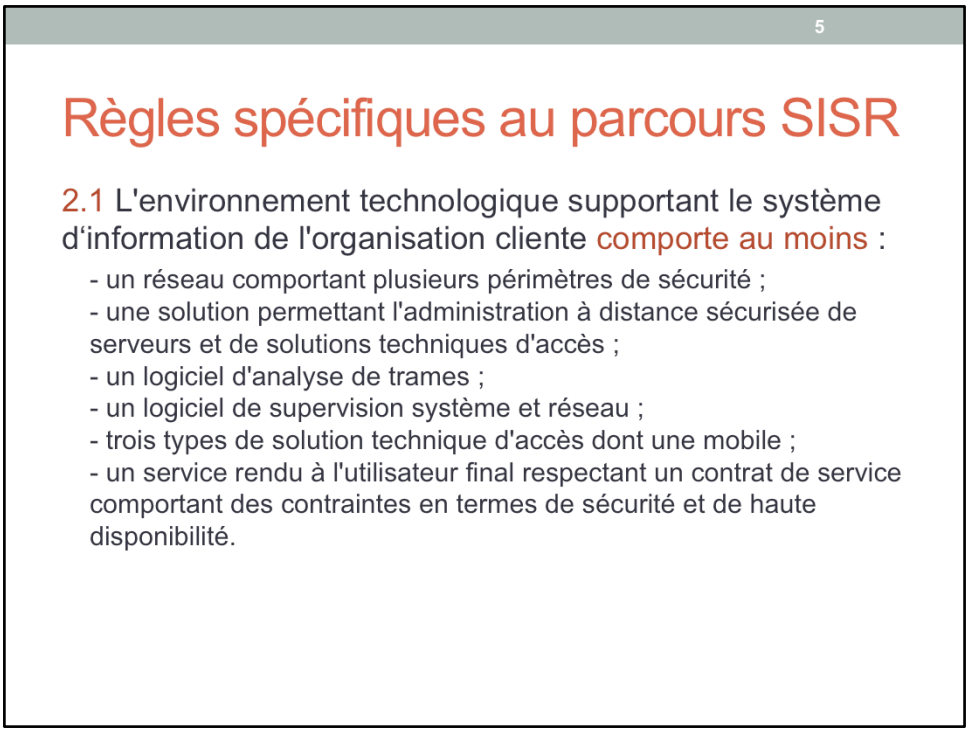
Les règles communes concernent tous les contextes, s'il y en a deux, ils doivent respecter chacun ces règles communes (cf. 1.6)



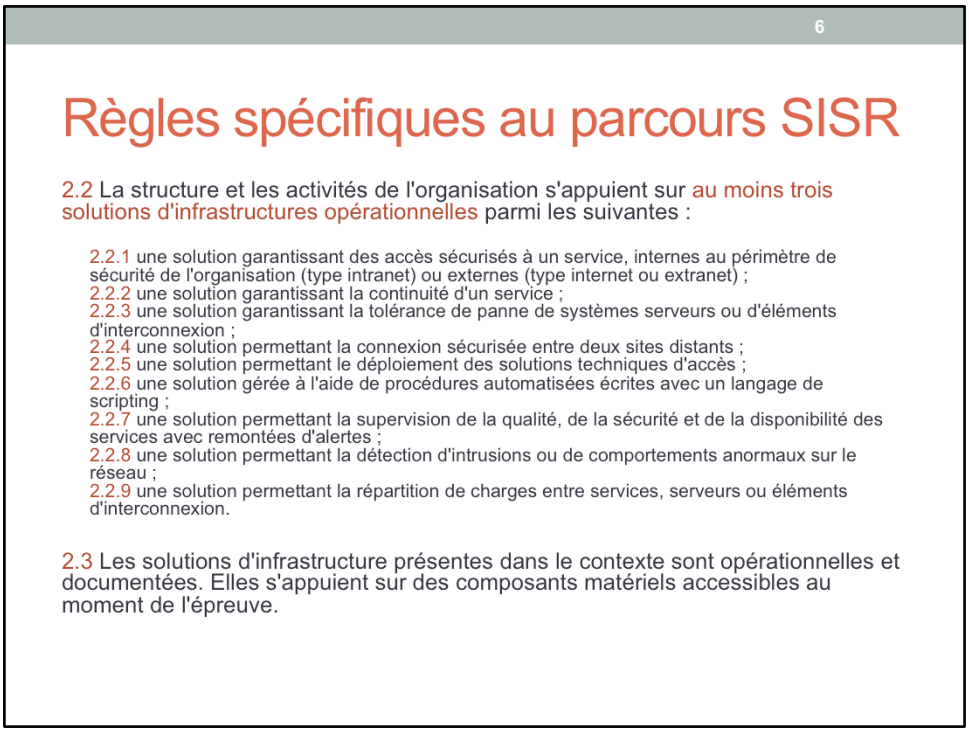
1.3 « Le cahier des charges parle de l'environnement technologique d'apprentissage, c'est-à-dire celui que les étudiants ont eu l'occasion d'au moins manipuler dans le cadre de leur PPE et pas seulement d'avoir exploité uniquement en tant qu'utilisateur ou d'avoir regardé de loin. » *Alan Van Sante*.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



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'issu 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*.



- 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.



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)…