Questionnaire CACIB

1. Des processus de gouvernance et de gestion des risques de sécurité de l'information sont-ils mis en place au niveau de l'organisation ?
2. L'organisation réalise-t-elle des analyses de risques (identifiant notamment les menaces internes et externes auxquelles elle est exposée) ?
3. Des plans de traitement des risques sont-ils mis en place ?
4. Les mesures de traitement dans ces plans font-elles l'objet d'un suivi et sont-elles priorisées ?
5. Une politique de sécurité de l'information est-elle formalisée ?
6. La politique de sécurité de l'information est-elle communiquée au sein de l'organisation (accessible aux parties prenantes) ?
7. La politique de sécurité de l'information est-elle validée par la Direction et régulièrement revue ?
8. Les principes relatifs à la sécurité du SI sont-ils définis (périmètre d'application/cadre réglementaire)
9. La politique précise-t-elle la gouvernance en place ?
10. La politique de sécurité de l'information aborde-t-elle les principaux thèmes à savoir : architecture du SI, gestion des accès, maintenance du SI, surveillance, gestion des incidents, résilience du SI, protection des données, externalisation… ?
11. Les rôles et les responsabilités vis-à-vis de la sécurité de l'information sont-ils définis au sein de l'organisation ? Ces éléments peuvent notamment être définis dans le cadre de la politique de sécurité de l'information, ou d'une matrice RACI.
12. Un responsable sécurité informatique (RSSI,CISO, etc..) est-il nommé au sein de l'organisation?
13. Le principe de séparation des tâches est-il respecté ?
14. Un organe de pilotage de la sécurité de l'information, type comité, est-il en palce ?
15. Les autorités avec lesquelles l'organisation peut être amenée à collaborer en matière de sécurité de l'information sont-elles identifiées ?
16. Existe-t-il un document document normatif (ex : politique/standard de sécurité) défissant les mesures de sécurité à mettre en place vis-à-vis de l'utilisation des appareils mobiles au sein de l'organisation (préciser les principales mesures en place ) ?
17. Existe-t-il un document normatif encadrant le télétravail d'un point de vue sécurité (préciser les principales mesures en place dans les commentaires) ?
18. Les collaborateurs de l'organisation sont-ils systématiquement sensibilisés à la sécurité de l'information (e-learning, campagnes de phishing…) ?
19. Des sensibilisations sur la sécurité de l'information sont-elles réalisées régulièrement, et mises à jour ?
20. Les collaborateurs dont les missions sont liées directement à la sécurité du SI (RSI, DSI, Administrateurs, développeurs) ont-ils reçus des formations adaptées sur le sécurité de l'information ?
21. Un processus de départ des collaborateurs est-il mis en place, traitant notamment du retour des actifs de l'organisation (smartphones, PC, etc…), et de la suppression/désactivation des comptes et accès utilisateurs ?
22. Un processus est-il en place afin d'identifier les actifs associés à l’information et aux moyens de traitement de l’information ?
23. Un inventaire des actifs de l'organisation en lien avec l'information et ses moyens de traitements est-il formalisé au sein de l'organisation ?
24. L'inventaire des actifs est-il régulièrement revu, et maintenu à jour ?
25. A chaque actif, un propriétaire nominatif est-il attribué ?
26. Des règles de classification des actifs sont-elles en place (ex : politique de classification de l'information) ? ET l'information au sein de l'organisation bénéficie-t-elle d’un niveau de protection conforme à son importance pour l’organisation ?
27. Les mesures de sécurité sont-elles adaptées en fonction d'une classification des actifs (ex : les actifs critiques/sensibles font-ils l'objet de mesures de sécurité adaptées) ?
28. Les données à supprimer au sein de l'organisation sont-elles détruites de manière sécurisé et selon un processus formalisé ?
29. Des mesures de sécurité vis-à-vis du contrôle des accès aux actifs de l'organisation (données, réseaux, applications, etc…) sont-elles formalisées et mises en place dans l'organisation (ex: dans une politique ou un standard de sécruité) ?
30. Un processus de gestion des droits d'accès à privilèges est-il mis en oeuvre, et comprenant l'attribution, la révocation, et les modifications des droits ?
31. Un processus de gestion des droits d'accès des utilisateurs est-il mis en oeuvre, et comprenant l'attribution, la révocation, et les modifications ?
32. Les droits d'accès sont-ils revus et contrôlés régulièrement, et dans le cadre d'un processus formalisé ?
33. Les évènements de connexion aux SI de l'organisation sont-ils journalisés (incluant les tentatives d'accès échouées) ?
34. Des contrôles sont-ils mis en place afin de s'assurer que les utilisateurs n'aient accès qu'aux applications, systèmes et informations auxquels leurs droits leur donnent accès ?
35. Les informations secrètes d'authentification temporaires sont-elles fournies aux utilisateurs de manière sécurisée ?
36. Les informations secrètes d'authentification par défaut des fournisseurs des systèmes ou des logiciels son-ellest modifiées ou désactiviées après leur l'installation ?
37. Des mesures de sécurité portant sur la gestion des mots de passe sont mises en place dans l'organisation (ex : politique/standard) ?
38. Les systèmes de gestion des mots de passe déployés sur les principaux actifs de l'organisation :
39. Imposent l'utilisation d'identifiants utilisateurs et de mots de passe nominatifs pour notamment garantir l’imputabilité ?
40. Permettent aux utilisateurs de sélectionner et de modifier leurs propres mots de passe avec la possibilité de confirmation pour éviter les erreurs de saisie ?
41. Imposent l'utilisation de mots de passe de qualité (longueur, lettres, chiffres, caractères spéciaux, etc…)?
42. Forcent les utilisateurs à changer leurs mots de passe lors de la première connexion ?
43. Sont configurés de manière à exiger un changement périodique des mots de passe, et permettent à l'utilisateur de changer son mot de passe au besoin et en toute sécurité ?
44. Sont configurés de manière à réaliser un enregistrement des mots de passe utilisés précédemment, empêchant ainsi leur réutilisation ?
45. Masquent les mots de passe sur l'écran lors de la saisie ?
46. Conservent et transmettent les mots de passe de manière sécurisée ?
47. Les accès physiques aux sites de l'organisation sont-ils sécurisés et contrôlés (contrôles via portiques d'accès, etc…)?
48. Les environnements de production sont-ils isolés des autres environnements (recette, développement, etc…) ?
49. Les postes de travail des utilisateurs sont-ils configurés de manière à limiter les fonctionnalités, et notamment la possibilité d'installer des logiciels non contrôlés par l'organisation ?
50. Un processus de contrôle des changements de configuration est-il mis en place au sein de l'organisation?
51. Des mesures de gestion des vulnérabilités sont-elles formalisées (ex : politique/standard) et déployées au sein de l'organisation ?
52. Des mesures de veille des vulnérabilités sont-elles formalisées et déployées dans l'organisation ?
53. Les vulnérabilités identifiées sur le SI de l'organisation font-elles l'objet d'un plan de remédiation, et d'une hierarchisation ?
54. L'installation des correctifs de sécurité se fait-elle à la suite d'une analyse d'impact ?
55. Des règles définissant le périmètre des évènements du SI à journaliser sont-elles formalisées et mises en œuvre ?
56. Les évènements (activités des utilisateurs, activités des sytèmes, accès au différentes ressources, etc…) sur les actifs (postes de travail, applications, systèmes, bases de données, équipements,etc…) sont-ils journalisés ?
57. Les journaux/logs contiennent-ils les informations nécessaires, et des informations exploitables (date/heure, activités systèmes etc…) ?
58. L'environnement d'administration fait-il l'objet de mesures de sécurité formalisées et appliquées (accès aux postes de travail, environnements SI d'administration, utilisation de bastions, etc...?
59. L'ensemble des évènements associés aux actes d'administration sont-ils journalisées ?
60. Les journaux/logs sont-ils centralisés dans un outil type SIEM afin d'être analysés ?
61. Un processus de traitemement des alertes est-il mis en place dans l'organisation (SOC, équipe de réponse à incident, etc..) ?
62. Des mécanismes de protection sont-ils mis en place afin de sécuriser les journaux/logs (notamment les accès et leur intégrité) ?
63. Les postes de travail sont-ils équipés de dispositifs afin de lutter contre les logiciels malveillants (antivirus, EDR, etc…)?
64. Les serveurs sont-ils équipés de dispositifs afin de lutter contre les logiciels malveillants (antivirus, EDR, etc…) ?
65. Des mesures de sécurité visant à encadrer les points d'accès internet sont-elles mis en place au sein de l'organisation ?
66. Les actifs sont-ils mis à jour (postes de travail, systèmes, etc…) ?
67. Des audits de sécurité (parenthèse tests d'intrusion et de vulnérabilités) sont-ils réalisés sur le SI de l'organisation (en particulier sur les systèmes exposés, sensibles ou critiques) ?
68. Une procédure de gestion des incidents est-elle formalisée ?
69. Un suivi de la bonne remédiation des incidents de sécurité est-il réalisé ?
70. Les incidents de sécurité sont-ils catégorisés (ex : faible, moyen, grave, critique) ?
71. Un document normatif défissant les mesures de sécurité à mettre en place vis-à-vis du développement d'applications/de systèmes est-il formalisé, et les mesures de sécurité sont-elles mises en œuvre ?
72. Des audits de code sont-ils réalisés régulièrement pendant la phase de développement
73. Des scans de vulnérabilités et des tests d'intrusion sont-ils mis en oeuvre avant les mises en production ?
74. En cas de développements confiés à des sociétés externes, des règles de sécurité sont-elles imposées contractuellement aux sociétés externes ?
75. Des mesures sont-elles mises en place pour encadrer les changements : validation, traçabilité, contrôle des version, revues des changements, etc… ?
76. Des scans de vulnérabilités et des tests d'intrision sont-ils mis en oeuvre avant les mises en production ?
77. Des tests de non régression sécurité sont-ils réalisés suite à la mise en œuvre des changements ?
78. "Un processus d'évaluation de la maturité cybersécurité des fournisseurs est-il déployé au sein de l'organisation ?
79. "
80. Les fournisseurs/les tiers délivrant des prestations en lien avec le SI de l'organisation (prestations IT, composants…) sont-ils identifés ?
81. Un PAS (Plan d'Assurance Sécurité) est-il mis en place avec les fournisseurs les plus critiques de l'organisation ?
82. "Les accès à distance au SI mis à disposition de fournisseurs tiers sont-ils sécurisés, surveillés et contrôlés par l'organisation ?
83. "
84. Les incidents de sécurité liés aux fournisseurs font-ils l'objet d'un processus afin d'assurer et d'encadrer leur traitement ?
85. L’organisation a-t-elle déterminé ses exigences en matière de continuité d'activité/résilience, afin d'être en mesure de continuer à fournir ses services en situation dégradée (sinistre, incident, etc..) ?
86. Des processus de sauvegarde alignés avec les exigences formulées sont-ils mis en place ?
87. Les sauvegardes sont-elles régulièrement réalisées ?
88. Les sauvegardes sont-elles régulièrement testées ?
89. Un PCA informatique est-il mis en oeuvre dans l'organisation ?
90. Le personnel est-il formé à la mise en oeuvre du PCA ?
91. Ce plan est-il mis à jour régulièrement avec les parties prenantes ?
92. Ce plan est-il testé régulièrement ?
93. L'organisation a-t-elle identifié et formalisé les exigences légales, réglementaires et contractuelles qui lui sont applicables, vis-à-vis des données que l'organisation traite ?
94. L'organisation met-elle en place des mesures de sécurité pour protéger l'accès aux données de ses clients ?
95. L'organisation met-elle en place des mesures de sécurité pour protéger le stockage, et l'utilisation des données de ses clients ?
96. L'organisation met-elle en place des mesures permettant de garantir la bonne suppression des données de ses clients si nécessaire ?
97. Des dispositifs sont-ils mis en place pour protéger l'organisation contre la fuite de données (outils de DLP au niveau de la messagerie, chiffrement des supports hébergeant des données des clients, anonymisation des données des clients, etc...)?
98. Des contrôles de conformité sont-ils en place afin de s'assurer que les exigences légales et les mesures de sécurité des politiques/standards/procédures sont appliquées au sein de l'organisation ?
99. Les contrôles font-ils l'objet d'un plan de suivi et de remédiation ?