



POLITIQUE DE SECURITE
DES SYSTEMES D'INFORMATION
DE LA DGAC

NIVEAU 3

OPERATIONNEL

Approbation du document

	NOM ET TITRE	SIGNATURE	DATE
RÉDACTION			
VÉRIFICATION	Jean CARLIOZ <i>Responsable de la Sécurité des Systèmes d'Information de la DGAC</i>		
APPROBATION	Patrick GANDIL, <i>Directeur Général de l'Aviation Civile</i>		

Relevé des modifications

ÉDITION	DATE	MOTIF DES CHANGEMENTS	SECTIONS / PAGES MODIFIÉES
Version 1.0	19/02/2018	Version de diffusion	
Version 1.2	07/05/2018	Version mise à jour suite retours SSIM	<ul style="list-style-type: none"> Formulation des exigences : AC-2.1; AC-2.5; AC-2.10; AC-2.13; AC-4-10; AC-6.0; AC-6-1; AC-6.7; AC-8.0; AC-17.3; AC-18.0 Revue de la traçabilité des liens avec les exigences LPM Modification des environnements : AC-6.8; AC-6.10; AC-19.4

Diffusion

MODE DE DIFFUSION / FORMAT	DESTINATAIRES
Diffusion simple / document papier	Directions de la DGAC
Diffusion simple / document électronique : GEODe	Tous

Responsable du document

Responsable de la Sécurité des Systèmes d'Information de la DGAC (RSSI DGAC)

Date d'application du document

18 octobre 2018

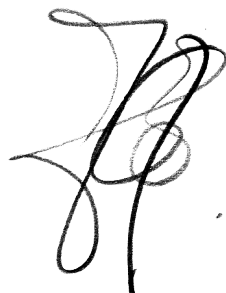


Table des matières

Introduction	7
❖ Démarche d'application de la PSSI opérationnelle.....	7
❖ Application des exigences par environnement.....	7
Gestion des accès	8
❖ Gestion des comptes	8
❖ Droits d'accès	10
❖ Contrôle des flux d'information	11
❖ Séparation des fonctions.....	12
❖ Principe de moindre privilège	12
❖ Tentatives infructueuses d'ouverture de session	13
❖ Information préalable lors de l'accès aux systèmes	14
❖ Verrouillage de session	14
❖ Actions autorisées sans identification ou authentification.....	14
❖ Accès à distance	15
❖ Accès sans fil	16
❖ Contrôle d'accès depuis un ordinateur portable ou un mobile	17
❖ Utilisation de systèmes d'information externes.....	18
❖ Contenu accessible au public	19
SENSIBILISATION ET FORMATION	20
❖ Sensibilisation à la sécurité des systèmes d'Information	20
❖ Formation à la sécurité des systèmes d'information	20
Journalisation et Traçabilité.....	21
❖ Événements de Journalisation	21
❖ Contenu des éléments de journalisation.....	21
❖ Collecte des événements	22
❖ Erreur de journalisation	22
❖ Revue des journaux, analyse et notification.....	23
❖ Agrégation des événements et génération de rapports	24
❖ Horodatage	24
❖ Protection des journaux d'événements	24
❖ Rétention des événements de journalisation.....	25
❖ Génération des audits	26
Evaluation de sécurité et Homologation	27
❖ Politiques et procédures d'évaluation et d'autorisation de sécurité	27

❖ Évaluations de sécurité	27
❖ Interconnexions système	28
❖ Plan d'action et jalons	28
❖ Autorisation de sécurité.....	29
❖ Contrôle continu	29
❖ Connexions système internes.....	29
<i>Gestion de la configuration.....</i>	30
❖ Configuration de base	30
❖ Contrôle de changement de configuration.....	30
❖ Analyse d'impact sur la sécurité	32
❖ Restrictions d'accès au changement.....	32
❖ Paramètres de configuration.....	33
❖ Limiter les fonctionnalités.....	33
❖ Inventaire des composants du système d'information.....	34
<i>Plan d'urgence</i>	36
❖ Test du plan d'urgence	36
❖ Site secondaire.....	36
❖ Services de télécommunications	37
❖ Sauvegarde du système d'information.....	38
❖ Récupération et reconstitution des systèmes d'information.....	39
<i>Identification et Authentification.....</i>	40
❖ Identification et authentification des usagers.....	40
❖ Identification et authentification des équipements	42
❖ Gestion des identificateurs	42
❖ Gestion des authentifiants.....	42
❖ Commentaires d'authentification	44
❖ Authentification du module cryptographique.....	44
❖ Identification et authentification des services	44
<i>Réponse aux incidents.....</i>	45
❖ Politique et procédures d'intervention en cas d'incident.....	45
❖ Formation sur la réponse aux incidents	45
❖ Gestion des incidents	46
❖ Suivi des incidents.....	47
❖ Rapports sur les incidents	47
❖ Assistance en cas d'incident.....	47
<i>Maintenance</i>	49

❖ Maintenance de contrôle	49
❖ Outils de maintenance	49
❖ Maintenance non locale.....	50
❖ Personnel de maintenance.....	52
Protection des médias.....	53
❖ Marquage des supports.....	53
❖ Protection cryptographique	53
❖ Désinfection des médias	54
❖ Utilisation des médias	54
Protection Physique et Environnementale	55
❖ Autorisations d'accès physique	55
❖ Contrôle des accès physiques.....	56
❖ Contrôle d'accès aux moyens de transmission	57
❖ Contrôle d'accès aux périphériques de sortie.....	57
❖ Suivi de l'accès physique	57
❖ Enregistrements d'accès des visiteurs	58
❖ Équipement électrique et câblage.....	59
❖ Arrêt d'urgence	59
• <i>Alimentation de secours</i>	59
❖ Éclairage d'urgence	60
❖ Protection contre le feu	60
❖ Contrôles de température et d'humidité.....	61
❖ Protection contre les dommages causés par l'eau.....	62
❖ Livraison et enlèvement.....	62
Planification	63
❖ Diversité des fournisseurs	63
Sécurité des Personnels.....	64
❖ Indice de risque	64
❖ Enquête de sécurité	64
❖ Cessation d'emploi du personnel	64
❖ Transfert de personnel.....	65
❖ Sécurité des personnels tiers.....	65
Analyse de risque	66
❖ Evaluation des risques.....	66
❖ Scan de vulnérabilité.....	66
❖ Surveillance des mesures de sécurité	67

<i>Acquisition de systèmes ou de services</i>	68
❖ Cycle de vie de développement du système.....	68
❖ Processus d'acquisition	68
❖ Dossier de sécurité d'exploitation.....	70
❖ Services externes au système d'information.....	70
❖ Gestion de la configuration des développeurs	71
❖ Test et évaluation de la sécurité des développeurs.....	72
❖ Protection de la chaîne d'approvisionnement.....	73
❖ Processus de développement, normes et outils	74
❖ Composants du système non supportés.....	75
<i>Protection des systèmes et des communications</i>	76
❖ Partitionnement des applications	76
❖ Isolation des fonctions de sécurité	76
❖ Informations dans les ressources partagées.....	77
❖ Détection / surveillance	77
❖ Périmètre de protection (zones de sécurité)	77
❖ Confidentialité et intégrité de la transmission	80
❖ Déconnexion du réseau.....	80
❖ Création et gestion des clés cryptographiques.....	80
❖ Dispositifs d'informatique collaborative	80
❖ Exécution de code à la volée	81
❖ Voix sur IP (VoIP).....	81
❖ Service de résolution de noms / adresses sécurisés (source autorisée)	81
❖ Architecture et approvisionnement pour service de résolution de noms / adresses	82
❖ Authenticité de session	82
❖ Retour dans un état stable en cas d'échec	82
❖ Protection de l'information au repos	83
<i>Intégrité des systèmes et de l'information</i>	84
❖ Correction de défauts.....	84
❖ Protection contre les codes malveillants.....	85
❖ Surveillance du système d'information	86
❖ Alertes de sécurité, avis et directives	88
❖ Vérification des fonctions de sécurité	89
❖ Intégrité des logiciels, firmwares et de l'information.....	89
❖ Protection contre les spams	91
❖ Validation d'entrée d'information.....	91

❖ Gestion des erreurs	92
❖ Protection mémoire	93
<i>ANNEXE : Glossaire</i>	94

Introduction

❖ Démarche d'application de la PSSI opérationnelle

Les exigences définies dans ce document présentent différents niveaux de préconisations conformes aux bonnes pratiques :

- **OBLIGATOIRE** : L'exigence indique une nécessité absolue de la politique de sécurité.
- **RECOMMANDÉ** : L'exigence peut être ignorée dans des circonstances particulières et pour des raisons valables et justifiées, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente.
- **INTERDIT** : L'exigence indique une prohibition absolue de la politique de sécurité.

Le non-respect des exigences de la PSSI peut donner lieu à des mesures disciplinaires, voire pénales (compromission d'informations protégées).

❖ Application des exigences par environnement

Les exigences définies dans ce document sont applicables selon les environnements de sécurité définis dans la PSSI Niveau 2. Pour chaque exigence, un tableau précise pour quel environnement l'exigence qui suit est applicable :

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Gestion des accès

❖ Gestion des comptes

AC-2-0 - Gestion de comptes - V1R1

Environnement	R	O	J	B
	☒	☒	☒	☐

Il est OBLIGATOIRE que la gestion des comptes du système d'information repose sur des outils et mécanismes automatisés comme des outils d'annuaire, des outils de gestion départ, arrivées et mutations, etc.

AC-2-1 - Gestion automatisé des comptes systèmes- V1R0

Environnement	R	O	J	B
	☒	☒	☒	☐

Il est OBLIGATOIRE que l'organisation utilise des mécanismes automatisés pour soutenir la gestion des comptes du système d'information.

AC-2-2 - Retrait des comptes temporaires / d'urgence - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☐

Il est OBLIGATOIRE que le système supprime automatiquement les comptes provisoires après un mois. Il est OBLIGATOIRE que le l'organisation réalise une procédure pour la gestion des comptes d'urgence.

AC-2-3 - Désactivation des comptes inactifs - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☐

Il est OBLIGATOIRE que le système verrouille automatiquement les comptes inactifs (inutilisés) après 2 mois.

Il est RECOMMANDE que le système verrouille automatiquement les comptes inactifs (inutilisés) après 1 mois.

AC-2-4 - Actions d'audit automatisées - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☐

Il est OBLIGATOIRE que le système journalise chaque action de création, modification, désactivation et suppressions de compte.

AC-2-5 - Déconnexion après inactivité - V1R1

Environnement	R	O	J	B
	☒	☒	☒	☐

Il est OBLIGATOIRE que le système déconnecte automatiquement toute connexion d'utilisateur après une période d'inactivité à définir selon les besoins fonctionnels du système et ne devant pas excéder 30 minutes.

AC-2-7 - Contrôle d'accès par rôle - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que l'organisation :

- établisse et administre des comptes d'utilisateurs privilégiés conformément à un système d'accès basé sur les rôles ;
- surveille l'attribution de rôles privilégiés ;
- supprime les rôles privilégiés du compte utilisateur lorsqu'ils ne sont plus appropriés.

AC-2-9 - Restrictions sur l'utilisation des comptes partagés / de groupe - V1R0

Environnement	R	O	J	B
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Il est RECOMMANDE que l'organisation n'utilise pas de comptes ou groupes d'utilisateurs partagés (compte générique).

Lorsque des raisons techniques ou opérationnelles ne permettent pas de créer de comptes individuels pour les utilisateurs ou pour les processus automatiques, il est OBLIGATOIRE que l'organisation mette en place des mesures permettant de réduire le risque lié à l'utilisation de comptes partagés et d'assurer la traçabilité de l'utilisation de ces comptes.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est INTERDIT que l'organisation utilise de comptes ou groupes d'utilisateurs partagés (compte générique).

Lorsque des raisons techniques ou opérationnelles ne permettent pas de créer de comptes individuels pour les utilisateurs ou pour les processus automatiques, il est OBLIGATOIRE que l'organisation mette en place des mesures permettant de réduire le risque lié à l'utilisation de comptes partagés et d'assurer la traçabilité de l'utilisation de ces comptes.

AC-2-10 - Clôture d'un compte partagé / de groupe - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Lorsque des raisons techniques ou opérationnelles nécessitent la création de comptes ou groupe partagé (cf. AC-2-9), alors il est OBLIGATOIRE que le système mette fin aux informations d'identification de compte ou groupe partagées (compte générique) lorsque les membres quittent le groupe.

AC-2-13 - Désactivation des comptes pour les personnes à haut risque - V1R1

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation désactive les comptes présentant un risque important au maximum 24h ouvrées après la découverte du risque (informations des autorités compétentes ou preuves internes, etc.).

❖ **Droits d'accès****AC-3-0 - Droits d'accès - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système applique des politiques de contrôle d'accès (ex: politique basée sur l'identité, politique accès sur les rôles...).

AC-3-4 - Contrôle d'accès discrétionnaire - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information applique une politique de contrôle d'accès discrétionnaire (DACL en opposition à Mandatory Access) dans lesquels la politique spécifie qu'un utilisateur qui a obtenu l'accès à l'information peut effectuer une ou plusieurs des opérations suivantes :

- passer l'information à des utilisateurs non autorisés ;
- accorder ses privilèges à d'autres utilisateurs ;
- modifier un ou plusieurs attributs de sécurité sur les utilisateurs, le système ou les composants du système ;
- choisir les attributs de sécurité et les valeurs d'attributs à associer aux objets nouvellement créés ou modifiés ;
- modifier les règles de contrôle d'accès.

AC-3-5 - Informations relatives à la sécurité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que les informations sensibles de paramétrage (clés de chiffrements, certificats, mot de passe, configuration FW, droits d'accès, gestion des ACL) soient classifiées "Confidentiel DGAC" et soient traitées avec des procédures adaptées.

AC-3-7 - Contrôle d'accès basé sur les rôles - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation applique une politique de contrôle d'accès axée sur les rôles (RBAC) précisés ci-dessous :

- Pour le système d'information Gestion et pilotage, les rôles ci-dessous doivent être appliqués
 - Administrateurs (exemple : AIG,...) - accès en modification de la configuration/du paramétrage du système, accès en modification à la configuration des mesures de sûreté (type privilèges, moyens d'authentification, gestion des notifications, etc.))
 - Utilisateurs : accès aux fonctions métier autorisées par l'application
- Pour le système d'information Navigation Aérienne, les rôles ci-dessous doivent être appliqués
 - Utilisateurs : accès aux fonctions métier autorisées par l'application,

- MO Opérateurs : accès en lecture aux notifications, aux opérations administrateur spécifiques définies aux cas par cas,
- MS Administrateurs Système : accès en modification de la configuration/du paramétrage du système, ne peuvent pas modifier la configuration des mesures de sûreté (type privilèges, moyens d'authentification, gestion des notifications, etc.),
- Administrateurs Sécurité : accès uniquement en modification à la configuration des mesures de sûreté (type privilèges, moyens d'authentification, gestion des notifications, etc.).

AC-3-8 - Révocation des autorisations d'accès - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les droits d'accès aux informations et aux moyens de traitement des informations de l'ensemble des salariés et utilisateurs tiers soient supprimés à la fin de leur période d'emploi, ou adaptés en cas de modification du contrat.

❖ Contrôle des flux d'information

AC-4-0 - Contrôle des flux d'information - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les flux d'information soient protégés par des mécanismes de chiffrement et d'authentification, sauf en cas de raisons techniques ou organisationnelles justifiées.

Il est OBLIGATOIRE que les flux d'information des comptes d'administration DOIVENT être protégés par des mécanismes de chiffrement et d'authentification.

AC-4-10 - Activation / désactivation des filtres de stratégie de sécurité - V1R1

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Lorsque le compte « administrateur sécurité » est créé, il est OBLIGATOIRE que le système d'information permette aux administrateurs sécurité d'activer / désactiver les fonctions de sécurité dans les conditions suivantes (dans le cadre de MISO avec l'avis de l'ASSI local).

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Lorsque le compte « administrateur sécurité » est créé, il est INTERDIT que le système d'information puisse permettre aux administrateurs non "Administrateurs Sécurité" de désactiver les mesures de sécurité du système d'information à l'exception des systèmes en environnement de test.

❖ Séparation des fonctions

AC-5-0 - Séparation des fonctions - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les tâches, privilèges et les domaines de responsabilité incompatibles soient cloisonnés afin de limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.

Il est OBLIGATOIRE que le système permette de séparer les tâches en fonction des rôles identifiés.

❖ Principe de moindre privilège

AC-6-0 - Principe de moindre privilège - V1R1

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation n'attribue à un utilisateur ou à un processus automatique les droits d'accès à une ressource que si cet accès est strictement nécessaire à l'exercice des missions de l'utilisateur ou au fonctionnement du processus automatique.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les opérations d'administration soient effectuées exclusivement à partir de comptes d'administration, et inversement, que les comptes d'administration soient utilisés exclusivement pour les opérations d'administration.

AC-6-1 - Autoriser l'accès aux fonctions de sécurité - V1R1

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation autorise explicitement l'accès à des fonctions de sécurité incluant par exemple :

- gestion des comptes
- configuration des événements à journaliser,
- paramétrage des outils de type IDS,
- paramétrage des règles de firewall,
- gestion des clés cryptographiques.

AC-6-2 - Accès non privilégié aux fonctions non sécurisées - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que les utilisateurs de comptes ou de rôles d'un système d'information ayant accès à des fonctions de sécurité utilisent des comptes ou des rôles non privilégiés lorsqu'ils accèdent à des fonctions non sécurisées.

AC-6-7 - Examen des privilèges des utilisateurs - V1R1

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les droits d'accès soient révisés tous les ans.

Il est RECOMMANDE que des revues périodiques soient réalisées tous les trimestres sur un périmètre restreint.

AC-6-8 - Niveaux de privilège pour l'exécution de code - V1R1

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que les logiciels ne fonctionnent pas avec des privilèges plus élevés que nécessaire.

AC-6-9 - Vérification de l'utilisation des fonctions privilégiées - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information vérifie et garde une trace de l'exécution des fonctions à privilèges.

AC-6-10 - Interdiction aux utilisateurs non privilégiés d'exécuter des fonctions privilégiées - V1R1

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que le système d'information empêche les utilisateurs non privilégiés d'exécuter des fonctions privilégiées incluant la désactivation, le contournement ou la modification des contre-mesures de sécurité mises en œuvre.

❖ **Tentatives infructueuses d'ouverture de session****AC-7-0 - Tentatives infructueuses d'ouverture de session - V1R1**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que des mécanismes de protection contre les attaques en « brute-force » soient implémentés sur les systèmes, comme l'implémentation d'une temporisation en fonction du nombre de connexions échouées :

- Temporisation de 10s après 3 tentatives de connexions échouées,
- Temporisation de 30s après 4 tentatives de connexions échouées,
- Temporisation de 1 min après 5 tentatives de connexions échouées.

Ces mécanismes peuvent être désactivés lorsque des raisons opérationnelles le justifient.

AC-7-2 - Protection d'accès d'un appareil mobile - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE l'organisation DOIT définir une politique d'accès des appareils mobiles ainsi que les mesures et mécanismes de sécurité à mettre en place conformément à la politique établie.

❖ **Information préalable lors de l'accès aux systèmes****AC-8-0 - Information préalable lors de l'accès aux systèmes - V1R1**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Lors du logon d'un utilisateur sur un système en production, Il est OBLIGATOIRE que ce dernier affiche des informations de dissuasion (bannière), à savoir qu'il s'agisse d'un système DGAC et que toute modification DOIVE être validée au préalable selon une procédure préétablie.

❖ **Verrouillage de session****AC-11-0 - Verrouillage de session - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

A l'exception des systèmes opérationnels de la navigation aérienne, il est OBLIGATOIRE que les sessions utilisateur soient verrouillées en cas de non utilisation prolongée après une période d'inactivité de 15 min.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'application ou la console utilisée pour administrer les équipements offre la possibilité aux administrateurs de verrouiller toute session utilisateur.

AC-11-1 - Obscurcir des informations – V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information dissimule, via le verrouillage de la session, les informations précédemment visibles sur l'écran avec une image ou information visible au public.

❖ **Actions autorisées sans identification ou authentification****AC-14-0 - Actions autorisées sans identification ou authentification - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE qu'un utilisateur soit identifié et authentifier avant d'autoriser des actions de modification ou d'exécution.

❖ **Accès à distance****AC-17-0 - Accès à distance - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation:

- établit et documente les restrictions d'utilisation/de connexion, les exigences de configuration et les conseils de mise en œuvre pour chaque type d'accès distant autorisé ;
- autorise préalablement et formellement l'accès à distance au système d'information avant d'accepter ces connexions.

AC-17-1 - Contrôle / contrôle automatisé des accès à distance - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information surveille et contrôle les méthodes d'accès à distance.

AC-17-2 - Protection de la confidentialité / intégrité avec des mécanismes cryptographiques - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information implémente des mécanismes cryptographiques préconisés par l'ANSSI pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.

AC-17-3 - Points de contrôle d'accès gérés - V1R2

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information achemine tous les accès à distance via les points de contrôle d'accès au réseau [ex: Narcisse, Snare, PFAI, Plateformes Internat], gérés par l'organisation.

AC-17-6 - Protection de l'information - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les informations des mécanismes d'accès à distance soient classifiées "confidentiel DGAC" et dans la mesure du possible, que ces informations ne soient pas accessibles aux utilisateurs eux-mêmes.

AC-17-9 - Déconnexion / désactivation des accès - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation offre la possibilité de déconnecter ou de désactiver rapidement l'accès à distance au système d'information dans un délai de 48 h ouvrées.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation offre la possibilité de déconnecter ou de désactiver rapidement l'accès à distance au système d'information dans un délai de 24 h ouvrées.

❖ Accès sans fil

AC-18-0 - Accès sans fil - V1R1

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est INTERDIT de connecter une borne WI-FI personnelle ou privée sur les réseaux des sites DGAC (NA et GP).

Environnement	R	O	J	B
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que toute mise en œuvre d'un réseau WI-FI au sein du domaine NA donne lieu à une étude de sûreté visant à identifier le niveau de risque associé à l'utilisation de ce type de réseau, et à définir des mesures de sûreté éventuellement spécifiques à l'utilisation de ce réseau autres que celles décrites dans ce document.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est INTERDIT de connecter un équipement ou un réseau Wi-Fi à cet environnement.

AC-18-1 - Authentification et chiffrement - V1R0

Environnement	R	O	J	B
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que toute installation d'un point d'accès Wi-Fi permettant de se connecter à un réseau local de l'organisation utilise au minimum le protocole WPA2 avec des certificats (802.1X et protocole EAP-TLS).

Dans le cas où l'utilisation d'un serveur d'authentification (802.1X) s'avère impossible, il est OBLIGATOIRE de mettre en œuvre le protocole WPA2 avec une clé partagée (PSK).

Dans ce cadre :

- Il est OBLIGATOIRE de maîtriser la gestion des clés,
- Il est OBLIGATOIRE de renouveler la clé partagée tous les deux mois, et dans les meilleurs délais suite à la perte ou à un vol d'un terminal disposant des informations de connexion,
- Il est OBLIGATOIRE de considérer cette clé partagée comme une donnée classifiée confidentielle DGAC
- Il est OBLIGATOIRE que la clé partagée dispose d'au moins 16 caractères avec au minimum 6 chiffres et 6 caractères alphabétiques

AC-18-3 - Désactivation des réseaux sans fil - V1R1

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation désactive les fonctionnalités de réseau sans fil internes intégrées aux composants du système d'information avant la délivrance et le déploiement des composants.

Environnement	R	O	J	B
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Dans la mesure du possible, il est RECOMMANDE que l'organisation établisse et mette en œuvre une politique de connexion au Wi-Fi qui n'activerait le Wi-Fi ou la connexion des usagers, que dans des plages horaires bien définies (i.e désactivation du Wi-Fi en dehors des horaires de bureaux par exemple).

AC-18-4 - Restreindre les configurations par les utilisateurs - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système interdise la connexion d'un équipement à un autre réseau que celui (ou ceux) sur lequel (lesquels) il est autorisé.

AC-18-5 - Antennes / niveaux de puissance de transmission - V1R0

Environnement	R	O	J	B
	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que la portée des points d'accès WI-FI soit strictement limitée au plus juste des besoins et ne pas permettre de connexion depuis une zone dont la sûreté ne peut être garantie.

Il est OBLIGATOIRE de vérifier/contrôler la portée effective des points d'accès.

Environnement	R	O	J	B
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que la portée des points d'accès WI-FI soit strictement limitée au plus juste des besoins et ne pas permettre de connexion depuis une zone dont la sûreté ne peut être garantie.

Il est OBLIGATOIRE de vérifier/contrôler la portée effective des points d'accès.

❖ **Contrôle d'accès depuis un ordinateur portable ou un mobile****AC-19-4 - Restrictions pour les informations classifiées - V1R1**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Si besoin d'accès à une information, il est OBLIGATOIRE que tout appareil non référencé soit connecté à un réseau dédié et cloisonné du système d'information de la DGAC.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est INTERDIT d'accéder au système d'information autrement que par des appareils mobiles référencés par l'organisation.

Sur les terminaux Wi-Fi, il est OBLIGATOIRE que les services et fonctionnalités qui ne sont pas indispensables au fonctionnement ou à la sécurité des terminaux soient désinstallés ou désactivés, et en particulier, il est OBLIGATOIRE de :

- Désactiver toute interface sans-fil autre que le Wifi (3G, Bluetooth, etc.)
- Désactiver des fonctionnalités de type connexion automatique à des réseaux sans fil.

AC-19-5 - Chiffrement complet des appareils mobiles - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les moyens de stockage de tout appareil mobile soient intégralement chiffrés

❖ Utilisation de systèmes d'information externes

AC-20-2 - Périphériques de stockage portables - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les périphériques de stockage amovibles soient fournis par l'administration, inventoriés et préalablement effacés et scannés avant toute connexion aux systèmes

AC-20-3 - Systèmes / composants / appareils non appartenant à l'organisation – V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est INTERDIT d'utiliser des systèmes/composants/appareils non référencés sur les systèmes d'information de l'organisation.

AC-20-4 - Périphériques de stockage accessibles en réseau - V1R1

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'utilisation de services de stockage externes (non gérés par la DGAC) respecte les mesures liées à la classification de l'information.

Dans ce cas où l'organisation fait appel à un prestataire d'information en nuage (cloud), il est OBLIGATOIRE que le prestataire respecte les exigences du référentiel SECNUMCLOUD de l'ANSSI ou équivalent.

❖ **Contenu accessible au public****AC-22-0 - Contenu accessible au public - V1R1**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation définisse une politique de gestion des informations accessibles au public en :

- Désignant des individus, seuls autorisés à publier des informations sur des systèmes accessibles au public,
- Formant les individus autorisés afin de s'assurer que les informations accessibles ne soient pas des informations classifiées,
- Organisant des revues des informations en préalable à leur publication,
- Organisant des revues des informations publiées.

SENSIBILISATION ET FORMATION

❖ Sensibilisation à la sécurité des systèmes d'Information

AT-2-0 - Sensibilisation à la sécurité des systèmes d'Information - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation dispense une sensibilisation de base à la sécurité pour tous les utilisateurs du système d'information :

- dans le cadre de la formation initiale pour les nouveaux utilisateurs ;
- lorsque requis par la modification du système d'information ;
- tous les 3 ans par la suite.

AT-2-1 - Exercices pratiques - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation inclut des exercices pratiques à la sécurité qui simulent des cyberattaques actuelles/réelles.

(exemple: ingénierie sociale pour la collecte d'informations, tentatives d'obtention d'accès non autorisé, simulation de l'impact de l'ouverture de pièces jointes malveillantes ou attaques de type "phishing" via des liens web malveillant envoyés par e-mail...)

❖ Formation à la sécurité des systèmes d'information

AT-3-0 - Formation à la sécurité des systèmes d'information - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le personnel de sécurité dispense une formation à la sécurité basée sur les rôles et responsabilités attribués au personnel de sécurité :

- avant d'autoriser l'accès au système d'information ou d'assigner des tâches à un exécutant ;
- lorsque requis par la modification du système d'information ;
- tous les 3 ans par la suite.

AT-3-3 - Formations pour les développeurs - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les développeurs soient en mesure d'effectuer un transfert de connaissance sur leurs systèmes pour toute personne contribuant aux phases de conception, de codage et développement, ainsi qu'aux phases de tests, au profit des exploitants ou d'autres parties prenantes.

Il est OBLIGATOIRE que les développeurs soient formés sur les techniques et bonnes pratiques liées au développement sécurisé et sur les vulnérabilités classiques liées au développement.

Journalisation et Traçabilité

❖ Événements de Journalisation

AU-2-0 - Événements de Journalisation - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système génère des événements de journalisation à minima pour les éléments suivants:

- L'activité locale sur un système
- Modification, création et destruction d'un utilisateur,
- Modification d'état du service concerné (démarrage, arrêt et redémarrage, plantage),
- Changement de configuration (du service, du matériel, etc.),
- Tentatives d'établissement, établissement et rupture de session (dans le cas d'un service impliquant une notion de connexion),
- Erreur de traitement du service [données absentes ou mal formées]
- Informations sur les utilisateurs (tentative de connexion, connexion, déconnexion, connexions concurrentes à partir de stations clientes différentes),
- Toute action ou exécution de fonctions, associée à une machine et/ou à un compte à privilèges élevés

Il est OBLIGATOIRE que tous les éléments listés ci-dessus soient notifiés à chaque occurrence de l'évènement.

Il est OBLIGATOIRE que la liste des éléments notifiés apparaisse dans les spécifications du système.

❖ Contenu des éléments de journalisation

AU-3-0 - Contenu des éléments de journalisation - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que tout évènement généré par le système contienne à minima les informations suivantes :

- Le type d'évènement (type d'action comme par exemple authentification, création, suppression),
- La date et l'heure précise de l'occurrence de l'évènement,
- L'identité de la source de l'évènement (adresses IP, nom d'hôte, nom du processus ou de la transaction, identification du processus ou de la transaction)
- L'identité du sujet de l'évènement (autant que possible comme par exemple le nom du processus, les comptes utilisateurs ou systèmes, les fichiers impliqués, etc.),
- Résultat de l'action décrite dans l'évènement (si l'action a été autorisée ou refusée),
- Description et/ou code erreur expliquant pourquoi l'action a été refusée,
- Commandes à privilèges qui ont été exécutées.

Il est RECOMMANDE que tout évènement généré par le système contienne les valeurs d'avant et d'après modification (lorsque le type d'évènement implique la mise à jour d'un élément).

AU-3-1 - Informations supplémentaires sur le contenu de la journalisation - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation fournisse et maintienne à jour une documentation référençant pour tous les événements applicatifs métier :

- Les informations contenues,
- Une note explicative permettant de modifier leur contenu.

AU-3-2 - Gestion centralisée des événements journalisés - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information dispose d'un outil de gestion permettant de configurer/paramétrer le contenu des événements générés.

❖ **Collecte des événements****AU-4-1 - Transfert des événements de journalisation - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les informations de journalisation soient envoyées sous un délai d'une minute maximum à un système dédié à cet effet : outil de collecte, de stockage et de corrélation de logs (SIEM).

Une copie de ses informations peut être stockée localement mais ces dernières ne serviront pas de référence.

❖ **Erreur de journalisation****AU-5-0 - Réponse aux échecs de journalisation - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système génère des alertes (warnings) en cas d'erreur d'enregistrement d'éléments de journalisation (événement devant donner lieu à des logs ou erreur dans le contenu même des logs) sous un délai d'une minute maximum.

AU-5-1 - Capacité de stockage des éléments de journalisation - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système génère des alertes (warnings) en cas de dépassement du seuil de stockage de 80% de la journalisation. Ces alertes DOIVENT être envoyées au SOC sous un délai d'une minute maximum.

❖ **Revue des journaux, analyse et notification****AU-6-0 - Revue des journaux, analyse et notification - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le *Security Operation Center* (SOC) génère des rapports d'analyse périodiques.

AU-6-5 - Capacité de corrélation et d'analyse - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est RECOMMANDE que l'analyse des événements de sécurité s'appuient sur (soient corrélées avec) des informations provenant des sources suivantes :

- Scans de vulnérabilités,
- Supervision système,
- Indicateur de performances.

AU-6-6 - Capacité de corrélation et d'analyse - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que les traces d'audit des accès physiques (événements des lecteurs de badges) soient centralisées dans le SIEM et corrélées avec les événements de sécurité afin d'identifier des comportements suspects.

AU-6-7 - Actions autorisées - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le *Security Operation Center* (SOC) exploite le système d'information de détection de la DGAC

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE qu'un prestataire qualifié PDIS (Prestataire de Détection d'Incidents de Sécurité) installe et exploite le système de détection qualifié ANSSI.

AU-6-8 - Analyse complète des commandes privilégiées - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que les machines utilisées pour l'analyse des commandes à privilèges contenues dans les événements soient connectées à un réseau physique dédié et séparées du système d'information DGAC.

AU-6-10 - Ajustement du niveau de reporting et d'analyse - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation ajuste le niveau d'analyse et de revue des événements en cas d'évolution avérée du niveau du risque. Cette évolution peut être introduite par des sources de confiances (autorités ou toutes autres sources crédibles).

❖ **Agrégation des événements et génération de rapports****AU-7-0 - Agrégation des événements et génération de rapports - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information agrège les événements et génère des rapports qui permettent, après coup, de revoir, analyser et investiguer sur des incidents de sécurité.

Il est INTERDIT d'altérer le contenu ou l'ordonnancement des événements.

AU-7-2 - Tri automatique et recherche – V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information permette de chercher dans les événements centralisés en fonction de leur contenu.

❖ **Horodatage****AU-8-0 – Horodatage - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que :

- le système d'information synchronise son horloge interne avec la référence de synchronisation horaire fournie selon le protocole NTP.
- le système d'information utilise l'horloge interne au système pour horodater les journaux d'événements et logs.
- le système de collecte et d'analyse dispose de sa propre synchronisation horaire et horodater tous les événements collectés.

❖ **Protection des journaux d'événements****AU-9-0 - Protection des journaux d'événements - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que le système de collecte sécurise les journaux d'information (événement) de tout accès non autorisé en lecture, en écriture (modification et suppression).

AU-9-2 - Sauvegarde des journaux sur des systèmes / composants physiques distincts - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que le système de stockage des événements sauvegarde toutes les 24 heures l'intégralité des événements bruts (événements non modifiés par le SIEM) reçus dans un espace de stockage physiquement séparé.

AU-9-3 - Protection cryptographique - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que le système de collecte et de stockage implémente un mécanisme de chiffrement des événements collectés, stockés et archivés.

AU-9-5 - Double autorisation - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est RECOMMANDE que l'organisation implémente une procédure et/ou un système de double autorisation en cas de suppression et déplacement des traces d'événements de journalisation et ce pour l'ensemble des événements générés par les systèmes critiques.

AU-9-6 - Accès en lecture seule - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que le système d'information autorise l'accès aux événements en lecture uniquement pour tous les utilisateurs à privilèges.

❖ Rétention des événements de journalisation

AU-11-0 - Rétention des événements de journalisation - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que la capacité de stockage des journaux des événements permette la rétention de ces informations pour une durée de 6 mois.

Il est OBLIGATOIRE que la capacité d'archivage des journaux des événements permette la rétention de ces informations pour une durée de 6 mois supplémentaires.

❖ **Génération des audits****AU-12-0 - Génération des audits - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les évènements définis en AU-2 et leurs contenus définis en AU-3 soient générés pour tous les composants du système d'information.

Il est OBLIGATOIRE que le système d'information autorise le SOC à sélectionner d'autres évènements générés par les composants spécifiques.

AU-12-2 - Formats normalisés - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le format et protocole des évènements soient compatibles avec les solutions SIEM du marché (SYSLOG, CEE, etc.).

Dans le cas où pour des raisons techniques les composants du système ne respectent pas ces formats, il est OBLIGATOIRE que le système de collecte (le système englobant les composants non interopérables) puisse en faire la conversion.

Evaluation de sécurité et Homologation

❖ Politiques et procédures d'évaluation et d'autorisation de sécurité

CA-1-0 - Politiques et procédures d'évaluation et d'autorisation de sécurité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place une politique d'homologation de ses systèmes.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que la politique d'homologation se conforme aux exigences édictées par l'ANSSI :

- Il est OBLIGATOIRE que l'organisation atteste que les risques pesant sur la sécurité du système ont été identifiés et que les mesures nécessaires pour le protéger sont mises en œuvre.
- Il est OBLIGATOIRE que l'organisation atteste que les risques résiduels ont été identifiés et acceptés par l'opérateur.
- Il est OBLIGATOIRE qu'un audit de la sécurité soit réalisé visant à vérifier l'application et l'efficacité des mesures de sécurité du système et notamment le respect des règles de sécurité mentionnées dans la présente PSSI. Il doit permettre d'évaluer le niveau de sécurité du système au regard des menaces et des vulnérabilités connues. Il comporte notamment la réalisation d'un audit d'architecture, d'un audit de configuration et d'un audit organisationnel et physique.

❖ Évaluations de sécurité

CA-2-0 - Évaluations de sécurité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation élabore un plan d'audit de sécurité qui décrit la portée de l'évaluation, les contrôles de sécurité et les améliorations de contrôle en cours d'évaluation, les procédures d'évaluation à utiliser pour déterminer l'efficacité du contrôle de la sécurité, l'environnement d'évaluation, l'équipe d'évaluation ainsi que leurs rôles et responsabilités.

Il est OBLIGATOIRE que l'organisation effectue des audits pour vérifier si les mesures et les contrôles sont correctement implémentés.

Il est OBLIGATOIRE que l'organisation produise un rapport d'audit de sécurité.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que Les rapports d'audit des systèmes soient classifiés confidentiels.

CA-2-1 - Évaluateurs indépendants - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place une équipe d'audit interne pour mener des audits de sécurité.

CA-2-2 - Évaluations spécialisées - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation détermine et valide quels sont les contrôles de sécurité utilisés lors d'un audit de sécurité au regard des environnements critiques.

CA-2-3 - Organisations externes - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation fasse appel à des auditeurs qualifiés PASSI (Prestataire d'Audit de la Sécurité des Systèmes d'Information).

❖ **Interconnexions système****CA-3-0 - Interconnexions système - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation formalise toute connexion de son SI avec d'autres SI (protocoles d'accord, lettre d'accord, clause contractuelle...) en précisant ; pour chaque interconnexion, les caractéristiques de l'interface, les besoins de sécurité et la nature des informations communiqués.

❖ **Plan d'action et jalons****CA-5-0 - Plan d'action et jalons - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation élabore un plan d'action afin de documenter les mesures correctives planifiées par l'organisation permettant de corriger les faiblesses ou les lacunes observées lors d'audit de sécurité (réduire ou éliminer le risque connu dans le système). Il est OBLIGATOIRE que l'organisation mette à jour ce plan d'actions en fonction des résultats d'audits, des analyses d'impact sur la sécurité et des activités de surveillance continue.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation élabore un plan d'action afin de documenter les mesures correctives planifiées par l'organisation permettant de corriger les faiblesses ou les lacunes observées lors d'audit de sécurité (réduire ou éliminer le risque connu dans le système). Il est OBLIGATOIRE que l'organisation mette à

jour ce plan d'actions tous les ans en fonction des résultats d'audits, des analyses d'impact sur la sécurité et des activités de surveillance continue.

CA-5-1 - Support d'automatisation pour l'exactitude / la devise - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que l'organisation utilise des outils automatisés pour s'assurer que le plan d'action soit à jour et facilement accessible.

❖ Autorisation de sécurité

CA-6-0 - Autorisation de sécurité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que tout système ait suivi le processus d'homologation défini dans la politique d'homologation de la DGAC.

❖ Contrôle continu

CA-7-0 - Contrôle continu - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place un SOC qui permettra de surveiller en continue l'état de la sécurité des systèmes d'information.

❖ Connexions système internes

CA-9-1 - Vérifications de conformité de sécurité - V1R1

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que L'organisation effectue des contrôles de conformité de sécurité sur les composants du système avant la connexion au système d'information.

Gestion de la configuration

❖ Configuration de base

CM-2-0 - Configuration de base - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation développe, documente et maintienne sous contrôle, une configuration de base du système d'information actuel.

CM-2-1 - Commentaires et mises à jour - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation définisse la fréquence et/ou les circonstances dans lesquelles la configuration de base est revue et mise à jour.

CM-2-3 - Maintien des configurations précédentes - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation conserve les versions antérieures des configurations de base du système afin de permettre la restauration.

CM-2-6 - Environnements de développement et de test - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que L'organisation maintienne une configuration de base pour le développement du système et les environnements de test gérés séparément de la configuration de base opérationnelle.

CM-2-7 - Configurer des systèmes, des composants ou des dispositifs pour les zones à haut risque - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation définisse et applique une configuration de base des appareils exposés à des risques élevés (voyages) et définisse les mécanismes de vérification lors du retour de ces appareils.

❖ Contrôle de changement de configuration

CM-3-0 - Contrôle de changement de configuration - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- a) Détermine les types de modifications apportées au système d'information contrôlé par la configuration ;

- b) Examine les modifications proposées par la configuration au système d'information et approuve ou désapprouve ces changements en tenant compte explicitement des analyses d'impact sur la sécurité ;
- c) Documente les décisions de changements des configurations associées au système d'information ;
- d) Mette en œuvre les modifications approuvées aux configurations dans le système d'information ;
- e) Conserve les enregistrements de modification aux configurations du système d'information ;
- f) Vérifie et examine les activités associées aux modifications des configurations du système d'information ; et
- g) Coordonne et surveille les activités de contrôle de changement de configuration.

CM-3-1 - Document automatisé / notification / interdiction des changements - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation utilise des mécanismes automatisés pour :

- a) Documenter les modifications ;
- b) Notifier [autorités d'approbation définies par l'organisation] des modifications proposées au système d'information et demander l'approbation du changement ;
- c) Souligner les modifications proposées au système d'information qui ont été approuvées et désapprouvées pour [Affectation : période définie par l'organisation] ;
- d) Interdire les modifications apportées au système d'information jusqu'à ce que les approbations désignées soient reçues ;
- e) Documenter toutes les modifications apportées au système d'information ; et
- f) Notifier [Affectation : personnel défini par l'organisation] lorsque les modifications approuvées au système d'information sont complétées.

CM-3-2 - Tester / valider / documenter les changements - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation teste, valide et documente les modifications apportées au système d'information avant de mettre en œuvre les modifications apportées au système opérationnel.

CM-3-5 - Réponse de sécurité automatisée - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information émette une alerte automatique si les configurations de base sont modifiées de manière non autorisées.

CM-3-6 - Gestion de la cryptographie - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation assure la gestion des artéfacts de mécanismes cryptographiques. (Validité des clés, certificats...)

❖ **Analyse d'impact sur la sécurité****CM-4-0 - Analyse d'impact sur la sécurité - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation analyse les modifications apportées au système d'information afin de déterminer les impacts potentiels sur la sécurité avant la mise en œuvre du changement.

CM-4-1 - Environnements de test distincts - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation analyse les modifications apportées au système d'information dans un environnement de test distinct avant la mise en œuvre dans un environnement opérationnel, en cherchant des impacts de sécurité en raison de défauts, de faiblesses, d'incompatibilité ou de mauvaises intentions.

CM-4-2 - Vérification des fonctions de sécurité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation vérifie, après la modification du système d'information, les fonctions de sécurité afin de s'assurer que les fonctions soient correctement implémentées, fonctionnent comme prévu et produisent les résultats souhaités en fonction des exigences de sécurité du système.

❖ **Restrictions d'accès au changement****CM-5-0 - Restrictions d'accès au changement - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation définisse, documente, approuve et applique les restrictions d'accès physiques et logiques liées aux modifications apportées au système d'information.

CM-5-1 - Application / vérification de l'accès automatisé - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information impose les restrictions d'accès et supporte l'audit des actions mis en œuvre.

CM-5-3 - Composants signés - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information empêche l'installation de logiciels sans vérification de la signature numérique à l'aide d'un certificat reconnu et approuvé par l'organisation.

CM-5-5 - Limiter les privilèges de production et d'exploitation - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que l'organisation limite les privilèges pour modifier les composants du système d'information et les informations liées au système dans un environnement de production ou opérationnel.

❖ **Paramètres de configuration****CM-6-0 - Paramètres de configuration - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- Établit et documente les paramètres de configuration pour les produits de technologie de l'information utilisés dans le système d'information en utilisant les guides de configurations;
- Implémente les paramètres de configuration ;
- Identifie, documente et approuve tout écart par rapport aux paramètres de configuration établis pour l'infrastructure réseau;
- Surveille et contrôle les modifications apportées aux paramètres de configuration conformément aux politiques et aux procédures de l'organisation.

CM-6-1 - Gestion / application / vérification centralisée automatisée - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que l'organisation utilise des mécanismes automatisés pour gérer, appliquer et vérifier de manière centralisée les paramètres de configuration pour les composants qui le supportent.

❖ **Limiter les fonctionnalités****CM-7-0 - Limiter les fonctionnalités - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système mette en œuvre des mesures de sûreté visant à réduire au minimum la surface d'attaque. Pour ce faire, il est OBLIGATOIRE que le système désactive les services et ports de

communications inutiles (non utilisés). Autant que possible, la surface d'attaque sera réduite en mettant en œuvre les principes ci-dessous:

- Minimiser le code exécutable par défaut,
- Restreindre les accès au code,
- Restreindre les privilèges d'exécution du code.

CM-7-1 - Examen périodique - V1R1

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation examine le système d'information pour identifier les fonctions, les ports, les protocoles et les services inutiles et / ou non sécurisés.

CM-7-4 - Logiciel non autorisé / liste noire - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation identifie et maintienne à jour une liste des programmes et logiciels dont l'exécution n'est pas autorisée sur les systèmes d'information de la DGAC.

❖ Inventaire des composants du système d'information

CM-8-0 - Inventaire des composants du système d'information - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation fournisse un inventaire comportant:

- les noms et les fonctions de chaque application installée sur les systèmes,
- les CPE (Common platform enumeration) des différents constituants logiciels et hardware,
- les plages d'adresses IP de sortie du système vers internet ou un réseau tiers,
- la description fonctionnelle et les lieux d'installation des systèmes,
- la description fonctionnelle des points d'interconnexion des systèmes, avec des réseaux tiers,
- la description des équipements et des fonctions de filtrage et de protection mis en œuvre au niveau de ces interconnexions,
- l'architecture des dispositifs d'administration du système (installation à distance, mise à jour, supervision, gestion des configurations),
- l'architecture et le positionnement des services de résolution de noms d'hôte, de messagerie, de relais internet et d'accès distant mis en œuvre.

CM-8-2 - Maintenance automatisée - V1R0

Environnement	R	O	J	B
	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation utilise des mécanismes automatisés pour aider à maintenir un inventaire actualisé, complet, précis et facilement disponible des composants du système d'information.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que l'organisation utilise des mécanismes automatisés pour aider à maintenir un inventaire actualisé, complet, précis et facilement disponible des composants du système d'information.

CM-8-5 - Pas de doublons des composants - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation vérifie que tous les composants du système d'information soient uniques.

CM-8-6 - Les configurations évaluées / les écarts approuvés - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation inclue les configurations des composants évalués et les écarts approuvés aux configurations déployées actuelles dans l'inventaire des composants du système d'information.

CM-8-7 - Dépôt centralisé - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation fournisse un référentiel centralisé pour l'inventaire des composants du système d'information.

Plan d'urgence

❖ Test du plan d'urgence

CP-4-0 - Test du plan d'urgence - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- teste le/les plan(s) d'urgence tous les ans (exercices étape par étape, checklist, simulations, exercices complets) afin de déterminer l'efficacité du plan et la capacité organisationnelle à l'exécuter ;
- passe en revue les résultats des tests (effets sur les activités organisationnelles, actifs et individus résultant des opérations d'urgence);
- lance/planifie des actions correctives si nécessaires.

CP-4-4 - Restauration complète / reconstitution - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation teste périodiquement le rétablissement complet d'un système afin que l'ensemble des activités décrites dans le plan de rétablissement soient testées au minimum une fois tous les 3 ans.

❖ Site secondaire

CP-7-0 - Site secondaire - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- mette en place un autre site secondaire distinct du site principal, pour permettre le transfert et la reprise des opérations et services essentiels à l'organisation en cas de sinistre sur le site principal. Il est OBLIGATOIRE que le transfert vers ce site soit effectué en moins de 4 heures après le sinistre repéré;
- s'assure que le matériel et les fournitures nécessaires pour transférer et reprendre les opérations soient disponibles sur le site secondaire ou que des contrats soient en place pour assurer la livraison sur le site dans le délai défini pour le transfert/la reprise;
- s'assure que le site secondaire fournisse des mesures de sécurité de l'information équivalentes à celles du site principal.

CP-7-1 - Séparation du site primaire - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le ou les sites secondaires identifiés par l'organisation soient séparés du site de traitement principal pour réduire l'exposition aux mêmes menaces (catastrophes naturelles, défaillances structurelles, cyberattaques).

❖ Services de télécommunications

CP-8-0 - Services de télécommunications - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information mette en œuvre des supports de télécommunication secondaires ou secours afin d'assurer la continuité des missions essentielles de l'organisation lorsque les services de télécommunication principaux ne sont pas disponibles.

CP-8-1 - Priorité de service - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation établisse des contrats de services de télécommunications principaux et secondaires qui contiennent des niveaux de service (SLA) conformes aux exigences de disponibilité de l'organisation.

CP-8-2 - Point unique de défaillance (SPOF) - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation installe des services de télécommunications secondaires pour réduire la probabilité de partager un point unique de défaillance avec les services de télécommunications principaux.

CP-8-4 - Plan d'urgence des fournisseurs - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- exige que les fournisseurs de services de télécommunications principaux et alternatifs disposent de plans d'urgence;
- examine le plan d'urgence du fournisseur pour s'assurer qu'il répond aux exigences de contingence;
- obtienne les preuves de test/formation du plan d'urgence par les fournisseurs de manière périodique.

CP-8-5 - Test des services de télécommunication secondaires - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation teste les services secours de télécommunication tous les ans.

❖ **Sauvegarde du système d'information****CP-9-0 - Sauvegarde du système d'information (RPO) - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que l'organisation effectue des sauvegardes d'informations des postes des utilisateurs de manière quotidienne.

Il est OBLIGATOIRE que l'organisation :

- effectue des sauvegardes d'informations des systèmes (état du système, système d'exploitation, applicatifs et licences, données) de manière quotidienne ;
- protège la confidentialité, l'intégrité et la disponibilité des informations de sauvegarde dans les emplacements de stockage (ex : chiffrement des supports, stockage sécurisé).

CP-9-1 - Tests de fiabilité / intégrité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation teste régulièrement les informations de sauvegarde pour vérifier la fiabilité des médias et l'intégrité de l'information.

CP-9-2 - Test de restauration par échantillonnage - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation utilise un échantillon d'informations de sauvegarde pour la restauration des fonctions sélectionnées dans le cadre du test du plan d'urgence.

CP-9-3 - Stockage séparé pour des informations critiques - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation stocke des copies de sauvegarde dans des systèmes de backup secondaires situés dans un local séparé.

CP-9-7 - Double autorisation - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation applique une double autorisation pour la suppression ou la destruction de sauvegardes.

❖ **Récupération et reconstitution des systèmes d'information****CP-10-4 - Restauration dans le délai imparti - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation s'assure que l'ensemble des sauvegardes puissent restaurer le système dans un état opérationnel connu et cohérent.

CP-10-6 - Protection des composants - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place des sauvegardes et permettre la restauration des paramètres des matériels et les logiciels (dont firmware).

Identification et Authentification

❖ Identification et authentification des usagers

IA-2-0 - Identification et authentification (utilisateurs organisationnels) - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que Le système identifie et authentifie de manière unique les utilisateurs et les services de l'organisation.

Il est OBLIGATOIRE que l'authentification des utilisateurs repose sur l'utilisation de certificats électroniques gérés par une IGC.

Il est RECOMMANDE que l'authentification des services repose sur l'utilisation de certificats électroniques gérés par une IGC.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que Les comptes permettant de manipuler les attributs sûreté soient soumis à double authentification, ou à une authentification de type PIV.

IA-2-1 - Accès réseau aux comptes privilégiés - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Selon ses attributions, chaque utilisateur peut disposer de plusieurs comptes sur des domaines fonctionnels et techniques différents en respectant le principe de séparation des responsabilités.

Il est OBLIGATOIRE que la configuration des comptes d'administration ou à privilèges soit réalisée à partir d'un serveur dédié à la Gestion des Accès.

Il est OBLIGATOIRE que Les comptes permettant de manipuler les attributs sûreté soient soumis à double authentification, ou à une authentification de type PIV (Personal Identity Verification).

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Lorsque des raisons opérationnelles ne permettent pas d'utiliser des comptes individuels (accès MO et contrôleur), il est INTERDIT d'accéder au SI autrement qu'à partir d'interfaces spécifiques et dédiées localisées dans des zones de sûreté physique à accès restreint et contrôlé.

IA-2-3 - Accès local aux comptes privilégiés - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE qu'un compte local « SECOURS » reste instancié sur chaque système.

Il est OBLIGATOIRE que son utilisation soit strictement réservée en cas de perte, d'oubli ou de non accès au service d'authentification centralisée conformément à la consigne "Gestion du compte local SECOURS".

Il est OBLIGATOIRE que ce type de compte soit lié à une entité physique (une personne), et soit utilisé uniquement par des personnes clairement identifiées, disposant de la légitimité et des compétences appropriées.

IA-2-6 - Accès réseau à des comptes privilégiés - périphérique distinct - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'authentification par certificat repose sur des tokens cryptographiques.

IA-2-8 - Accès réseau aux comptes privilégiés - résistant aux replays - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système mette en place une authentification robuste au jeu. (Cela peut se faire par synchronisation temporelle ou par des systèmes de question réponse (jetons d'authentifications KERBEROS) ou autres Single Sign On.)

IA-2-10 - authentification unique - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que la mise en œuvre du *Single sign on* (SSO) repose sur le guide SSO.

IA-2-11 - Accès distant - dispositif distinct - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les accès distants (ex : ssh, RDP...) soient authentifiés.

IA-2-12 - Acceptation des références piv - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que les supports de stockage des certificats soient conformes au modèle PIV (Personal Identity Verification).

❖ Identification et authentification des équipements

IA-3-0 - Identification et authentification des équipements - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Dans le cas où les conditions physiques d'hébergement ne sont pas standards (à spécifier, ex : dans les bureaux), Il est OBLIGATOIRE que les équipements connectés au réseau soient authentifiés.

❖ Gestion des identifiants

IA-4-0 - Gestion des identifiants - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre un processus de gestion des accès prenant en compte :

- la validation de la demande en application du principe de moindre privilège,
- la mise en œuvre, la traçabilité et la surveillance des accès
- la gestion des départs /mutation /changement de rôle.

IA-4-1 - Interdire les identifiants de compte en tant qu'identifiants publics - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est INTERDIT d'utiliser des identifiants de compte système identiques à des identifiants publics pour les comptes de courrier électronique individuels.

IA-4-4 - Identifier le statut de l'utilisateur - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les certificats d'authentification incluent le statut [interne/externe DGAC...] et la fonction [rôle dans l'organisation] de l'individu identifié.

❖ Gestion des authentifiants

IA-5-0 - Gestion des authentifiants - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Lorsque des raisons techniques ou opérationnelles ne permettent pas l'utilisation de certificats, Il est OBLIGATOIRE que les accès aux ressources se fassent au moyen d'un mécanisme d'authentification basé sur un élément secret:

Le cas échéant, Il est OBLIGATOIRE que l'organisation respecte les règles de gestion suivantes :

- modification des mots de passe par défaut lors de la première utilisation,
- interdiction de réutiliser les mots de passes entre comptes privilégiés et un compte non privilégié,
- définition des durées de vie moyenne d'authentification ,
- potentiellement vérifier et empêcher la réutilisation d'anciens mots de passe.
- choisir un mot de passe suivant règles édictées par l'ANSSI.

Il est OBLIGATOIRE que les systèmes :

- vérifient de la complexité des mots de passe,
- ne montrent jamais les mots de passe en clair,
- ne stockent que des représentations chiffrées (hash) des mots de passe,
- permettent la modification du mot de passe autant de fois que nécessaires.

Il est INTERDIT qu'un mot de passe du fabricant ou de l'intégrateur soit présent sur l'équipement lorsque celui-ci est déployé.

Il est OBLIGATOIRE de changer les mots de passe au maximum tous les 6 mois.

IA-5-1 - Authentification par mot de passe - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Lorsque la ressource ne permet pas de modifier l'élément secret d'authentification, il est OBLIGATOIRE que l'opérateur mette en place un contrôle d'accès physique à la ressource concernée ainsi que des mesures de traçabilité des accès.

IA-5-2 - Authentification basée sur IGC - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'identification des usagers soit basée sur l'IGC nationale.

Pour authentification par certificat, il est OBLIGATOIRE que le système :

- valide le certificat en établissant un chemin de confiance vers une autorité de certification reconnue et en s'assurant de sa non révocation;
- vérifie l'identité de l'utilisateur par l'utilisation de la clef privée correspondante ;
- connecte l'identité authentifiée à son compte utilisateur.

IA-5-3 - Enregistrement en personne ou en tiers de confiance - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place une IGC.

IA-5-7 - Aucun authentifiant statique non chiffré intégré - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est INTERDIT que les systèmes stockent les mots de passes en dur dans les codes ou fichiers de configuration.

❖ **Commentaires d'authentification****IA-6-0 - Commentaires d'authentification - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information minimise le retour d'information pendant le procédé d'authentification afin de protéger cette information d'une exploitation non autorisée.

❖ **Authentification du module cryptographique****IA-7-0 - Authentification du module cryptographique - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les modules cryptographiques utilisés pour authentifier les administrateurs sûreté soient compatibles OPENSIC (privilegier PIV).

❖ **Identification et authentification des services****IA-9-0 - Identification et authentification des services - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système permette d'identifier et authentifier les services externes utilisés.

IA-9-1 - échange d'informations - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation s'assure que les fournisseurs de services reçoivent, valident et transmettent les informations d'identification et d'authentification.

Réponse aux incidents

❖ Politique et procédures d'intervention en cas d'incident

IR-1-0 - Politique et procédures d'intervention en cas d'incident - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation déclare les incidents suivants à l'ANSSI :

- Transmission illicite de données entre un système critique et un autre,
- Maintien illicite d'un système,
- Accès illicite à un système,
- Mise en œuvre d'un code malveillant installé sur un système,
- Atteinte à la disponibilité d'un système d'origine inconnue ou malveillante,
- Modification illicite d'un site internet nécessaire au fonctionnement d'un système,
- Collecte illicite de données permettant d'obtenir des droits d'accès privilégiés à un système,
- Dysfonctionnement d'un système, lié notamment à une panne matérielle ou logicielle, susceptible d'affecter significativement la sécurité ou le fonctionnement du système,
- Utilisation illicite des ressources du système
- Manquement à la politique de sécurité d'un système susceptible d'affecter significativement la sécurité ou le fonctionnement du système,
- Tentative d'attaque informatique ciblant un système et présentant un caractère particulièrement inhabituel,
- Tentative d'attaque informatique ciblant un système et menée de façon répétitive pendant une période de temps limité,
- Tentative d'attaque informatique s'avérant particulièrement complexe et conçue pour cibler spécifiquement un système.

Il est OBLIGATOIRE que l'organisation tienne à jour et mette en œuvre une procédure de gestion de crises en cas d'attaques informatiques majeures.

❖ Formation sur la réponse aux incidents

IR-2-0 - Formation sur la réponse aux incidents - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation dispense une formation en réponse aux incidents aux utilisateurs du système d'information en accord avec les rôles et les responsabilités assignés.

❖ **Gestion des incidents****IR-4-0 - Gestion des incidents - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- Il est OBLIGATOIRE que l'organisation :
- Mette en œuvre une capacité de traitement des incidents pour les incidents de sécurité comprenant la préparation, la détection et l'analyse, le confinement, la suppression et la récupération;
- Coordonne les activités de traitement des incidents avec les activités de planification d'urgence; et
- Intègre les leçons tirées des activités de traitement des incidents en cours dans les procédures de réponse aux incidents, la formation et les tests, et mettre en œuvre les modifications qui en résultent.

IR-4-1 - Processus automatisés de traitement des incidents - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation utilise des mécanismes automatisés pour soutenir le processus de traitement des incidents (ex: Systèmes de gestion des incidents en ligne).

IR-4-2 - Reconfiguration dynamique - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation tienne à jour et mette en œuvre une procédure de gestion de crises en cas d'attaques informatiques majeures décrivant les mesures suivantes:

- appliquer une configuration système afin d'éviter les attaques ou d'en limiter les effets. Cette configuration peut viser notamment:
 - o à proscrire l'utilisation de supports de stockage amovibles ou la connexion d'équipements nomades aux systèmes d'information de l'opérateur;
 - o à installer une mesure correctrice de sécurité sur un système d'information particulier;
 - o à imposer un protocole de routage;
- mettre en place des règles de filtrage sur les réseaux ou des configurations particulières sur les équipements terminaux. Cette mesure peut viser notamment:
 - o à effectuer des restrictions d'accès sous forme de listes blanches et de listes noires d'utilisateurs;
 - o à bloquer les échanges de fichiers d'un type particulier;
 - o à isoler de tout réseau des sites internet, des applications, ou des équipements informatiques de l'opérateur en sollicitant le cas échéant l'appui des opérateurs publics de communications électroniques;
- isoler du réseau internet les systèmes d'information de l'opérateur. Cette mesure impose de déconnecter physiquement ou logiquement les interfaces réseau des systèmes d'information concernés.

IR-4-8 - Corrélation avec des organisations externes - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation se coordonne avec l' ANSSI pour corréler et partager les information de réponse aux incidents dans le but de sensibiliser l'organisation aux incidents et de répondre aux incidents plus efficacement.

❖ **Suivi des incidents****IR-5-0 - Suivi des incidents - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation suive et documente les incidents de sécurité du système d'information.

IR-5-1 - Suivi automatisé / collecte / analyse de données - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation utilise des mécanismes automatisés pour faciliter le suivi des incidents de sécurité, la collecte et l'analyse de l'information sur les incidents.

❖ **Rapports sur les incidents****IR-6-0 - Rapports sur les incidents - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation sensibilise son personnel afin qu'il puisse signaler les incidents de sécurité soupçonnés et indiquer les informations sur les incidents de sécurité à l'organisation/au personnel s'occupant de la réponse aux incidents.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation conserve les relevés techniques relatifs aux analyses des incidents pendant une durée d'au moins six mois. Elle tient ces relevés techniques à la disposition de l'ANSSI.

❖ **Assistance en cas d'incident****IR-7-0 - Assistance en cas d'incident - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les AIG et ASSI soient en mesure de faire le lien entre la cellule de gestion de crise et les utilisateurs.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que l'organisation procède au traitement des incidents en s'appuyant sur les exigences du référentiel PRIS (Prestataire de Réponse aux Incidents de Sécurité).

Maintenance

❖ Maintenance de contrôle

MA-2-0 - Maintenance contrôlée - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- planifie, exécute, documente et examine les registres de maintenance et de réparation sur les composants matériels et logiciels du système d'information conformément aux spécifications du fabricant ou du fournisseur et / ou aux exigences de l'organisation;
- approuve et surveille toutes les activités de maintenance;
- efface sur les équipements toutes les informations avant maintenance ou réparations hors site;
- vérifie que tous les contrôles de sécurité fonctionnent correctement suite aux opérations de maintenance ou de réparation;
- inclue les informations relatives à la maintenance (date et heure de la maintenance, nom des individus ou du groupe effectuant l'entretien, description de la maintenance effectuée...) dans les registres de maintenance.

MA-2-2 - Activités de maintenance automatisées - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation:

- mette en place des mécanismes automatisés pour planifier, piloter et documenter les opérations de maintenances et de réparations;
- produise des enregistrements à jour, précis et complets de toutes les actions de maintenance et de réparation demandées, programmées, en cours et complétées.

❖ Outils de maintenance

MA-3-0 - Outils de maintenance - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation maîtrise les outils de maintenance afin de s'assurer de l'innocuité vis-à-vis du système d'information.

MA-3-1 - Inspection des outils - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation inspecte les outils de maintenance modifiés de façon non autorisée par le personnel de maintenance.

MA-3-2 - Inspection des supports - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation vérifie que les supports contenant des programmes de diagnostic et de test pour la maintenance ne contiennent pas de code malveillant et ce avant que les supports soient utilisés dans le SI.

MA-3-3 - Mise au rebut non autorisée de supports - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE qu'un équipement contenant des données non chiffrées quitte le SI. Ainsi :

- Il est OBLIGATOIRE que les supports d'information soient détruits ou effacés avant tout envoi en maintenance externe ou mise au rebut
- si ce n'est pas possible (équipement défectueux), Il est OBLIGATOIRE que l'équipement soit détruit ou conservé en sécurité

De plus, Il est OBLIGATOIRE que les matériels en retour de maintenance soient systématiquement être réinitialisés

MA-3-4 - Restriction sur l'utilisation des outils - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation restreigne l'utilisation des outils de maintenance au seul personnel autorisé.

❖ **Maintenance non locale****MA-4-0 - Maintenance non locale - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- approuve et contrôle les activités de maintenances non locales (ex: internet) et de diagnostic ;
- permette l'utilisation d'outils de maintenances non locales et de diagnostic uniquement système d'information cela est conforme à la politique organisationnelle et est documenté dans le plan de sécurité du système d'information ;
- mette en place des authentifications fortes lors de l'établissement de sessions de maintenance non locale et de diagnostic (ex. : PKI, certificats, biométrie) ;
- conserve les enregistrements des activités de maintenance non locale et de diagnostic ;
- ferme les sessions et les connexions réseau lorsque la maintenance non locale est effectuée.

MA-4-2 - Documenter la maintenance non locale - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation documente les procédures à suivre pour l'utilisation des connexions de maintenance non locale et de diagnostic.

MA-4-3 - Sécurité / assainissement comparables - V1R1

Environnement	R	O	J	B
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que l'organisation :

- exige que les services de maintenance non locale et de diagnostic soient réalisés depuis un système d'information et via des systèmes, outils, équipements mettant en œuvre des mesures/fonctions de sécurité comparables à celle du système d'information pris en charge ; ou
- retire le composant devant être pris en charge par les services de maintenance, assainir le composant avant son retrait et l'inspecter avant sa reconnexion au système d'information (SI).

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- exige que les services de maintenance non locale et de diagnostic soient réalisés depuis un système d'information et via des systèmes, outils, équipements mettant en œuvre des mesures/fonctions de sécurité comparables à celle du système d'information pris en charge ; ou
- retire le composant devant être pris en charge par les services de maintenance, assainir le composant avant son retrait et l'inspecter avant sa reconnexion au système d'information (SI).

MA-4-5 - Approbations et notifications - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation valide les modalités d'accès et de traçabilité pour la maintenance non locale.

MA-4-6 - Protection cryptographique - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que le système mette en œuvre des mécanismes cryptographiques pour protéger l'intégrité et la confidentialité des canaux de communication utilisés pour les activités de maintenance non locale et de diagnostic.

❖ **Personnel de maintenance****MA-5-0 - Personnel de maintenance - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- établit un processus pour la gestion des autorisations du personnel de maintenance sur le système d'information;
- maintient à jour une liste des personnels de maintenance autorisés;
- s'assure que le personnel de maintenance non escorté dispose des autorisations d'accès requises ;
- désigne le personnel de l'organisation disposant des autorisations d'accès et les compétences techniques requises pour superviser les activités du personnel de maintenance qui ne disposent pas des autorisations d'accès requises.

MA-5-3 - Exigences de citoyenneté pour les systèmes classifiés - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation s'assure que le personnel chargé des activités de maintenance et de diagnostic sur un système d'information traitant, stockant ou transmettant des informations manipulées par les systèmes ne présente pas de risques inhérents à la personne.

MA-5-4 - Ressortissants étrangers - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation fasse en sorte :

- d'employer des ressortissants étrangers ayant les habilitations de sécurité appropriées pour effectuer les activités de maintenance et de diagnostic sur les systèmes d'information classifiés uniquement lorsque les systèmes sont conjointement détenus et exploités par la France et les gouvernements alliés étrangers, ou détenus et exploités uniquement par les gouvernements alliés étrangers ;
- documenter dans les mémorandums d'accords l'ensemble des approbations, consentements et conditions opérationnelles détaillées concernant l'emploi des ressortissants étrangers pour mener des activités de maintenance et de diagnostic sur les systèmes d'information classifiés.

MA-5-5 - Maintenance non liée au système - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation s'assure que le personnel non escorté exécutant des activités de maintenance, non directement associées avec le système d'information, mais dans la proximité physique du système, dispose d'autorisations d'accès requises.

Protection des médias

❖ Marquage des supports

MP-3-0 - Marquage des supports - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation marque les médias de stockage afin d'identifier soit :

- le niveau et classification d'information contenue,
- le type d'utilisation autorisée (clés USB blanche, bureautique...).

MP-4-0 - Stockage des médias - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation identifie individuellement chaque support amovible réinscriptible.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que Les supports amovibles réinscriptibles connectés aux systèmes soient utilisés exclusivement pour les besoins de ces systèmes.

MP-4-2 - Accès restreint au travers de mécanismes automatisés - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation définisse et implémente une procédure sur la classification de l'information définissant les mesures de sureté à appliquer en prenant de la durée de vie de l'information

❖ Protection cryptographique

MP-5-4 - Protection cryptographique - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que Les médias soient chiffrés. Lorsque des raisons techniques ou opérationnelles ne le permettent pas, il est OBLIGATOIRE que des mesures particulières de protection de ces médias soient définies:

- envoi par pli sécurisé ou information répartie sur plusieurs envois ou plusieurs types de support,
- transport par l'intermédiaire d'un personnel ou un tiers de confiance.

❖ **Désinfection des médias****MP-6-0 - Désinfection des médias - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Avant chaque utilisation de supports amovibles, Il est OBLIGATOIRE que l'organisation analyse leur contenu, notamment à la recherche de code malveillant et mette en place des mécanismes de protection sur ces supports.

MP-6-1 - Analyser / approuver / tracer / documenter / vérifier - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les outils permettant d'analyser le contenu des supports amovibles à la recherche de code malveillant, tracent les opérations effectuées.

MP-6-3 - Techniques non destructrices - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation analyse le contenu à la recherche de code malveillant des supports de stockage portables dès que ces derniers sont fournis par des entités tierces et avant toute connexion au système d'information.

MP-6-6 - Destruction des médias - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation s'assure de la destruction des données sur les médias avant toute décommissions ou réparation.

❖ **Utilisation des médias****MP-7-0 - Utilisation des médias - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que l'organisation restreigne l'utilisation des médias de type (USB, mobile...) sur les systèmes sensibles.

Protection Physique et Environnementale

❖ Autorisations d'accès physique

PE-2-0 - Autorisations d'accès physique - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☒

Il est OBLIGATOIRE que l'organisation :

- définisse, approuve et maintienne une liste de personnes ayant une autorisation d'accès aux locaux hébergeant le SI;
- détaille dans cette liste les droits d'accès de chacune des personnes autorisées;
- émette des accréditations pour l'accès aux locaux;
- revoit annuellement la liste des autorisations;
- supprime les droits d'accès individuels quand l'accès aux locaux n'est plus nécessaire.

PE-2-1 - Accès par poste / rôle - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☒

Il est OBLIGATOIRE que l'organisation autorise l'accès physique aux locaux hébergeant le système d'information aux personnes et des rôles.

PE-2-2 - Deux formes d'identification - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☒

Il est OBLIGATOIRE que l'organisation demande une forme d'identification pour l'accès des visiteurs aux locaux hébergeant le SI.

PE-2-3 - Restreindre l'accès sans escorte - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☒

Il est OBLIGATOIRE que l'organisation autorise l'accès au personnel, n'ayant pas les autorisations d'accès aux locaux hébergeant le SI, uniquement s'ils sont accompagnés et surveillés, et ce pendant la durée de présence sur site.

❖ **Contrôle des accès physiques****PE-3-0 - Contrôle des accès physiques - V1R0**

Environnement	R	O	J	B
	☒	☒	☒	☒

Il est OBLIGATOIRE que l'organisation :

- mette en œuvre des d'accès physiques aux points d'entrée/sortie des zones de sécurité physiques et :
 - vérifie les autorisations d'accès individuel avant d'accorder les droits d'accès aux locaux hébergeant le système d'information;
 - contrôle les entrées/sorties;
- tienne à jour les registres d'accès physiques ;
- fournisse les moyens de contrôle d'accès aux zones définies comme accessibles au public;
- accompagne les visiteurs et surveille leur activité;
- sécurise les clés, les combinaisons et autres dispositifs d'accès physique;
- fasse l'inventaire des dispositifs d'accès physiques tous les ans;
- modifie les codes d'accès et les clés tous les ans et/ou dès lors que des clés sont perdus, des codes sont compromis ou que des personnes quittent l'organisation.

PE-3-1 - Accès au système d'information - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☒

Il est OBLIGATOIRE que l'organisation applique des autorisations d'accès physique au système d'information en plus des contrôles d'accès physique aux locaux hébergeant le SI pour [définir; ex: espaces physiques définis par l'organisation contenant un ou plusieurs composants du système d'information (par exemple, les salles de serveurs, les zones de stockage des médias, les centres de données et de communications)].

PE-3-2 - Limites des installations et des systèmes d'information - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☒

Il est OBLIGATOIRE que l'organisation effectue un audit sur la sécurité physique tous les 3 ans.

PE-3-3 - Gardes / alarmes / surveillance continue - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☒

Il est OBLIGATOIRE que l'organisation emploie des gardes et/ou utilise des alarmes pour surveiller 24/7 tous les points d'accès physiques aux locaux hébergeant le système d'information.

PE-3-4 - Baies verrouillables - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☒

Il est OBLIGATOIRE que l'organisation utilise des baies verrouillables pour stocker des équipements et composants du système d'information dans le cas où le contrôle d'accès physique ne répondrait pas aux exigences de cette PSSI. Pour les systèmes noirs, Il est OBLIGATOIRE que les baies soient verrouillées.

PE-3-5 - Autoprotection - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation effectue une inspection des équipements serveur et réseau du système d'information afin de détecter la présence d'équipements inconnus.

❖ **Contrôle d'accès aux moyens de transmission****PE-4-0 - Contrôle d'accès aux moyens de transmission - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place des placards de câblage verrouillés / prises de secours verrouillées ou dans des locaux sécurisés pour sécuriser les transmissions des informations du système d'information (câblage et équipements réseau).

❖ **Contrôle d'accès aux périphériques de sortie****PE-5-0 - Contrôle d'accès aux périphériques de sortie - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation restreigne l'accès aux périphériques de sortie du système d'information (imprimantes, copieurs, scanners, télécopieurs, vidéo projecteurs...).

PE-5-3 - Marquage des périphériques de sortie - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation identifie et référence les périphériques de sortie (ex: étiquetage).

❖ **Suivi de l'accès physique****PE-6-0 - Suivi de l'accès physique - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre un dispositif de détection d'intrusion dans les locaux contenant les composants physiques du système d'information y compris les composants, les supports de données et les équipements de liaisons, en dehors des périodes d'utilisation opérationnelle.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre un dispositif de détection d'intrusion en temps réel dans les locaux contenant les composants physiques du système d'information en dehors des périodes d'utilisation opérationnelle.

Les locaux contenant les composants, les supports de données et les liaisons utilisées pour les sauvegardes des données ne sont concernés par cette obligation que si les informations sauvegardées ne sont pas chiffrées.

Les locaux contenant les équipements terminaux des utilisateurs ne sont concernés par cette obligation que si les équipements contiennent des données sensibles non chiffrées ou peuvent accéder au système d'information sans authentification forte.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre pendant les périodes d'utilisation opérationnelle un dispositif de détection de présence anormale dans les locaux contenant les composants physiques du système d'information pour lesquels l'exploitation ne nécessite qu'une présence occasionnelle.

Les locaux contenant les composants, les supports de données et les liaisons utilisées pour les sauvegardes des données ne sont concernés par cette obligation que si les informations sauvegardées ne sont pas chiffrées.

PE-6-1 - Alarmes d'intrusion / équipement de surveillance - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation supervise les alarmes d'intrusion physique et les équipements de surveillance.

PE-6-3 - Vidéosurveillance - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation emploie une surveillance vidéo des salles techniques et conserver les enregistrements pendant 6 mois. Il est OBLIGATOIRE que les systèmes de vidéosurveillance rentrent dans le dispositif RGPD.

❖ Enregistrements d'accès des visiteurs

PE-8-0 - Enregistrements d'accès des visiteurs - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation enregistre chaque visiteur pénétrant dans les locaux contenant les composants physiques du système d'information.

Les locaux contenant les composants, les supports de données et les liaisons utilisées pour les sauvegardes des données ne sont concernés par cette obligation que si les informations sauvegardées ne sont pas chiffrées.

Il est OBLIGATOIRE que l'organisation examine périodiquement la liste des visiteurs enregistrés.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation utilise un système d'enregistrement numérique pour faciliter l'examen de la liste des visiteurs.

❖ Équipement électrique et câblage

PE-9-0 - Équipement électrique et câblage - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation protège les dispositifs utilisés pour l'alimentation électrique des composants du système d'information contre des dommages et la destruction.

PE-9-1 - Câblage redondant - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation utilise deux chemins de câblage indépendants pour amener l'énergie électrique aux composants du système d'information.

PE-9-2 - Contrôle automatique de la tension - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation emploie des dispositifs de contrôle automatique de la tension électrique des systèmes du système d'information.

❖ Arrêt d'urgence

PE-10-0 - Arrêt d'urgence - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre dans les locaux contenant des concentrations de composants de système d'information (par exemple, les centres de calculs, salles de serveur, salles d'unité centrale), des dispositifs permettant de couper à distance l'alimentation électrique de n'importe quel composant qui peut fonctionner mal (par exemple, en raison d'un feu électrique) ou qui est menacé (par exemple, en raison d'une fuite d'eau) sans mettre en danger le personnel.

• Alimentation de secours

PE-11-0 - Alimentation de secours - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre une alimentation électrique de secours permettant :

- de réaliser un arrêt maîtrisé les composants du système d'information en cas de perte de l'alimentation électrique primaire;
- en cas de perte prolongée de l'alimentation électrique primaire ;
- de faire fonctionner de façon autonome le système d'information permettant de respecter le besoin de disponibilité du système d'information.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre une alimentation électrique de secours permettant :

- en cas de perte prolongée de l'alimentation électrique primaire;
- de faire fonctionner de façon autonome la climatisation des locaux informatiques.

PE-11-2 - Alimentation alternative à long terme - autonome - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre une alimentation électrique de secours permettant de faire fonctionner de façon autonome tous les moyens mis en œuvre pour la détection d'intrusion et le contrôle d'accès pendant une durée de 96 heures en cas de perte prolongée de l'alimentation électrique primaire.

❖ Éclairage d'urgence

PE-12-0 - Éclairage d'urgence - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre un dispositif d'éclairage alternatif qui est activé en cas de panne de l'alimentation électrique primaire et qui permet de poursuivre l'exploitation.

❖ Protection contre le feu

PE-13-0 - Protection contre le feu - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

En complément des moyens de protection contre l'incendie du bâtiment, Il est OBLIGATOIRE que l'organisation définisse, installe et maintienne en fonctionnement des moyens de détection et d'extinction d'incendie protégeant les composants du système d'information.

PE-13-1 - Dispositifs / systèmes de détection - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation installe et maintienne en fonctionnement un dispositif automatique de détection et d'alerte d'incendie.

PE-13-3 - Extinction automatique des incendies - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place des systèmes d'extinction automatique d'incendie.

PE-13-4 - Inspections - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation s'assure que ses locaux soient soumis à une inspection annuelle de ses installations anti-incendie par des inspecteurs autorisés et qualifiés, et que les lacunes identifiées soient résolues rapidement.

❖ **Contrôles de température et d'humidité****PE-14-0 - Contrôles de température et d'humidité - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation prenne les dispositions pour maintenir la température et l'humidité en dessous des valeurs maximales autorisées pour le fonctionnement des composants du système d'information et génère une alerte en cas de dépassement.

Il est OBLIGATOIRE que l'organisation mette en place un dispositif d'affichage de la température dans les locaux informatiques.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place un dispositif de climatisation secondaire permettant de pallier l'indisponibilité du dispositif de climatisation principal.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place un dispositif automatique d'allumage du dispositif de climatisation secondaire en cas de défaillance du dispositif de climatisation principal.

PE-14-1 - Contrôles automatiques - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que la température et l'humidité des salles serveurs soient contrôlées automatiquement tous les 3 jours. Il est OBLIGATOIRE qu'une alarme soit déclenchée lors de variations potentiellement dangereuses pour le personnel ou les équipements.

PE-14-2 - Surveillance avec alarmes / notifications - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place un dispositif d'enregistrement de la température et de l'humidité et d'alerte lorsque la température ou l'humidité approche la valeur maximale autorisée.

❖ Protection contre les dommages causés par l'eau

PE-15-0 - Protection contre les dommages causés par l'eau - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place un dispositif de détection de présence d'eau dans les locaux informatiques et techniques.

PE-15-1 - Support d'automatisation - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation emploie des mécanismes automatisés pour détecter la présence d'eau dans les environs du système d'information et alerter le personnel (exemple : capteurs de détection de l'eau, alarmes, systèmes de notification).

❖ Livraison et enlèvement

PE-16-0 - Livraison et enlèvement - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place un dispositif automatique de détection et d'alerte de présence d'eau dans les locaux informatiques et techniques.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre un dispositif de coupure automatique des robinets d'isolement en cas de fuite significative d'eau pouvant menacer des composants du système d'information.

Planification

❖ Diversité des fournisseurs

PL-8-2 - Diversité des fournisseurs - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation diversifie les solutions de sécurité (firewall, antivirus, IDS) pour la conception de ses architectures sécurisées:

L'objectif étant :

- de limiter le risque lié à une/des vulnérabilités communes à plusieurs équipements pouvant impacter l'intégrité, confidentialité, disponibilité du système d'information;
- augmenter la capacité de détection de malwares de l'organisation.

Sécurité des Personnels

❖ Indice de risque

PS-2-0 - Indice de position de risque - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation identifie un niveau de "risque" à tous les postes de l'organisation afin d'établir les critères de sélection et attributs du poste en question comme le besoin en formation, les accréditations de confidentialité, etc. Il est OBLIGATOIRE que ces critères de sélection et attributs de poste soient revus tous les ans dans le cadre des entretiens annuels des personnels sur la fiche de poste.

❖ Enquête de sécurité

PS-3-0 - Enquête de sécurité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation s'assure que les personnels accédant à une information classifiée ou en exercice sur un poste, disposent bien de l'accréditation nécessaire.

PS-3-1 - Informations classifiées - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les stagiaires ou prestataires dont la nationalité n'est pas UE aient fait l'objet d'une enquête par les services compétents et aient reçu un avis favorable par ces services avant toute prise de fonction, quel que soit leur rôle.

NB : pour les sites non opérationnels, une déclaration en tant que ZRR (Zone à Régime Restrictif) sera nécessaire.

❖ Cessation d'emploi du personnel

PS-4-0 - Cessation d'emploi du personnel - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation, lors du départ d'un personnel de l'organisation :

- désactive les accès au système d'information dans les 24h ouvrées qui suivent son départ ;
- supprime/désactive les identifiants et supports d'identification (badge, carte à puce, etc.) associés à l'individu ;
- si possible, conduise des entrevues de sortie incluant une discussion sur les sujets de sécurité (exemple : rappel des accords de non-divulgence...), en priorité pour les personnes ayant des habilitations ;
- récupère tous les biens confiés à l'individu (PC, smartphone, tablette, clé USB, etc.);

- conserve les journaux et les accès de l'employé au système d'information.

PS-4-2 - Notification automatisée - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation utilise des mécanismes automatisés pour notifier, mettre à jour et publier les informations sur les mouvements de personnel (départ, arrivée, mutation).

❖ Transfert de personnel

PS-5-0 - Transfert de personnel - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation modifie les accès physiques ou logiques au système d'information au maximum 24h après le transfert effectif, pour chaque mouvement de personnel.

❖ Sécurité des personnels tiers

PS-7-0 - Sécurité des personnel tiers - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation inclue dans ces contrats avec des personnels tiers des exigences ci-dessous :

- Il est OBLIGATOIRE que les personnels Tiers se conforment aux politiques de sécurité du personnel et aux procédures établies par l'organisation,
- Il est OBLIGATOIRE que tout départ, mutation, arrivée d'un personnel tiers qui possèdent des identifiants et/ou badges ou qui ont des comptes à privilèges pour l'accès au système d'information, soit notifié à l'organisation au plus tard, le jour de son départ.

Analyse de risque

❖ Evaluation des risques

RA-3-0 - L'évaluation des risques - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation effectue une analyse de risque sur son SI afin de réduire, supprimer transférer ou éviter le risque le cas échéant. Cette Analyse de Risque pourra être réalisée de manière globale à un environnement.

Il est OBLIGATOIRE que les résultats de chaque analyse de risque donnent lieu à un plan de sûreté visant la mise en œuvre des mesures définies, et suivi périodiquement.

Il est OBLIGATOIRE que cette analyse de risque soit mise à jour au moins une fois tous les trois ans ou s'il y a des changements importants dans le système d'information constituant le périmètre de l'étude.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation réalise une analyse de risques pour chaque système et réaliser un dossier d'homologation comprenant :

- les mesures de sécurité appliquées au SIIV;
- les rapports d'audit de la sécurité du SIIV;
- les risques résiduels et les raisons justifiant leur acceptation.

❖ Scan de vulnérabilité

RA-5-0 - Scan de vulnérabilité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre :

- des outils de vérification de conformité (exécutés de manière hebdomadaire) ;
- des outils de recherche des IOC ;
- une procédure de maintien en condition de sécurité (MCS) incluant:
 - la veille en vulnérabilités,
 - l'application de correctifs de sécurité ou l'installation de nouvelles versions dans un délai à déterminer (pour les systèmes de gestion et pilotage ce délai ne pourra pas excéder un mois) incluant les tests avant et après installation,
 - l'application de mesures organisationnelles ou techniques temporaires afin de mitiger le risque.

RA-5-5 - Accès privilégié - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les activités de scan de vulnérabilités soient réalisées par des personnes autorisées. Le rapport de scan est classifié confidentiel.

❖ **Surveillance des mesures de sécurité****RA-6-0 - Enquête sur la surveillance technique des contre-mesures - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place des indicateurs relatifs au maintien en conditions de sécurité des ressources :

- le pourcentage de postes utilisateurs dont les ressources systèmes ne sont pas installées dans une version supportée par le fournisseur ou le fabricant ;
- le pourcentage de serveurs dont les ressources systèmes ne sont pas installées dans une version supportée par le fournisseur ou le fabricant ;
- le pourcentage de postes utilisateurs dont les ressources systèmes ne sont pas mises à jour ou corrigées du point de vue de la sécurité depuis au moins 15 jours à compter de la disponibilité des versions mises à jour ;
- le pourcentage de serveurs dont les ressources systèmes ne sont pas mises à jour ou corrigées du point de vue de la sécurité depuis au moins 15 jours à compter de la disponibilité des versions mises à jour.

Acquisition de systèmes ou de services

❖ Cycle de vie de développement du système

SA-3-0 - Cycle de vie de développement du système - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- Gère le système d'information en utilisant un cycle de vie de développement de système qui intègre des considérations de sécurité de l'information;

- Définisse et documente les rôles et responsabilités de sécurité de l'information tout au long du cycle de vie du développement du système;
- Identifie les personnes ayant des rôles et des responsabilités en matière de sécurité de l'information;
- Intègre le processus de gestion des risques de la sécurité de l'information dans les activités du cycle de vie du développement du système.

Pour les systèmes acquis et développés dans le cadre d'une prestation, il est OBLIGATOIRE que le fournisseur identifie un responsable sûreté, point de contact pour toutes les contributions touchant à la sûreté.

❖ Processus d'acquisition

SA-4-0 - Processus d'acquisition - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le processus de développement produise un plan de gestion de sécurité de l'information (ISMP) ou plan d'assurance sûreté (PAS) incluant les éléments suivants :

- Une description fonctionnelle du système, objet du marché de haut niveau, spécifiant les systèmes, et sous-systèmes ou constituants ainsi que les interfaces physiques et logiques externes ou internes au système,
- des exigences fonctionnelles de sûreté du système,
- le niveau des exigences fonctionnelles (en fonction des couleurs du bundle d'appartenance conformément à cette présente PSSI),
- les exigences d'assurance
- le niveau de classification de la documentation fournie ainsi que les mesures de protection associées
- la description de l'environnement de développement ainsi que l'environnement dans lequel il sera exploité
- les critères d'acceptation.

SA-4-1 - Propriétés fonctionnelles des contrôles de sécurité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les développeurs documentent les fonctionnalités des mécanismes de sécurité qu'ils mettent en œuvre (fonctions, conception, implémentation, limitations).

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les développeurs documentent les fonctionnalités des mécanismes de sécurité qu'ils mettent en œuvre (fonctions, conception, implémentation, limitations) dans le plan de gestion de la sécurité de l'information (ISMP) ou plan d'assurance sûreté (PAS).

SA-4-2 - Information sur la conception et la mise en œuvre des contrôles de sécurité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les développeurs documentent la conception et l'implémentation des mesures de sûreté mises en œuvre incluant :

- une description fonctionnelle haut niveau et bas niveau des mesures de sûreté implémentées ou à implémenter,
- (la description fonctionnelle de haut niveau précise les systèmes et constituants utilisés, ainsi que les interfaces entre systèmes et sous-systèmes; la description de bas niveau précise les modules applicatifs utilisés (logiciels, firmwares, OS) et les interfaces entre ces modules)
- une description des interfaces logiques et physiques
- une liste des matériels, firmwares, logiciels et versions de logicielles utilisées,

SA-4-5 - Configurations système / composant / service - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les développeurs fournissent par défaut une configuration du système dite sécurisée à savoir que toutes les fonctionnalités et paramètres permettant d'augmenter le niveau de sûreté du dit système sont activés à l'exception de ceux remettant en question le fonctionnement nominal du système. En outre, il est OBLIGATOIRE que tous les services inutiles (non utilisés) du système soient supprimés ou désactivés.

SA-4-9 - Fonctions / ports / protocoles / services en cours d'utilisation - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les développeurs identifient au plus tôt du cycle de vie du développement du système, les fonctions, les ports, les protocoles et les services utilisés par le système développé, et documenter les types de données échangées en interne ou avec d'autres systèmes. Il est OBLIGATOIRE que seuls les éléments strictement nécessaires au fonctionnement nominal du système soient activés et décrits ainsi.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le processus de développement valide les orientations retenues en incluant un ensemble de revues SSI à chaque étape du processus (conception, implémentation, développement).

❖ Dossier de sécurité d'exploitation

SA-5-0 - Dossier de sécurité d'exploitation - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le fournisseur ou développeur fournisse la documentation administrateur qui décrit :

- la configuration, l'installation, les opérations systèmes ou services;
- l'utilisation et la maintenance des mécanismes de sécurité;
- les vulnérabilités connues portant sur la configuration et l'utilisation des fonctions d'administration.

Il est OBLIGATOIRE que le fournisseur ou développeur fournisse la documentation utilisateur qui décrit la manière d'utiliser le système de manière sécurisée.

❖ Services externes au système d'information

SA-9-0 - Services externes au système d'information - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le fournisseur de service externalisé s'engage à respecter l'ensemble des exigences de la PSSI du donneur d'ordre et décrit l'ensemble des dispositions spécifiques afin de les respecter (Guide ANSSI sur l'externalisation: plan de gestion de la sécurité de l'information (ISMP) ou plan d'assurance sûreté (PAS))

Le Plan d'Assurance Sécurité (PAS) doit être demandé dans l'appel d'offres. Document contractuel, il décrit l'ensemble des dispositions spécifiques que les candidats s'engagent à mettre en œuvre pour garantir le respect des exigences de sécurité du donneur d'ordres.

C'est aussi un cadre de réponse : il offre une structure pour la réponse des candidats aux exigences de sécurité, ce qui permet de mieux évaluer la pertinence de la couverture des exigences. Il facilite ainsi la comparaison entre les différentes offres.)

SA-9-2 - Identification des fonctions / ports / protocoles / services - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les fournisseurs de services externalisés identifient les fonctions, les ports, les protocoles, les autres services requis pour l'utilisation de leurs services et documentent les types de données échangées en interne ou avec d'autres systèmes.

SA-9-4 - Intérêts cohérents des fournisseurs de services - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation inclue dans ses contrats, la capacité à réaliser ou faire réaliser des audits de sûreté sur l'organisation interne du Fournisseur. Il est OBLIGATOIRE que le Fournisseur mette en œuvre tous les moyens dont le Client a besoin pour réaliser ces audits.

SA-9-5 - Emplacement des traitements de l'information - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les emplacements de stockage et de traitement des informations soient définis et documentés. Hors contrainte technique forte, Il est OBLIGATOIRE que les données et traitements soient localisés sur le territoire de l'UE.

Environnement	R	O	J	B
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Dans le cas où l'hébergement d'une partie du système d'information est externalisé, il est OBLIGATOIRE que le système d'information externalisé soit localisé sur le territoire national.

Dans ce cas où l'organisation fait appel à un prestataire d'information en nuage (cloud), il est OBLIGATOIRE que le prestataire respecte les exigences du référentiel SECNUMCLOUD de l'ANSSI ou équivalent.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est INTERDIT que le système d'information soit externalisé.

❖ Gestion de la configuration des développeurs

SA-10-0 - Gestion de la configuration des développeurs - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les personnels développant le système d'information :

- Gèrent la configuration pendant la conception, le développement, les phases de tests et d'évaluation, et l'exploitation...
- Effectuent la gestion de la configuration pendant la conception, le développement, l'évaluation et la mise en production de chaque système ou service ;
- Documentent, gèrent et contrôlent l'intégrité des modifications des éléments de configuration, notamment du code source;
- Documentent les modifications du système ou du service et les impacts potentiels de sécurité suite à ces changements;
- Suivent les failles de sécurité du système ou service et leurs résolutions;
- Signalent les résultats des résolutions de failles;
- Documentent et communiquent le résultat du processus de correction des failles de sécurité.

SA-10-1 - Vérification de l'intégrité du logiciel / firmware - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les développeurs mettent en place des mécanismes de sécurité afin de garantir et de vérifier l'intégrité des firmwares et constituants logiciels.

SA-10-6 - Distribution de confiance - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre une procédure afin de garantir la confidentialité et l'intégrité des constituants logiciels lors de la livraison (firmware, OS, application, configuration, documentation, code).

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les constituants logiciels soient signés par un certificat reconnu par l'organisation.

❖ Test et évaluation de la sécurité des développeurs

SA-11-0 - Test et évaluation de la sécurité des développeurs - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les développeurs :

- Documentent et appliquent un plan d'assurance sûreté basé sur des outils et procédures permettant de minimiser les erreurs introduites durant les phases de développement (outils d'analyse statique ou dynamique de code, utilisation de bibliothèques réputées pour leur sécurité, revues de code, etc.);
- Effectuent des tests / évaluations sur les systèmes;
- Produisent des preuves de l'exécution du plan d'assurance sûreté et des résultats des tests / évaluations de sécurité;
- Mettent en œuvre un processus de gestion des vulnérabilités de l'identification à la correction (patches correctifs ou actions de vérification);
- Corrigent les failles et faits techniques identifiées lors des tests de sécurité / évaluation.

SA-11-1 - Analyse de code statique - V1R0

Environnement	R	O	J	B
	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que les développeurs utilisent des outils d'analyse statique de code et des outils de robustesse de code afin d'identifier les failles de sécurité, les documentent et les corrigent le cas échéant.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les développeurs utilisent des outils d'analyse statique de code et des outils de robustesse de code afin d'identifier les failles de sécurité, les documentent et les corrigent le cas échéant.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les développeurs utilisent des outils d'analyse statique et dynamique de code et des outils de robustesse de code afin d'identifier les failles de sécurité, les documentent et les corrigent le cas échéant.

SA-11-3 - Vérification indépendante des plans d'évaluation et des preuves - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- Définisse un agent indépendant pour vérifier la mise en œuvre correcte du plan d'assurance sureté du développeur et les preuves produites lors des tests / évaluation de sécurité; et
- S'assure que l'agent indépendant reçoit les informations suffisantes pour compléter le processus de vérification.

SA-11-5 - tests de pénétration - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation effectue des tests de pénétration sur les services ou systèmes déployés accessibles depuis internet.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Suite à l'analyse de risque, l'organisation POURRA :

- effectuer des tests de pénétration sur les services ou systèmes déployés,
- effectuer des tests plus approfondis comme du « fuzzing » (tests à données aléatoires) sur tout ou partie du système.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les tests d'intrusion soient réalisés par un PASSI (Prestataire d'Audit de la Sécurité des Systèmes d'Information).

❖ Protection de la chaîne d'approvisionnement

SA-12-0 - Protection de la chaîne d'approvisionnement - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le fournisseur mette en œuvre et documente des mesures de protection de l'environnement de développement et de conception visant à s'assurer que l'environnement de développement du produit, de sa conception à l'implémentation est protégée et qu'aucune menace ne peut modifier le système dans son environnement de développement afin d'y intégrer des vulnérabilités.

Il est OBLIGATOIRE que le fournisseur assure un niveau de sûreté physique de ses locaux.

Il est OBLIGATOIRE que Le plan de gestion de sécurité de l'information (ISMP) ou plan d'assurance sûreté (PAS) décrive les mécanismes de sûreté mis en œuvre afin de protéger la conception du produit et son implémentation, de son environnement de développement.

Il est OBLIGATOIRE que les locaux du Fournisseur abritant les phases de conception, de développement, et de tests du système mettent en œuvre des mesures de sûreté afin de maintenir un niveau de sûreté suffisant et garantir qu'aucune modification d'origine illicite ou malveillante ne puisse se produire en phase de conception et développement du produit (type backdoor, espionnage, vol, etc.).

SA-12-14 - Identification et Traçabilité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que toutes données relatives à la conception, au développement et à la spécification du système, de son stockage, à l'envoi jusqu'à sa suppression, et hébergées sur tout type de support, soient protégées de manière adéquate afin de s'assurer de l'intégrité et de la confidentialité des données.

Il est OBLIGATOIRE que l'organisation utilise une méthode d'authentification pour contrôler et sécuriser l'accès des membres de ses équipes au code source et aux paramètres de configuration.

SA-12-15 - Pour remédier aux faiblesses ou aux lacunes - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le fournisseur corrige toutes vulnérabilités découvertes, et introduites durant les phases de conception, de développement ou à la suite d'audits sûreté, et qui lui sont remontées en incluant automatiquement les corrections des autres occurrences des mêmes erreurs de programmation

❖ Processus de développement, normes et outils

SA-15-0 - Processus de développement, normes et outils - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les développeurs définissent, documentent, appliquent et contrôlent des normes de développement sécurisé (bonnes pratiques de développement, normes,... ex : Critères Communs) qu'ils appliquent pour le développement du système ainsi que le niveau d'assurance qu'ils suivent, s'il existe au niveau du plan de gestion de sécurité de l'information (ISMP) ou plan d'assurance sûreté (PAS) .

Il est OBLIGATOIRE que l'ensemble des sous-traitants du Fournisseur impliqués dans ce contrat suivent ces standards et niveaux d'assurance.

Il est OBLIGATOIRE que les développeurs précisent et documentent en Annexe de l'ISMP la liste des outils et les parties du logiciel (bibliothèques, composants ou autres produits logiciels, COTS, outillage de génération de code, compilation, analyse statique....) qu'ils utilisent dans le développement de l'environnement du système.

Cette liste inclut les outils de compilation, de développement et les outils de vérification de code

SA-15-2 - Processus de développement, normes et outils | Outils de suivi de la sécurité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les développeurs utilisent un outil de gestion des erreurs, au moins en ce qui concerne les vulnérabilités.

SA-15-7 - Analyse de vulnérabilité automatisée - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les développeurs mettent en place :

- une gestion de toutes les vulnérabilités du système découvertes pendant le cycle de vie du système,
- déterminer l'exploitabilité des vulnérabilités découvertes,
- déterminer l'impact de la mise en place des patchs correctifs ou des actions de mitigation des vulnérabilités découvertes,
- documenter et fournir le résultat de ces analyses au SOC.

SA-15-9 - Utilisation de données en direct - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'environnement de test assure la confidentialité des données en fonction de leur niveau de classification.

❖ **Composants du système non supportés****SA-22-0 - Composants du système non supportés - V1R1**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Sauf en cas de difficultés techniques ou opérationnelles justifiées, Il est OBLIGATOIRE que l'organisation installe et maintienne toutes les ressources matérielles et logicielles de ses composants/constituants dans des versions supportées par leurs fournisseurs ou leurs fabricants et mises à jour du point de vue de la sécurité ;

Il est OBLIGATOIRE que l'organisation procède au remplacement des composants dont le maintien en condition de sécurité n'est plus assuré, et anticipe ces changements de façon à ne pas avoir de période où les risques sont élevés. En cas de difficultés techniques ou opérationnelles justifiées, Il est OBLIGATOIRE que l'organisation gère (dans le temps) les risques et éventuellement mette en œuvre les mesures de diminution de risques associées.

Protection des systèmes et des communications

❖ Partitionnement des applications

SC-2-0 - Partitionnement des applications - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☐

Il est OBLIGATOIRE que les systèmes d'information disposent de réseaux et de systèmes dédiés à la gestion du système d'information et cloisonnés (SI d'administration dédié à l'administration et la supervision).

Environnement	R	O	J	B
	☒	☒	☐	☐

Il est OBLIGATOIRE que le réseau de gestion du système d'information (administration et supervision) soit connecté aux ressources à administrer au travers d'une interface réseau dédiée.

SC-2-1 - Interfaces pour les utilisateurs non privilégiés - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☐

Il est OBLIGATOIRE que le système d'information autorise l'accès aux fonctions d'administration uniquement sur les interfaces dédiées.

❖ Isolation des fonctions de sécurité

SC-3-0 - Isolation des fonctions de sécurité - V1R0

Environnement	R	O	J	B
	☒	☒	☒	☐

Il est RECOMMANDE que les fonctions de sécurité assurant le filtrage des flux de données soient implémentées sur des équipements dédiés à cet effet (firewall).

Rq : Un équipement de type routeur peut assurer une fonctionnalité de cloisonnement.

Environnement	R	O	J	B
	☒	☒	☐	☐

Il est OBLIGATOIRE que les fonctions de sécurité assurant le filtrage des flux de données soient implémentées sur des équipements dédiés à cet effet (firewall).

Rq : Un équipement de type routeur peut assurer une fonctionnalité de cloisonnement.

❖ Informations dans les ressources partagées

SC-4-0 - Informations dans les ressources partagées - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que le système d'information empêche le transfert d'informations non autorisé et non spécifié via des ressources système partagées.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information empêche le transfert d'informations non autorisé et non spécifié via des ressources système partagées.

❖ Détection / surveillance

SC-5-3 - Détection / surveillance - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information surveille les capacités et les performances des systèmes (Charge CPU) et des réseaux (bande passante) afin d'identifier les attaques de type DDS

❖ Périmètre de protection (zones de sécurité)

SC-7-0 - Périmètre de protection (zones de sécurité) - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information :

- A. Surveille et contrôle les communications aux limites externes du système d'information et entre zone de criticité différente en interne du système d'information (environnement),
- B. Isole les réseaux de composants du système accessibles au public, des réseaux internes ; et
- C. Se connecte à des réseaux externes ou à des systèmes d'information externes uniquement à travers des interfaces dédiées et sécurisées.

SC-7-3 - Points d'accès - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation limite le nombre de points d'accès à des réseaux externes/Tiers.

SC-7-4 - Services de télécommunications externes - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- A. Implémente une interface gérée dédiée à chaque service de télécommunication externe ;
- B. Définit et Limite le trafic échangé aux seuls flux autorisés ;
- C. Définisse un processus de dérogation pour chaque exception à la politique de flux de trafic définissant les exceptions de sécurité, le besoin, la durée de la dérogation ainsi que la feuille de route permettant de lever la dérogation.

SC-7-5 - Refuser par défaut / autoriser par exception - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information interdise tout trafic ou communication entre environnement de criticité distincte à l'exception des flux explicitement autorisés.

Rq : implique la mise en œuvre de firewall entre les environnements de criticité distincte

SC-7-7 - Empêcher la tunnelisation partagée pour les périphériques distants - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information, en conjonction avec un dispositif distant, empêche ce dispositif d'établir simultanément des connexions non-distantes avec le système et de communiquer via une autre connexion aux ressources de réseaux externes.

SC-7-10 - Empêcher l'exfiltration non autorisée - V1R0

Environnement	R	O	J	B
	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que l'organisation prévienne toute exfiltration non autorisée d'informations en :

- s'assurant du respect des protocoles des flux échangés sur les interfaces avec des systèmes d'information tiers
- superviser la bande passante des flux de données échangées et notifier toute utilisation anormale ou non autorisée

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation prévienne toute exfiltration non autorisée d'informations en :

- s'assurant du respect des protocoles des flux échangés sur les interfaces avec des systèmes d'information tiers
- superviser la bande passante des flux de données échangées et notifier toute utilisation anormale ou non autorisée

SC-7-11 - Restreindre le trafic de communications entrantes - V1R0

Environnement	R	O	J	B
	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que les infrastructures réseaux offrent un niveau de cloisonnement/filtrage au niveau du site (concrètement entre les réseaux locaux et toute E/S du site) afin de permettre le confinement d'un site en cas d'incident ou de limiter, ralentir voire contrôler la propagation d'un incident ;

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les infrastructures réseaux offrent un niveau de cloisonnement/filtrage au niveau du site (concrètement entre les réseaux locaux et toute E/S du site) afin de permettre le confinement d'un site en cas d'incident ou de limiter, ralentir voire contrôler la propagation d'un incident ;

SC-7-12 - Protection basée sur l'hôte - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les serveurs de données critiques implémentent des mesures de filtrage des données entrantes afin de n'autoriser que les flux strictement nécessaires.

Il est OBLIGATOIRE que ces modules de filtrage respectent le principe de moindre privilège.

SC-7-14 - Protège contre les connexions physiques non autorisées - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation protège l'accès physique aux systèmes critiques.

SC-7-20 - Isolation / ségrégation dynamique - V1R0

Environnement	R	O	J	B
	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que le système d'information offre la possibilité d'isoler / ségréger dynamiquement des postes clients ou nomades des autres composants du système [règles de FW]

SC-7-21 - Isolement des composants du système d'information - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation utilise des mécanismes de protection pour séparer les composants du système d'information soutenant différentes missions ou fonctions. Parmi ces mécanismes : routeur, pare-feu, virtualisation, sous-réseaux, etc.

Il est OBLIGATOIRE que les réseaux soient cloisonnés en sous-réseaux afin de limiter l'accès aux flux de communication aux seuls systèmes qui en ont besoin.

Il est OBLIGATOIRE que chaque constituant du système NA appartienne à l'environnement strictement nécessaire vis à vis de sa criticité (principe de moindre environnement).

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les services métier dédiés à la communication vocale (radio, téléphone) soient cloisonnés vis à vis des autres services et en particulier des services ATM (service de traitement radar, plan de vol, etc.)

Il est OBLIGATOIRE que les infrastructures PAL et SEC (backup) du service Communications Vocales (COMV) soient cloisonnées, logiquement et si possible physiquement.

❖ Confidentialité et intégrité de la transmission

SC-8-0 - Confidentialité et intégrité de la transmission - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système mette en œuvre des mécanismes de chiffrement afin de garantir la confidentialité et l'intégrité des informations transmises à partir des sites de la DSNA.

S'il y a des exceptions, Il est OBLIGATOIRE qu'elles soient justifiées, documentées et approuvées par les autorités compétentes.

❖ Déconnexion du réseau

SC-10-0 - Déconnexion du réseau - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information mette fin à la connexion réseau associée à une session de communication à la fin de la session ou après 10 min d'inactivité.

❖ Création et gestion des clés cryptographiques

SC-12-0 - Création et gestion des clés cryptographiques - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'utilisation de mécanismes de chiffrement ainsi que la gestion des certificats et des clés (PKI) soient conformes avec les normes en vigueur définies par l'ANSSI.

❖ Dispositifs d'informatique collaborative

SC-15-0 - Dispositifs d'informatique collaborative - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est INTERDIT d'utiliser des outils collaboratifs autres que ceux validés par la DGAC pour partager les informations.

Il est OBLIGATOIRE que ces outils collaboratifs respectent les mesures de sécurité liées à la classification de l'information et au besoin d'en connaître.

❖ **Exécution de code à la volée****SC-18-0 - Exécution de code à la volée - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que l'organisation définisse les technologies d'exécution de code à la volée jugées acceptables et déploie les mécanismes pour limiter tout autre technologie de pouvoir s'exécuter. Parmi ces technologies on trouve : Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VB Script, etc.

SC-18-5 - Autorisation de code uniquement dans un environnement confiné - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système exécute le code à la volée autorisé, uniquement dans un environnement confiné (Sandbox).

❖ **Voix sur IP (VoIP)****SC-19-0 - Voix sur IP (VoIP) - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- Établisse les restrictions d'utilisation et les directives de mise en œuvre pour les technologies VoIP basées sur le risque d'endommager le système d'information s'il est utilisé malicieusement; et
- Autorise, surveille et contrôle l'utilisation de la VoIP dans le système d'information.

❖ **Service de résolution de noms / adresses sécurisés (source autorisée)****SC-20-0 - Service de résolution de noms / adresses sécurisés (source autorisée) - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système puisse résoudre un nom de domaine au travers d'un mécanisme DNS (interne et/ou externe).

Sauf contrainte technique forte, il est OBLIGATOIRE de mettre également en œuvre la résolution inverse.

SC-20-2 - Origine / intégrité des données - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Pour les systèmes accessibles depuis internet, Il est OBLIGATOIRE que la résolution de nom (directe/indirecte) soit sécurisée via DNSSEC.

❖ Architecture et approvisionnement pour service de résolution de noms / adresses

SC-22-0 - Architecture et approvisionnement pour service de résolution de noms / adresses - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système sépare le service de résolution de noms / adresses entre les résolutions internes (ex : poste de travail) et externes (domaines externes) à l'organisation et déploie des mécanismes de tolérance aux pannes.

❖ Authenticité de session

SC-23-0 - Authenticité de session - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système mette en place un mécanisme de protection des identifiants de session (Web Services) (ex: chiffrement de chaque session id par SSL).

SC-23-1 - Invalider les identifiants de session lors de la déconnexion - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les identifiants de session soient renouvelés après la déconnexion de celles-ci.

SC-23-3 - Identificateurs de session uniques avec randomisation - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les identifiants de session soient aléatoires et non prédictibles (utilisation d'algorithmes reconnus).

SC-23-5 - Autorités de certification autorisées - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les sessions ouvertes soient sécurisées par le biais de validation par certificat (PKI). Il est OBLIGATOIRE que ces certificats soient autorisés par des organismes de certification reconnu (ex: Verisign)

❖ Retour dans un état stable en cas d'échec

SC-24-0 - Retour dans un état stable en cas d'échec - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

En cas de dysfonctionnement, Il est OBLIGATOIRE que le système mette en défaut de manière sécurisée afin d'éviter qu'un éventuel attaquant puisse accéder au système pendant ce fonctionnement dégradé:

- En cas d'échec, annuler les changements et restaurer un état sécurisé
- Vérifier les données de retour de l'échec
- Pendant une mise en défaut (en cas d'échec), les attaquants éventuels ne DOIVENT pas pouvoir accéder à des ressources inaccessibles habituellement
- Un système mis en défaut ne DOIT pas révéler d'informations dont la connaissance pourrait permettre une attaque ultérieure.

❖ Protection de l'information au repos

SC-28-0 - Protection de l'information au repos - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information garantisse la confidentialité et l'intégrité des données stockées au moyen de mécanismes de chiffrement, conformément à la politique de classification de l'information.

SC-28-2 - Stockage hors ligne - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre une procédure de gestion de l'information définissant :

- les critères de classification de l'information,
- les mesures de sûreté à mettre en œuvre pour le stockage, l'archivage, la diffusion et la destruction de l'information.

Le système DOIT se conformer à ladite procédure.

Intégrité des systèmes et de l'information

❖ Correction de défauts

SI-2-0 - Correction de défauts - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation prenne en compte les vulnérabilités, identifie les systèmes d'information concernés et prenne les mesures conservatoires ou correctives adéquates.

Il est OBLIGATOIRE que l'organisation assure également le déploiement des correctifs de sécurité et informer le SOC des délais d'application effectif de ces correctifs.

SI-2-1 - Gestion centrale - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation centralise la gestion des corrections des failles de sécurité.

SI-2-2 - État de correction automatique des défauts - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en œuvre un outil lui permettant de dresser pour l'ensemble des éléments du système d'information, annuellement et sur demande, un état des failles de sécurité non corrigées.

SI-2-3 - Temps pour corriger les défauts / repères pour les actions correctives - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que L'organisation mesure la durée moyenne de correction d'une faille identifiée. En outre, Il est OBLIGATOIRE que l'organisation mette en place des benchmark vis à vis de ces actions correctives.

SI-2-5 - Mises à jour logicielles / firmware automatiques - V1R0

Environnement	R	O	J	B
	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation installe automatiquement les mises à jour de sécurité des composants du système d'information (fournies par les constructeurs) sur les serveurs de service, équipements de sécurité (fw, IPS/IDS) et équipements réseaux après avoir mesuré l'impact de manière à ne pas interrompre les opérations.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation installe automatiquement les mises à jour de sécurité des composants du système d'information (fournies par les constructeurs) sur les serveurs de service, équipements de sécurité (fw, IPS/IDS) et équipements réseaux après avoir mesuré l'impact de manière à ne pas interrompre les opérations.

En cas d'impossibilité technique ou opérationnelle, il est OBLIGATOIRE qu'une Analyse de Risque soit menée afin d'identifier le risque résiduel lié à la non prise mise à jour de sécurité des composants associés.

❖ Protection contre les codes malveillants

SI-3-0 - Protection contre les codes malveillants - V1R1

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Sauf contrainte technique ou opérationnelle, Il est OBLIGATOIRE que l'organisation mette en place des outils de type antivirus sur les systèmes Windows.

Il est OBLIGATOIRE que ces systèmes soient maintenus à jour dès que les mises à jour sont délivrées par le constructeur.

Il est OBLIGATOIRE que ces mécanismes de protection permettent de scanner les systèmes une fois par semaine et détectent en temps réel, du code malveillant présent dans les fichiers entrant et sortant du système d'information. Par la suite, Il est OBLIGATOIRE que ces mécanismes de protection alertent les administrateurs sécurité et mettent en quarantaine les fichiers incriminés.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information soit protégé contre les programmes malveillants:

- en vérifiant l'intégrité des fichiers de configuration, des bibliothèques, les programmes,
- en mettant en œuvre des systèmes de détection d'intrusion (HIDS) au niveau du système.

SI-3-1 - Gestion centrale - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que la gestion des antivirus soit réalisée centralement.

SI-3-4 - Mises à jour uniquement par des utilisateurs privilégiés - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que la mise à jour des systèmes de protection contre les codes malveillants soit réalisée par des utilisateurs ou des services avec des accès dédiés (admin-sec, lorsque le rôle est défini).

SI-3-6 - Vérification - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation teste le SIEM (règles de corrélations entre les équipements ou fonctionnalités dédiés à la sécurité) tous les 3 mois. Il est OBLIGATOIRE qu'une alerte soit levée en cas de détection positive.

SI-3-9 - Authentifier les commandes à distance - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les systèmes implémentent des mécanismes de cloisonnement (Bastion) permettant d'authentifier les activités distantes.

❖ Surveillance du système d'information

SI-4-0 - Surveillance du système d'information - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation monitore les systèmes d'information afin de détecter :

- les communications non autorisées (locales, réseaux, distantes),
- attaques et potentielles attaques en accord avec les scénarios de menace,
- utilisation non autorisé du SI (via analyse des logs et/ou trafic).

Il est OBLIGATOIRE que cette supervision soit assurée par des sondes IDS/IPS placées en périphérie du système d'information ainsi qu'aux E/S des zones sensibles.

Il est OBLIGATOIRE que l'accès à ces sondes et à leur contenu soit uniquement autorisé au SOC (ou au PDIS - Prestataire de Détection d'Incidents de Sécurité le cas échéant).

De plus, il est RECOMMANDE que des alertes spécifiques et/ou temporaires soient mis en places sur les sondes (ex: lors d'une apt avérée).

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place des sondes de type "sonde d'analyse et de protocoles" recommandées par l'ANSSI.

Il est OBLIGATOIRE que seuls les PDIS (Prestataire de Détection d'Incidents de Sécurité)/PRIS (Prestataire de Réponse aux Incidents de Sécurité) soient autorisés à exploiter les sondes recommandées par l'ANSSI

SI-4-1 - Surveillance du système d'information | Système de détection d'intrusion à l'échelle du système - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation connecte et configure des sondes pouvant être connectées à un SIEM centralisant toutes les détections d'intrusion.

SI-4-2 - Surveillance du système d'information | Outils automatisés pour l'analyse en temps réel - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place des outils automatisés permettant d'analyser en temps réel (IDS/IPS/SIEM).

SI-4-4 - Trafic de communications entrantes et sortantes - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système surveille en continu le trafic des communications entrantes, sortantes et internes dans le but de détecter des événements inhabituels ou non autorisés (NIDS).

SI-4-5 - Alertes générées par le système - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système envoie des alertes de sécurité aux [administrateurs sécurité si ce rôle existe et dans le cas contraire aux administrateurs du système] lors d'un incident de sécurité avéré.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système envoie les alertes de sécurité à l'ANSSI [selon le guide] au travers d'un formulaire.

SI-4-7 - Réponse automatisée aux événements suspects - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les administrateurs soient notifiés dès une détection d'intrusion et suivent la procédure de traitement des incidents.

SI-4-11 - Analyser les anomalies de la circulation des communications - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation analyse le trafic des communications sortantes pour détecter des anomalies (transferts de fichiers importants, connexions persistantes de longue durée, protocoles et ports inhabituels utilisés, tentative de communication avec des adresses externes malveillantes identifiées).

SI-4-14 - Détection d'intrusion sans fil - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place un outil de détection d'intrusion wifi pour détecter les points d'accès wifi non autorisés et les attaques sur le système d'information.

SI-4-15 - Sans fil aux communications filaires - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation utilise un outil de détection d'intrusion pour surveiller le trafic sur le réseau wifi.

SI-4-16 - Corréler les informations de surveillance - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation soit capable de générer des logs à destination d'un SIEM.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation soit capable de corréler les logs systèmes afin de détecter des incidents SSI.

SI-4-20 - Utilisateur privilégié - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation analyse les accès des utilisateurs privilégiés (accès physiques)

SI-4-22 - Services réseau non autorisés - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation détecte les services réseaux qui ne sont pas autorisés [par les processus officiel d'implémentation DGAC], et envoie une alerte le cas échéant [admin sec]

SI-4-24 - Indicateurs de compromission - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation collecte, distribue et utilise des IOC dans le but d'améliorer et rendre plus efficace la détection.

❖ **Alertes de sécurité, avis et directives****SI-5-0 - Alertes de sécurité, avis et directives - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- reçoive des directives, alertes et avis de sécurité d'un CERT de façon continue,
- génère des directives, alertes et avis de sécurité,

- diffuse des directives, alertes et avis de sécurité.

SI-5-1 - Alertes et avis automatisés - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation utilise des mécanismes automatisés pour générer des alertes et/ou recommandations de sécurité à travers toute l'organisation.

❖ Vérification des fonctions de sécurité

SI-6-0 - Vérification des fonctions de sécurité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation vérifie les fonctionnements du SIEM, sondes. En cas de tests échoués, il est OBLIGATOIRE que les ASSI en soient informés.

SI-6-3 - Résultats de la vérification des rapports - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le rapport de sécurité réalisé à la suite de tests de vérification des fonctions de sécurité soit envoyé au SOC.

❖ Intégrité des logiciels, firmwares et de l'information

SI-7-1 - Vérifications d'intégrité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Sauf incompatibilité technique, Il est OBLIGATOIRE que le système vérifie l'intégrité des logiciels, microprogramme et informations au démarrage/redémarrage du système.

SI-7-2 - Notifications automatisées de violations de l'intégrité - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation mette en place des outils automatisés qui fournissent une notification aux administrateurs lors de la découverte de divergences lors de la vérification de l'intégrité.

SI-7-3 - Outils d'intégrité gérés centralement - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation utilise des outils de vérification d'intégrité gérés de façon centralisé.

SI-7-6 - Protection cryptographique - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Sauf incompatibilité technique, Il est OBLIGATOIRE que le système d'information mette en place des mécanismes cryptographiques pour détecter les modifications non autorisées du logiciel, du microprogramme et de l'information.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système d'information mette en place des mécanismes cryptographiques pour détecter les modifications non autorisées du logiciel, du microprogramme et de l'information.

SI-7-7 - Intégrité de la détection et de la réponse - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation :

- Identifie les violations d'intégrité ayant un lien avec la sécurité des systèmes (modifications non-autorisées de fichiers de configuration par exemple) ;
- S'assure que ces événements soient remontés vers le SIEM afin d'en garder un historique pour pouvoir identifier et discerner les actions d'un attaquant sur une période prolongée et pour des actions juridiques possibles.

SI-7-8 - Capacité d'audit pour les événements importants - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Lors de la détection d'une violation d'intégrité, il est OBLIGATOIRE que le système génère un enregistrement d'audit et alerte le SOC.

SI-7-13 - Exécution de code dans des environnements protégés - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Il est RECOMMANDE que l'organisation définisse le cas échéant, l'environnement dans lequel peuvent s'exécuter des binaires non répertoriés en SI 7-14.

SI-7-14 - Code exécutable binaire ou machine - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation répertorie les exécutables et les codes sources pouvant être exécutés sur les postes.

❖ **Protection contre les spams****SI-8-0 - Protection contre les spams - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation prévoit la mise en place de protections contre les SPAM à tous les points d'entrées ou de sortie critiques (pare-feu, serveurs de messagerie, serveur internet, serveur mandataire – serveur proxy-, serveur d'accès à distance) et sur tous les postes de son périmètre d'action se connectant au réseau.

SI-8-1 - Gestion centrale - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation gère centralement les mécanismes de protection anti-spam

SI-8-2 - Mises à jour automatiques - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système mette en place et maintienne à jour automatiquement les mécanismes de protection contre les spams dès qu'une nouvelle version est disponible.

SI-8-3 - Capacité d'apprentissage continu - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que le système utilise un mécanisme d'apprentissage automatique continu pour l'anti-spam.

❖ **Validation d'entrée d'information****SI-10-0 - Validation d'entrée d'information - V1R0**

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système contrôle l'exactitude, l'exhaustivité, la validité et l'authenticité des protocoles grands publics (web), protocoles réseaux sécurisés (ssh, tls, snmpv3) mis en œuvre dans les communications (vérification de validation des certificats). En cas d'échec, il est INTERDIT au système de traiter la donnée.

Environnement	R	O	J	B
	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est RECOMMANDE que le système s'assure que :

- les données reçues soient bien comprises dans les limites de la plage de données attendues (contrôle des données),

- dans chaque expression indexant un tableau ou une plage, l'index soit bien compris dans les limites du tableau ou de la plage de valeurs (contrôle d'indexation).

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système s'assure que le protocole des données entrantes soit bien celui attendu et que la syntaxe des données reçues correspondent bien à la syntaxe attendue par le système avant traitement (contrôle protocolaire et syntaxique).

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que le système s'assure que les données reçues soient cohérentes vis à vis du type de données attendues.

Il est OBLIGATOIRE que le système s'assure que :

- les données reçues soient bien comprises dans les limites de la plage de données attendues (contrôle des données),
- dans chaque expression indexant un tableau ou une plage, l'index soit bien compris dans les limites du tableau ou de la plage de valeurs (contrôle d'indexation).

SI-10-2 - Examen / résolution des erreurs - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que toute erreur liée à la non validation de données en entrée soit notifiée.

SI-10-3 - Comportement prévisible - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que l'organisation documente la réaction du système en cas d'entrée indésirable reçue et les actions à entreprendre.

❖ Gestion des erreurs

SI-11-0 - La gestion des erreurs - V1R0

Environnement	R	O	J	B
	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Lorsqu'un système rencontre des erreurs, il est RECOMMANDE que le système fournisse des messages d'erreurs d'une manière succincte [aux exploitants], contenant des informations utiles et non sensibles.

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Lorsqu'un système rencontre des erreurs, il est OBLIGATOIRE que le système fournisse des messages d'erreurs d'une manière succincte [aux exploitants], contenant des informations utiles et non sensibles.

❖ Protection mémoire

SI-16-0 - Protection de la mémoire - V1R0

Environnement	R	O	J	B
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Il est OBLIGATOIRE que les mesures de protection mémoire soient activées par les logiciels et applications.

ANNEXE : Glossaire

ACL	Access Control List (liste de contrôle d'accès)
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AQSSI	Autorité Qualifiée pour la Sécurité des Systèmes d'Information
ASLR	Address Space Layout Randomization (Distribution aléatoire de l'espace d'adressage)
ASSI	Agent de la Sécurité des Systèmes d'Information
BIA	Business Impact Analysis / Bilan de l'Impact sur l'Activité
BYOD	Bring Your Own Device (apportez vos appareils personnels)
CCTP	Cahier des Clauses Techniques Particulières
CERT-FR	Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques
CERTA	Centre d'Études et de Ressources en Technologies Avancées
CIL	Correspondant Informatique et Liberté
CISIA	Centre d'Instruction en Sécurité Industrielle de l'Armement
CNIL	Commission Nationale Informatique et Libertés
DEP	Data Execution Prevention (prévention de l'exécution des données)
DG	Direction Générale
DGAC	Direction Générale de l'Aviation Civile
DPO	Data Protect Officer (officier pour la Protection des Données)
DSI	Direction des Systèmes d'Information
EBIOS	Expression des besoins et identification des objectifs de sécurité
EIVP-PIA	Etude d'Impact sur la Vie Privée. Privacy Impact Assessment.
GPO	Group Policy Objects (Objets de stratégie de groupe)
IGC	Infrastructure à Gestion de Clés
ISO	International Organization for Standardization (Organisation internationale de normalisation)
ITIL	Information Technology Infrastructure Library (Bibliothèque pour l'infrastructure des technologies de l'information)
LAN	Local Area Network (Réseau local)
LPM	Loi de Programmation Militaire
MAC	Media Access Control
MCO	Maintien en Condition Opérationnelle
MCS	Maintien en Condition de Sécurité
OS	Operating System (Système d'exploitation)
OSSI	Officier de Sécurité des Systèmes d'Information
OWASP	Open Web Application Security Project (communauté en ligne travaillant sur la sécurité des applications Web)
PAS	Plan d'Assurance Sécurité
PCA	Plan de Continuité d'Activité
PDIS	Prestataires de Détection d'Incidents de Sécurité
PIN	Personal Identification Number
PRI	Plan de Reprise Informatique
PRIS	Prestataires de Réponse aux Incidents de Sécurité
PSSI	Politique de Sécurité des Systèmes d'Information
RACI	Matrice des responsabilités (Responsable, Autorité, Consulté, Informé)
RGPD	Règlement Général sur la Protection des Données à caractère personnel
RGS	Règlement Général de Sécurité

ROP	Return-Oriented Programming (Technique d'exploitation qui permet malgré de détourner de flux d'exécution d'un programme afin d'en prendre le contrôle)
RSSI	Responsable de la Sécurité des Systèmes d'Information
SI	Système d'Information
SIGP	Système d'Information Gestion et de Pilotage
SIIV	Système d'Information d'Importance Vitale
SSI	Sécurité des Systèmes d'Information
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On (Authentification unique)
USB	Universal Serial Bus
VLAN	Virtual Local Area Network (Réseau Local Virtuel)
VoIP	Voix sur IP
VPN	Virtual Private Network (réseau privé virtuel)
ZP	Zone Protégée
ZR	Zone Réservée