European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

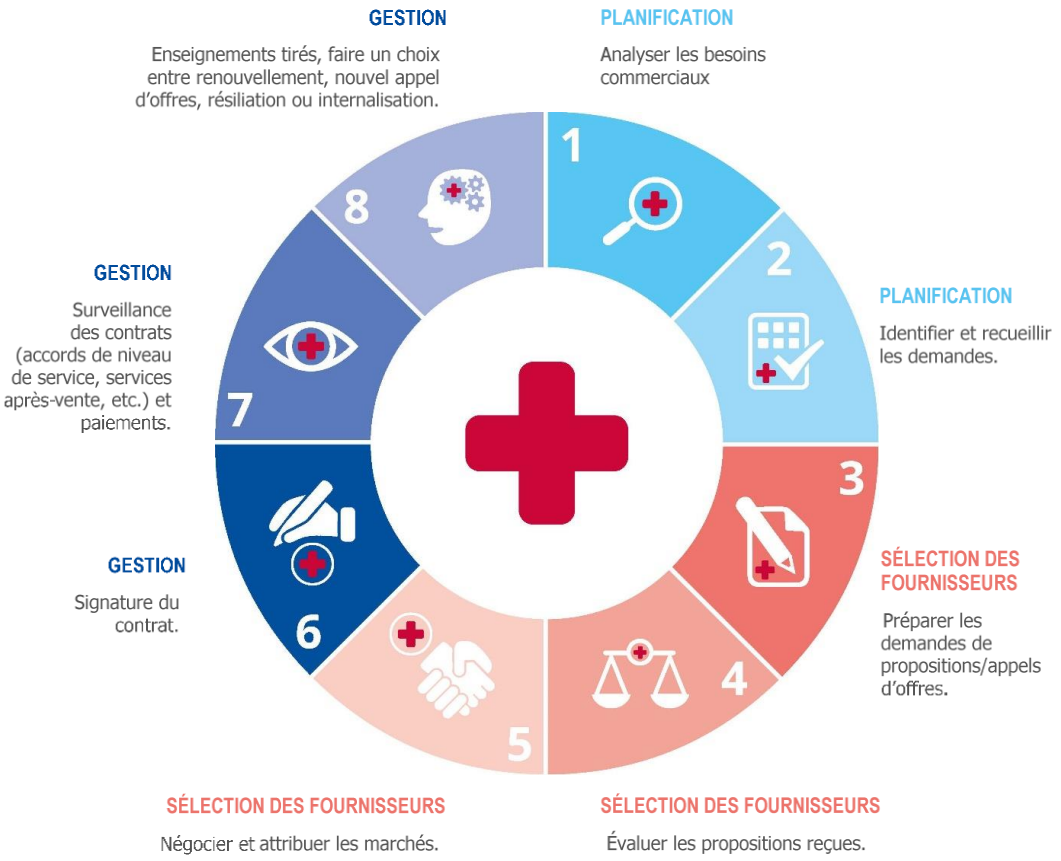
LIGNES DIRECTRICES EN MATIERE DE PASSATION DE MARCHES POUR LA CYBERSECURITE DES HOPITAUX

Le rapport se veut un «guide» à l'intention des professionnels de la santé. De nombreuses pratiques et recommandations seront également profitables à d'autres organisations de soins de santé, car les procédures de passation de marchés peuvent être très similaires. Il est utile aux professionnels de la santé qui occupent des postes techniques dans les hôpitaux, c'est-à-dire les cadres supérieurs: le directeur des systèmes d'information (DSI), le responsable de la sécurité des systèmes d'information (RSSI), le responsable de la technologie (CTO), les équipes informatiques ainsi que les responsables des achats dans les organisations de soins de santé. Le présent document aborde les points clés du rapport - pour plus d'informations, le lecteur est invité à se reporter à la publication de l'ENISA: Bonnes pratiques de l'ENISA pour la sécurité des services de santé, publiées en février 2020.

PROCEDURE DE PASSATION DE MARCHES

L'écosystème hospitalier étant constitué de plusieurs composantes informatiques, la cybersécurité devrait être examinée séparément dans toutes ces différentes composantes. La cybersécurité devrait être intégrée à toutes les étapes de la procédure de passation de marchés. Dans cette section, nous présentons les étapes communes de la procédure de passation de marchés pour l'obtention de produits et de services, notamment de dispositifs médicaux, de systèmes d'information et d'infrastructures.

Figure 1: Cycle de vie de la procédure de passation de marchés pour les hôpitaux



- Phase de planification: Dans un premier temps, l'hôpital analyse ses besoins et recueille en interne les demandes de plusieurs divisions. Par exemple, dans le cas de l'obtention de nouveaux services d'informatique en nuage, le CTO doit identifier les besoins et comprendre l'utilité que ces services offriront.

- Phase de sélection des fournisseurs: Ensuite, les demandes sont traduites en spécifications techniques et, en collaboration avec les responsables des achats, le processus de sélection des fournisseurs commence (par exemple, un appel d'offres est publié). L'hôpital reçoit les offres désignées, le comité (comprenant le CTO/RSSI et/ou un membre de l'équipe informatique) évalue les offres et sélectionne les produits les plus appropriés. Des négociations sont menées avec le contractant et le marché est attribué.

- Phase de gestion: Enfin, le contrat (gestion et suivi) est cédé au propriétaire de l'hôpital. L'agent désigné est responsable de la clôture de l'appel d'offres et de la réception de toute information reçue en retour des utilisateurs sur les performances réelles de l'équipement/du système/du service.

TYPES DE MARCHES DANS LES HOPITAUX

Tableau 1: Types de marchés (classification des biens)

Type de marché	Description du type
Systèmes d'information clinique	Comprend la passation de marchés pour tout type de logiciel relatif aux soins médicaux.
Dispositifs médicaux	Toute pièce de matériel informatique dédiée au traitement, au contrôle ou au diagnostic des maladies.
Équipements de réseau	Lignes de réseau (coaxiales, optiques), passerelles, routeurs, commutateurs, pare-feu, VPN, IPS, IDS, etc.
Systèmes d'accès aux soins à distance	Installations ou dispositifs destinés à fournir des soins en dehors du milieu hospitalier, en particulier ce qu'on appelle aujourd'hui les «services de soins de type hospitalier à domicile».
Dispositifs clients mobiles	Tout logiciel qui fournit une assistance de soins de santé ou une collecte de données médicales, non directement connecté au réseau de l'hôpital; par exemple, des applications de télémédecine.
Systèmes d'identification	Systèmes permettant d'identifier de manière unique les patients ou le personnel médical (scanners biométriques, lecteurs de cartes, etc.) et de garantir l'identification et/ou l'autorisation d'accès aux systèmes informatiques.
Systèmes de gestion des bâtiments	Tout type de construction pouvant accueillir des installations médicales.
Systèmes de commande industriels	Des systèmes qui contrôlent tous les aspects physiques des centres tels que les systèmes de régulation de l'énergie, les systèmes de verrouillage des portes, les systèmes de sécurité en circuit fermé.
Services professionnels	Tout type de services externalisés ou non, fournis par des professionnels ou des entreprises: services médicaux, transports, comptabilité, ingénierie, informatique, juridique, entretien, nettoyage, restauration, etc.
Services en nuage	Tout système d'information et de communication (SIC) ou tout autre système d'information qui n'est pas situé dans les bâtiments abritant les services médicaux ou dans un centre informatique sous le contrôle complet de la division informatique du centre médical.

CLASSIFICATION DES MENACES

Différents types de marchés sont associés à diverses menaces pour l'environnement TIC d'un hôpital. Consultez la classification des menaces présentée dans cette section avec votre département informatique, de la sécurité ou des risques afin d'identifier les menaces les plus pertinentes pour votre organisation. Cette activité devrait être intégrée dans les tâches informatiques de l'hôpital, indépendamment du potentiel offert par les marchés.

Tableau 2: Types de menaces (classification des menaces)

Menace	Exemples
Phénomènes naturels	Incendies, inondations ou tremblements de terre
Défaillance de la chaîne d'approvisionnement	Défaillance du fournisseur de services en nuage, défaillance du fournisseur de réseau, défaillance de l'alimentation en énergie, défaillance/irresponsabilité du fabricant de dispositifs médicaux
Erreurs humaines	Erreur de configuration du système médical, absence de journaux d'audit, contrôle d'accès non autorisé ou absence de processus, non-conformité (BYOD), erreur commise par le personnel médical/patient
Actions malveillantes	Logiciel malveillant (virus, rançongiciel, BYOD), intervention illicite (hijack) (minage pirate, piratage médical), ingénierie sociale (hameçonnage, appâtage, clonage d'appareil), vol (données, appareils), altération de dispositifs médicaux, copiage de carte, déni de service, cyberattaques, attaques dirigées contre les applications web, menace interne, manipulation/dommage physique, usurpation d'identité, cyberespionnage, endommagement mécanique des composants
Défaillances des systèmes	Défaillance d'un logiciel, micrologiciel obsolète, défaillance d'un dispositif, défaillance de composants de réseau, entretien insuffisant

BONNES PRATIQUES POUR LA CYBERSECURITE DANS LE CADRE DE LA PASSATION DE MARCHES

La liste des bonnes pratiques ci-dessous n'est en aucun cas exhaustive; elles sont cependant un atout certain pour les professionnels des technologies de l'information du secteur de la santé chargés des achats d'équipements dans les hôpitaux. L'ensemble des bonnes pratiques est le résultat collectif de toutes les contributions reçues par les professionnels de santé interrogés. Le lecteur peut adapter la liste en fonction des priorités de son organisation.

BP 1. Impliquer le département informatique dans les différentes étapes de la procédure de passation de marchés pour s'assurer que l'expertise en matière de cybersécurité est prise en considération.

Phases de la procédure de passation de marchés: Toutes

Types de marchés connexes: Toutes

Menaces connexes: Toutes

BP 2. Mettre en œuvre un processus d'identification et de gestion des vulnérabilités pour s'assurer qu'elles sont prises en compte avant de lancer la procédure de passation de marchés pour de nouveaux produits ou services et que celles des produits/services existants sont contrôlées tout au long de leur cycle de vie.

Phases de la procédure de passation de marchés: Toutes

Types de marchés connexes: Systèmes d'information clinique, dispositifs médicaux, équipements de mise en réseau, système d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Toutes

BP 3. Élaborer une politique de mise à jour du matériel et des logiciels pour s'assurer que les derniers correctifs de votre système d'exploitation et de vos logiciels sont appliqués et que l'antivirus est mis à jour.

Phases de la procédure de passation de marchés: Toutes

Types de marchés connexes: Dispositifs médicaux, systèmes d'information clinique, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement, défaillances des systèmes

BP 4. Renforcer les contrôles de sécurité des communications sans fil pour s'assurer que l'accès aux réseaux Wi-Fi de l'hôpital est limité et strictement contrôlé.

Phases de la procédure de passation de marchés: Toutes

Types de marchés connexes: Dispositifs médicaux, dispositifs clients distants, systèmes d'identification, services en nuage

Menaces connexes: Actions malveillantes, erreurs humaines

BP 5. Établir des politiques de test pour s'assurer que les produits nouvellement acquis ou nouvellement configurés subissent un test de pénétration et que les mesures correctives prises sont conformes aux paramètres opérationnels de l'environnement réel.

Phases de la procédure de passation de marchés: Toutes

Types de marchés connexes: Systèmes d'information clinique, dispositifs médicaux, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, système de gestion technique des bâtiments, systèmes de commande industriels, services en nuage

Menaces connexes: Actions malveillantes, défaillances des systèmes, erreurs humaines

BP 6. Établir des plans de continuité des activités pour s'assurer que la défaillance d'un système ne perturbera pas les services essentiels de l'hôpital et que le rôle du fournisseur est bien défini.

Phases de la procédure de passation de marchés: Toutes

Types de marchés connexes: Dispositifs médicaux, systèmes d'information clinique, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement, défaillances des systèmes

BP 7. Prendre en compte les questions d'interopérabilité pour s'assurer qu'il n'y a pas de failles de sécurité avec les composants existants (système informatique existant).

Phases de la procédure de passation de marchés: Toutes

Types de marchés connexes: Systèmes d'information clinique, dispositifs médicaux, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Défaillances des systèmes, erreurs humaines, actions malveillantes

BP 8. Permettre le test de tous les composants pour garantir qu'ils assurent leurs fonctions: vérifier la facilité d'utilisation, contrôler l'exactitude des résultats en cours de chargement et rechercher les failles de sécurité (politique de mots de passe, injection SQL).

Phases de la procédure de passation de marchés: Toutes

Types de marchés connexes: Systèmes d'information clinique, dispositifs médicaux, dispositifs clients distants, systèmes d'identification, services en nuage, systèmes de commande industriels, systèmes d'accès aux soins à distance, système de gestion technique des bâtiments, dispositifs clients mobiles

Menaces connexes: Actions malveillantes, erreurs humaines, défaillances des systèmes, défaillance de la chaîne d'approvisionnement

BP 9. Autoriser l'audit et la journalisation pour tracer les pirates et estimer quelles informations ont été perdues/volées lorsque le système a été compromis.

Phases de la procédure de passation de marchés: Toutes

Types de marchés connexes: Dispositifs médicaux, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement, défaillances des systèmes

BP 10. Crypter les données à caractère personnel sensibles, au repos et en transit, en définissant une politique pour les systèmes, les services ou les dispositifs qui traite les catégories particulières de données à caractère personnel visées par l'article 9 du RGPD.

Phases de la procédure de passation de marchés: Toutes

Types de marchés connexes: Dispositifs médicaux, systèmes d'information clinique, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement, défaillances des systèmes

GP11. Effectuer une évaluation des risques dans le cadre de la procédure de passation de marchés.

Phases de la procédure de passation de marchés: Planification

Types de marchés connexes: Toutes

Menaces connexes: Toutes

BP 12. Planifier à l'avance les besoins en matière de réseaux, de matériel et de licences pour déterminer si des mises à niveau et/ou des achats supplémentaires doivent être effectués avant l'installation pour intégrer le nouveau système.

Phases de la procédure de passation de marchés: Planification

Types de marchés connexes: Systèmes d'information clinique, équipements de mise en réseau, systèmes d'identification, systèmes de commande industriels.

Menaces connexes: Défaillance de la chaîne d'approvisionnement, défaillances des systèmes, phénomènes naturels, erreurs humaines

BP 13. Identifier les menaces liées aux produits ou services faisant l'objet de la passation de marchés et s'assurer que l'identification des menaces est continue tout au long de la procédure de passation de marchés.

Phases de la procédure de passation de marchés: Planification, gestion

Types de marchés connexes: Toutes

Menaces connexes: Toutes

BP 14. Segmenter le réseau pour s'assurer que le trafic du réseau peut être isolé et/ou filtré pour limiter et/ou empêcher l'accès entre les zones du réseau.

Phases de la procédure de passation de marchés: Planification, sélection des fournisseurs

Types de marchés connexes: Dispositifs médicaux, systèmes d'information clinique, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement, défaillances des systèmes

BP 15. Déterminer les exigences du réseau pour assurer l'interopérabilité et éviter les failles après avoir créé la topologie du réseau et des composants.

Phases de la procédure de passation de marchés: Planification

Types de marchés connexes: Systèmes d'information clinique, équipements de mise en réseau, systèmes d'identification, systèmes de commande industriels, services en nuage, systèmes de soins à distance, dispositifs clients mobiles.

Menaces connexes: Défaillance de la chaîne d'approvisionnement, défaillances des systèmes, phénomènes naturels

BP 16. Établir les exigences de base en matière de sécurité et les traduire en critères d'éligibilité pour la sélection des fournisseurs.

Phases de la procédure de passation de marchés: Planification, sélection des fournisseurs

Types de marchés connexes: Dispositifs médicaux, systèmes d'information clinique, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement, défaillances des systèmes

BP 17. Créer une demande de propositions spécifique pour l'acquisition de services en nuage en tenant compte des exigences réglementaires et politiques.

Phases de la procédure de passation de marchés: Planification, sélection des fournisseurs

Types de marchés connexes: Services en nuage

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement

BP 18. Donner la priorité aux passations de marchés de biens qui sont certifiées conformes aux systèmes/normes de cybersécurité.

Phases de la procédure de passation de marchés: Sélection des fournisseurs

Types de marchés connexes: Dispositifs médicaux, systèmes d'information clinique, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement, défaillances des systèmes

BP 19. Réaliser des évaluations d'impact sur la protection des données lors de la planification de la passation de marchés pour un nouveau système ou service.

Phases de la procédure de passation de marchés: Sélection des fournisseurs

Types de marchés connexes: Systèmes d'information clinique, dispositifs médicaux, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, services professionnels, services en nuage

Menaces connexes: Actions malveillantes, erreurs humaines

BP 20. Mettre en place des passerelles qui maintiennent les systèmes/machines existants connectés et assurer un «contrôle aux frontières» en cas de problèmes au sein de ces groupes.

Phases de la procédure de passation de marchés: Sélection des fournisseurs, gestion

Types de marchés connexes: Dispositifs médicaux, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement, défaillances des systèmes

BP 21. Offrir une formation en cybersécurité axée sur les pratiques de sécurité de l'organisation pour s'assurer que le personnel interne ou les contractants/consultants externes qui travaillent dans les locaux sont correctement formés.

Phases de la procédure de passation de marchés: Sélection des fournisseurs, gestion

Types de marchés connexes: Toutes

Menaces connexes: Actions malveillantes, erreurs humaines

BP 22. Élaborer des plans d'intervention en cas d'incident qui couvrent les produits ou systèmes nouvellement acquis.

Phases de la procédure de passation de marchés: Sélection des fournisseurs, gestion

Types de marchés connexes: Dispositifs médicaux, systèmes d'information clinique, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement, défaillances des systèmes

BP 23. Impliquer le vendeur/fabricant dans la gestion des incidents et fixer des conditions claires dans la demande de propositions.

Phases de la procédure de passation de marchés: Sélection des fournisseurs, gestion

Types de marchés connexes: Dispositifs médicaux, systèmes d'information clinique, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement, défaillances des systèmes

BP 24. Programmer et surveiller les opérations de maintenance de tous les équipements pour assurer un niveau de fonctionnalité adéquat et décider de toute mise à jour/tout correctif, etc.

Phases de la procédure de passation de marchés: Sélection des fournisseurs, gestion

Types de marchés connexes: Systèmes d'information clinique, équipements de mise en réseau, dispositifs médicaux, systèmes de gestion des bâtiments, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Erreurs humaines, défaillances des systèmes, phénomènes naturels

BP 25. L'accès à distance devrait être réduit à un minimum et administré de telle sorte que les communications externes avec le fournisseur soient limitées au seul dispositif qu'il doit contrôler.

Phases de la procédure de passation de marchés: Sélection des fournisseurs, gestion

Types de marchés connexes: Dispositifs médicaux, systèmes d'information clinique, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement, défaillances des systèmes, erreurs humaines

BP 26. Exiger l'installation de correctifs pour tous les composants et inclure les informations s'y rapportant dans la demande de propositions.

Phases de la procédure de passation de marchés: Sélection des fournisseurs, gestion

Types de marchés connexes: Dispositifs médicaux, systèmes d'information clinique, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement, défaillances des systèmes

BP 27. Sensibiliser le personnel à la cybersécurité afin de s'assurer qu'il est conscient des risques associés aux produits ou services nouvellement acquis.

Phases de la procédure de passation de marchés: Gestion

Types de marchés connexes: Toutes

Menaces connexes: Toutes

BP 28. Procéder à un inventaire des biens et mettre en œuvre la gestion de la configuration pour s'assurer que l'inventaire est correctement mis à jour lorsqu'un composant est ajouté ou retiré de l'environnement TIC et que des configurations de sécurité de base pour les composants TIC existent et sont gérées de manière appropriée.

Phases de la procédure de passation de marchés: Gestion

Types de marchés connexes: Systèmes d'information clinique, dispositifs médicaux, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification

Menaces connexes: Actions malveillantes, erreurs humaines, défaillances des systèmes

BP 29. Mettre en place des mécanismes de contrôle d'accès aux installations de dispositifs médicaux qui devraient également être physiquement protégées et accessibles uniquement au personnel spécialisé.

Phases de la procédure de passation de marchés: Gestion

Types de marchés connexes: Dispositifs médicaux, système de gestion technique des bâtiments, systèmes d'identification

Menaces connexes: Actions malveillantes, erreurs humaines

BP 30. Programmer des tests de pénétration fréquemment ou après un changement d'architecture/de système et inclure les conditions dans la demande de propositions.

Phases de la procédure de passation de marchés: Sélection des fournisseurs, gestion

Types de marchés connexes: Dispositifs médicaux, systèmes d'information clinique, équipements de mise en réseau, systèmes d'accès aux soins à distance, dispositifs clients mobiles, systèmes d'identification, systèmes de commande industriels, services en nuage

Menaces connexes: Actions malveillantes, défaillance de la chaîne d'approvisionnement, défaillances des systèmes