CYBERSÉCURITÉ

En bref

La cybersécurité regroupe l'ensemble des mesures techniques, organisationnelles et humaines visant à protéger les systèmes d'information contre les menaces numériques : attaques externes, erreurs internes, compromission de comptes, etc.

Ces menaces peuvent altérer la disponibilité, l'intégrité ou la confidentialité des données critiques, avec un impact direct sur la fiabilité des états financiers et la continuité d'exploitation de l'entité.

Pour le commissaire aux comptes, la cybersécurité constitue désormais un facteur de risque transversal, à intégrer dans la cartographie (NEP 315) et à articuler avec les autres volets SI (accès, exploitation, sous-traitance, PCA/PRI…).

Les points de vigilance majeurs portent notamment sur :
- La présence d'un Responsable Sécurité des Systèmes d'Information (RSSI) identifié et d'une Politique de Sécurité du Système d'Information (PSSI) formalisée et actualisée ;
- L'existence de procédures de gestion d'incident (détection, traitement, notification, documentation) ;
- La sécurisation des accès critiques (authentification renforcée – MFA, journalisation, accès distants) ;
- La résilience opérationnelle, via des sauvegardes effectives, testées, et un plan de reprise informatique (PRI) adapté ;
- La sensibilisation du personnel aux risques cyber (phishing, fraude au président, erreurs humaines) ;
- La prise en compte des tiers critiques (éditeurs, infogérants, hébergeurs) dans la politique de sécurité.

Une faiblesse sur ces points peut affecter directement l'information financière et justifier un renforcement des contrôles ou prise en considération dans la stratégie d'audit.

Séquence 1

Comprendre la thématique

Contexte et enjeux

La cybersécurité permet de lutter contre la cybercriminalité qui désigne les délits perpétrés à distance par des systèmes de communication comme Internet.

La cybercriminalité concerne non seulement les formes traditionnelles de criminalité, opérées via Internet, mais aussi l'atteinte à la confidentialité, l'intégrité et la disponibilité des systèmes d'information.

Une cyberattaque est donc un acte malveillant destiné à perturber le bon fonctionnement d'un système d'information.

Elles peuvent être distinguées :
- **L'attaque technique par le canal internet :** ces attaques exploitent une faille technique du site web ou du réseau de l'entreprise pour ensuite s'introduire dans son système d'information ou installer des logiciels malveillants. Ce type d'attaque nécessite des outils informatiques capables de contourner les dispositifs de sécurité du système d'information.
- **L'ingénierie sociale :** ces attaques exploitent les failles humaines, le maillon faible de la sécurité informatique. Grâce à des techniques manipulatoires, les cybercriminels amènent les collaborateurs de l'entreprise à compromettre la sécurité du système d'information.

NEP, textes et références :
- **NEP 240 :** Conformément à cette norme, le commissaire aux comptes doit évaluer les risques d'anomalies significatives dans les comptes résultant de ce type de fraude. La cybercriminalité a toutes les caractéristiques de la fraude telles que définies par cette norme.

FICHE 08

CYBERSÉCURITÉ

→ **Doctrine de la CNCC** relative aux prestations entrant dans le cadre des Services Autres que la Certification des Comptes (SACC)

→ **NIS2** : Directive européenne visant à renforcer la sécurité des réseaux et des systèmes d'information au sein de l'UE, en imposant des mesures de sécurité plus strictes et des sanctions harmonisées.
Pour les PME non directement concernées, cette directive peut servir de référentiel de bonnes pratiques.
Elle contient :
- Des mesures de sécurité informatique adaptées,
- La notification des incidents graves,
- Et prévoit des sanctions harmonisées.

→ **DORA** : Réglementation européenne visant à garantir la résilience opérationnelle des entités financières face aux risques numériques, en imposant des exigences en matière de gestion des risques informatiques et de notification des incidents.
Bien que DORA ne s'applique pas aux PME en dehors du secteur financier, elle constitue un cadre de référence pertinent pour renforcer les dispositifs de cybersécurité dans toute organisation, en s'inspirant de ses principes : gestion des risques, continuité d'activité, et protection des systèmes critiques.
Les exigences clés de la réglementation incluent :
- Une gestion structurée des risques TIC (identification, protection, détection, réponse et rétablissement)
- Des tests réguliers de résilience numérique, adaptés à la taille et à la complexité de l'entité
- Une surveillance renforcée des prestataires de services numériques (cloud, hébergeurs, etc.)
- L'obligation de notifier rapidement les incidents majeurs aux autorités compétentes

→ **CobiT** dont les défaillances peuvent rendre l'entité vulnérable aux cyberattaques.

Conséquences pour le commissaire aux comptes

La cybersécurité est un enjeu crucial pour les commissaires aux comptes, car les cyberattaques peuvent gravement compromettre la fiabilité des états financiers et la continuité des activités de l'entité auditée.

Il est important pour les commissaires aux comptes d'intégrer les risques liés à la cybersécurité dans leur évaluation globale des risques, en identifiant les vulnérabilités potentielles et les menaces spécifiques à l'entité.

Ils doivent également évaluer les dispositifs de gestion de la cybersécurité mis en œuvre par l'entreprise (stratégie, gouvernance, comitologie, procédure, cartographies des risques cyber, plans de formation, veille, etc.).

Ils doivent également vérifier l'efficacité des contrôles internes mis en place pour prévenir, détecter et suivre les cyberattaques, en portant une attention particulière aux failles humaines exploitées par l'ingénierie sociale.

Les cyberattaques peuvent entraîner des pertes financières directes, telles que des rançons payées, et indirectes, comme des interruptions d'activité. Il est essentiel d'évaluer l'impact de ces pertes sur les états financiers et de vérifier si l'entité a correctement comptabilisé et divulgué les incidents de cybersécurité.

De plus, il est nécessaire de s'assurer que des plans de continuité des activités et de reprise après sinistre sont en place et efficaces, afin de garantir la pérennité des opérations de l'entité.

Il faut également être conscient des obligations légales et réglementaires en matière de cybersécurité auxquelles l'entité est soumise, telles que les exigences de notification des incidents dans le cadre de la réglementation DORA et les normes de protection des données personnelles RGPD.

Le non-respect de ces obligations peut entraîner des sanctions et des amendes, impactant la situation financière de l'entité.

Séquence 2

Mission du CAC : objectifs, bonnes pratiques et outils

Thématique

Analyse des risques et facteurs de criticité

Objectifs

Dans le cadre de sa mission et conformément à la NEP 240 (évaluation des risques d'anomalies significatives dans les comptes résultant de fraudes), le commissaire aux comptes doit intégrer les risques liés à la cybersécurité dans son évaluation globale des risques.

Il s'attache à identifier les vulnérabilités potentielles et les menaces spécifiques à l'entité auditée.

Il doit évaluer la conception et l'efficacité des dispositifs de gestion de la cybersécurité mis en œuvre par l'entreprise (stratégie, gouvernance, comitologie, procédures, cartographies des risques cyber, plans de formation, veille, etc.).

Il doit vérifier l'efficacité des contrôles internes mis en place pour prévenir, détecter et suivre les cyberattaques, en portant une attention particulière aux failles humaines exploitées par l'ingénierie sociale.

Le commissaire aux comptes doit également s'assurer que l'entité a correctement comptabilisé et divulgué les incidents de cybersécurité dans ses états financiers. De plus, il est nécessaire de valider l'existence et l'efficacité des plans de continuité des activités et de reprise après sinistre, afin de garantir la pérennité des opérations de l'entité.

Ces travaux visent à garantir la fiabilité des états financiers, la sécurité des systèmes d'information et la continuité des activités de l'entité auditée.

Les failles usuellement exploitées par les attaques techniques concernent principalement la sécurité des applications Web. Trois raisons peuvent en être à l'origine :
- La gestion incorrecte de l'authentification, des habilitations et du contrôle d'accès,
- L'injection de données qui est une technique consistant à insérer des données en entrée d'un programme informatique afin de les détourner de leur fonction d'origine,
- Les fuites d'information si les fonctionnalités ou composants internes à une application ne sont pas suffisamment « cloisonnés ».

Certes l'ingénierie sociale tire profit de la naïveté et de la crédulité de ses victimes, mais plusieurs autres facteurs de criticité sont de nature à favoriser ce type de cyberattaques :
- La facilité d'accès aux informations décrivant l'organisation de l'entreprise,
- L'accès aux informations personnelles des collaborateurs via les réseaux sociaux ou des portails RH,
- L'utilisation par les collaborateurs de technologies non sécurisées,
- L'utilisation par les collaborateurs d'équipements personnels dans un contexte professionnel (BYOD : Bring Your Own Device ou AVEPC en français : Apportez Votre Équipement Personnel de Communication),
- La complexité et la décentralisation des organisations,
- La généralisation du travail à distance,
- Le nomadisme professionnel et le télétravail,
- Le manque d'exemplarité des dirigeants,
- Et bien évidemment, le manque de contrôle interne et de formations associées.

Quelques exemples de cyberattaque

- Hameçonnage (phishing) ou harponnage (spear phishing),
- Logiciel malveillant (malware),
- Cassage de mot de passe,
- Attaques par déni de service (DoS) et par déni de service distribué (DDoS),

Quelques exemples récents

- **Virus Cryptolocker** : Un mail intitulé « relance facture impayée » est envoyé au comptable d'une entreprise. Le document joint contient un virus qui va chiffrer toutes les données accessibles par l'ordinateur contaminé et les rendre inutilisables. La clé de déchiffrement est fournie contre le paiement d'une rançon.

FICHE 08

CYBERSÉCURITÉ

- **Fraude aux virements :** Un important groupe industriel français a reçu un avis de changement de RIB, expédié soi-disant par un fournisseur, juste avant le règlement d'échéances importantes. Cette escroquerie a permis de dérober 1,6 M€ à la victime.
- **Espionnage économique :** Un Ministère français a fait l'objet d'une intrusion informatique et d'un vol de données. Le point de départ a été l'ouverture de fichiers contaminés par des utilisateurs manipulés et crédules.
- **Ransomware sur l'infrastructure cloud :** Une grande entreprise de services numériques a été touchée par une attaque de ransomware. L'attaque a entraîné le chiffrement de données hébergées dans le cloud, causant une paralysie partielle des opérations pendant plusieurs jours. Les attaquants ont exigé une rançon en cryptomonnaie pour fournir la clé de déchiffrement.
- **Fuite de données via un fournisseur tiers :** Une entreprise de distribution a subi une fuite massive de données, impliquant une faille chez un prestataire externe. Des données personnelles de millions de clients ont été rendues publiques. La fuite incluait des adresses, numéros de téléphone, et historiques d'achat, provoquant un tollé auprès des clients et des autorités de régulation.
- **Compromission par phishing ciblé :** Une société financière a été victime d'une attaque de type spear-phishing. Des employés ont été piégés, ce qui a permis aux attaquants de s'introduire dans les systèmes internes et d'accéder à des informations sensibles. L'attaque a été facilitée par l'utilisation de faux mails imitant parfaitement ceux de la direction, rendant la détection très difficile.
- **Attaque DDoS à grande échelle :** Une plateforme en ligne a été visée par une attaque par déni de service distribuée, qui a rendu ses services indisponibles durant près de 24 heures à un moment crucial de l'année. Des millions de requêtes malveillantes ont saturé les serveurs, empêchant les utilisateurs d'accéder à la plateforme pendant le pic des ventes saisonnières.
- **Fraude au président :** Une entreprise française de BTP a été victime d'une fraude au président. Un escroc s'est fait passer par téléphone pour le PDG, prétextant une opération confidentielle et urgente. Grâce à une mise en scène soignée et à des techniques de manipulation psychologique, il a convaincu la directrice financière de réaliser plusieurs virements internationaux. Le préjudice s'est élevé à plus de 20 millions d'euros. Cette attaque a été rendue possible grâce à une phase de renseignement préalable sur l'organigramme et les procédures internes de l'entreprise.

Top menaces

Menace	Principales contre-mesures
Phishing / Spear-phishing	→ Formation et sensibilisation régulières des collaborateurs → Simulations d'attaques → Filtrage des e-mails (anti-spam, antivirus) → Authentification multifactorielle (MFA)
Ransomware (ex : Cryptolocker)	→ Sauvegardes régulières et hors ligne → Plan de continuité et reprise d'activité (PCA / PRA) → Mise à jour régulière des systèmes → Détection comportementale (EDR)
Fuite de données via tiers (prestataires)	→ Audit des prestataires (sécurité, conformité RGPD) → Clauses de sécurité dans les contrats → Contrôles d'accès stricts → Cartographie des flux de données sensibles
Attaques DoS / DDoS	→ Pare-feu applicatifs (WAF) → Services de mitigation DDoS (ex. CDN) → Surveillance du trafic réseau (SOC) → Test de résilience des systèmes critiques

Bonnes pratiques

Mesures préventives :

- Nommer un responsable de la sécurité du système d'information (RSSI) qui serait garant de la correcte applications des règles de sécurité,
- Définir et formaliser une politique globale de sécurité des systèmes d'information (PSSI) reflétant la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information (SSI) et incluant les règles et les principes en matière de cybersécurité permettant ainsi de renforcer considérablement la sécurité de l'organisation en définissant des mesures de sécurité proactives pour les systèmes et les données, la PSSI et en prévenant les accès non autorisés, les pertes de données et les cyberattaques.

La PSSI doit se composer à minima des sections suivantes :
- L'introduction permettant de situer la place de la PSSI dans le référentiel normatif de la SSI au sein de l'organisme et de préciser les bases de légitimité sur lesquelles elle s'appuie,
- La méthodologie présente, de façon détaillée, la conduite de projet d'élaboration d'une PSSI, ainsi que des recommandations pour la construction des règles de sécurité,
- Le référentiel de principes de sécurité détaillant les différents domaines de la sécurité généralement couverts par une PSSI,
- Une liste de documents de références de la SSI (critères d'évaluation, textes législatifs, normes, codes d'éthique, notes complémentaires...).

→ Définir une stratégie et une gouvernance dédiées à la gestion de cybersécurité (organisation, rôles et responsabilités, procédures et politiques, comitologie, reporting, monitoring, veille etc.),
→ Définir une procédure de gestion et de suivi des incidents de cybersécurité,
→ Formaliser et mettre à jour régulièrement une cartographie des risques de cybersécurité, en considérant les risques cybersécurité liés aux nouvelles technologies, les événements redoutés apparus, les dispositifs de maîtrise de risques mis en place, les évaluations brutes et nettes des risques de cybersécurité, etc.,
→ Définir et mettre en place un cadre de contrôle internes permettant de prévenir, détecter et suivre les cyberattaques,
→ Définir un processus permettant d'inclure des exigences de cybersécurité par défaut dans les nouveaux projets,
→ Définir des procédures de sélection et d'autorisation de nouveaux matériels ou logiciels,
→ Définir des procédures de gestion d'accès aux informations par des tiers,
→ Définir une politique de déclassement de matériel informatique,
→ Définir une politique de cryptage des données,
→ Renforcer les mécanismes d'authentification au travers la mise en place de l'authentification multi-facteurs (MFA) et l'utilisation de mot de passe fort et conformes aux bonnes pratiques en place (CNIL, ANSSI, etc.),
→ Mettre à jour de manière régulière les logiciels, les anti-virus et configurer le pare-feu,
→ Limiter les accès aux informations sensibles au travers la correcte définition des profils et des droits et la mise en place des règles de séparation des tâches,
→ Différencier les usages personnels des usages professionnels du matériel informatique,
→ Sensibiliser et former le personnel à la question de la cybersécurité et aux risques liés aux emails,
→ Sécuriser les accès réseaux de l'entreprise.

Mesures détectives :
→ Mettre en place des diagnostics pré ou post implémentation permettent d'identifier les insuffisances en termes de cybersécurité dans la conception et dans l'implémentation d'un projet et de vérifier le respect des bonnes pratiques de sécurité,
→ Réaliser régulièrement des audits de cybersécurité afin de fournir au management une vue globale de la maturité de la cybersécurité, de se comparer par rapport aux pairs et d'identifier les actions correctives à mettre en œuvre,
→ Réaliser périodiquement des tests d'intrusion permettant de mettre en évidence les vulnérabilités du SI, les risques de cybersécurité encourus et les actions correctives nécessaires,
→ Réaliser régulièrement des tests de continuité d'activité et de secours informatique,
→ Réaliser des diagnostic cyber-résilience conformément à la réglementation NIS2 afin d'évaluer le potentiel de résilience par rapport à des attaques de type ransomware et d'identifier les actions pragmatiques pour renforcer la résilience de l'entreprise,
→ Vérifier la conformité RGPD afin d'obtenir une vision globale du niveau de conformité, puis identifier les non-conformités et le reste à faire afin de répondre aux exigences du régulateur.

FICHE 08

CYBERSÉCURITÉ

Outils & documentations mises à disposition

Après avoir analysé la prise en compte des risques par la direction générale, l'auditeur pourra se consacrer à l'évaluation des dispositifs de prévention de l'entreprise avec des questions telles que :

Thème / Question	Enjeu / Risque	Interlocuteur	Niveau de maturité : Non implémenté Démarche en cours de mise en œuvre Démarche en place
Existe-t-il une stratégie de cybersécurité définie ? Une gouvernance dédiée à la gestion cybersécurité est-elle définie et mise en place ?	Opérationnel	DSI	
Existe-t-il une gouvernance dédiée à la gestion de la sécurité de l'information : un comité sécurité, un responsable de la sécurité du système d'information (RSSI) et des correspondants sécurité dans les unités ?	Opérationnel	DSI	
Une politique de sécurité des systèmes d'information est-elle formalisée et mise à jour ?	Opérationnel	DSI	
Existe-t-il une attribution claire des responsabilités pour la mise en œuvre et le suivi des évolutions à apporter en matière de sécurité du SI ?	Opérationnel	DSI	
La direction a-t-elle mis en place une organisation et des contrôles Diagnostic pré ou post implémentation permettant d'identifier les insuffisances en termes de cybersécurité dans la conception et dans l'implémentation d'un projet et de vérifier le respect des bonnes pratiques de sécurité ?	Opérationnel	DSI	
Existe-t-il des procédures d'autorisation de nouveaux matériels ou logiciels ?	Opérationnel	DSI	
Existe-t-il des procédures applicables à l'accès aux informations par des tiers ?	Opérationnel	DSI	
Existe-t-il des modalités de réaction aux incidents de sécurité et aux défauts de fonctionnement conformément aux exigences réglementaires en vigueur (ex. NIS2) : → Signalement rapide des incidents de sécurité → Signalement dysfonctionnements de logiciels → Capitalisation sur la résolution d'incidents → Processus disciplinaire	Opérationnel	DSI	
Les connexions à distance sont-elles réalisées de manière sécurisée ? (VPN par exemple) Les dispositifs de cybersécurité ont-ils été adaptés par rapport à la généralisation du télétravail par suite de la crise sanitaire ?	Opérationnel	DSI	
Les échanges d'informations sont-ils réalisés de manière chiffrée ?	Opérationnel	DSI	
Les ordinateurs de bureau et les serveurs de l'organisation sont-ils tous protégés par un anti-virus ? Les vulnérabilités de de sécurité font-elles l'objet d'une analyse et d'un suivi réguliers ?	Opérationnel	DSI	
L'organisation s'assure-t-elle que tous les anti-virus sont à jour et fonctionnent correctement ? Si possible de façon centralisée, sinon selon une procédure documentée.	Opérationnel	DSI	
Les règles de contrôle d'accès sont-elles formalisées dans un format « tout est interdit sauf » plutôt que « tout est permis sauf » ? Ces règles sont-elles transmises aux salariés ?	Opérationnel	DSI	

Thème / Question	Enjeu / Risque	Interlocuteur	Niveau de maturité : Non implémenté Démarche en cours de mise en œuvre Démarche en place
La gestion des mots de passe et les systèmes de déconnexion automatique vérifient-ils les règles suivantes : Tout compte utilisateur doit être protégé par un mot de passe ; → Engagement des utilisateurs à ne pas divulguer leur mot de passe ; ne pas écrire leur mot de passe de façon trop évidente ; ne pas stocker leur mot de passe dans une procédure automatique ; changer leur mot de passe dès qu'ils le soupçonnent d'être compromis ; → Contrôle qu'un mot de passe temporaire est envoyé pour la première utilisation et qu'il est bien changé par l'utilisateur dès la première utilisation ; → Contrôle que les mots de passe temporaires sont transmis aux utilisateurs de manière sûre ; → Contrôle que le système impose un changement régulier du mot de passe ; → Contrôle que le système impose le choix de mots de passe robustes ;	Opérationnel	DSI	
La direction a-t-elle mis en place des contrôles suffisants et efficaces permettant d'évaluer le niveau de sécurité de l'annuaire Active Directory, système névralgique de l'entreprise, dont dépend la sécurité de la majeure partie du SI ?	Opérationnel	DSI	
La direction générale a-t-elle mobilisé les compétences requises pour comprendre les risques de cybercriminalité et déterminer si le management prend les actions appropriées ?	Opérationnel Juridique	DG	
La direction générale bénéficie-t-elle d'un retour direct du responsable de la sécurité pour lui expliquer en des « termes opérationnels et stratégiques » les cyber risques et leur prévention ?	Opérationnel Juridique Image	DG	
Une attention suffisante est-elle aussi bien consacrée à la défense a priori contre les attaques qu'aux opérations de remise en état des systèmes a posteriori ? La DG a-t-elle mis en place un reporting pour centraliser et suivre les différentes tentatives de fraude au sein de l'organisation ?	Opérationnel Juridique Image	DG	
Les fonctions essentielles de l'entreprise ont-elles été sécurisées pour préserver la résilience de l'entreprise en cas d'attaque ?	Opérationnel	DG	
La DG a-t-elle mis en place une cartographie des risques cybersécurité ? La DG a-t-elle identifié les scénarios possibles en fonction des types d'attaques ? Les données sensibles sont-elles identifiées et protégées ? Les plans d'actions en cas de crise sont-ils effectivement mis à jour en fonction des évolutions technologiques ou opérationnelles ?	Opérationnel Juridique Image	DG	
La cartographie des risques cybersécurité est-elle mise à jour régulièrement ? Les exigences cybersécurité liés aux nouvelles réglementations et les nouvelles menaces sont-elles prises en compte dans la mise à jour de la cartographie des risques cybersécurité (ex. DORA, NIS2)	Opérationnel	DG	
Existe-il un plan de formation et des campagnes de sensibilisation pour les collaborateurs aux règles de cybersécurité mises en place et aux nouvelles menaces de cybersécurité ?	Opérationnel	DSI	
La cartographie des risques cybersécurité est-elle mise à jour régulièrement par rapport aux nouvelles technologies et prend-elle en compte les nouveaux risques liés à l'intelligence artificielle ?	Opérationnel	DSI	

FICHE 08

CYBERSÉCURITÉ

Thème / Question	Enjeu / Risque	Interlocuteur	Niveau de maturité : Non implémenté Démarche en cours de mise en œuvre Démarche en place
La direction a-t-elle réalisé un diagnostic de maturité cybersécurité afin de fournir au management une vue globale de la maturité de la cybersécurité, de se comparer par rapport aux pairs et d'identifier les actions correctives à mettre en œuvre ?	Opérationnel	DSI	
La direction a-t-elle réalisé un diagnostic de la résilience conformément à la réglementation DORA afin d'évaluer le potentiel de résilience par rapport à des attaques de type ransomware et d'identifier les actions pragmatiques pour renforcer la résilience de l'entreprise ?	Opérationnel	DSI	

Dans le contexte d'une TPE / PME ou autre entité ne disposant pas de service informatique interne avec des personnes dédiées, le questionnaire simplifié suivant peut s'appliquer :

1. L'entité a-t-elle un annuaire ou une cartographie des applications critiques pour son activité ?
2. Des processus de gestion des comptes utilisateurs sont en place pour gérer les arrivées et les départs de collaborateurs (trices) ? *Cf. Fiche 02 - Contrôle des accès*
3. L'entité réalise-t-elle régulièrement des revues de comptes utilisateurs ? *Cf. Fiche 02 - Contrôle des accès*
4. Les paramétrages de mot des applications sensibles respectent-ils les bonnes pratiques en matière de longueur, de complexité, de durée de vie, etc. Se référer aux règles de l'ANSSI applicables à la date de l'intervention chez le client. *Cf. Fiche 02 - Contrôle des accès*
5. Les matériels nomades (PC portables, tablettes, smartphone) sont-ils dotés de moyens de protection non désactivable (chiffrement, mot de passe, etc.) *Cf. Fiche 02 - Contrôle des accès*
6. Les matériels de type PC portables, PC fixes ou serveur sont-ils dotés d'un antivirus avec des mises à jour automatiques ?
7. Un pare-feu est-il déployé et non désactivable ? Un VPN est-il déployé ?
8. Les collaborateurs sont-ils sensibilisés régulièrement aux risques liés à la cybercriminalité ?
9. L'entité a initié une démarche de continuité informatique que ce soit avec ses fournisseurs de logiciels que pour les matériels hébergés en interne ? *Cf. Fiche 07 - Plan de continuité d'activité et plan de reprise informatique*
10. L'entité a défini des modalités d'utilisation des outils d'IA (ex : ChatGPT) selon les bonnes pratiques ?

Impact dans la stratégie du commissaire aux comptes

L'intégration des risques liés à la cybersécurité dans la stratégie d'audit est essentielle pour garantir la fiabilité des états financiers et la sécurité des systèmes d'information de l'entité auditée.

Il est crucial d'être particulièrement vigilant quant aux vulnérabilités potentielles et aux menaces spécifiques à l'entité, en évaluant les contrôles internes et les plans de continuité des activités.

En promouvant les bonnes pratiques de cybersécurité, on contribue à l'amélioration des contrôles internes, ce qui permet de prévenir et de détecter les cyberattaques plus efficacement.

De plus, la vérification de la comptabilisation et de la divulgation des incidents de cybersécurité dans les états financiers assure une transparence et une fiabilité accrues des informations financières.

Un rôle clé est également joué dans la sensibilisation et la formation du personnel de l'entité auditée aux risques de cybersécurité.

En intégrant ces risques dans l'évaluation globale, on contribue à la réduction des risques d'anomalies significatives dans les comptes résultant de fraudes.

Cette approche permet de mieux protéger l'entité auditée contre les cybermenaces, d'assurer la continuité des opérations et de garantir la fiabilité des états financiers.

L'évaluation des risques cybersécurité en CAC, permet ainsi de garantir que les comptes reflètent fidèlement la réalité économique, tout en répondant aux exigences normatives et en contribuant à la sécurité financière de l'entreprise.

L'évaluation des risques liés à la cybersécurité conjointement à l'évaluation des dispositifs de contrôle interne IT dans le cadre d'un commissariat aux comptes (CAC) est devenue indispensable, car la cybersécurité peut directement impacter la fiabilité de l'information financière, permet d'avoir une vision globale et une compréhension détaillée de l'environnement informatique d'une organisation.

En effet, les cyberattaques peuvent provoquer des pertes financières directes (ex. : fraude, ransomware), affecter la disponibilité, l'intégrité ou la confidentialité des données comptables et entraîner des provisions, des dépréciations ou des pertes à constater. Par conséquent, le commissaire aux comptes doit donc évaluer si les risques liés à la cybersécurité sont susceptibles d'affecter significativement les comptes.

En outre, le CAC doit évaluer si des cybermenaces, des fraudes ou des anomalies identifiées peuvent compromettre la fiabilité des documents audités car ces attaques peuvent être l'origine de fraudes comptables (manipulation de données), d'usurpation d'identité (faux ordres de virement, faux fournisseurs) ou de disparition ou altération de preuves d'audit.

Par ailleurs, le CAC a pour mission d'évaluer la qualité du système de contrôle interne, dont la cybersécurité est aujourd'hui un maillon essentiel.

En effet, des faiblesses en cybersécurité peuvent révéler une maîtrise insuffisante des risques globaux de l'entreprise.

Une attaque cyber peut compromettre la capacité de l'entreprise à poursuivre son activité ce qui est indispensable pour assurer la fiabilité et l'intégrité des états financiers.

L'évaluation des autres dispositifs de contrôle interne IT peut s'appuyer sur les fiches CRCC dédiées à chacune des thématiques, à savoir :
→ Gouvernance des systèmes d'information,
→ Exploitation des systèmes d'information,
→ Contrôle des accès,
→ Conformité Réglementaire,
→ Plan de continuité d'activité,
→ Etc.

Séquence 3

Cas d'usage

Contexte

Dans le cadre de notre mission légale auprès de l'entité « Data & Flow », nous avons identifié, dès la phase de prise de connaissance, que le contexte de télétravail généralisé et l'utilisation massive des outils collaboratifs présentaient un risque accru d'usurpation d'identité et d'ingénierie sociale.

Au cours de l'exercice, l'entreprise a été victime d'une fraude au président : un fraudeur, en se faisant passer par e-mail pour le PDG, a convaincu un cadre du service comptabilité d'effectuer plusieurs virements urgents vers un compte à l'étranger. Le préjudice s'élève à 350 000 euros.

L'enquête interne a révélé l'absence de procédure de vérification des demandes exceptionnelles, une sécurité insuffisante des boîtes mail, et un faible niveau de sensibilisation des équipes.

Travaux à réaliser

→ **Investigation à la suite de la fraude cyber :** Vérification que les causes et conséquences de la fraude cyber ont bien été identifiées en analysant la chronologie de la fraude encourue, que les leçons ont été tirées et sont traduites en recommandations réalistes en ligne avec les attentes du top management.
→ **Revue de la messagerie électronique professionnelle :** Vérification de la configuration des protections contre l'usurpation d'identité (SPF, DKIM, DMARC) et recherche de domaines similaires à celui de l'entreprise. Analyse des journaux d'accès à la messagerie et des règles de transfert.
→ **Entretiens avec les équipes comptables et financières :** Compréhension du processus habituel de validation des virements, analyse de la réaction face à une demande inhabituelle et évaluation du niveau de vigilance des collaborateurs. Vérification avec les équipes que des actions de formation et de sensibilisation au cas de fraude identifiés sont bien menés suite à l'incident.

FICHE 08

CYBERSÉCURITÉ

- **Examen du contrôle interne :** Revue de l'existence de procédures formelles de validation en cas de paiement exceptionnel ou confidentiel, et évaluation de l'efficacité du principe de séparation des tâches.
- **Analyse de la sensibilisation au risque cyber :** État des lieux des formations internes, tests de phishing éventuels et communication interne autour des risques de fraude.

Impact pour notre stratégie d'audit

Ces éléments sont susceptibles d'influencer :
- Notre appréciation du contrôle interne sur les flux financiers et la fiabilité des systèmes d'information,
- Notre stratégie d'audit sur les opérations bancaires sensibles, notamment les paiements exceptionnels ou non récurrents,
- L'évaluation de l'environnement de contrôle et de la culture de sécurité dans l'entité,
- Le contenu de nos recommandations à destination de la gouvernance en matière de cybersécurité,
- L'analyse de la nécessité d'un ajustement de l'approche substantielle, notamment en cas de doutes sur la fiabilité des processus automatisés.

Démarche

Investigation à la suite de la fraude cyber :
Compréhension des causes et des conséquences de la fraude cyber, analyse de la chronologie de la fraude encourue, que les leçons ont été tirées et sont traduites en recommandations réalistes en ligne avec les attentes du top management.

Évaluation de la conception du contrôle (Design Effectiveness)
Objectif : Vérifier que les processus de validation de paiements et les mesures de cybersécurité préviennent efficacement ce type de fraude.
Question clé : Les processus de validation et la sécurité des communications sont-ils suffisamment robustes pour détecter une usurpation d'identité ?

Évaluation de l'efficacité opérationnelle du contrôle (Operating Effectiveness)
Objectif : tester si les dispositifs sont réellement appliqués et si les collaborateurs sont capables d'identifier une tentative d'escroquerie.

Méthodologie

- Analyse de la chronologie de la fraude encourue,
- Prise de connaissance des recommandations identifiées, des actions correctives définies à court, moyen et long terme et vérification du correct suivi des plans d'action associés par le top management,
- Analyse de la messagerie électronique de l'entreprise (SPF, DKIM, DMARC, MFA, journalisation),
- Revue des processus de validation des paiements exceptionnels : double signature, seuils d'alerte, confirmation téléphonique,
- Entretiens avec les collaborateurs exposés (comptabilité, direction financière) pour évaluer leur niveau de vigilance et de formation,
- Analyse de l'incident de fraude : déclencheur, détection, traitement, actions correctives,
- Vérification des actions de sensibilisation menées et du suivi post-incident.

Séquences de tests détaillées

Revue de la sécurité des échanges électroniques
- Les mesures anti-usurpation (SPF, DKIM, DMARC) sont-elles configurées ?
- L'authentification multifacteurs est-elle activée sur les boîtes sensibles ?
- Y a-t-il un système d'alerte pour les connexions inhabituelles ?

Analyse de l'incident de fraude au président
- Comment l'usurpation a-t-elle été rendue possible ?
- L'utilisateur ciblé avait-il reçu une formation sur les risques de fraude ?
- Des procédures existaient-elles pour vérifier les ordres de paiement exceptionnels ?

Contrôle des bonnes pratiques internes
- Des seuils de validation sont-ils définis pour les virements ?
- Existe-t-il une séparation des tâches dans le processus de paiement ?
- Les formations cybersécurité sont-elles à jour et diffusées à l'ensemble des équipes ?
- Des campagnes de simulation de fraude ou de phishing sont-elles organisées ?

Observations attendues

Sur la conception du contrôle :
- La gouvernance cyber intègre-t-elle les risques liés à l'ingénierie sociale ?
- Les procédures de validation financière incluent-elles des étapes de vérification systématique ?
- Une stratégie anti-fraude est-elle formalisée et diffusée en interne ?

Sur l'application du contrôle :
- Des mesures concrètes ont-elles été prises après la fraude ? (MFA, procédures, sensibilisation)
- Le personnel a-t-il été sensibilisé spécifiquement à la fraude au président ?
- Les incidents sont-ils documentés et utilisés comme base d'amélioration ?

Conclusion

L'audit réalisé chez « Data & Flow » a mis en lumière un environnement exposé aux risques de fraude par ingénierie sociale, notamment en raison d'un télétravail étendu, d'un usage massif des outils collaboratifs et de procédures internes insuffisamment robustes.

L'incident de fraude au président a révélé l'absence de mécanismes de vérification adaptés aux demandes inhabituelles, une sécurité technique des messageries perfectible, ainsi qu'un déficit de sensibilisation des équipes aux risques cyber.

Bien que certaines mesures aient été prises après l'incident (comme l'instauration de l'authentification multi-facteurs ou la mise à jour des procédures), ces actions doivent s'inscrire dans une démarche globale et pérenne de sécurisation des flux sensibles.

Il est ainsi recommandé de formaliser une politique anti-fraude complète, d'intégrer les contrôles de cybersécurité aux processus financiers critiques, et d'intensifier les formations ainsi que les tests de simulation auprès des équipes à risque.

Mini-checklist CAC – Cybersécurité

- L'entreprise a-t-elle été victime d'une fraude par ingénierie sociale ?
- Existe-t-il une procédure spécifique pour les paiements exceptionnels ?
- Un système de double validation est-il en place pour les virements sensibles ?
- Les collaborateurs sont-ils formés à détecter les fraudes par usurpation d'identité ?
- Un MFA est-il activé pour les comptes à privilèges et les boîtes de direction ?
- La messagerie est-elle sécurisée via SPF, DKIM, DMARC ?
- Les incidents sont-ils documentés et analysés ?
- Une culture de cybersécurité est-elle portée par la gouvernance ?
- Des tests de sensibilisation (phishing, fraude simulée) sont-ils organisés ?
- Les sous-traitants (comptabilité externalisée, DAF externalisé) sont-ils sensibilisés ?
- Les contrôles liés à la chaîne de paiement sont-ils à jour et testés ?

Séquence 4

Allez plus loin

Ressources pratiques

Outils CRCC, NEP spécifiques, guides techniques rapides
- Checklist cybersécurité – CNCC
- Grille d'audit cybersécurité (inspirée EBIOS/NIST)
- Liste des 42 mesures essentielles de l'ANSSI
- NEP 315, 330, 240, 265
- CRCC, « La cybersécurité dans la mission du CAC en PME » et « Questions types à poser au DSI / RSSI »

Formations recommandées

- CNCC – Formation « Cybersécurité et missions du CAC »
- CNAM – « Cybersécurité pour les non-informaticiens »
- ANSSI – MOOC SecNumAcadémie