



Institut Supérieur des Etudes Technologiques de Sfax  
Départements informatiques

# Rapport

En Projet Analyse de Risque ISO 27005

**Sujet: Conseillé Bancaire**

Elaboré et présenté par:

**Abdelly Fahd,**

**Ben Ameer Amel,**

**Dhifaoui Achref,**

**& Slimene Montassar**

Groupe: MP ASSCC 2

# Table des matière

Étude de Cas – Conseiller Bancaire .....	3
Enoncé : .....	3
Echelle de valorisation des actifs : .....	3
Critères d'impact : .....	5
Echelle de mesure des conséquences:.....	5
Critères d'évaluation des risques.....	6
Critères d'acceptation du risque: .....	7
Cartographie des actifs : Liste des processus métiers.....	8
Liste des actifs valorisés : .....	8
Liste des actifs sélectionnés : .....	9
Menaces sur les actifs : .....	10
Vulnérabilités des actifs.....	11
Conséquences et impacts sur les actifs.....	12
Mesures de sécurité existantes .....	13
Scénarios d'incident appréciés.....	14
Vraisemblance des scénarios d'incident .....	17
Calcul du niveau de risque .....	21
Risques sélectionnés pour traitement .....	22
Plan de traitement des risques.....	23
Bibliographie .....	25

## Étude de Cas – Conseiller Bancaire

### Énoncé :

Un conseiller bancaire itinérant utilise un ordinateur portable professionnel pour gérer les dossiers de ses clients.

Il travaille en agence mais se déplace régulièrement chez des clients entreprises.

Dans son ordinateur sont stockés :

- dossiers financiers complets,
- documents d'ouverture de compte,
- emails professionnels,
- simulations de crédit,
- contrats en cours de validation,
- données confidentielles (revenus, identités, bilans d'entreprises).

Lors de ses déplacements, il travaille :

- dans les trains,
- dans des cafés,
- dans des espaces de **“coworking”** souvent via **des réseaux Wi-Fi publics**.

La seule sécurité en place est:

- un mot de passe Windows simple,
- aucune authentification forte,
- aucun chiffrement du disque,
- des fichiers sensibles stockés en clair,
- pas de VPN.

### Echelle de valorisation des actifs :

Valeur	Signification adaptée au conseiller bancaire
<b>1 - Faible</b>	- Actif facilement remplaçable
	- Coût très faible pour la banque - Impact minimal sur l'activité- Aucun besoin de compétences particulières pour le remplacer <b>Exemple</b> : chargeur de téléphone, casque audio
<b>2 - Moyen</b>	- Remplaçable dans la journée
	- Coût d'achat moyen
	- Coût de maintenance limité
	- Nécessite des connaissances basiques <b>Exemple</b> : carte SIM pro, petit périphérique (clé USB sécurisée)
<b>3 - Élevé</b>	- Remplaçable dans la semaine
	- Coût élevé pour la banque
	- Maintenance plus complexe
	- Nécessite des compétences techniques (configuration, sécurité) <b>Exemple</b> : téléphone professionnel, accès aux applications bancaires
<b>4 - Très Élevé</b>	- Remplaçable dans le mois
	- Coût très élevé
	- Maintenance très coûteuse
	- Nécessite des compétences spécifiques (sécurité bancaire, MFA, chiffrement)
	- Impact direct sur la confidentialité des données clients <b>Exemple</b> : ordinateur portable bancaire, base de données clients, contrats numériques

## Critères d'impact :

Qualification du besoin	Confidentialité	Intégrité	Disponibilité	Niveau d'impact	
<b>Informations pouvant être publiques</b>	Accès autorisé à tous les employés de la banque	Peut ne pas être totalement intègre	Arrêt > 3 jours acceptable	<b>Faible</b>	<b>1</b>
<b>Informations internes sensibles</b>	Accès autorisé à l'équipe locale	Simple validation possible	Arrêt entre 1 et 3 jours	<b>Significatif</b>	<b>2</b>
<b>Données clients financières</b>	Accès restreint à un groupe métier	Validation croisée	Arrêt < 1 jour	<b>Fort</b>	<b>3</b>
<b>Données bancaires critiques (contrats, crédits, identité, IBAN)</b>	Accès strictement individuel	Triple validation	Aucun arrêt tolérable	<b>Majeur</b>	<b>4</b>

## Echelle de mesure des conséquences:

Financier	Juridique	Commercial (Clients)	Activité	Image	Niveau d'impact	
<b>Perte financière faible ou nulle</b>	Risque juridique faible ou inexistant	Légère détérioration de la relation client	Perte de productivité ponctuelle	Impact image très faible ou nul	<b>Faible</b>	<b>1</b>
<b>Perte financière modérée</b> (erreur mineure, petite fuite de données non sensibles)	Amende mineure (non-respect procédure interne)	Perte d'un petit contrat ou d'un client	Arrêt de travail court (réorganisation du planning)	Mention négative interne ou commentaire client isolé	<b>Significatif</b>	<b>2</b>
<b>Perte financière significative</b> (>30%) causée par fuite de données sensibles ou erreur commerciale	Retrait temporaire d'accès à certaines applications internes (mesure sécurité)	Perte d'un client important	Arrêt de travail long (blocage dossier, enquête interne)	Impact médiatique interne (mauvaise réputation dans l'agence)	<b>Fort</b>	<b>3</b>
<b>Perte financière critique</b> (>50%) causée par fuite massive de données bancaires, escroquerie ou fraude	Procès, responsabilité pénale ou violation grave des règles de confidentialité	Perte d'un groupe de clients ou comptes majeurs	Travail impossible, suspension d'activité	Atteinte forte à la réputation, escalade au niveau national	<b>Majeur</b>	<b>4</b>

### Critères d'évaluation des risques

Vraisemblance (Scénario d'incident)	1	2	3	4
<b>1 - Faible (peu probable)</b>	1	2	3	4
<b>2 - Moyenne (possible)</b>	2	4	6	8
<b>3 - Élevée (probable)</b>	3	6	9	12
<b>4 - Très élevée (fréquente)</b>	4	8	12	16

Vraisemblance (Scénario d'incident)	1	2	3	4
Impact Max (SOM (C + I + D))	1	2	3	4
5	5	10	15	20
6	6	12	18	24
7	7	14	21	28
8	8	16	24	32
9	9	18	27	36
10	10	20	30	40
11	11	22	33	44
12	12	24	36	48

### Critères d'acceptation du risque:

Niveau de risque	Score	Acceptation	Interprétation pour le conseiller bancaire
Risque faible	1 - 8	Oui	Impact faible : aucune donnée sensible affectée, activité pas bloquée. Risque acceptable sans action immédiate.
Risque moyen	9 - 23	Non	Données clients ou outils bancaires potentiellement touchés. Nécessite un plan de réduction du risque.
Risque élevé	24 - 48	Non	Données bancaires sensibles, identité client, contrats ou accès aux systèmes en danger. Traitement obligatoire et urgent.

## Cartographie des actifs : Liste des processus métiers

Actif	Propriétaire
Processus de conseil bancaire	Conseiller bancaire
Processus d'ouverture de comptes / services	Conseiller bancaire
Processus de gestion des dossiers clients	Conseiller bancaire
Données clients (fiches, revenus, historique)	Banque
Contrats bancaires (PDF, formulaires)	Banque
Simulations financières (crédit, épargne, assurance)	Conseiller bancaire
Ordinateur portable professionnel	Banque
Téléphone professionnel	Banque
Application bancaire interne	Banque
Connexion internet (Wi-Fi, 4G)	Conseiller bancaire
Logiciel de messagerie professionnelle	Banque
Emails professionnels	Banque
Accès aux services bancaires en ligne (portail interne)	Banque
Documents transmis aux clients	Conseiller bancaire
Agenda des rendez-vous clients	Conseiller bancaire

## Liste des actifs valorisés :

Actif	Propriétaire
<b>Actifs Primordiaux</b>	
1 - Processus de conseil bancaire	Conseiller bancaire
2 - Processus de souscription (ouverture compte / crédit)	Conseiller bancaire
3 - Dossiers clients en cours de traitement	Conseiller bancaire
4 - Documents contractuels non finalisés	Conseiller bancaire
5 - Dossiers finalisés / contrats signés	Banque
6 - Base de contacts clients et prospects	Conseiller bancaire
7 - Ordinateur portable professionnel	Banque
8 - Application bancaire (CRM, outils internes)	Banque
9 - Application de messagerie professionnelle	Banque
10 - Connexion internet / Wi-Fi public / 4G	Conseiller bancaire
11 - Emails professionnels	Conseiller bancaire
12 - Fichiers clients (PDF, contrats, scans)	Conseiller bancaire
13 - Conseiller bancaire (ressource humaine)	Banque

### Liste des actifs sélectionnés :

Actif	Propriétaire	Valeur	Sélectionné
<b>Actifs Primordiaux</b>			
1. Données clients	Banque	4	oui
2. Dossiers / contrats bancaires	Banque	4	oui
3. Application bancaire	Banque	4	oui

Actif	Propriétaire	Valeur	Sélectionné
4. Processus de conseil bancaire	Conseiller	3	oui
5. Emails professionnels	Conseiller	2	non
6. Simulation financière	Conseiller	2	non
<b>Actifs en support</b>			
7. Ordinateur portable	Banque	4	oui
8. Téléphone professionnel	Banque	3	oui
9. Connexion internet (Wi-Fi / 4G)	Conseiller	1	non
10. Logiciel messagerie	Conseiller	2	non
11. Outils bureautiques	Conseiller	2	non
12. Notes personnelles	Conseiller	2	non
13. Conseiller bancaire (humain)	Banque	4	oui

### Menaces sur les actifs :

Actif	Valeur	Sélectionné	Menaces
<b>Actifs Primordiaux</b>			
1 - Processus de rédaction	4	oui	Identification de menaces non effectuée sur les actifs primordiaux
2 - Processus de vente	3	oui	Identification de menaces non effectuée
3 - Articles en cours de rédaction	4	oui	Identification de menaces non effectuée

Actif	Valeur	Sélectionné	Menaces
4 - Articles non publiés et non vendus	4	oui	Identification de menaces non effectuée
5 - Articles publiés	2	non	—
6 - Contacts	2	non	—
<b>Actifs en support</b>			
7 - Ordinateur	4	oui	Vol / Destruction / Panne électrique
8 - Logiciel de traitement de texte	2	non	—
9 - Logiciel de messagerie	2	non	—
10 - Connexion internet	1	non	—
11 - Mails	2	non	—
12 - Fichier d'article	4	oui	Fraude / Maladie / Destruction copie
13 - Journaliste	4	oui	Enlèvement / Maladie

## Vulnérabilités des actifs

Actif	Valeur	Sélectionné	Menaces	Vulnérabilité
<b>Actifs Primordiaux</b>				
<b>1 - Données clients</b>	4	oui	Vol de données / Fuite / Piratage	Stockage en clair / Pas de chiffrement / Accès non restreint
<b>2 - Dossiers / contrats bancaires</b>	4	oui	Vol / Destruction / Altération	Pas de sauvegarde chiffrée / Fichiers sensibles accessibles facilement

Actif	Valeur	Sélectionné	Menaces	Vulnérabilité
<b>3 - Application bancaire</b>	4	oui	Piratage / Malfonction	Absence d'authentification forte / Pas de VPN / Mises à jour irrégulières
<b>4 - Processus de conseil bancaire</b>	3	oui	Mauvaise manipulation / Perte d'information	Dépend du conseiller / Pas de procédure standardisée / Absence de journalisation
<b>Actifs en support</b>				
<b>7 - Ordinateur portable professionnel</b>	4	oui	Vol / Perte / Panne	Mot de passe simple / Pas de chiffrement du disque / Transport fréquent hors agence
<b>8 - Téléphone professionnel</b>	3	oui	Vol / Perte / Piratage	Mot de passe faible / Pas de chiffrement / Synchronisation non sécurisée
<b>11 - Emails professionnels</b>	2	non	Phishing / Vol de mails	Accès via Wi-Fi public / Pas de chiffrement end-to-end
<b>12 - Fichiers clients (PDF, contrats, scans)</b>	4	oui	Fuite / Altération / Destruction	Stockés en clair / Pas de contrôle d'accès / Pas de sauvegarde sécurisée
<b>13 - Conseiller bancaire (humain)</b>	4	oui	Maladie / Enlèvement / Erreur humaine	Manque de sensibilisation / Dépendance aux compétences individuelles

### Conséquences et impacts sur les actifs

Scénario d'incident	Actifs impactés	Confidentialité (C)	Intégrité (I)	Disponibilité (D)	SOM (C+I+D)	Max (SOM)	Conséquences
Vol de l'ordinateur du fait de sa portabilité	Processus de rédaction	4	2	2	8	11	Perte financière jugée modérée
	Articles en cours de rédaction	4	4	3	11	11	Perte juridique faible ou nulle
	Articles non publiés et non vendus	4	4	3	11	11	Perte de contrat / transaction, perte de client mineur
	Ordinateur portable	4	4	3	11	11	Perte de productivité
	Fichier d'article	4	4	3	11	11	Perte image faible ou nulle

### Mesures de sécurité existantes

Scénario d'incident	Actifs impactés	C	I	D	SOM (C+I+D)	Max	Conséquences	Mesures de sécurité existantes
Vol de l'ordinateur portable du fait de sa portabilité dans des lieux publics (cafés, trains)	Données clients	4	4	3	11	11	Majeur (Fuite massive de données, Procès, Perte de clients majeurs, Suspension d'activité)	Mot de passe Windows simple
	Dossiers/contrats bancaires	4	4	3	11	11	Majeur	Aucune authentification forte, Aucun chiffrement du disque
	Ordinateur portable	4	4	3	11	11	Majeur	Fichiers sensibles stockés en clair

Scénario d'incident	Actifs impactés	C	I	D	SOM (C+I+D)	Max	Conséquences	Mesures de sécurité existantes
Interception de données lors de la connexion à l'application bancaire via un Wi-Fi public non sécurisé	Application bancaire	4	3	3	10	10	Fort (Fuite de données sensibles, Amende/Retrait d'accès, Arrêt de travail long)	Pas de VPN
	Données clients	4	2	3	9	10	Fort	Pas de chiffrement du disque
Perte de l'ordinateur suite à une panne électrique/logicielle non corrigée	Données clients	2	2	4	8	8	Significatif (Perte de productivité, Détérioration relation client, Réorganisation du planning)	Aucune sauvegarde sécurisée mentionnée
	Dossiers/contrats bancaires	2	3	4	9	8	Significatif	Fichiers sensibles stockés en clair
	Ordinateur portable	2	2	4	8	8	Significatif	Pas de procédure de continuité d'activité mentionnée

### Scénarios d'incident appréciés

Scénario d'incident	Actifs impactés	C	I	D	SOM (C+I+D)	Max (SOM)	Conséquences	Valeur de conséquences	Mesures de sécurité existantes
Vol de l'ordinateur du fait de sa portabilité	Données clients	4	4	3	11	11	Perte financière critique (>50%)	4	Mot de passe Windows simple
	Dossiers/contrats bancaires	4	4	3	11	11	Procès, violation grave des règles (RGPD)	4	Aucun chiffrement du disque

Scénario d'incident	Actifs impactés	C	I	D	SOM (C+I+D)	Max (SOM)	Conséquences	Valeur de conséquences	Mesures de sécurité existantes
	Ordinateur portable	4	4	3	11	11	Perte d'un groupe de clients ou comptes majeurs	4	Fichiers sensibles stockés en clair
Interception de données lors de la connexion via un Wi-Fi public non sécurisé	Application bancaire	4	3	3	10	10	Perte financière significative (>30%)	3	Pas de VPN
	Données clients	4	2	3	9	10	Amende mineure / Retrait d'accès (mesure de sécurité)	2	Pas d'authentification forte
	Dossiers/contrats bancaires	4	3	3	10	10	Perte d'un client important	3	Travail sur Wi-Fi public
Perte de l'ordinateur suite à une panne électrique/logiciel (sans sauvegarde)	Ordinateur portable	2	2	4	8	9	Perte financière modérée (coût remplacement, erreur mineure)	2	Aucune sauvegarde n'est appliqué
	Dossiers/contrats bancaires	2	3	4	9	9	Risque juridique faible ou inexistant	1	—

Scénario d'incident	Actifs impactés	C	I	D	SOM (C+I+D)	Max (SOM)	Conséquences	Valeur de conséquences	Mesures de sécurité existantes
	<b>Données clients</b>	2	2	4	8	9	Détérioration de la relation client (dossier bloqué)	2	—

Vol de l'ordinateur du fait de sa portabilité	Données clients	4	4	3	11	11	Mot de passe Windows simple	Perte financière critique	4	Très Élevée	44
	Dossiers/contrats bancaires	4	4	3	11	11	Aucun chiffrement du disque	Procès, violation grave (RGPD)	4	Très Élevée	44
	Ordinateur portable	4	4	3	11	11	Fichiers sensibles stockés en clair	Perte d'un groupe de clients	4	Très Élevée	44
Interception de données via Wi-Fi public non sécurisé	Application bancaire	4	3	3	10	10	Pas de VPN	Perte financière significative	3	Élevée	30
	Données clients	4	2	3	9	10	Pas d'authentification forte	Perte d'un client important	3	Élevée	27
	Dossiers/contrats bancaires	4	3	3	10	10	Travail sur Wi-Fi public	Arrêt de travail long	3	Élevée	30
Perte de l'ordinateur suite à panne électrique/logicielle (sans sauvegarde)	Ordinateur portable	2	2	4	8	9	Aucune sauvegarde mentionnée	Perte financière modérée	2	2 Moyenne	16
	Dossiers/contrats bancaires	2	3	4	9	9		Fichiers sensibles stockés en clair	Détérioration de la relation client	2	2 (Moyenn

### Vraisemblance des scénarios d'incident

Scénario d'incident	Actifs impactés	C	I	D	SOM (C+I+D)	Max (SOM)	Vraie mblance	Risque (Max SOM x Vrais.)	Acceptation du Risque	Interprétation pour le Conseiller Bancaire
Vol de l'ordinateur du fait de sa portabilité	Données clients	4	4	3	11	11	4 (Très Élevée)	44	Non	Risque Élevé : Données bancaires sensibles, identité client, contrats ou accès aux systèmes en danger. Traitement obligatoire et urgent.
	Dossiers/contrats bancaires	4	4	3	11	11	4 (Très Élevée)	44	Non	Risque Élevé : Données bancaires sensibles, identité client, contrats ou accès aux systèmes en danger. Traitement obligatoire et urgent.
	Ordinateur portable	4	4	3	11	11	4 (Très Élevée)	44	Non	Risque Élevé : Données bancaires sensibles, identité client, contrats ou accès aux systèmes en danger. Traitement

Scénario d'incident	Actifs impactés	C	I	D	SOM (C+I+D)	Max (SOM)	Vraie semblance	Risque (Max SOM x Vrais.)	Acceptation du Risque	Interprétation pour le Conseiller Bancaire
										obligatoire et urgent.
Interception de données via Wi-Fi public non sécurisé	Application bancaire	4	3	3	10	10	3 (Élevée)	30	Non	Risque Élevé : Données bancaires sensibles, identité client, contrats ou accès aux systèmes en danger. Traitement obligatoire et urgent.
	Données clients	4	2	3	9	10	3 (Élevée)	27	Non	Risque Élevé : Données bancaires sensibles, identité client, contrats ou accès aux systèmes en danger. Traitement obligatoire et urgent.

Scénario d'incident	Actifs impactés	C	I	D	SOM (C+I+D)	Max (SOM)	Vraie blanche	Risque (Max SOM x Vrais.)	Acceptation du Risque	Interprétation pour le Conseiller Bancaire
	Dossiers/contrats bancaires	4	3	3	10	10	3 (Élevée)	30	Non	Risque Élevé : Données bancaires sensibles, identité client, contrats ou accès aux systèmes en danger. Traitement obligatoire et urgent.
<b>Perte de l'ordinateur suite à une panne électrique/logicielle (sans sauvegarde)</b>	Dossiers/contrats bancaires	2	3	4	9	9	2 (Moyenne)	18	Non	Risque Moyen : Données clients ou outils bancaires potentiellement touchés. Nécessite un plan de réduction du risque.
	Ordinateur portable	2	2	4	8	9	2 Moyenne	16	Non	Risque Moyen : Données clients ou outils bancaires potentiellement touchés. Nécessite un plan de réduction du risque.

Scénario d'incident	Actifs impactés	C	I	D	SOM (C+I+D)	Max (SOM)	Vraie semblance	Risque (Max SOM x Vrais.)	Acceptation du Risque	Interprétation pour le Conseiller Bancaire
	Données clients	2	2	4	8	9	2 Moyenne	16	Non	Risque Moyen : Données clients ou outils bancaires potentiellement touchés. Nécessite un plan de réduction du risque.

### Calcul du niveau de risque

Scénario d'incident	Les actifs impactés	C	I	D	SOM (C,I,D)	Max (SOM)	Mesures de sécurité existantes	Conséquences	Valeur des conséquences	Vraisemblance	Niveau de risque = Max(SOM) × Vrais.
<b>1. Vol de l'ordinateur du fait de sa portabilité</b>	Processus de rédaction	4	4	3	11	<b>11</b>	Chiffrement du disque, mot de passe BIOS, verrou Kensington	Perte juridique faible ou nulle	1	2	<b>22</b>
	Articles en cours de rédaction	4	4	3	11			Perte de contrat / fuite d'information	2	2	
	Articles non publiés et en action	4	4	3	11			Retard opérationnel, perte mineure	1	2	

Scénario d'incident	Les actifs impactés	C	I	D	SOM(C,I,D)	Max (SOM)	Mesures de sécurité existantes	Conséquences	Valeur des conséquences	Vraisemblance	Niveau de risque = Max(SOM) × Vrais.
	Rédaction de Fichier d'article	4	4	3	11			Perte image faible ou nulle	1	2	
<b>2. Interception des données sur un Wi-Fi public</b>	Application bancaire / outil métier	4	3	3	10	<b>10</b>	VPN obligatoire + chiffrement TLS	Perte juridique faible ou nulle	1	3	<b>30</b>
	Données clients	4	3	2	9			Perte de client potentielle	2	3	
	Contrats	4	3	3	10			Dégradation de la relation client	2	3	
<b>3. Panne matériel / absence de sauvegarde</b>	Ordinateur portable	2	2	4	8	<b>9</b>	Sauvegarde manuelle peu fréquente	Perte d'image faible	1	2	<b>18</b>
	Dossiers / contrats	2	3	4	9			Arrêt de travail, perte de données	2	2	
	Données clients	2	2	4	8			Dégradation relation client	2	2	

### Risques sélectionnés pour traitement

Scénario d'incident	Niveau de risque	Statut	Justification de sélection
1. Vol de l'ordinateur du fait de sa portabilité	22 (élevé)	Sélectionné	Risque élevé lié à la perte d'équipement, fuite potentielle de données sensibles et impact organisationnel.
2. Interception des données sur un-Wi-Fi public	30 (élevé)	Sélectionné	Risque critique : interception de données clients, contrats et informations sensibles. Impact juridique important.
3. Panne matériel / absence de sauvegarde	18 (moyen à élevé)	Sélectionné	Risque important : perte totale de données, arrêt de travail, impact client et réputation.

### Plan de traitement des risques

Scénario	Niveau des risques initial	Traitement	Mesure de Sécurité (ISO27002)	SOM (C, I, D) résiduel	Vraie mblanc e résiduelle	Risque Résiduel (SOM x Vrais.)	Acceptation	Justification de l'acceptation
Vol de l'ordinateur portable	44	Réduction	Chiffrement de disque (BitLocker), MFA pour l'ouverture de session, Sensibilisation	3	1	3	Oui	Impact faible. Le chiffrement empêche la fuite de données (C=1). Le risque est acceptable sans action immédiate (Score < 8).
Interception de données	30	Réduction	VPN systématique pour toute connexion, MFA sur l'accès aux applications	3	1	3	Oui	Impact faible. Le VPN chiffre le trafic, rendant l'interception inefficace (C=1). L'accès aux systèmes est protégé par MFA.

Scénario	Niveau des risques initial	Traitement	Mesure de Sécurité (ISO27002)	SOM (C, I, D) résiduel	Vraie mblanc e résidue lle	Risque Résiduel (SOM x Vrais.)	Acceptati on	Justification de l'acceptation
<b>Panne/Perte technique</b>	18	Réduc tion	Sauvegarde chiffrée automatique et régulière, Formation sur la gestion des fichiers	4	1	4	Oui	Impact faible. La sauvegarde garantit la récupération des données (D=1, I=1). Le seul risque résiduel est le délai de remplacement de l'ordinateur.

## Bibliographie

Référence	Type	Contenu / Utilité
ISO/IEC 27002:2022	Norme	Guide des bonnes pratiques pour la gestion de la sécurité de l'information. Sert à définir les mesures de sécurité à appliquer sur les actifs bancaires.
ISO/IEC 27005:2018	Norme	Gestion des risques liés à la sécurité de l'information. Utilisé pour l'analyse, l'évaluation et le traitement des risques dans l'étude de cas.
CNIL – Guide RGPD pour les entreprises	Guide	Fournit les règles de protection des données personnelles et la gestion des incidents liés aux données clients.
ANSSI – Guide de la sécurité informatique	Guide	Bonnes pratiques pour la protection des postes de travail, VPN, Wi-Fi public, chiffrement et sensibilisation des utilisateurs.
Banque de France – Risques opérationnels	Publication	Donne des exemples de risques en banque et les impacts financiers ou juridiques liés aux fuites de données et incidents.
NIST Special Publication 800-30	Norme / Guide	Guide américain sur l'évaluation des risques IT, utile pour structurer la cartographie des actifs et l'évaluation de la vraisemblance.
Livre : "Sécurité informatique pour les banques" – Éditions Eyrolles	Livre	Présente des cas concrets de risques bancaires et les mesures de prévention adaptées aux conseillers et aux systèmes bancaires.