

Un cadre de modélisation dirigée par les exigences pour les architectures réseau IP multisites évolutives et sécurisées des institutions financières en République Démocratique du Congo, sous contrainte prudentielle

Byorn Tandu Suamunu

Département de Physique et Sciences Appliquées, Faculté des Sciences et Technologies, Université Pédagogique Nationale (UPN), Kinshasa, République Démocratique du Congo

Abstract

Financial institutions in Democratic Republic of the Congo especially Commercial Banks, operate with network and telecommunications infrastructures under multiple constraints and are subject to a territorial expansion to grow their banking networks. Common practice addresses these dimensions separately and sequentially; compliance being verified only after an architectural choice has been made. This article proposes a modelling framework that addresses them simultaneously and upstream. The framework rests on three operations. The expected properties of a network are first converted into determinable quantities, namely node connectivity, structural severity and the marginal cost of extension. The prudential obligations arising from the instructions of the Central Bank of Congo, the Basel principles on operational resilience, the payment card and interbank messaging security frameworks and the international standards for information security and business continuity management are then translated into a vector of quantified constraints acting as design inputs. Admissible architectures are finally ranked through an explicit multicriteria trade-off subjected to sensitivity analysis. The framework is completed by a reference architectural model organized into four functional compartments, namely data center, edge, campus and out-of-band administration, each assigned a required property that can be verified on the design graph before deployment. Since the constraint vector derives from obligations common to all supervised credit institutions, the framework applies to any bank operating in the Democratic Republic of Congo.

Keywords: Business Continuity, Network Security, Scalability, Multicriteria Decision Analysis, Zero Trust Architecture, Graph Theory

Résumé

Les institutions financières en République Démocratique du Congo particulièrement les banques commerciales, possèdent des infrastructures réseaux et des télécommunications fonctionnant sous diverses contraintes et, sont sujettes à une expansion territoire pour accroître leurs réseaux. La multiplicité des nouveaux sites à raccorder nécessite une architecture conçue sous un cadre prudentiel qui durcit les obligations de continuité, de contrôle interne et de gouvernance, et une ressource de transmission rare,

coûteuse et de moindre qualité. La pratique courante traite ces dimensions séparément et séquentielle, la conformité n'étant vérifiée qu'après l'adoption d'un choix architectural. Cet article propose un cadre de modélisation qui les traite simultanément et en amont. Ce cadre repose sur trois opérations. Les propriétés attendues d'un réseau sont d'abord converties en grandeurs déterminables, à savoir la connexité en nœuds, la sévérité structurelle et le coût marginal d'extension. Les obligations prudentielles issues des instructions de la Banque Centrale du Congo, des principes du Comité de Bâle sur la résilience opérationnelle, des référentiels de sécurité des cartes de paiement et de la messagerie interbancaire ainsi que des normes internationales de management de la sécurité de l'information et de la continuité d'activité sont ensuite transposées en un vecteur de contraintes quantifiées tenant lieu de paramètres d'entrée. Les architectures admissibles sont enfin classées par un arbitrage multicritère explicite, soumis à une analyse de sensibilité. Le cadre est soutenu par un modèle architectural de référence organisé en quatre compartiments fonctionnels, centre de données, périphérie, campus et administration hors bande, chacun assorti d'une propriété exigée et vérifiable sur le graphe de conception avant tout déploiement. Le vecteur de contraintes dérivant d'obligations communes à l'ensemble des établissements assujettis, le cadre s'applique à toute banque exerçant en République Démocratique du Congo.

Mots-clés: Continuité d'Activité, Sécurité Réseau, Évolutivité, Aide Multicritère à la Décision, Architecture à Confiance Nulle, Théorie des Graphes.

1. Introduction

La conception d'un réseau d'entreprise est souvent présentée comme un problème de sélection technologique : il s'agirait de choisir, parmi des familles d'architectures documentées, celle dont les propriétés annoncées correspondent le mieux aux besoins exprimés [1, 2]. Cette présentation est erronée pour les institutions financières de la République Démocratique du Congo dont l'infrastructure de transmission demeure une contrainte. Trois raisons la justifient.

- a. L'expansion des sites : L'ouverture régulière de points de service et la densification des parcs de guichets automatiques imposent un déploiement répété d'infrastructures sur des sites nouveaux. Le coût réel d'une architecture ne se lit alors pas dans son investissement initial mais dans ce que coûte le raccordement du site suivant, grandeur que les catalogues ne documentent pas.
- b. Le cadre réglementaire : Les obligations prudentielles édictées par la Banque Centrale du Congo (BCC) en matière de contrôle interne [3], de gouvernement d'entreprise [4], de gestion des risques [5] et de continuité d'activité [6], prises dans le cadre de la loi n° 22/069 relative à l'activité et au contrôle des établissements de crédit [7] et convergentes avec les principes du Comité de Bâle sur la résilience opérationnelle [8], auxquelles s'ajoutent les référentiels sectoriels applicables aux flux monétiques [9] et à la messagerie interbancaire [10] ainsi que les normes de management de la sécurité de l'information et de la continuité [11, 12, 13], ne relèvent pas de la seule couche applicative : elles engagent la topologie, la finesse du cloisonnement et les modalités d'administration.
- c. L'instabilité au transport : suivant les types de médias utilisés, le délai de propagation y fonction et, est relativement élevé pour les sites en provinces. L'augmentation en double voire triple de la capacité n'est pas une stratégie donc, la solution. La conception doit être effectuée suivant un arbitrage documenté plutôt que par accumulation de capacité.

Cet article propose un cadre de modélisation qui traite les trois dimensions mentionnées ci-haut comme des entrées du problème de conception. Les sections 3, 4 et 5, respectivement, pose les formalisations y relatives, en dérive un modèle architectural de référence et la démarche d'arbitrage l'accompagnant ; et aborde la portée et les limites du cadre.

2. Travaux Connexes

Les travaux consacrés aux institutions financières de la République Démocratique du Congo et principalement aux banques commerciales portent sur la solidité prudentielle des banques [28, 29], la gestion des risques informatiques liés à la digitalisation [30], l'extension des points de service par les agents bancaires [31] et la modernisation de l'infrastructure nationale de paiement (switch national Mosolo) [32]. Tous ces travaux abordent la conformité sous l'aspect financier ou de la gouvernance, tandis que ceux d'ingénierie réseau se limitent à la mise en œuvre d'une solution retenue d'avance. À notre connaissance ce jour, aucun ne traduit les instructions de la Banque Centrale du Congo en paramètres de conception réseau, ni ne propose de grandeurs vérifiables avant déploiement pour la résilience et l'évolutivité. De ce manque que cet article propose un cadre pour combler ce vide.

3. Matériel et Méthodes

3.1. Grandeurs Opératoires

Le cadre implique l'emploi de tout concept en grandeur déterminable [14]. Les propriétés habituellement invoquées dans les cahiers des charges, résilience, évolutivité, sécurité, ne sont pas des critères tant qu'elles ne sont pas assorties d'un mode de détermination [15]. Le Tableau 1 rassemble les grandeurs retenues.

Tableau 3.1 : Grandeurs Opératoires du Cadre Proposé

Grandeur	Symbole	Mode de détermination et rôle dans la conception
Connexité en nœuds	$\kappa(G)$	- Parcours en profondeur sur le graphe de conception ; - Critère d'absence de point de défaillance unique.
Sévérité structurelle	Φ	- Fraction du service isolée par une défaillance élémentaire ; - Hiérarchise les compartiments à traiter.
Coût marginal d'extension	C_m	- Comptage sur la procédure de raccordement d'un site ; - Critère opératoire d'évolutivité.
Écart au vecteur de contraintes	ΔC	- Évaluation contrainte par contrainte ; - Mesure la conformité par construction.
Disponibilité prévisionnelle	A	- Blocs de fiabilité sur chemins indépendants [16] ; - Objectif de continuité.
Budget de délai	D	- Somme des composantes de délai sur le chemin ; - Contrainte des flux monétiques.

3.2. Résilience et Connexité

La représentation du réseau par un graphe fournit un cadre approprié pour établir sa résilience :

$$G = (V, E) \quad (1)$$

où V désigne l'ensemble des nœuds, soit les commutateurs, routeurs, pare-feux ou sites, et E l'ensemble des liaisons. La décomposition fonctionnelle induit une famille de sous-graphes G_i , un par compartiment. La grandeur pertinente n'est pas la connexité simple, qui traduit la seule accessibilité mutuelle, mais la connexité en nœuds :

$$\kappa(G_i) = \min \{ |S| : S \subset V_i, G_i - S \text{ non connexe} \} \quad (2)$$

Si v est un point d'articulation de G_i , alors $\{v\}$ est un ensemble séparateur, d'où $\kappa(G_i) = 1$. Réciproquement, le théorème de Menger établit que $\kappa(G_i) \geq 2$ équivaut à l'existence de deux chemins intérieurement disjoints entre toute paire de nœuds [16]. L'exigence d'absence de point de défaillance unique équivaut donc à la 2-connexité, vérifiable en temps linéaire par parcours en profondeur [17, 18]. Du point de vue pratique, cette équivalence rend la propriété contrôlable sur le plan de conception, avant tout déploiement.

La connexité seule ne hiérarchise cependant pas les défauts. Deux compartiments également non redondés diffèrent par l'étendue du service qu'une défaillance élémentaire isole. Considérant que r_i étant le nœud du raccordement du compartiment, A_i étant l'ensemble de ses points d'articulation, T_i représentant ses nœuds de service et $\text{Iso}_i(v)$ étant le sous-ensemble des nœuds de T_i dépourvus de tout chemin vers r_i dans le graphe $G_i - v$:

$$\varphi_i = \max_{v \in A_i} \frac{|\text{Iso}_i(v)|}{|T_i|} \quad (3)$$

Notons qu'un compartiment est défaillant de façon structurelle lorsque $\kappa(G_i) \leq 1$ et $\varphi_i = 1$. De ce fait, cette qualification dissocie la connexité unitaire confinée à un domaine de défaillance local de celle affectant le chemin de transit commun, et fournissant ainsi un ordre de priorité de remédiation qui est fondé sur la topologie et non sur l'appréciation.

Ainsi, il est à noter que deux chemins qui partagent un équipement, une alimentation, un fourreau de génie civil ou un même opérateur ne constituent pas une redondance : la 2-connexité du graphe logique n'implique la tolérance à la panne que si les domaines de défaillance sous-jacents sont disjoints.

3.3.Évolutivité

L'évolutivité, formalisée par le coût marginal d'extension, quadruplet associant au raccordement d'un site supplémentaire le nombre d'opérations de configuration requises, le délai de mise à disposition, le nombre d'équipements existants affectés et le besoin d'intervention sur site :

$$C_m(n) = (N_{op}, T_{prov}, N_{eq}, I) \quad (4)$$

Une architecture est évolutive lorsque ces quatre composantes demeurent bornées indépendamment de n , et non évolutive lorsqu'elles croissent avec la taille du parc. Le cas le plus documenté est celui des tunnels établis en maille complète [19] :

$$N_t = \frac{n(n-1)}{2} \quad (5)$$

Dont la conséquence est que chaque adjonction impose une intervention sur les terminaisons déjà déployées, de sorte que N_{eq} n'est pas borné. De ce fait, l'évolutivité n'est plus une qualité attribuée à une famille de produits mais une propriété vérifiable sur la procédure de déploiement.

3.4.Obligations Prudentielles Considérées comme Paramètres

Tout établissement de crédit exerçant en République Démocratique du Congo est assujéti à un corpus prescriptif composite : la loi n°22/069 [7], les instructions de la Banque Centrale du Congo [3, 4, 5, 6], le Code du numérique [20], ainsi que les référentiels sectoriels et les normes internationales. Ce corpus des obligations de résultat sans prescrire de moyens techniques : l'Instruction n°36 impose un dispositif de continuité et un plan de continuité d'activité (PCA), sans fixer ni objectif de temps de reprise, ni architecture de secours, ni périodicité d'essai. Le passage de l'obligation juridique à la contrainte d'ingénierie constitue dès lors une opération de traduction dont la méthode explicite.

Chaque obligation est transposée en cinq temps :

- Identification de la disposition et prescriptive ;
- Détermination de l'événement redouté et de l'actif affecté ;
- Identification de la propriété technique qui prévient cet événement ;
- Conversion de cette propriété en indicateur assorti d'une valeur cible ;
- Spécification du mode de vérification.

Lorsque la disposition demeure silencieuse sur le niveau attendu, la valeur cible procède d'un référentiel technique applicable au même risque, d'une exigence métier documentée ou d'une analyse de risque conduite selon ISO/IEC 27005 [21]. Les principes du Comité de Bâle, qui conçoivent la résilience opérationnelle comme la capacité à assurer les opérations critiques au travers des perturbations [8, 22], fournissent le cadre d'interprétation de ces seuils. Le Tableau 2 présente le vecteur ainsi obtenu.

Tableau 3.2 : Vecteur de Contraintes de Conception et Sources Prescriptives

Réf.	Domaine	Source prescriptive	Indicateur	Valeur cible
C-01	Continuité	Instruction BCC n° 36 ; ISO 22301	Objectif de temps de reprise (RTO)	Issue de l'analyse d'impact
C-02	Continuité	Instruction BCC n° 36 ; ISO 22301	Objectif de point de reprise (RPO)	Issue de l'analyse d'impact
C-03	Continuité	Instruction BCC n° 36 ; principes de Bâle	Périodicité d'essai du chemin de secours	Fixée par le PCA
C-04	Données de porteurs	PCI DSS v4.0 ; ISO/IEC 27001, A.8.22	Systèmes inclus dans le périmètre de conformité	Minimal
C-05	Flux monétaires et interbancaires	PCI DSS v4.0 ; SWIFT CScF	Suite cryptographique en transit	Imposée

Réf.	Domaine	Source prescriptive	Indicateur	Valeur cible
C-06	Contrôle interne	Instruction BCC n° 17 ; ISO/IEC 27001, A.5.15 et A.8.20	Ports d'accès sous contrôle d'accès réseau	100 %
C-07	Contrôle interne	Instruction BCC n° 17 ; ISO/IEC 27001, A.8.15 et A.8.16	Couverture de la journalisation	100 %
C-08	Gouvernance	Instruction BCC n° 21 ; ISO/IEC 27001, A.8.32	Changements tracés et approuvés	100 %
C-09	Gestion des risques	Instruction BCC n° 22 ; ISO/IEC 27005	Disponibilité prévisionnelle des services critiques	Déduite de C-01
C-10	Cadre national	Ordonnance-loi n° 23/010	Territorialité des données	Binaire

L'ensemble de contraintes forment un vecteur dont l'écart ΔC est évalué sur toute architecture candidate. Ainsi, la conformité n'est plus un contrôle a posteriori et devient plutôt une condition d'admissibilité. Les valeurs cibles « issues de l'analyse d'impact », demeurent propres à chaque établissement ; la structure du vecteur, en revanche, dérive d'obligations communes à l'ensemble des établissements assujettis et constitue de ce fait un invariant du cadre.

4. Résultats

4.1. Modèle Architectural de Référence

Ce cadre ne désigne pas une architecture ; il définit plutôt ce qu'une architecture doit démontrer. Le modèle de référence proposé organise l'infrastructure en compartiments fonctionnels, chacun assorti d'une propriété exigée et du mécanisme qui l'établit. La partition en compartiments délimite les domaines de défaillance et conditionne la finesse avec laquelle la politique de sécurité peut être exprimée.

Tableau 4.1 : Compartiments du Modèle de Référence et Propriétés Exigées

Compartiment	Fonction	Propriété exigée et mécanisme
Data Center	Hébergement applicatif, flux Est-Ouest et Nord-Sud	$\kappa \geq 2$; micro-segmentation native par contrats entre groupes de points terminaux ; politique découplée du substrat physique
Périphérie (Edge)	Agrégation des accès distants, partenaires et Internet	$\kappa \geq 2$; agrégation active des transports sur mesure de qualité ; contrôle d'accès par session
Campus	Raccordement des utilisateurs finaux	Rattachement double de la couche d'accès ; authentification et évaluation de posture du terminal
Administration (Out-Of-Band)	Gestion, supervision et dépannage.	Compartiment hors bande physiquement distinct de la production ; accès indépendant du plan de service

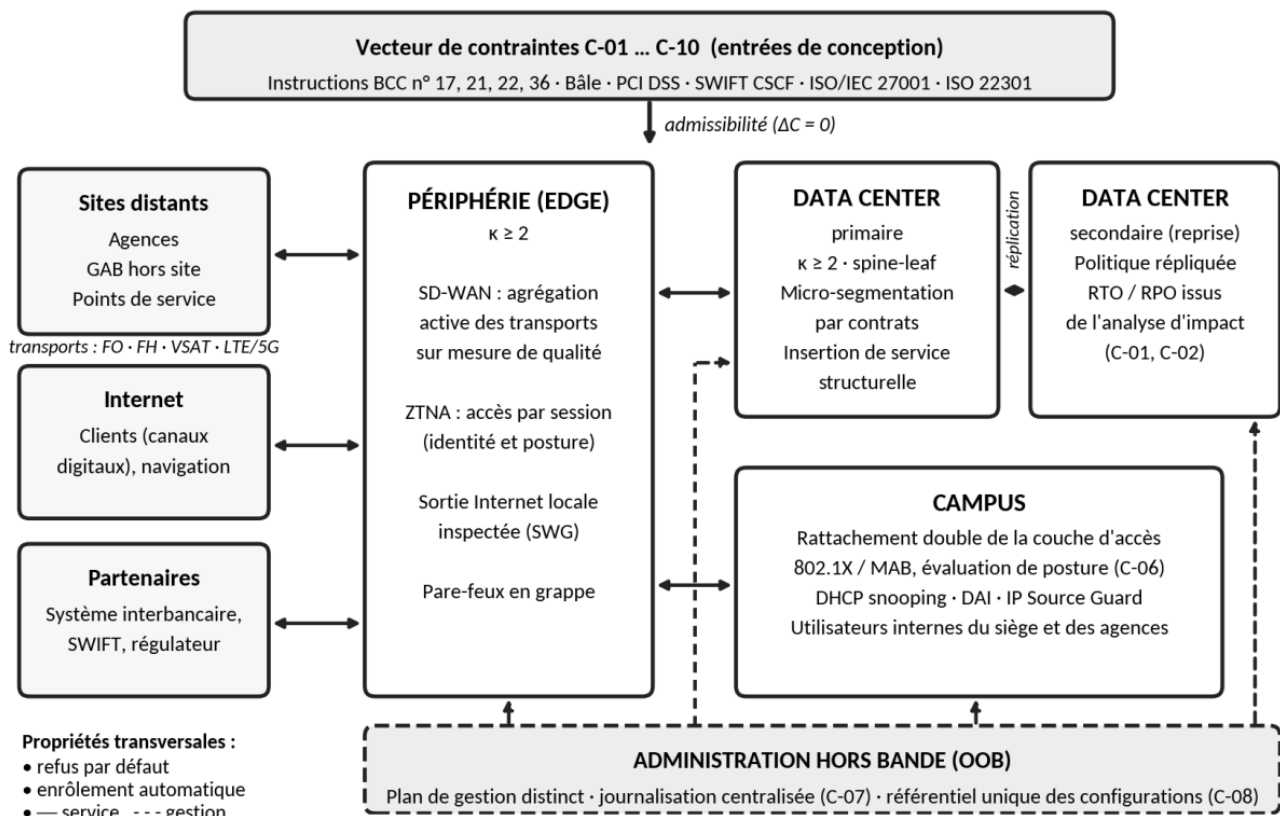
Le découpage est complété par trois propriétés transversales :

- La posture de sécurité conformément au modèle de confiance nulle (zero-trust) [23] : la connectivité est nulle tant qu'une relation n'est pas explicitement déclarée ;
- L'insertion de service rendue structurelle, aucun chemin contourne une fonction d'inspection par ajout d'un itinéraire manuel ;
- L'enrôlement automatique des sites nouveaux avec une gestion centralisée du plan d'adressage.

Le modèle admet plusieurs réalisations technologiques étant donné que le cadre conserve sa validité même si l'arbitrage désigne une fabrique à plan de contrôle réparti [24], dès lors que les propriétés du Tableau 3 demeurent démontrables.

La Figure 4.1 synthétise l'organisation fonctionnelle du modèle. Le vecteur de contraintes y intervient en amont, comme condition d'admissibilité ; la périphérie constitue le point de passage obligé de tout flux entrant ou sortant ; le compartiment hors bande forme un plan de gestion distinct qui dessert l'ensemble des compartiments.

Figure 4.1 : Diagramme Fonctionnel de Haut Niveau du Modèle Architectural de Référence



4.2.Démarche d'Arbitrage

Le choix d'une architecture admissible, c'est-à-dire qui satisfait le vecteur de contraintes, est établi par notation pondérée, qui est une méthode de référence de l'aide multicritère à la décision [25, 26] :

$$S_j = \sum_i w_i \times n_{ij}, i = 1 \dots m \quad (6)$$

Avec w_i qui désigne le poids du critère i , de somme unitaire, et n_{ij} la note de l'alternative j sur une échelle commune d'un à cinq. Le tableau ci-dessous retrace lesdits critères, les poids ainsi que les fondements de la pondération qui y sont associés.

Tableau 1.2 : Pondération de Référence pour une Institution Financière sous Contrainte Prudentielle

Critère	Poids	Fondement de la pondération
Disponibilité	0,25	Obligation prudentielle de continuité (Instruction BCC n° 36 ; ISO 22301 ; principes de Bâle)
Sécurité et conformité	0,20	Secteur réglementé (Instructions BCC n° 17 et 22 ; ISO/IEC 27001), périmètre monétique (PCI DSS) et cadre interbancaire (SWIFT CSCF)
Performance	0,15	Contrainte de délai des flux transactionnels
Coût total de possession	0,15	Contrainte budgétaire et volatilité du taux de change
Évolutivité	0,10	Plan d'extension du réseau de points de service
Exploitabilité	0,10	Effectif restreint et compétences à constituer
Indépendance constructeur	0,05	Réversibilité des choix

Il est à noter que ladite pondération n'est pas universelle c'est-à-dire, elle exprime un ordre de priorité propre au secteur considéré. Sa publication est précisément ce qui rend l'arbitrage transposable, puisqu'une institution soumise à une contrainte budgétaire plus forte ou à une exigence de réversibilité plus stricte peut en modifier les poids et rejouer le calcul.

Une analyse de sensibilité doit accompagner tout résultat [27]. Une variation d'un point de la note d'une alternative sur le critère i déplaçant son score de w_i , le classement n'est pas robuste lorsque l'écart entre les deux premières alternatives est inférieur au plus grand poids ; la décision doit alors être présentée comme telle, en indiquant quel critère la détermine.

5. Discussion

Ce cadre a pour objectif de produire les résultats vérifiables avant tout déploiement. La connexité, la sévérité structurelle, le coût marginal d'extension donc, l'évolutivité, et l'écart au vecteur de contraintes est déterminé par une analyse du graphe de conception ainsi que des procédures d'exploitation. De ce fait, une architecture peut déjà être considérée non évolutive et non sécurisée sur plan, ce qui ramène le contrôle en amont de tout investissement.

Considérant la nature du vecteur de contraintes, seuls les seuils issus de l'analyse d'impact et la pondération relèvent de l'établissement ; la procédure, la structure du vecteur et les propriétés exigées pour chaque compartiment identique quel que soit l'établissement. Ainsi, le cadre est un modèle de référence transposable à tout établissement exerçant en République Démocratique du Congo.

6. Conclusion

Cet article a proposé un cadre de modélisation dirigée par les exigences pour les architectures réseau IP multisite des institutions financières exerçant sous contrainte de transmission et sous cadre prudentiel dense. Le cadre est basé sur la conversion préalable des propriétés attendues en grandeurs déterminables, sur la transposition des obligations réglementaires en contraintes d'admissibilité, et sur un arbitrage explicite et analysé. Il est soutenu par un modèle architectural de référence dont chaque compartiment porte une propriété exigée et vérifiable sur plan.

Ainsi, trois apports sont à considérer pour ce cadre :

- a. Une procédure transposable des obligations prudentielles de la Banque Centrale du Congo et des référentiels internationaux en paramètres de conception ;
- b. Une formalisation opératoire de l'évolutivité par le coût marginal d'extension, qui substitue un critère vérifiable à une propriété invoquée ;
- c. Et un critère de défaillance structurelle distinguant la connexité unitaire selon l'étendue du domaine isolé, qui fournit un ordre de priorité de remédiation fondé sur la topologie.

Références

1. Z. Zsiga, "CCDE 400-007 Official Cert Guide", Cisco Press, Indianapolis, 2023;
2. D. Prajapati, J. Bowman, N. Suvarna, "Designing Real-World Multi-Domain Networks", Cisco Press, Indianapolis, 2024;
3. Banque Centrale du Congo, "Instruction n° 17 (modification n° 3) aux établissements de crédit et sociétés financières relative aux règles prudentielles en matière de contrôle interne", Banque Centrale du Congo, Kinshasa, 2023 ;
4. Banque Centrale du Congo, "Instruction n° 21 (modification n° 2) relative au gouvernement d'entreprise des établissements de crédit", Banque Centrale du Congo, Kinshasa, 2023 ;
5. Banque Centrale du Congo, "Instruction n° 22 (modification n° 2) aux établissements de crédit et sociétés financières relative à la gestion des risques", Banque Centrale du Congo, Kinshasa, 2023 ;
6. Banque Centrale du Congo, "Instruction n° 36 aux établissements de crédit et institutions de microfinance relative à la continuité d'activité", Banque Centrale du Congo, Kinshasa, 2018 ;
7. République Démocratique du Congo, "Loi n° 22/069 du 27 décembre 2022 relative à l'activité et au contrôle des établissements de crédit", Journal officiel, 2022 ;
8. Basel Committee on Banking Supervision, "Principles for Operational Resilience", Bank for International Settlements, Basel, 2021;
9. PCI Security Standards Council, "Payment Card Industry Data Security Standard", Version 4.0, 2022;
10. SWIFT, "Customer Security Programme — Customer Security Controls Framework", SWIFT, La Hulpe;
11. ISO/IEC 27001:2022, "Information security, cybersecurity and privacy protection — Information security management systems — Requirements", ISO, Geneva, 2022;
12. A. Calder, S. Watkins, "IT Governance: An International Guide to Data Security and ISO27001/ISO27002", 7th Edition, Kogan Page, London, 2020;

13. ISO 22301:2019, “Security and resilience — Business continuity management systems — Requirements”, ISO, Geneva, 2019;
14. J.-L. Le Moigne, “La modélisation des systèmes complexes”, Dunod, Paris, 1990 ;
15. ISO/IEC/IEEE 42010:2022, “Systems and software engineering — Architecture description”, ISO, Geneva, 2022;
16. K. Menger, “Zur allgemeinen Kurventheorie”, *Fundamenta Mathematicae*, 1927, 10, 96–115;
17. R.E. Tarjan, “Depth-first search and linear graph algorithms”, *SIAM Journal on Computing*, 1972, 1 (2), 146–160;
18. J. Hopcroft, R.E. Tarjan, “Algorithm 447: Efficient algorithms for graph manipulation”, *Communications of the ACM*, 1973, 16 (6), 372–378;
19. S. Hooda, et al., “Software-Defined Wide Area Networks (SD-WAN)”, Cisco Press, Indianapolis, 2021;
20. République Démocratique du Congo, “Ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique”, *Journal officiel*, 2023 ;
21. ISO/IEC 27005:2022, “Information security, cybersecurity and privacy protection — Guidance on managing information security risks”, ISO, Geneva, 2022;
22. Basel Committee on Banking Supervision, “Revisions to the Principles for the Sound Management of Operational Risk”, Bank for International Settlements, Basel, 2021;
23. S. Rose, O. Borchert, S. Mitchell, S. Connelly, “Zero Trust Architecture”, NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, 2020;
24. D. Kreutz, et al., “Software-defined networking: A comprehensive survey”, *Proceedings of the IEEE*, 2015, 103 (1), 14–76;
25. B. Roy, “Méthodologie multicritère d'aide à la décision”, Economica, Paris, 1985 ;
26. E. Triantaphyllou, “Multi-Criteria Decision-Making Methods: A Comparative Study”, Kluwer, Dordrecht, 2000;
27. A. Saltelli, et al., “Global Sensitivity Analysis: The Primer”, Wiley, Chichester, 2008;
28. F. Mapamboli Posa, Y. Kabanga Kadima, “Les banques en République Démocratique du Congo : Enjeux de la solidité et de la conformité aux normes prudentielles de gestion”, *International Journal of Financial Accountability, Economics, Management, and Auditing (IJFAEMA)*, 2025, <https://doi.org/10.5281/zenodo.14840777>
29. International Monetary Fund, “Democratic Republic of the Congo: Technical Assistance Report— Financial Sector Stability Review”, IMF Staff Country Reports, September 2022;
30. F. Tuyikorere Barajiginwa, “La gestion des risques informatiques dans le système financier de la République Démocratique du Congo”, *International Journal of Financial Accountability, Economics, Management, and Auditing (IJFAEMA)*, 2025, <https://doi.org/10.5281/zenodo.17159155>
31. R. Cull, X. Giné, S. Harten, S. Heitmann, A.B. Rusu, “Agent Banking in a Highly Under-Developed Financial Sector: Evidence from Democratic Republic of Congo”, *World Development*, 2018, 107, 54–74;
32. MicroSave Consulting, “Interopérabilité en RDC : 20 ans d'évolution (2005–2025)”, FinDev Gateway, September 2025.