Move2Cloud

• WHITE PAPER — ÉDITION 2027

CLOUD & ARCHITECTURE AZURE

Auditer son architecture Azure
de la revue à la remédiation

Méthode complète pour conduire une Well-Architected Review sur Azure, transformer les constats en plan de remédiation priorisé et piloter les risques résiduels dans la durée.

11 pages · Grille de scoring des risques, matrice de priorisation et plan de remédiation 30/90/180 jours inclus

5
piliers Azure Well-Architected évalués lors de la revue

30/90/180
jours : les trois horizons du plan de remédiation

100%
des constats rattachés à un risque tracé et à un propriétaire nommé

PRÉPARÉ PAR
Move2Cloud — Conseil Cloud & Infrastructure, Paris

PUBLICATION
Octobre 2026

SOMMAIRE

Ce que vous allez trouver dans ce document

Ce document part du contexte et des déclencheurs d'un audit Well-Architected, détaille la méthode de collecte, d'évaluation et de scoring des risques, puis aboutit à un plan de remédiation priorisé et à un dispositif de suivi opérationnel.

01 **Synthèse — l'essentiel en une page** p.3

02 **Pourquoi auditer son architecture maintenant** p.4

03 **Cadrer le périmètre et collecter les preuves** p.5

04 **Outils d'évaluation : que choisir** p.6

05 **Scorer et prioriser les risques** p.7

06 **Plan de remédiation et suivi** p.8

07 **Grille d'auto-évaluation** p.9

08 **Feuille de route en 5 étapes** p.10

09 **Conclusion & à propos de Move2Cloud** p.11

À qui s'adresse ce document ? CTO, architectes cloud, responsables plateforme et RSSI d'organisations exploitant déjà des charges de production sur Azure, qu'il s'agisse d'une landing zone mature ou d'un patrimoine migré sans revue formelle. Utile également aux équipes SRE et FinOps chargées de porter les actions correctives.

Copyright Move2Cloud — move2cloud.fr

SYNTHÈSE

L'essentiel en une page

Transformer une revue d'architecture en décisions d'ingénierie datées, chiffrées et suivies — plutôt qu'en rapport classé sans suite.

Le Microsoft Azure Well-Architected Framework structure l'évaluation d'une charge de travail autour de **5 piliers** : fiabilité, sécurité, optimisation des coûts, excellence opérationnelle et efficacité des performances. La plupart des organisations exploitent pourtant des architectures conçues lors de migrations accélérées, où ces piliers n'ont jamais été instruits de façon explicite : les enquêtes Flexera sur l'état du cloud situent année après année le gaspillage estimé autour de **30 % de la dépense cloud**, un symptôme direct d'architectures jamais revues.

L'écart se creuse pour deux raisons. D'une part, la plateforme évolue plus vite que les architectures qui tournent dessus : dépréciations de services, nouveaux SKU, nouvelles garanties de disponibilité — une VM en instance unique reste à **99,9 %** de SLA quand un déploiement multi-zones atteint **99,99 %**. D'autre part, le modèle de responsabilité partagée place l'essentiel des défaillances de sécurité du côté de la configuration client, et non du fournisseur : Gartner estime de longue date que la quasi-totalité des incidents de sécurité cloud relèvent d'erreurs du client.

La bonne nouvelle : une Well-Architected Review est outillée et reproductible. Entre l'évaluation WAF de Microsoft, Azure Advisor, Defender for Cloud et les métriques de la plateforme, l'essentiel des constats est mesurable sans instrumentation supplémentaire. Ce document fournit la méthode pour conduire la revue en quelques semaines, coter chaque écart selon son impact et son effort, bâtir un plan de remédiation priorisé par vagues, et tenir un registre des risques résiduels assumés au niveau direction.

5
piliers du Well-Architected Framework Azure

~30 %
de la dépense cloud estimée gaspillée (Flexera, State of the Cloud)

99,99 %
SLA d'une VM multi-zones, contre 99,9 % en instance unique

La question à laquelle répond ce document n'est pas « notre architecture Azure est-elle bonne ? », mais « quels écarts corriger en premier, à quel coût, et quels risques assumons-nous consciemment jusqu'à la prochaine revue ? ». Les sections qui suivent déroulent la méthode complète, du cadrage de la revue au registre des risques résiduels, avec les grilles et check-lists directement réutilisables.

Copyright Move2Cloud — move2cloud.fr

SECTION 02

Pourquoi auditer son architecture maintenant

Une architecture Azure n'est pas figée : elle dérive, sous l'effet des migrations rapides, des évolutions de la plateforme et des arbitrages faits dans l'urgence. La question n'est donc pas de savoir s'il faut l'auditer, mais à quel moment le coût du report dépasse celui de la revue.

1. Une dette d'architecture héritée des migrations

La majorité des patrimoines Azure s'est constituée par migrations successives, souvent en lift & shift, sans revue d'architecture formelle. Les choix d'alors — instance unique, redondance locale, réseau à plat — restent en production bien après que les charges soient devenues critiques.

2. Le design dicte la disponibilité réelle

Les écarts de disponibilité se jouent sur des détails de design : une VM en instance unique sur disque Premium est couverte à 99,9 %, contre 99,99 % dès lors qu'elle est déployée sur plusieurs zones de disponibilité. Un audit rend ces écarts explicites avant l'incident, pas après.

3. Une plateforme qui bouge plus vite que les architectures

Microsoft fait évoluer et déprécie ses services en continu (retraits de TLS 1.0/1.1, de ressources classiques, d'API héritées). Sans revue périodique, une architecture conforme hier devient non supportée, non conforme NIS2/DORA, ou simplement plus chère que son équivalent moderne.

« On n'audite pas une architecture pour produire un rapport, mais pour décider ce que l'on corrige lundi matin. »

Les sections suivantes détaillent la méthode : cadrage de la revue, instruction des cinq piliers, cotation des constats, construction du plan de remédiation et pilotage des risques résiduels.

Copyright Move2Cloud — move2cloud.fr

SECTION 03

Cadrer le périmètre et collecter les preuves

Une Well-Architected Review ne s'applique jamais à « tout Azure » : elle s'applique à une charge de travail délimitée, avec ses abonnements, ses dépendances et ses engagements de service.

ÉLÉMENT DE CADRAGE	CE QU'IL FAUT ACTER AVANT DE DÉMARRER
Périmètre technique	La liste nominative des abonnements, groupes de ressources et dépendances externes (SaaS, systèmes on-premises, DNS, identités) inclus dans la revue — et ce qui en est explicitement exclu.
Objectifs de service	Les RTO, RPO, SLO de disponibilité et de latence attendus par le métier, formalisés par charge de travail : sans cible, aucun constat de fiabilité n'est démontrable.
Preuves attendues	Pour chaque pilier, les exports qui font foi : inventaire Resource Graph, conformité Azure Policy, secure score Defender for Cloud, recommandations Advisor, données Cost Management et dossiers d'architecture existants.

> **À retenir :** Fixez le périmètre sur une charge de travail nommée, avec son propriétaire et ses objectifs de service, et exigez une preuve exportable pour chaque constat : sans artefact daté, un constat n'est qu'une opinion.

Automatiser la collecte avant d'ouvrir les ateliers

La collecte doit être majoritairement automatisée et reproductible : un export Azure Resource Graph de l'inventaire (SKU, redondance zonale, versions de runtime), l'état de conformité Azure Policy, le secure score Defender for Cloud, les recommandations Azure Advisor et un export Cost Management sur douze mois constituent le socle factuel. Ces extractions sont rejouables à l'identique en fin de remédiation, ce qui permet de mesurer le delta plutôt que de le déclarer. Les ateliers avec les équipes viennent ensuite : ils servent à expliquer les écarts observés (dette assumée, contrainte réglementaire, arbitrage budgétaire) et non à découvrir l'existant, ce qui réduit typiquement la phase d'entretiens à deux ou trois sessions de deux heures par pilier.

Copyright Move2Cloud — move2cloud.fr

SECTION 04

Outils d'évaluation : que choisir

Aucun outil ne couvre seul les cinq piliers : l'évaluation structurée donne le cadre, la télémétrie Azure donne les preuves, et les requêtes sur mesure comblent le reste.

OUTIL	COUVERTURE	FONCTIONNEMENT	À RÉSERVER À
Azure Well-Architected Review (Microsoft Assessments)	Les 5 piliers, par questionnaire	Questionnaire guidé sur une charge de travail, restituant un score par pilier et des recommandations exportables en CSV	Structurer la revue et obtenir une base de recommandations alignée sur le référentiel Microsoft
Azure Advisor + Defender for Cloud	Fiabilité, sécurité, coûts, performance	Analyse continue de la configuration réelle des ressources, avec secure score et recommandations priorisées	Objectiver les écarts de configuration et mesurer la progression après remédiation
Azure Resource Graph + Azure Policy	Conformité et inventaire sur mesure	Requêtes KQL à l'échelle du tenant et évaluation d'ensembles de règles définis par l'entreprise	Vérifier les exigences internes et réglementaires que les outils standards ne couvrent pas

Piège fréquent : Confondre un secure score ou un score Advisor avec un niveau de maturité architecturale : ces scores notent la configuration des ressources existantes, pas les choix de conception. Une architecture mono-région parfaitement configurée peut afficher un excellent score tout en étant incapable de tenir son RTO.

Consolider les trois sources dans un référentiel unique de constats

Le bon montage consiste à faire converger les trois niveaux dans un référentiel unique de constats. Concrètement : on importe l'export CSV de l'assessment Well-Architected, on y rattache chaque recommandation Advisor et chaque contrôle Defender for Cloud non conforme, puis on complète par les requêtes Resource Graph qui matérialisent les angles morts (ressources hors zones de disponibilité, bases sans sauvegarde géo-redondante, comptes de stockage encore ouverts sur l'Internet public). Chaque ligne porte alors un identifiant, un pilier, un propriétaire, une preuve et une cotation — c'est ce tableau, et non le rapport PDF, qui devient l'objet de travail des sections suivantes.

Copyright Move2Cloud — move2cloud.fr

SECTION 05

Scorer et prioriser les risques

Un constat non coté est un constat qui ne sera jamais arbitré : la cotation transforme une liste d'écarts en ordre de passage défendable devant un comité.

Coter l'impact et la probabilité, pas la gêne technique

Cotez chaque constat sur deux axes : l'impact métier s'il se matérialise (indisponibilité, fuite de données, dépassement budgétaire) et la probabilité d'occurrence au vu de l'exposition réelle. Le produit des deux donne la gravité brute.

Pondérer par l'effort pour isoler les quick wins

Deux constats de gravité égale ne se traitent pas dans le même ordre : rapportez la gravité à la charge de remédiation estimée en jours-homme. Les quotients les plus élevés forment la vague des quick wins, à engager sous 30 jours.

Réserver un couloir prioritaire à la sécurité et à la restauration

Un constat lié à l'authentification, au chiffrement ou à la restauration des sauvegardes passe devant, quelle que soit sa cotation : ces défauts n'ont pas de mode dégradé acceptable et conditionnent la capacité à encaisser un incident majeur.

NIVEAU DE CRITICITÉ	RÈGLE D'ENGAGEMENT ASSOCIÉE
Critique	Perte de données, exposition publique ou non-tenue du RTO : correction engagée sous 30 jours ou dérogation signée par le sponsor.
Majeur	Dégradation significative de service, de coût ou d'exploitabilité : planifié dans le trimestre, avec propriétaire et date cible.

Copyright Move2Cloud — move2cloud.fr

SECTION 06

Plan de remédiation et suivi

La valeur d'une revue se mesure au nombre de constats effectivement refermés six mois plus tard, pas au nombre de pages du rapport.

Transformer les constats en lots livrables avec critère de clôture

Regroupez les constats en lots cohérents par équipe et par domaine technique — « durcir l'exposition réseau », « rendre les données restaurables », « fiabiliser le plan de reprise » — plutôt qu'en liste de tickets isolés. Chaque lot reçoit un propriétaire nommé, une charge estimée, une date cible et un critère de clôture vérifiable : la requête Resource Graph ou le contrôle Policy qui doit passer au vert. Cette formulation permet de refermer un lot sans débat et d'intégrer directement les éléments dans les sprints existants, au lieu de créer un chantier parallèle qui entre en concurrence avec la roadmap produit.

Tenir un registre des risques résiduels vivant

Tous les constats ne seront pas corrigés, et c'est un arbitrage légitime. Ce qui ne l'est pas, c'est de laisser le risque sans trace : chaque écart non traité rejoint un registre qui précise la nature du risque, l'impact estimé, la raison de l'acceptation, le responsable qui l'assume et la date de réexamen. Ce registre se relit en comité, trimestriellement, en même temps que les indicateurs de progression — conformité Azure Policy, secure score Defender for Cloud, dérive de coût mensuelle et, surtout, résultat du dernier test de restauration réellement exécuté.

> **À retenir :** Formalisez chaque risque non traité dans un registre daté, nominatif et assorti d'une date de réexamen : un risque accepté explicitement est un risque piloté, un risque oublié est une surprise d'astreinte.

Le plan de remédiation n'est pas un livrable de fin de mission mais un élément du backlog produit, revu au même rythme que les autres engagements d'ingénierie. Une revue trimestrielle de trois heures, appuyée sur les mêmes exports qu'au cadrage, suffit à maintenir la trajectoire : on y mesure le delta de conformité, on y referme les lots livrés, on y réexamine les risques acceptés et on y intègre les constats nés des évolutions depuis la revue précédente. C'est cette répétition, plus que la qualité du rapport initial, qui distingue un audit utile d'un audit classé.

Copyright Move2Cloud — move2cloud.fr

SECTION 07

Grille d'auto-évaluation

Passez ces six questions en revue avant de lancer votre prochaine Well-Architected Review, ou dans les semaines qui suivent la restitution d'un audit déjà réalisé.

- [ ] **Chaque charge de travail critique a-t-elle un propriétaire nommé et des objectifs de service (SLO, RTO, RPO) écrits et validés par le métier ?** Sans propriétaire ni objectif chiffré, aucun constat d'architecture ne peut être arbitré ni priorisé.
- [ ] **Disposez-vous, pour chaque constat de votre dernière revue, d'un artefact daté et exportable (export ARM/Bicep, capture Advisor, diagramme, extrait de politique) ?** Un constat sans preuve datée se discute indéfiniment et perd toute valeur lors de la revue suivante.
- [ ] **Savez-vous distinguer, dans votre reporting, ce qui relève de la configuration des ressources (secure score, Advisor) et ce qui relève des choix de conception ?** Un excellent score de configuration peut masquer une architecture structurellement incapable de tenir son RTO.
- [ ] **Vos constats sont-ils cotés selon une échelle explicite croisant impact et probabilité, plutôt que classés par ressenti d'expert ?** Seule une cotation homogène permet de défendre un ordre de passage devant un comité d'investissement.
- [ ] **Les lots de remédiation sont-ils intégrés au backlog produit, avec une charge estimée et un sprint cible, plutôt que conservés dans un document séparé ?** Un plan qui vit hors du backlog n'est jamais arbitré face aux fonctionnalités et finit classé sans suite.
- [ ] **Les risques que vous avez décidé de ne pas traiter sont-ils formellement acceptés, datés, signés et réexaminés au moins une fois par an ?** Un risque accepté sans échéance de revue devient un angle mort dès que le contexte technique ou réglementaire évolue.

> **Comment lire vos réponses :** Deux « non » signalent un point de vigilance à traiter dans le trimestre ; trois « non » ou plus indiquent que votre démarche d'audit produira des constats sans effet durable.

Copyright Move2Cloud — move2cloud.fr

SECTION 08

Feuille de route en 5 étapes

Cette trajectoire se déroule sur un à deux trimestres et s'appuie sur les instances existantes — comités produit, revues de sprint, comité de sécurité — sans créer de gouvernance parallèle ni geler les développements en cours.

1

Cadrer une charge de travail

Choisissez une charge de travail nommée, identifiez son propriétaire métier et formalisez ses objectifs de service. Délimitez les abonnements, groupes de ressources et dépendances externes inclus, et ce qui est explicitement hors périmètre.

2

Collecter les preuves

Exportez les configurations (Bicep/ARM, politiques Azure Policy, topologies réseau), les recommandations Advisor et Defender for Cloud, les métriques de disponibilité et les coûts. Datez et archivez chaque artefact : il servira de référence à la revue suivante.

3

Conduire la revue

Confrontez les preuves aux cinq piliers du Well-Architected Framework lors d'ateliers avec les équipes de build et de run. Distinguez systématiquement les écarts de configuration des écarts de conception, que les scores automatisés ne détectent pas.

4

Coter et arbitrer

Appliquez une échelle impact × probabilité à chaque constat, rattachez-le à un objectif de service mesurable et classez-le. Validez l'ordre de passage en comité, en actant formellement les risques que vous choisissez d'accepter.

5

Industrialiser le suivi

Transformez les constats prioritaires en lots d'ingénierie chiffrés, injectés dans le backlog produit avec un sprint cible. Instaurez une revue trimestrielle de trois heures appuyée sur les mêmes exports pour mesurer le delta, refermer les lots livrés et intégrer les nouveaux constats.

Copyright Move2Cloud — move2cloud.fr

CONCLUSION

Un audit ne vaut que par la trajectoire qu'il déclenche

Les organisations qui tirent un bénéfice réel d'une Well-Architected Review ne sont pas celles qui produisent le rapport le plus exhaustif, mais celles qui savent convertir une poignée de constats bien cotés en lots d'ingénierie livrés, puis vérifier que les écarts refermés le restent. Elles gagnent sur trois plans : une visibilité partagée entre la DSI et le métier sur ce qui tient et ce qui ne tient pas, un arbitrage budgétaire documenté entre dette d'architecture et nouvelles fonctionnalités, et une capacité à répondre en quelques heures, preuves à l'appui, à un auditeur ou à un client exigeant.

Au-delà d'Azure, la discipline décrite ici — périmètre nommé, preuve datée, cotation explicite, lots au backlog, revue trimestrielle — est transposable à n'importe quel socle cloud et à des exercices voisins : revue FinOps, préparation NIS2 ou DORA, qualification d'un plan de reprise. Le cadre change, la mécanique reste la même. L'enjeu n'est pas d'ajouter un rituel de plus, mais de raccrocher l'architecture aux instances de pilotage qui existent déjà.

Move2Cloud	est un cabinet de conseil spécialisé en infrastructure, cloud et transformation IT. Nous accompagnons les organisations dans l'audit, la remédiation et la gouvernance continue de leur environnement cloud.
Contact	Move2Cloud — Paris · move2cloud.fr
Prochaine étape	Si plusieurs réponses de la grille d'auto-évaluation sont négatives, un diagnostic ciblé de deux à trois semaines sur une seule charge de travail critique suffit à produire un périmètre cadré, une liste de constats cotés et un premier lot de remédiation chiffré.

Sources

Microsoft — Azure Well-Architected Framework, documentation Microsoft Learn — Microsoft — Azure Well-Architected Review et Azure Advisor (Microsoft Learn) — Microsoft — Cloud Adoption Framework for Azure, Govern et Manage — CIS — Microsoft Azure Foundations Benchmark — ANSSI — Recommandations pour les architectures et l'usage de l'informatique en nuage

Document rédigé à titre d'exemple et d'illustration par Move2Cloud à des fins pédagogiques. Les outils Azure et les recommandations du Well-Architected Framework évoluent fréquemment : vérifiez la documentation Microsoft en vigueur avant toute décision d'architecture.